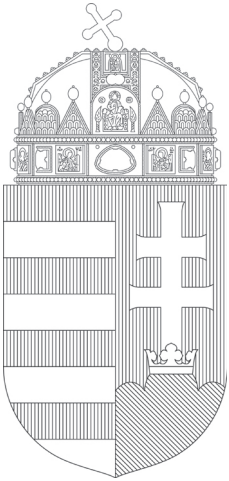
A Nemzeti Adatvédelmi és Információszabadság Hatóság

Beszámolója

a 2018. évi tevékenységéről

B/4542

Nemzeti Adatvédelmi és Információszabadság Hatóság
Budapest, 2019



Bevezető

Köszöntöm az Olvasót!

2018. május 25-től az Európai Unió tagállamaiban kötelező alkalmazni a 2016-ban elfogadott uniós adatvédelmi norma, az általános adatvédelmi rendelet – a GDPR – szabályait. 2018-ban megtörtént az adatvédelmi csomag részét képező másik jogi aktus, a bűnügyi adatvédelmi irányelv magyar jogba való átültetése is, és az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény 2018-as novellája (ha a tervezetthez képest kicsit késve is, de) megteremtette a felügyeleti hatóság működésének, eljárásának és jogértelmezésének megfelelő jogi alapjait. Ezzel elérkeztünk egy jogi folyamat fontos mérföldkövéhez. E folyamat azonban még korántsem zárult le, hiszen a jogalkalmazás számos új, izgalmas kihívással küzd nap mint nap és emellett számos egyéb (szektorális) adatvédelmi előírást tartalmazó jogszabály GDPR-hoz való „igazítása" vagy jelenleg is folyik, vagy a jövőben jelent jogalkotási munkát.

Ha visszanézünk az időben, az uniós adatvédelmi „csomag", a javaslatok előkészítése, megtárgyalása és elfogadása több, mint négy évig tartott egy hihetetlenül bonyolult, ugyanakkor összehangolt jogalkotási eljárás eredményeként. A Lisszaboni Szerződés és az Európai Unió Alapjogi Chartája – melynek 8. cikke önálló alapjogként biztosítja a személyes adatok védelméhez való jogot – példátlan lehetőséget teremtett a tagállami adatvédelmi rezsimek összehangolására, a jogegységesítésre. Az együttműködési mechanizmusok, az egyablakos ügyintézés keretei lassan helyükre kerültek. A nemzeti felügyeleti hatóságok elkezdték működtetni adatvédelmi incidensbejelentő rendszerüket, lezárultak az első GDPR alapján lefolytatott vizsgálatok és korrekciós hatáskörüket gyakorolva a tagállami adatvédelmi hatóságok kiszabták első a megújult előírások alapján megállapított adatvédelmi bírságaikat – vagyis elkezdett működni az a bonyolult szerkezet, melyek fogaskerekeit a GDPR indította be. Mindez nagy figyelmet, érdeklődést vonz mind a szűkebb szakmai, mind a tágabb általános közvélemény oldaláról és természetesen nagy felelősséget jelent számunkra. A mérleget természetesen csak évek múlva lehet és érdemes megvonni, de a NAIH részéről a felkészülés fázisa – különösebb buktatók nélkül – 2018-ban szerencsésen lezárult.

A NAIH által felügyelt másik információs alapjog, az információszabadság jogszabályi háttere nem változott, ugyanakkor a jog magyarországi bevezetésének

30 éves története alapján már számos alapvetés, fontos következtetés levonható. 2018. november 22-én jelent meg az a kormányhatározat, mely nevesíti a KÖFOP 2.2.6.-VEKOP-18 *„Jogszabályban rögzített közzétételi kötelezettségek alá eső adatok körének felülvizsgálata”* című kiemelt projektet. A több éves projekt célja a magyar jogszabályokban rögzített közzétételi kötelezettségek alá eső adatok körének felülvizsgálata, felmérése és ez alapján az átláthatóság növelése érdekében további adatkörök hozzáférhetőségnek biztosítása tudományos kutatások, felmérések alapján. Ezen projekt keretein belül lehetővé válna a közfeladatot ellátó szervek és szervezetek tájékoztatási gyakorlatának átfogó magyarországi vizsgálata, a hatékonysági vagy egyéb jogalkalmazási, jogkövetési problémák, valamint az átláthatóságot hátráltató tényezők beazonosítása, továbbá az ezek kezeléséhez szükséges beavatkozási javaslatok kidolgozása. A NAIH kiemelten figyeli a felhívást és készül a projektben való esetleges részvételre, hiszen ez kiemelkedő lehetőséget teremtene arra, hogy megbízható és átfogó képet kapjunk a közszféra működése átláthatóságának hazai gyakorlatáról, az információszabadság jogi szabályozórendszerének hatékonyságáról, a nehézségekről és akadályokról, valamint a „jó gyakorlatokról” egyaránt.

Budapest, 2019. március 1.

Dr. Péterfalvi Attila
címzetes egyetemi tanár
a Nemzeti Adatvédelmi és Információszabadság Hatóság
Elnöke

I. A Hatóság működésének statisztikai adatai

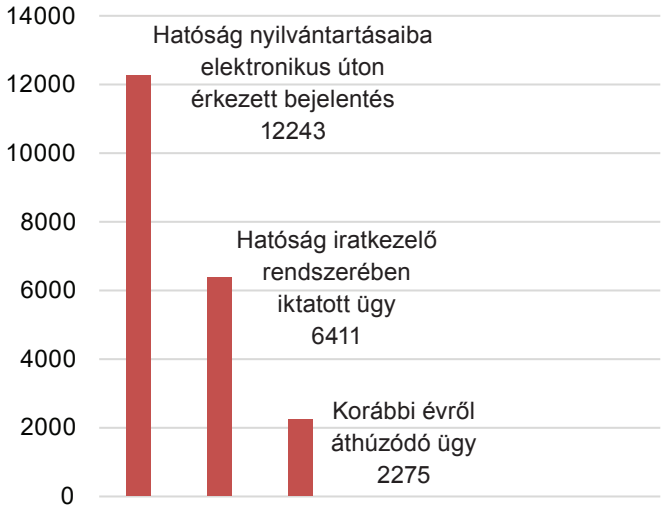
I.1. Ügyeink statisztikai jellemzői

A Nemzeti Adatvédelmi és Információszabadság Hatóság (a továbbiakban: Hatóság, NAIH) 2012. január 1-jei megalapítása óta immár hét év telt el.

A természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK irányelv hatályon kívül helyezéséről szóló, 2016. április 27-i (EU) 2016/679 európai parlamenti és tanácsi rendelet (a továbbiakban: általános adatvédelmi rendelet, GDPR, Rendelet) 2018. május 25-től alkalmazandó.

A megváltozott jogszabályi környezetre tekintettel a 2018. év statisztikai fejezetében a korábbi években megszokottaktól eltérően kerülnek ismertetésre a Hatóság működését érintő számadatok.

A Hatóság ügyszáma 2018-ban

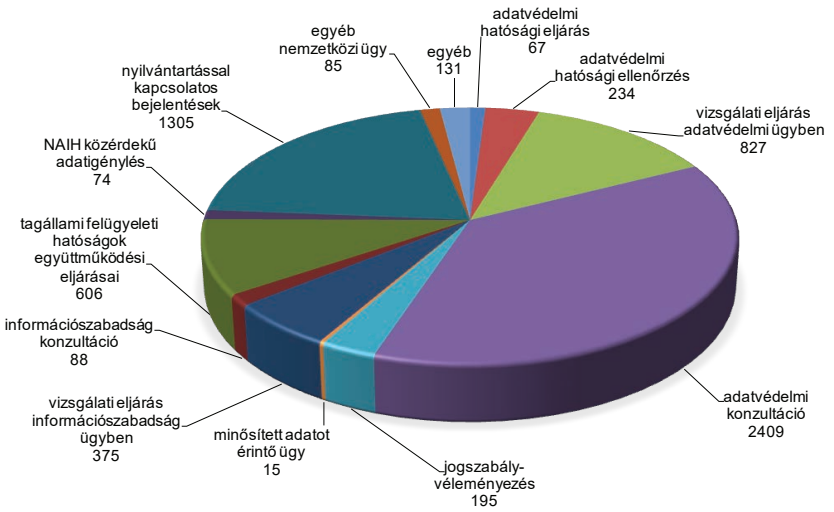


A Hatóság 2018-ban 18654 db új ügyet iktatott. A Hatóság iratkezelő rendszerében 6411 új ügy került ügykezelésre, a Hatóság elektronikus nyilvántartásaiba (az adatvédelmi nyilvántartásba, továbbá az adatvédelmi tisztviselő nyilvántar-

tásba) 12243 bejelentés érkezett. A Hatóság elektronikus nyilvántartásaiba érkezett bejelentések a Hatóság iratkezelő rendszerétől elkülönülten, elektronikus úton kerültek iktatásra.

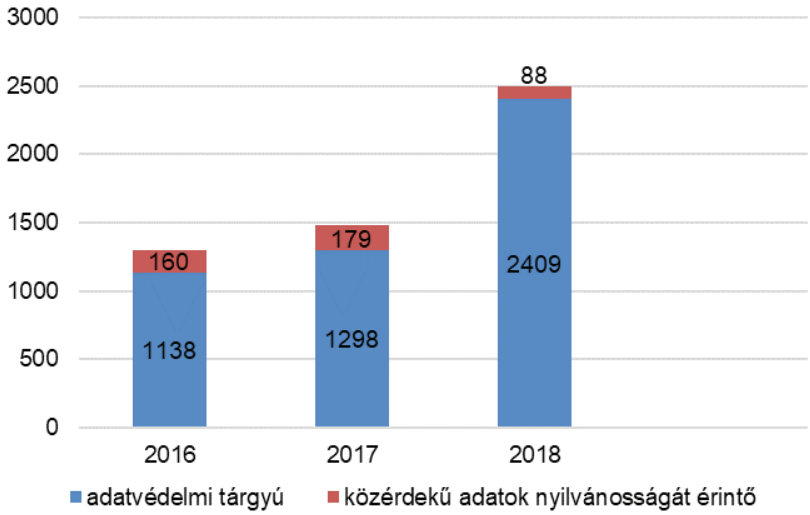
Az iktatott ügyek száma az előző évi ügyiratok számához képest növekedett. A növekedés annak ellenére is megfigyelhető, hogy a Hatóság által vezetett adatvédelmi nyilvántartás jogintézménye 2018. május 25-ét követően megszűnt, így az adatkezelők bejelentési kötelezettsége is, valamint az adatvédelmi nyilvántartásba történő bejelentéssel összefüggő konzultációs beadványok száma is jelentősen csökkent.

A Hatóság 2018-ban indult ügyei



A Hatósághoz érkezett adatvédelmi tárgyú konzultációs beadványok száma megközelítőleg a duplájára emelkedett a korábbi évek számadataihoz viszonyítva, mely jelentős munkatöbbletet jelentett a Hatóság számára. A konzultációs beadványok közül 2409 adatvédelmi tárgyú, 88 pedig a közérdekű vagy közérdekből nyilvános adatok megismerhetőségére vonatkozott. Az adatvédelmi tárgyú konzultációs beadványok nagy száma – melyekben valamely polgár, adatkezelő vagy közfeladatot ellátó szerv tanácsot, tájékoztatást kér egy általa leírt adatkezelést érintően – azt mutatta, hogy a jogalkalmazók számára nagy volt a bizonytalanság a GDPR-ral kapcsolatban.

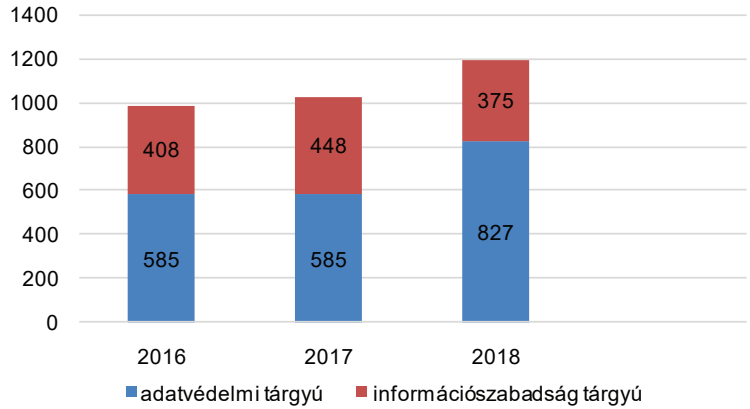
Az információs jogokat érintő konzultációs beadványok száma



A 2018-as országgyűlési választások következtében mérsékeltebb jogalkotási aktivitás miatt a korábbi évekhez képest kevesebb jogszabálytervezet érkezett véleményezésre a Hatósághoz. A Hatóság 195 jogszabály-véleményezést készített, emellett hivatalból is rendszeresen figyelemmel kíséri az információs jogokat érintő kodifikációs tevékenységet és amennyiben az szükséges, hivatalból véleményezi a Hatósághoz el nem küldött jogszabálytervezeteket, vagy az országgyűlési tárgysorozatba vételt követően benyújtott módosító javaslatokat.

Az 1205 vizsgálati eljárásból 827 adatvédelmi és 375 információszabadság tárgyú volt. 2018-ban az adatvédelmi tárgyú vizsgálati eljárások száma jelentősen növekedett.

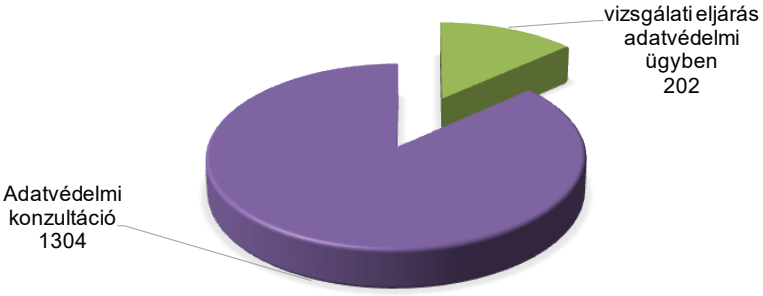
Vizsgálati eljárások száma



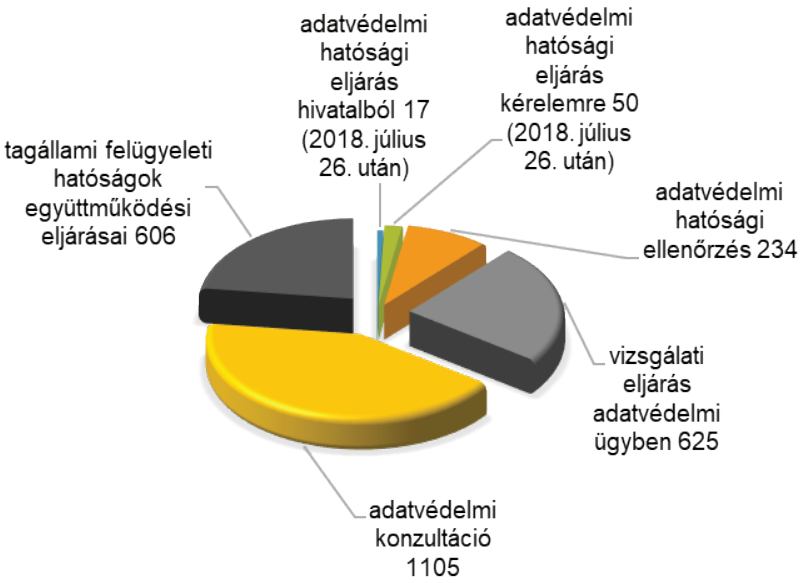
A Hatóság a GDPR alkalmazandóvá válása, tehát 2018. május 25-e és – az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvénynek (a továbbiakban: Infotv.) az Európai Unió adatvédelmi reformjával összefüggő módosításáról, valamint más kapcsolódó törvények módosításáról szóló 2018. évi XXXVIII. törvény (a továbbiakban: Módtv.) hatálybalépése, azaz – 2018. július 26-a közötti időszakban nem indított adatvédelmi hatósági eljárást, tekintettel arra, hogy a Hatóság eljárásának az általános adatvédelmi rendelet szabályaival való összhangja érdekében szükséges előírások hatálybalépésére csak a Módtv. megalkotását követően került sor.

Ebben az időszakban a Hatóság az adatvédelmi hatósági eljárás helyett az Infotv. által biztosított, ombudsmani típusú eszközeit alkalmazta, azaz ún. vizsgálati eljárások keretében kezelte a beérkezett panaszokat.

Adatvédelmi eljárások a GDPR alkalmazandóságát megelőző időszakban



Adatvédelmi eljárások a GDPR alkalmazadóságát követően



A 2018. július 26. utáni panaszok tekintetében már indultak hatósági eljárások, melyekből érintetti kérelemre 50, hivatalból 17 eljárás indult.

Továbbra is lehetőség van bejelentéssel adatvédelmi vizsgálati eljárás kezdeményezésére.

A Módtv. megteremtette a lehetőségét annak, hogy adatvédelmi vizsgálati eljárás hivatalból is indítható legyen akkor, ha a Hatóság felé más szerv jelzi vagy a Hatóság maga észleli, hogy személyes adatok kezelésével kapcsolatban jogsérelem következett be vagy annak közvetlen veszélye áll fenn és hatósági eljárás megindítása az Infotv. szerint nem kötelező.

2018. július 26. után 1105 konzultációs beadvány érkezett a Hatósághoz és 625 ügyben indult vizsgálati eljárás.

A tagállami felügyeleti hatóságok együttműködési eljárásai a GDPR 56. és 60-67. cikkei szerinti, az együttműködési és egységességi mechanizmus körébe tartozó eljárások. Az együttműködési eljárások során a tagállami hatóságok az Európai Unió belső piaci információs rendszerét (IMI, Internal Market System) használják.

A Hatóság 233 ügyben adatvédelmi hatósági ellenőrzés keretében vizsgálta az incidensekkel kapcsolatos kötelezettségek adatkezelő általi teljesítését és további egy esetben az adatkezelés jogszerűségét.

2018-ban 15 minősített adatok védelmével kapcsolatos ügye volt a Hatóságnak.

A NAIH-hoz 74 közérdekű adatigénylés érkezett, melyből 59-et teljesített, 3-at részben teljesített és 12-t pedig elutasított a Hatóság.

A GDPR alkalmazandóságát megelőzően jelentős számban érkezett adatvédelmi nyilvántartással összefüggő beadvány is (1086), valamint az adatvédelmi tisztviselő bejelentő rendszer indulását megelőzően postai vagy elektronikus úton tisztviselő bejelentés (219), illetőleg egyéb nemzetközi ügy (85). Az egyéb iktatott ügyek száma: 151, mely magában foglalja többek között a nem a NAIH feladat- és hatáskörét érintő ügyeket, továbbá a Hatóság üzemeltetésével, gazdálkodási tevékenységével összefüggő ügyeket.

2018-ban a Hatóság telefonos ügyfélszolgálatára mintegy 2800 telefonhívás érkezett. A hívások száma a GDPR alkalmazandóvá válásának hónapjában kiugróan magas, az azt követő hónapokban pedig magasabb volt az év eleji időszakhoz képest.

Személyes ügyfélszolgálatot a Hatóság 27 esetben előre egyeztetett időpontban, 24 esetben előzetes időpont nélkül biztosított, melynek során az érintettek a személyes adatok kezelésével, illetve a közérdekű vagy a közérdekből nyilvános adatok megismeréséhez fűződő jogok gyakorlásával kapcsolatos jogsérelem miatti konkrét panaszt terjesztettek elő vagy az eljárás irataiba való betekintési jogukat gyakorolták.

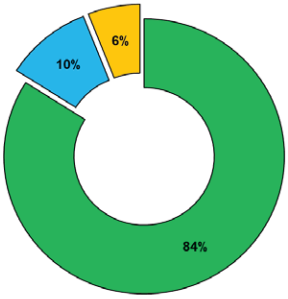
A Hatóság az adatkezelők, illetve adatfeldolgozók számára külön erre a célra létrehozott elektronikus felületen 2018. szeptember 17-től tette lehetővé az adatvédelmi tisztviselő, illetve tisztviselők bejelentését. Az adatvédelmi tisztviselő bejelentő rendszerbe 2018-ban 1786 bejelentés érkezett.

I.2. A Nemzeti Adatvédelmi és Információszabadság Hatóság megjelenése a médiában

A következőkben a Hatóság 2018. évi média megjelenéseit összegezzük. 2018. január 1. és december 31. között összesen 5016 hírt közöltek a médiaszereplők a Nemzeti Adatvédelmi és Információszabadság Hatóságról. A médiatípu-

sok közül legtöbbször továbbra is az online médiában találkozhattunk a Hatóság tevékenységéről szóló híradásokkal, szám szerint 4229 alkalommal (84%). A nyomtatott sajtóban, 309 esetben, (6%), az elektronikus médiában pedig 478-szor (10%) szerepelt a NAIH.

A NAIH megjelenéseinek aránya a különböző médiumokban 2018-ban



Forrás: Observer Budapest Médiafigyelő Kft.

II. Az általános adatvédelmi rendelet alkalmazása

II.1. Adatvédelmi ügyek

II.1.1. A NAIH eljárásai

A GDPR alkalmazandóvá válása természetesen jelentős változásokat jelentett a NAIH működésében is. A magyar adatvédelmi hatóságnak is át kellett tekintenie, felül kellett vizsgálnia tevékenységét, amely több szempontból – anyagi jogi és eljárási kérdésekben is – módosult.

A Hatóság eljárásainak a GDPR szabályaival való összhangja érdekében szükséges volt az Infotv. módosítása. 2018. május 25. és az Infotv. módosításának hatályba lépése közötti átmeneti időszakban – a fennálló szabályozási problémák miatt – nem indult adatvédelmi hatósági eljárás a Hatóságnál.

Ebben az időszakban a Hatóság az addigi, Infotv. által biztosított ombudsmani típusú eszközeit alkalmazta, vagyis a beérkezett panaszokat vizsgálati eljárás keretében vizsgálta ki. Ez esetben jogsértés észlelése esetén az adatkezelőt felszólította a jogsérelem orvoslására, bírság kiszabására azonban ebben az eljárástípusban nincs lehetőség.

2018. július 26-án hatályba lépett a Módtv. A GDPR-ral való összhang érdekében a Módtv. bevezette az érintett kérelmére induló adatvédelmi hatósági eljárást. Ennek alapja a GDPR 77. cikkében foglalt, az érintett felügyeleti hatóságnál történő panasztételhez való joga, amely szerint minden érintett jogosult arra, hogy panaszt tegyen egy felügyeleti hatóságnál, ha megítélése szerint a rá vonatkozó személyes adatok kezelése megsérti a rendeletet.

2018. július 26-tól kezdődően tehát már indultak adatvédelmi hatósági eljárások az érintett polgárok kérelmére a GDPR, a módosított Infotv. és az Ákr. szabályai alapján.

A legjellemzőbb témakörök, amelyekhez kapcsolódóan sor került hatósági eljárás iránti kérelem benyújtására:

- munkahelyi adatkezelés
- hozzáféréshez való jog
- egészségügyi adatkezelés

– követelés engedményezésével kapcsolatos adatkezelés
– kamerás ügyek
– érintetti jogok teljesítésének megtagadása, illetve elmulasztása
– banki adatkezelés.

Amennyiben az érintett polgár a bejelentésének hatósági eljárás keretében történő kivizsgálását kívánja, a kérelmének meg kell felelnie formai és tartalmi követelményeknek is. (Az e-mail útján előterjesztett kérelmek esetében elsősorban vizsgálati eljárás lefolytatására kerül sor.)

A kérelemnek az Infotv. 60. § (5) bekezdésében foglaltak alapján tartalmaznia kell:

– a feltételezett jogsértés megjelölését;
– a feltételezett jogsértést megvalósító konkrét magatartás vagy állapot leírását;
– a feltételezett jogsértést megvalósító adatkezelő, illetve adatfeldolgozó azonosításához szükséges, a kérelmező rendelkezésére álló adatokat;
– a feltételezett jogsértéssel kapcsolatos állításokat alátámasztó tényeket és azok bizonyítékait;
– a megjelölt jogsértés orvoslása iránti döntésre vonatkozó határozott kérelmet.

A kérelemnek továbbá tartalmaznia kell a kérelmező és képviselője azonosításához szükséges adatokat és elérhetőségét. A kérelem tartalmi hiányossága esetén a Hatóság határidő megjelölésével, a mulasztás jogkövetkezményeire történő figyelmeztetés mellett egy ízben hiánypótlásra hívja fel a kérelmezőt. Ha a kérelmező a kérelem hiányosságait nem pótolja, a Hatóság az eljárást megszünteti. 2018-ban a benyújtott kérelmek meglehetősen nagy arányában került sor erre.

A Hatóság mérlegelése alapján hivatalból is indíthat adatvédelmi hatósági eljárást. Kötelező az adatvédelmi hatósági eljárás megindítása, ha

– azt vizsgálati eljárás előzte meg, és a jogsérelem orvoslása vagy annak közvetlen veszélyének elhárítása a vizsgálati eljárásban nem történt meg, illetve
– a Hatóság a vizsgálata alapján megállapítja, hogy a személyes adatok kezelésével kapcsolatban jogsérelem következett be, vagy annak közvetlen veszélye áll fenn és a GDPR alapján bírság kiszabásának van helye.

Az adatvédelmi hatósági eljárásban az ügyintézési határidő 120 nap. Ha a Hatóság a kérelem benyújtásától számított 90 napon belül az eljárást nem szüntette meg, vagy az ügy érdemében nem döntött, az érintettet tájékoztatja a megtett eljárási cselekményekről.

2018. július 26-át követően 57 ügyben indult adatvédelmi hatósági eljárás, amelyből 8 esetben a hatósági eljárás hivatalból indult, a többi esetben kérelemre. A beszámoló elkészültének időpontjáig 27 döntés született, amelyek nagy részében (17 ügyben) az eljárás megszüntetésére került sor azokból az okokból, hogy a kérelmező nem tett eleget a hiánypótlási felhívásnak, a sérelmezett adatkezelés GDPR előtti volt, vagy pedig a beérkezett dokumentumok alapján a Hatóság megállapította, hogy az ügy nem tartozik a hatáskörébe. Három esetben a Hatóság már a hatáskörének hiánya miatt visszautasította a kérelmet.

Kérelemnek helyt adó, illetve részben helyt adó határozat 7 ügyben született, e határozatokban 3 esetben a Hatóság bírság fizetésére is kötelezte az adatkezelőt, illetve másik esetben eljárási bírság kiszabására került sor.

Bejelentéssel továbbra is bárki kezdeményezhet adatvédelmi vizsgálati eljárást, aki úgy véli, hogy a személyes adatok kezelésével kapcsolatos jogsérelem következett be, vagy annak közvetlen veszélye áll fenn.

A Módtv. hatálybalépésével az adatvédelmi vizsgálati eljárás hivatalból is indítható, ha a Hatóság felé más szerv jelzi, vagy a Hatóság maga észleli, hogy személyes adatok kezelésével kapcsolatban jogsérelem következett be vagy annak közvetlen veszélye áll fenn és hatósági eljárás megindítása az Infotv. szerint nem kötelező. A vizsgálati eljárás nem közigazgatási hatósági eljárás, az eljárásra a GDPR-ban meghatározott eltérésekkel az Infotv. rendelkezéseit kell alkalmazni.

II.1.1.1. A belső piaci információs rendszer használatával összefüggő tapasztalatok

A NAIH eljárásrendjében jelentős változás, hogy megjelent egy speciális eljárásszakasz, az Európai Unió más tagállamainak adatvédelmi hatóságaival folytatott, a GDPR-ban meghatározottak szerint formalizált együttműködés szakasza.

Az adatvédelmi reformot megelőzően a 95/46/EK irányelv (adatvédelmi irányelv) arra vonatkozóan nem állapított meg részletes szabályokat, hogy a tagállamoknak miként kell együttműködniük. Ezen hiányosságot pótolva írta elő a GDPR,

hogy a tagállamok az együttműködési eljárásban kötelesek együttesen fellépni a határon átnyúló ügyekben (GDPR 60. cikk).

A GDPR 56. és 60-67. cikkei szerinti, az együttműködési és egységességi mechanizmus körébe tartozó eljárások során a tagállami felügyeleti hatóságok az Európai Unó belső piaci információs rendszerét (Internal Market System, a továbbiakban: IMI) használják. Az IMI funkcióját tekintve csak és kizárólag a felügyeleti hatóságok közötti kommunikációt szolgálja (így pl. a döntéshozatal maga nem az IMI-ben történik), melyre a GDPR egyes eljárásaihoz igazodó követelményeire tekintettel kialakított, ahhoz igazodó modulok segítségével kerül sor (pl. külön modul tartozik a felügyeleti hatóságok GDPR 62. cikke szerinti közös műveletei lebonyolításához, amely valójában csak egy része a GDPR 60. cikke szerinti eljárásnak).

A magyar felügyeleti hatóság által az IMI-n keresztül fogadott ügyek jelentős része a GDPR 56. cikke szerinti, a fő- és érintett felügyeleti hatóságok azonosítására vonatkozó megkeresés. 2018. december 12. napjáig kb. 500 ilyen megkeresés érkezett. A GDPR 56. cikke szerinti eljárások eredménye lényegében a fő- és érintett felügyeleti hatóságok által a 60. cikk szerint lefolytatandó eljárás előkérdésének tekinthető, hiszen a fő- és érintett hatóságok meghatározása után kerülhet sor a 60. cikk szerinti, és ennek keretében szükség esetén a 61. és / vagy 62. cikk szerinti eljárásra. A GDPR 56. cikke szerinti eljárásokban a hatóság abban az esetben vesz részt, ha az adatkezelés jellegét tekintve úgynevezett határon árnyúló az adatkezelés, és a magyar hatóság érintett hatóságnak minősül a GDPR 4. cikk 22. pontja értelmében, mivel az adatkezelő Magyarországon is rendelkezik tevékenységi hellyel, vagy az adatkezelés jelentős mértékben érint, illetve valószínűsíthetően jelentős mértékben érint Magyarországon lakóhellyel rendelkező érintetteket. Eddig csak néhány esetben került sor az érintett hatósági minőség megállapítására arra hivatkozással, hogy a panaszt a magyar hatósághoz nyújtotta be az érintett.

A 2018-ban IMI-n keresztül érkezett, 56. cikk szerinti, nagyságrendileg 500 ügynek kicsivel több, mint a felében merült fel a magyar felügyeleti hatóság szerepe érintett hatóságként, lényeges azonban, hogy kb. 290 ügyben az 56. cikk szerinti eljárás még folyamatban van, nem született tehát döntés arra nézve, hogy a magyar hatóság érintett hatóságnak minősül-e, vagy sem.

A magyar hatósághoz érkezett, a GDPR 56. cikke szerinti ügyek jelentős számban a népszerű közösségi média felületeket, keresőprogramokat üzemeltető adatkezelőkhöz kapcsolódnak: gyakoriak a szolgáltató által az érintetteknek

nyújtott, az adatkezelés körülményeire vonatkozó tájékoztatás teljes vagy részleges hiányát kifogásoló panaszok (GDPR 12-14. cikk), a törlési kérelmek (GDPR 17. cikk), valamint a tiltakozó nyilatkozatok teljesítésével kapcsolatos kifogások (GDPR 21. cikk). A bejelentők több esetben sérelmezték, hogy – különösen a közösségi oldalak adatkezelői, néhány esetben okostelefonok szoftveres támogatását biztosító adatkezelők – az érintett hozzájárulására alapozzák (kívánják alapozni) adatkezelési tevékenységüket olyan esetekben is, amikor az érintetteknek ténylegesen nem volt lehetősége a GDPR 4. cikk 11. pontja szerint elkülönült hozzájáruló nyilatkozatot tenni sem az adatkezelési célok, sem a kezelt adatok köre tekintetében (tipikus a kifogásolt adatkezelők által alkalmazott fordulat pl. *„a szolgáltatás használatával hozzájárulsz ahhoz, hogy XY adatkezelő hozzáférjen a böngészési adataidhoz”*).

Több alkalommal érkezett olyan 56. cikk szerinti ügyben véleményezendő bejelentés a Hatósághoz, amely a szolgáltató által az érintetti jogok gyakorlásának előfeltételeként szabott (személy)azonosítás érdekében kért adatokkal kapcsolatos, pl. több szolgáltató szkennelt személyazonosító okmányt kér ebből a célból, egy esetben maga a hatóság is 56. cikk szerinti eljárást kezdeményezett egy hasonló gyakorlatot folytató adatkezelővel kapcsolatban.

Az 56. cikk szerinti eljárások alkalmazandók adatvédelmi incidens kezelésével kapcsolatos ügyekben akkor is, ha az incidenssel érintett tagállamok felügyeleti hatóságok azonosítása szükséges.

A NAIH-nál indult, az IMI-n keresztül történő kommunikációt igénylő ügyek közül a magyar hatóság 2018. december végéig 7 alkalommal kezdeményezett 56. cikk szerinti eljárást. A NAIH fő felügyeleti hatósági szerepet vállal egy közlekedési társaság adatkezelésének vizsgálatában, melynek során romániai, németországi valamint nagy-britanniai érintettek kifogásolták az adatkezelést. A francia érintett panasza alapján nem tudta érvényesíteni a GDPR 17. cikke szerinti törléshez való jogát, a romániai érintett pedig a személyes adatainak marketingcélú felhasználását panaszolja. Mivel az adatkezelő adatkezelési tevékenységének tényleges és valós, tartós jelleget biztosító keretek közötti gyakorlása Magyarországon valósul meg, így a határon átnyúló adatkezelések során a magyar hatóság jár el főhatóságként. A GDPR 61. cikke szerinti eljárás (ún. kölcsönös segítségnyújtás) a hatóság tapasztalatai szerint felhasználható egyrészt arra, hogy a hatóságok egyes konkrét ügyekkel, adatkezelőkkel kapcsolatban felhívják egymás figyelmét bizonyos lényeges információkra, másrészt alkalmas tapasztalatcserére a GDPR alkalmazásával összefüggő jogkérdéseket illetően is (pl. szükséges-e DPO kinevezése szakszervezetek esetében; „szom-

szédkamerás" adatkezelés és háztartási célú adatkezelés értelmezése; közös adatkezelők felelőssége a GDPR szabályainak alkalmazásában; a hatóságok tapasztalatai a GDPR 55. cikk (3) bekezdése alkalmazásával kapcsolatban: tekintettel arra, hogy felügyeleti hatóságok hatásköre nem terjed ki a bíróságok által igazságügyi feladataik ellátásával kapcsolatban végzett adatkezelésekre). A magyar hatóság több témakörben kezdeményezett a GDPR 61. cikke szerint eljárást: 2 db incidens-bejelentés mellett a fentiekben részben már említett, általános jellegű kérdésekben, így például a tekintetben, hogy a DPO-k kinevezése kötelező-e szakszervezetek által; kamerás megfigyeléssel, továbbá a bírósági tárgyalási jegyzékek nyilvánosságával, valamint egyes, a magánnyomozókat érintő tevékenységekkel kapcsolatban.

A NAIH továbbá részt vesz olyan eljárásokban is, ahol érintett hatóságként véleményt nyilvánított más felügyeleti hatóság által hozott intézkedésekkel, döntésekkel összefüggésben (a fő felügyeleti hatóság az ügyben hozott döntés tervezetét benyújtja a többi érintett felügyeleti hatóságnak, hogy azok véleményezhessék).

Ilyen például az egyik szállodai szolgáltatást nyújtó adatkezelővel szemben megindult eljárás, melynek során a francia adatvédelmi hatóság küldött döntéstervezetet a magyar hatóság, mint érintett hatóság számára. Az eljárás egy hűségprogrammal kapcsolatos adatkezeléssel összefüggésben indult, amely során az adatkezelő az érintetti jogok gyakorlásának feltételeként személyazonosító okmányok másolatát kéri rendelkezésre bocsátani. A GDPR alapján az érintetti jogok gyakorlása során ugyan az adatkezelő feladata megbizonyosodni az érintett személyazonosságáról, azonban csupán akkor, ha megalapozott kétség merül fel e tekintetben. Ekkor kérheti az érintettet, hogy erősítse meg személyazonosságát a GDPR 12. cikk (6) bekezdése alapján. Ez azonban az adattakarékosság alapelvének megfelelően nem vezethet oda, hogy az érintett a szükségesnél több adatot adjon meg, a kért dokumentumoknak relevánsaknak és arányosnak kell lenniük a kitűzött célhoz képest. Így aránytalan például személyazonosító igazolványt kérni attól az érintettől, aki a kérelmét olyan helyen nyújtotta be, ahol a személyazonosságát már korábban igazolták. Személyazonosító igazolványt ugyanakkor olyan esetben indokolt kérni, ha felmerül például a személyazonosság-lopás vagy okmányhamisítás gyanúja.

A Hatóság a döntéstervezettel alapvetően egyetértett, felhívta azonban a figyelmet arra, hogy egyes azonosítókat csak a külön nemzeti jogszabályban felhatalmazott szerv kezelhet, ezért ilyen tagállami szabályozás esetén erről az adatkezelési tájékoztatónak is rendelkeznie kell, valamint bizonyos, arcképet tar-

talmazó okmányok esetében azt is rögzítette, hogy a képmás nem minden esetben tekinthető szükségesnek az adatkezeléshez.

II.1.1.2. A Hatóság tájékoztatási, konzultációs tevékenysége

A beszámoló tárgyát képező időszakban – különösen a GDPR alkalmazandóvá válását megelőző és követő hetekben – fokozatosan emelkedett az érdeklődő, tájékoztatást kérő, állásfoglalást kezdeményező beadványok száma, amely azt mutatja, hogy jelentős volt a bizonytalanság a jogalkalmazókban a GDPR rendelkezéseinek értelmezésével kapcsolatban.

Számos megkeresés érkezett a Hatósághoz a GDPR alkalmazását és értelmezését érintően, ezek tekintetében a Hatóság mozgástere azonban korlátozott, hiszen a GDPR autentikus absztrakt értelmezésére mindenekelőtt – az egységes jogalkalmazás biztosítása céljából – az Európai Adatvédelmi Testület jogosult. A Hatóság ennek megfelelően továbbra is az érintettek jogsérelmének orvoslását, az adatvédelmi előírások megfelelő alkalmazásának ellenőrzését tekinti elsődleges feladatának. Mindez természetesen nem érinti az adatvédelmi hatásvizsgálat eredményének függvényében lefolytatandó előzetes konzultációkat, illetve a tanúsítás keretei között esetlegesen sorra kerülő egyeztetéseket, valamint a jogszabályokból fakadó tájékoztatási kötelezettség teljesítését.

A megkeresések jelentős részét az adatkezelők által a Hatósághoz intézett, konkrét adatkezelés, adatkezelési műveletek értékelését célzó beadványok tették ki. A GDPR szerint és az Infotv. 38. §-a szerint sem feladata a Hatóságnak, hogy valamely meghatározott adatkezelés értékelését elvégezze, és annak jogszabályi megfelelőségéről előzetesen állásfoglalást alakítson ki vagy adatkezelési kérdésekben konzultációt folytasson. Ilyen tevékenység folytatása jelentősen meg is haladná a Hatóság erőforrásait. Az adatkezelés valamennyi ismérve az adatkezelőnél áll rendelkezésre, ezért elsősorban ő képes annak megítélésére, hogy a jogszabályi megfelelés érdekében milyen intézkedések lehetnek szükségesek; a Hatóság – a GDPR-ban rögzített, ún. elszámoltathatóság alapelvéből is fakadóan – nem veheti át az adatkezelő e tekintetben fennálló felelősségét. A fentiekre tekintettel annak megítélésére, hogy az általános adatvédelmi rendelet által támasztott követelményeknek való megfeleléshez konkrét esetben milyen technikai és szervezési intézkedések szükségesek, elsősorban az adatkezelő képes, miután ahhoz ismerni szükséges az adatkezelés valamennyi jellemzőjét, ezek az információk pedig az adatkezelőnél állnak rendelkezésre. Egy adatkezelés teljes átvilágítása mind a jogi, mind az informatikai intézkedések teljes körű vizsgálatával lehetséges csak. Ilyen, ún. audit eljárást a Hatóság már nem

folytat, hiszen a GDPR alkalmazandóvá válását követően megszűnt a Hatóság számára az adatvédelmi audit szolgáltatás nyújtásának lehetősége. Az általános adatvédelmi rendelettel kapcsolatos absztrakt jogértelmezés, iránymutatás, vélemény kialakítása az Európai Adatvédelmi Testület feladata, ezért és az egységesség elve miatt a Hatóság állásfoglalás kiadására csak kivételesen, illetve a hazai jog vonatkozásában tartja magát feljogosítottnak.

A megváltozott jogi környezet, az Európai Adatvédelmi Testület jogegységesítő szerepe és a Hatósághoz érkező egyedi ügyekre vonatkozó álláspont kialakítása iránti kérések nagy száma miatt tehát – a Hatóság vizsgálati és hatósági eljárásaihoz szükséges erőforrásokra is tekintettel – főszabály szerint a Hatóság a személyes adatok védelmére vonatkozó előírások értelmezésére és magyarázatára irányuló megkeresésekre, különösen, ha azok nem az érintetti jogok gyakorlására vonatkozó, nem az érintett természetes személytől származó kérdések, nem ad ki egyedi állásfoglalást.

A GDPR azt írja elő a Hatóság egyik feladatául, hogy felhívja az adatkezelők (adatfeldolgozók) figyelmét a rendelet szerinti kötelezettségeikre, és kérésre tájékoztatást nyújtson az érintettnek az őt megillető jogok gyakorlásával kapcsolatban [általános adatvédelmi rendelet 57. cikk (1) bekezdés d) és e) pontja]. A 2018-as évben e kötelezettségének a Hatóság a honlapon közzétett tájékoztatókon, valamint a Hatóság részére címzett, adatkezelőktől, érintettektől, szakmai és társadalmi szervezetektől, ügyvédi irodáktól érkező, egyedi megkeresésekre adott állásfoglalásokban törekedett felvilágosítást adni. A Hatóság e szerepét a GDPR-ban meghatározottak szerint az Európai Adatvédelmi Testület jogegységesítő tevékenységében közreműködve tölti be.

A beszámolóval érintett időszakban számos megkeresés érkezett a Hatósághoz azzal kapcsolatban, hogy a GDPR alapján milyen szabályzatot kell alkotni, elegendő-e a meglévő szabályzat módosítása a GDPR-nak való megfeleléshez, emellett jelentős számban az adatkezelők szabályzatuk véleményezésére, jóváhagyására kérték a Hatóságot (NAIH/2018/3690/2/V., NAIH/2018/3193/2/V.).

A GDPR kifejezetten adatvédelmi szabályzatalkotási kötelezettséget nem ír elő az adatkezelők számára. A 24. cikk (2) bekezdése alapján az adatkezelőnek akkor kell belső adatvédelmi szabályokat is alkalmaznia – a személyes adatok védelmének biztosítása céljából megvalósított technikai és szervezési intézkedések részeként – ha ez az adatkezelési tevékenység vonatkozásában arányos. Ennek a rendelkezésnek az értelmezését a (78) preambulum bekezdés segíti. Ez alapján azt kell tehát az adatkezelőnek mérlegelnie, hogy a kezelt adatok

mennyisége és köre alapján „arányosnak” mutatkozik-e adatvédelmi szabályzat vagy más szabályrendszer (például: utasítás, folyamatleírás, biztonsági szabályzat) elkészítése.

Mindezekre figyelemmel, ha az adatkezelő az adatvédelmi szabályzat elkészítése mellett dönt, úgy a GDPR nem tartalmaz speciális előírást arra vonatkozóan, hogy a szabályzatnak milyen kötelező tartalmi elemei legyenek. Az adatvédelmi szabályzat elkészítése az adatkezelő feladata, nincsen formanyomtatvány, vagy mintasablon, minden adatkezelő önállóan gondoskodik a tartalom összeállításáról.

Az adatkezelő (adatfeldolgozó) felelőssége a GDPR 5. cikk (2) bekezdésében foglalt elszámoltathatóság alapelv alapján, hogy a szabályzat és az az alapján kialakított adatkezelési gyakorlat a GDPR-ral összhangban legyen. A Hatóság azt nem véleményezi, nem engedélyezi, hanem az eljárásai során ellenőrzi. Az adatvédelmi szabályzat elkészítését nem szükséges bejelenteni a Hatóságnak. (NAIH/2018/942/2/K; NAIH/2018/1594/2/K; NAIH/2018/1868/2/K; NAIH/2018/2162/2/K; NAIH/2018/2471/2/K ügyszámú állásfoglalások)

A Hatóság a jogszerű adatkezelési gyakorlat kialakítása érdekében tájékoztatást bocsátott ki a GDPR alkalmazásáról, továbbá több állásfoglalás született az adatvédelmi tisztviselőkkel, adatvédelmi nyilvántartással, szabályzattal kapcsolatban. A Hatóság a fentieken kívül több, az adatvédelmi reformmal kapcsolatos, és a felkészülés elősegítését célzó tájékoztatást adott, többek között az alábbi témákban:

- a kis- és középvállalkozások adatkezelései
- munkahelyi adatkezelések
- háziorvosi tevékenység adatkezelése
- egyéni vállalkozók adatkezelése
- szálláshely szolgáltatás adatkezelése
- ügyvédi tevékenység
- hírlevél-szolgáltatás keretében történő adatkezelés.

Ezen kívül a Hatóság feladata az is, hogy a tagállami joggal összhangban tanácsot adjon a nemzeti parlamentnek, a kormánynak és más intézményeknek és szerveknek a természetes személyek jogainak és szabadságainak a személyes adatok kezelésével kapcsolatban. A Hatóság e feladatával összhangban tájékoztatást tett közé a helyi önkormányzatok GDPR-ra való felkészülésével (NAIH/2018/788/2/K., NAIH/2017/5364/2/V.), illetve az adatkezelői minőség és szabályzat-alkotási kötelezettséggel, továbbá a civil szervezetek-egyesü-

letek, szakmai kamarák adatkezelésével kapcsolatban (NAIH/2018/2919/2/V., NAIH/2018/3134/2/V. NAIH/2018/789/2/V.). Fentieken kívül a Hatóság az iratkezelési tevékenység megítélésével, békéltető testületek GDPR alapján teljesítendő egyes kötelezettségeivel, gyermekotthon-idősek otthona adatkezelési tevékenységével, illetve jogalkotási eljárás során végzett adatkezeléssel kapcsolatos állásfoglalást is közzétett honlapján, illetve megválaszolta a felmerülő kérdéseket.

A Hatóság – eljárási kereteket nélkülöző, konzultációs válaszként kiadott – tájékoztatása sem jogszabálynak, sem egyéb jogi eszköznek nem tekinthető, az normatív jelleggel, jogi erővel, illetve kötelező tartalommal nem rendelkezik. A Hatóság konkrét ügyben rendelkezésre bocsátott információk alapján kialakított jogértelmezése más hatóságot, a bíróságot és az adatkezelőt nem köti, annak csak iránymutató jellege van. Az állásfoglalás, tájékoztatás kiadása tehát nem mentesíti annak címzettjét illetve az adatkezelőt saját jogi álláspontja kialakításának szükségessége, illetve az adatkezelés jogszerűségéért fennálló felelősség alól.

II.1.2. Az adatvédelmi követelményrendszer változásai

II.1.2.1. A GDPR tárgyi hatálya

1. A Hatóság elé kerülő ügyekben vizsgálni szükséges minden egyes adatkezelés esetén, hogy az adatkezelés a GDPR tárgyi hatálya alá tartozik-e. E szempontból a GDPR 1. és 2. cikkében foglaltak képezik a kiindulópontot.

A GDPR alkalmazási köre kiterjed 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.

A GDPR 2. cikk (2) bekezdése szerint annak rendelkezései nem alkalmazandóak a személyes adatok kezelésére, ha azt

- az uniós jog hatályán kívül eső tevékenységek során végzik;
- a tagállamok az Európai Unióról Szóló Szerződés V. cím 2. fejezetének hatálya alá tartozó tevékenységek során végzik;
- természetes személyek kizárólag személyes vagy otthoni tevékenységük keretében végzik;

- az illetékes hatóságok bűncselekmények megelőzése, nyomozása, felderítése, vádeljárás lefolytatása vagy büntetőjogi szankciók végrehajtása céljából végzik, ideértve a közbiztonságot fenyegető veszélyekkel szembeni védelmet és e veszélyek megelőzését.

Csak olyan adatkezelésekre terjed ki tehát a GDPR hatálya, amely
- természetes személyekre vonatkozik;
- részben vagy egészben automatizált módon történő adatkezelés;
- nem automatizált módon történő olyan adatkezelés, amely valamely nyilvántartási rendszer részét képezi, vagy annak részéve kívánják tenni; valamint
- amely az uniós jog hatálya alá tartozó tevékenységhez kapcsolódik.

Nem alkalmazandó a GDPR olyan adatkezelésekre, amely
- a közös kül- és biztonságpolitika tárgykörébe tartozik;
- bűncselekmények felderítéséhez, megakadályozásához, közbiztonsághoz kapcsolódik;
- kizárólag személyes, vagy otthoni tevékenység keretében végzik.

A GDPR hatálya tehát nem terjed ki az adatvédelmi reform másik elemét képező bűnügyi adatvédelmi irányelv hatálya alá tartozó adatkezelésekre, és a reform keretében elfogadott aktusok hatálya együttesen sem terjed ki az adatkezelési jogviszonyok teljes körének szabályozására, így egyrészt természetesen azon jogviszonyokra, amelyek egyáltalán nem tartoznak az uniós jog hatálya alá (pl. nemzetbiztonsági célú adatkezelések), másrészt amelyeket noha az alapítószerződések nem zárnak ki az uniós jog hatálya alól, az uniós jogalkotó nem kívánt szabályozni (pl. papír alapú, nyilvántartásba nem rendezett adatkezelések).

A magyar jogalkotó azonban a Módtv. megalkotásával az Alaptörvény VI. cikk (2) bekezdésében biztosított, a személyes adatok védelméhez fűződő alapvető jog érvényesülését az uniós jog által nem szabályozott, Magyarország joghatósága alá tartozó adatkezelési jogviszonyokban – ahogyan azt a személyes adatok védelmére vonatkozó általános szabályokat tartalmazó törvényi szabályozás a magyar jogban hagyományosan megtette – továbbra is biztosítja, összhangban az Európa Tanács – az 1998. évi VI. törvénnyel kihirdetett – adatvédelmi egyezményéhez tett magyar nyilatkozattal is.

2. Külön megemlítendő, hogy a GDPR – az Infotv. korábbi rendelkezéséhez hasonlóan – tartalmazza az ún. „háztartási kivételt", azaz az adatkezelések bizonyos körére nem terjeszti ki a szabályozás tárgyi hatályát. A GDPR 2. cikk (2)

bekezdés c) pontja szerint a rendelet nem alkalmazandó a személyes adatok kezelésére, ha azt természetes személyek kizárólag személyes vagy otthoni tevékenységük keretében végzik.

A (18) preambulum-bekezdés szerint a háztartási kivétel alkalmazásának feltétele, hogy az adatkezelést ne lehessen összefüggésbe hozni semmilyen szakmai vagy üzleti tevékenységgel.

A „háztartási kivételek" közé tartozik többek között a levelezés, a címtárolás, valamint az említett személyes és otthoni tevékenységek keretében végzett, közösségi hálózatokon történő kapcsolattartás és online tevékenységek.

A GDPR-t kell azonban alkalmazni azonban azokra az adatkezelőkre és adatfeldolgozókra, akik a személyes adatok ilyen személyes vagy otthoni tevékenység keretében végzett kezeléséhez az eszközöket biztosítják, így tehát a közösségi hálózat, a levelezőrendszer, a telefonos applikáció üzemeltetőjének tevékenységére.

A Hatósághoz érkezett beadványok közül jellemzően a közösségi médiával kapcsolatos, illetve a kamerás ügyekben merült fel a háztartási kivétel alkalmazásának lehetősége.

Több megkeresés is érkezett a Hatósághoz a Facebook közösségi oldalon létrehozott csoportokkal kapcsolatban, amely csoportokat óvodai csoportok (NAIH/2018/3922/V.), iskolai osztályok (NAIH/2018/5727/V.), hoztak létre a szülők és a pedagógusok közötti kommunikáció megkönnyítése érdekében. A Hatóság e megkeresésekre adott válaszban úgy foglalt állást, hogy az elhatárolás szempontjából a csoport összetételének van jelentősége: amennyiben e csoportok tagjai kizárólag a gyermekek és szülők, úgy az e csoportokban megosztott tartalom nem tartozik a GDPR tárgyi hatálya alá, azonban, amennyiben egy pedagógus is tagja a csoportnak, úgy nem mondható el, hogy a tevékenységnek ne lenne szakmai jellege, így az nem minősülhet háztartási kivételnek.

A Hatóság nem sorolta a háztartási kivételek közé a közösségi médiafelületeken nyilvánosan megosztott tartalmakat – például egy személy társkereső oldalon használt, képmást is tartalmazó profiljának egy nyilvános Facebook-csoportban történő megosztását (NAIH/2018/6455/V.) –, annak ellenére, hogy e tevékenységeknek sincs szakmai vagy üzleti vonzata, tekintettel arra, hogy ha a személyes adatot meghatározhatatlan számú ember ismeri meg, vagy ha az nyilvánosságra hozatalra kerül, akkor a kivétel nem alkalmazható.

A Hatóság a beadványok megválaszolása során a háztartási célú kivételek közé sorolta a turisták utazáson készült felvételeit, illetve a családi és baráti összejöveteleken történő képfelvétel-készítést is (NAIH/2018/3389/V.), továbbá az iskolai rendezvényeken a szülők által gyermekükről készített felvételeket is, akkor is, ha azokon más gyermekek is szerepelnek (NAIH/2018/6083/V.). Hangsúlyozandó, hogy a Hatóság kizárólag e felvételek elkészítését értékelte háztartási célú adatkezelésnek, amennyiben e képeket a készítő feltöltötte volna az internetre, az adatkezelés a GDPR hatálya alá tartozna.

A Hatósághoz nagy számban érkeztek olyan panaszok is, amelyben a panaszosok a szomszédjuk ingatlanán elhelyezett kamerákat panaszolták, miszerint az az ő ingatlanukon történteket is rögzíti (NAIH/2018/3550/V.).

A Hatóság kezdeményezésére uniós szinten egyeztetés folyt azzal kapcsolatban, hogy az egyes tagállamok felügyeleti hatóságai az ilyen kamerás megfigyelést a háztartási kivételek közé sorolják-e. A megkérdezett hatóságok túlnyomó többsége úgy foglalt állást, hogy a kérdéses adatkezelés a GDPR hatálya alá tartozik, csupán két tagállam hatósága nem sorolta egyértelműen az adatkezelést a rendelet szabályozási körébe. A Hatóság az ilyen jellegű beadványok megválaszolása során azt hangsúlyozta, hogy amennyiben az üzemelő kamera úgy van beállítva, hogy csak azon az ingatlanon történteket rögzíti, amelyen a kamerát elhelyezték, úgy az adatkezelésre nem vonatkoznak a GDPR rendelkezései, amint azonban a más ingatlanán vagy közterületen történteket is rögzíti, nem alkalmazandó a kivételszabály és az adatkezelő köteles megfelelni a GDPR által támasztott követelményeknek.

3. A GDPR tárgyi hatálya kiterjed a bíróságok adatkezelésére is azzal a fő különbséggel, hogy a GDPR 55. cikk (3) bekezdése alapján a felügyeleti hatóságok hatásköre nem terjed ki a bíróságok által igazságügyi feladataik ellátása során végzett adatkezelési műveletek felügyeletére.

Ennek magyarázatát a GDPR (20) preambulum-bekezdése úgy határozza meg, hogy annak érdekében, hogy az igazságszolgáltatási feladataik ellátása során, beleértve a döntéshozatalt is, biztosítva legyen a bírói kar függetlensége, a felügyeleti hatóságok hatásköre nem terjedhet ki a személyes adatok olyan kezelésére, amelyet a bíróságok igazságszolgáltatási feladatkörükben eljárva végeznek.

A bírósági adatkezelési műveletek ellenőrzésére vonatkozó szabályokat az Infotv. – a Módtv.-nyel megállapított – VI/A. fejezete tartalmazza.

Az Infotv. 71/A. § (1) bekezdése értelmében a bírósági döntés meghozatalára irányuló peres és nemperes eljárásokban, az azokra vonatkozó előírások alapján a bíróságok által végzett adatkezelési műveletekkel kapcsolatban a személyes adatok védelméhez való jog érvényesülésének ellenőrzésére adatvédelmi kifogás útján kerül sor.

A kifogást az alapügyben eljáró bíróságnál írásban lehet előterjeszteni, a kifogás elbírálására hatáskörrel rendelkező bírósághoz címezve. Az illetékekről szóló 1990. évi XCIII. törvény 56. § (5) bekezdése szerint illetékmentes a bírósági adatkezelési műveletek ellenőrzésére irányuló adatvédelmi kifogás.

A kifogást az eljáró bíróság feletti szinten lévő bíróság, vagy a Kúria esetén a Kúria egy másik tanácsa bírálja el. Az Infotv. 71/B. § (1) bekezdésének megfelelően *„[a] kifogás alapján a bíróság azt vizsgálja, hogy az eljáró bíró, ülnök vagy igazságügyi alkalmazott az adatkezelési tevékenysége során a személyes adatok védelmére vonatkozó jogszabályi és uniós jogi előírásoknak megfelelően járt-e el.”*

A Hatóság tehát a GDPR 55. cikk (3) bekezdésének és az Infotv. VI/A. fejezetének hatálya alá tartozó adatkezelések felügyeletére nem jogosult, ezen adatkezelések esetén eljárást nem folytat le, azok lefolytatása a bíróságok feladat- és hatáskörébe tartozik.

II.1.2.2. Alapelvek

A GDPR az alapelvek tekintetében egyrészt az Infotv.-ben már az adatvédelmi reformot megelőzően is szereplő alapelveket tartalmazza, másrészt új elnevezéseket ad bizonyos alapelveknek, harmadrészt új alapelveket vezetett be az alábbiak szerint:

Alapelv elnevezése	
az Infotv.-ben	a GDPR-ban
célhoz kötöttség [Infotv. 4. § (1)-(2) bek.]	célhoz kötöttség [GDPR 5. cikk (1) bek. b) pont]
tisztességesség, törvényesség, [Infotv. 4. § (1) bek.]	jogszerűség, tisztességes eljárás és átláthatóság [GDPR 5. cikk (1) bek. a) pont]

pontosság, teljesség, naprakészség [Infotv. 4. § (4) bek.]	pontosság [GDPR 5. cikk (1) bek. d) pont]
adatkezelés céljához szükséges ideig történő kezelés és azonosítás elve [Infotv. 4. § (2) és (4) bek.]	korlátozott tárolhatóság [GDPR 5. cikk (1) bek. e) pont]
adattakarékosság [Infotv. 4. § (2) bek.]	adattakarékosság [GDPR 5. cikk (1) bek. c) pont]
	integritás és bizalmas jelleg [GDPR 5. cikk (1) bek. f) pont]
	elszámoltathatóság [GDPR 5. cikk (2) bek.]

Az adatkezelési elvek a teljes adatkezelési folyamatot végigkísérik, ide értve az adatgyűjtést, a megfelelő jogalap kiválasztását, az érintettek tájékoztatását.

Kiemelkedő jelentőséget kap a GDPR 5. cikk (2) bekezdésében meghatározott elszámoltathatóság elve, amely alapján az adatkezelő felelős a GDPR 5. cikk (1) bekezdésben rögzített alapelvek érvényesülésének biztosításáért, továbbá képesnek kell lennie arra, hogy az adatkezelés ezen alapelveknek történő megfelelését igazolja. Az elszámoltathatóság elve az adatkezelő által tett adatvédelmi intézkedésekért való felelősségvállalást jelenti, valamint tartalmazza az adatkezelés megtervezésétől kezdődően annak végzésén keresztül az adatkezelési cél megvalósítása érdekében tett valamennyi intézkedést, a személyes adatokhoz való hozzáférést, adattovábbítást és azok adminisztrálását, igazolását.

II.1.2.3. Az alapelvekhez kapcsolódó jogesetek a Hatóság gyakorlatából

1. Célhoz kötöttség, adattakarékosság

A Hatóság egy biztosítónak a hírlevelekről való leiratkozásra vonatkozó, a biztosító honlapján elérhető tájékoztatása tanulmányozását követően megállapította, hogy a leiratkozáshoz csak a vezetéknév, keresztnév és a kérést rögzítő nevének megadása kötelező, illetve az elérhetőségi adat (e-mail cím vagy telefonszám), így az adatkezeléssel érintett tevékenység nem veti fel sem a célhoz kötöttség, sem az adattakarékosság elveinek sérelmét, a Hatóság a személyes adatok védelméhez fűződő jog szempontjából nem tartotta aggályosnak a biztosító szóban forgó adatkezelési gyakorlatát. (NAIH/2018/3559/V.)

A Hatóság megállapította, hogy egy sportegyesület jogszerű cél nélkül kezel személyes adatokat, megsértve ezzel a GDPR 5. cikk (1) bekezdés b) pontjában szabályozott célhoz kötöttség elvét, amikor a bárki által használható futópályára történő belépéshez a sportolni szándékozó személy nevét és telefonszámát rögzíti. Az adatkezelés célját, illetve a mögötte húzódó érdeket adatkezelés nélkül is meg lehet valósítani.

A kitiltott vagy eltiltott személyek belépésének megtagadása és ezzel összefüggésben a jogsértés miatt eltiltott személyek azonosítása mint adatkezelési cél jogszerű lehet, ehhez azonban nem alkalmas eszköz valamennyi sportolni kívánó személy adatának a felírása, elegendő csupán a jogsértést elkövető személyek adatainak a rögzítése. Ez következik a GDPR 5. cikk (1) bekezdés c) pontja szerinti adattakarékosság elvéből is, mely szerint a személyes adatok az adatkezelés céljai szempontjából megfelelőek és relevánsak kell hogy legyenek, és a szükségesre kell korlátozódniuk.

A sportolók aktuális létszámának nyilvántartásával kapcsolatban a Hatóság álláspontja az volt, hogy ahhoz nem szükséges személyes adatok kezelése. Amennyiben a pályát használók számát szeretné nyilvántartani a sportegyesület, az megvalósítható bármilyen, az érintett azonosításra nem alkalmas jelzés alapján is.

A Hatóság felszólította a sportegyesületet, hogy vizsgálja felül adatkezelési gyakorlatát és alakítsa át azt a GDPR rendelkezéseinek megfelelően, vagy szüntesse meg a kifogásolt adatkezelést, továbbá amennyiben az Egyesület a sportpálya használatával összefüggésében szükségesnek tartja személyes adatok kezelését, úgy célonként, arányosítva végezzen érdekmérlegelést a fent kifejtettek szerint és készítsen megfelelő adatkezelési tájékoztatót, kitérve valamennyi adatkezelési körülményre. (NAIH/2018/3750/V.)

Egy esetben mozgásukban korlátozott személyek parkolási igazolványához kötődő kedvezmény igénybevételének feltételeivel kapcsolatban érkezett a Hatósághoz megkeresés. Az adatkezelő a parkolási igazolvány kihelyezésén túl további személyes adatok megadásával és nyilvántartásával kívánt volna behajtási engedélyt adni egy közforgalom elől elzárt területre.

A Hatóság válaszában felhívta a figyelmet arra, hogy a GDPR (53) preambulum-bekezdése és 9. cikke alapján „a mozgáskorlátozottság különleges személyes adatnak minősül". *„A mozgássérült személyeknek a közlekedésben való részvétel elősegítése és a parkolás biztosítása céljából a parkolási igazol-*

ványban kezelt személyes adatai nem kapcsolhatók hozzá más célú adatkezelésekhez". Ezért a Hatóság álláspontja szerint a GDPR 5. cikk (1) bekezdés b) pontjában rögzített célhoz kötött adatkezelés és az adatminimalizálás elvére figyelemmel nem fogadható el, ha a behajtási lehetőséget csak a parkolási igazolvány használata mellett további személyes adatok megadása, rögzítése után tette volna lehetővé az adatkezelő (NAIH/2018/1997/V).

2. Átláthatóság

Egy panaszos bejelentésében arról kért felvilágosítást, hogy adatvédelmi szempontból kifogásolható-e az, hogy egy műszaki áruházban a biztosító által nyújtott garancia vásárlásakor nem töltettek ki velük adatvédelmi nyomtatványt.

A GDPR (58) preambulumbekezdése és a GDPR 12. cikk (1) bekezdése alapján az átláthatóság elve megköveteli, hogy a nyilvánosságnak vagy az érintettnek nyújtott tájékoztatás tömör, könnyen hozzáférhető és könnyen érthető legyen, valamint hogy azt világos és közérthető nyelven fogalmazzák meg, illetve – ezen túlmenően – szükség esetén vizuálisan is megjelenítsék. Az ilyen tájékoztatás nyújtható elektronikus formátumban is, például a nyilvánosságnak szánt tájékoztatás közölhető honlapon keresztül. Ez különösen olyan helyzetekben lehet fontos, amikor a szereplők nagy száma és a gyakorlat technológiai összetettsége megnehezíti az érintett számára annak megismerését és megértését, hogy gyűjtenek-e róla személyes adatokat, és ha igen, ki és milyen célból, ilyen például az online marketing esete.

Válaszában a Hatóság rámutatott, hogy az adatkezelőt terheli annak bizonyítása, hogy megfelel a GDPR követelményeinek, pl. hogy eleget tett az átláthatóság elvéből (GDPR 5. cikk (1) bekezdés a) pont) levezethető kötelezettségnek, így különösen a GDPR 13-14. cikk szerinti tájékoztatásnak, vagy – ha hozzájárulás az adatkezelés jogalapja – annak bizonyítása, hogy az érintett a hozzájárulását adta. A fenti kötelezettségek teljesítésének dokumentálása az adatkezelő érdeke és kötelezettsége, annak hiányában az adatfelvétel jogszerűsége, illetve a megfelelő jogalap fennállta nehezen bizonyítható. (NAIH/2018/5913/V.)

Egy másik ügyben – ahol a bejelentő aziránt érdeklődött, hogy jogszerűen kéri-e a közös képviselő a lakások tulajdonosainak személyi azonosítóit –, a Hatóság azt az állásfoglalást adta, hogy a személyi azonosító a közös képviselői feladatok ellátásához általában nem szükséges személyes adat.

A GDPR 6. cikk (1) bekezdés c) pontja szerinti jogalap kizárólag célhoz kötött, minimálisan szükséges személyes adatokra alkalmazható a GDPR 5. cikk (1) bekezdés b) és c) pontjainak megfelelően (célhoz kötöttség, adattakarékosság elve).

A személyi azonosító adott esetben a társasházi alapító okirat módosításához lehet szükséges, de ott is csak az eljáró ellenjegyző ügyvédnek szükséges ezt nyilvántartásban kezelnie. A személyi azonosító állandó nyilvántartására akkor lenne joga a közös képviselőnek, ha erre egy jogszerű célt tud megjelölni, amely a személyi azonosító állandó kezelése nélkül ésszerűen nem megvalósítható, továbbá amennyiben a GDPR 6. cikk szerinti más jogalap nem áll fenn, akkor szükséges az érintettek hozzájárulása is. Ezen célt és a közös képviselői megbízási szerződésének teljesítéséhez szükséges és arányos adatkezelési érdeket a közös képviselő köteles az adatkezelési tájékoztatásában világosan és érthetően bemutatni a fentebb hivatkozott GDPR 5. cikknek megfelelően. (NAIH/2018/3464/V.)

Biztosító által baleseti kárrendezésével összefüggésben kért, *„Adat- és Titokvédelmi Nyilatkozat”* elnevezésű nyomtatvány kitöltésével és ezzel egyidejűleg az érintett egészségügyi adatainak megismeréséhez, kezeléséhez történő hozzájárulással kapcsolatban a Hatóság kifejtette, hogy a biztosítási tevékenységről szóló 2014. évi LXXXVIII. törvény (a továbbiakban: Bit.) 135. § és 136. §-aiból[1] következően a biztosító az érintett hozzájárulásával jogosult kezelni a bejelentő egészségügyi adatait, amennyiben például az a biztosítási igény megalapozottságának vizsgálatához szükséges, a GDPR 5. cikkének (1) bekezdésének b) és c) pontjában található célhoz kötöttség és adattakarékosság elvének betartásával. A Hatóság álláspontja szerint a Biztosító adatkérése, illetőleg adatkezelése csak abban az esetben, mértékben, illetve adatkörben jogszerű, amennyiben a bekért és kezelt adatok ténylegesen elengedhetetlenül szükségesek valamely, a biztosítási szerződéssel összefüggő célból, például a biztosítási jogviszonyra alapított igények elbírálásához.

A Hatóság állásfoglalásában kifejtette, hogy egy olyan hozzájárulás-kérés, mely általánosságban a csatolt dokumentumban megjelölt szervektől, személyektől[2] történő tájékoztatás kérésére, nyilvántartásokba, dokumentumokba történő betekintés nyújtására, valamint az (egészségügyi) adatokat tartalmazó doku-

1 Bit. 135. § Valamely biztosító társaság jogosult kezelni ügyfeleinek mindazon személyes adatait, melyek a biztosítási szerződésre alapított szolgáltatással összefüggenek.
Bit. 136. § Az ügyfél egészségi állapotával összefüggő az egészségügyi és a hozzájuk kapcsolódó személyes adatok kezeléséről és védelméről szóló törvényben (a továbbiakban: Eüak) meghatározott egészségügyi adatokat a biztosító a 135. § (1) bekezdésében meghatározott célokból, az Eüak. rendelkezései szerint, kizárólag az érintett írásbeli hozzájárulásával kezelheti.

2 *„A károsult a háziorvosától, a Nemzeti Egészségbiztosítási Alapkezelőtől, a Nemzeti Rehabilitációs és Szociális Hivataltól, a Magyar Államkincstártól, a társadalombiztosítási kifizetőhelyektől, valamint mindazon egészségügyi intézményektől, orvosoktól, természetgyógyászoktól és a károsult gyógykezelésével foglalkozó más személyektől, szervezetektől”*

mentumokról történő másolatkészítésre biztosít lehetőséget, a GDPR 5. cikk (1) bekezdés b) és c) pontjának sérelmét látszik megvalósítani, ha olyan adatok is kikérésre kerülnek ennek következtében, amelyek a bejelentő kárigényének elbírálásához nem szükségesek. Adatvédelmi jogi szempontból általános hozzájárulás helyett konkrét hozzájárulás lehet csak érvényes, ezért az általános felhatalmazás-kérés kifejezetten aggályos. Az adatkérés jogszerűsége azonban nem ítélhető meg a biztosítási jogviszonyra vonatkozó valamennyi dokumentum, így különösen a biztosítási szerződés ismerete nélkül. Ezen dokumentumok ugyanis tartalmazhatnak olyan szerződési feltételeket, melyek a biztosító társaság adatigénylését kellően alátámasztják, így például a biztosítási szerződés megkötését eleve kizáró feltételek, kizáró okok vonatkozásban. (NAIH/2018/5815/V.)

3. Pontosság elve

A NAIH/2018/6408/H. számú ügyben a kérelmező, aki nem a pénzügyi intézmény ügyfele, a pénzügyi intézménytől kérte, hogy ne használják a telefonszámát és ne küldjenek más személy számlatartozásáról részére rövid szöveges üzeneteket (SMS).

A pénzügyi intézmény a kérelmező bejelentése alapján küldött adatpontosításra felhívó leveleket az ügyfelének, továbbá a kérelmezőt is felhívta az előfizetői szerződése bemutatására. A kérelmező – a bejelentése ellenére – továbbra is SMS-üzenetet kapott az adatkezelőtől más személy tartozásával kapcsolatban.

A Hatóság megállapítása szerint az adatkezelő adatkezelése, az általa tárolt telefonszámra való SMS küldése csak addig volt jogszerűnek tekinthető, amíg vélelmezhető volt, hogy a nyilvántartott telefonszám az ügyfeléé. Amikor ez kétségessé vált a kérelmező bejelentése folytán, az adatkezelőnek intézkednie kellett volna az adat kezelésének korlátozásáról a helyzet tisztázásáig, az adatpontosság ellenőrzéséig. Az adatkezelő ennek a kötelezettségének nem tett eleget, mert a kérelmező bejelentése után – amikor már kétségessé vált a kezelt adat pontossága és naprakészsége – is küldött SMS üzenetet, ezzel megsértette az általános adatvédelmi rendelet 5. cikk (1) bekezdés d) pontját.

A Hatóság álláspontja szerint az, hogy az adatkezelő megkereste az ügyfelét az adatpontosításra felhívó levelével, megfelelő, de nem elegendő intézkedésnek tekinthető. Az adatkezelő bejelentés alapján tett intézkedéseinek elő kell segítenie a pontosság elvének érvényesülését és meg kell akadályoznia a pontatlan

adatok felhasználását. Ilyen esetben az adatkezelőnek a pontatlan adat kezelését átmenetileg korlátoznia kell.

4. Elszámoltathatóság

Egy panaszos azzal kereste meg a Hatóságot, hogy egy általa korábban böngészett honlap hirdetéseket jelenít meg a telefonján és laptopján anélkül, hogy ehhez hozzájárult volna.

A GDPR 4. cikk 1. pontjában meghatározott személyes adat fogalmába az úgynevezett „pszeudonim" vagy álnevesített személyes adatok is beletartoznak, mint az e-mail vagy IP cím akkor is, ha nem tartalmazza a természetes személy valódi nevét. A GDPR 5. cikk (2) bekezdésében megfogalmazott elszámoltathatóság elve alapján az adatkezelő köteles úgy dokumentálni és nyilvántartani az adatkezelést, hogy annak jogszerűsége utólag bizonyítható legyen. Például a hozzájárulás mint jogalap alkalmazása esetén a hozzájárulás megtörténtét észszerű szinten bizonyítania kell tudni (e-mail, online jóváhagyás naplózása IP címmel), a GDPR azonban nem határozza meg tételesen, hogy hogyan kell az adatkezelési tevékenység jogszerűségét bizonyítani. Az adatkezelő köteles megadni az érintettnek a GDPR rendelkezései szerinti tájékoztatást, többek között az adatokhoz való hozzáférés, helyesbítés és törlés, illetve tiltakozás módjáról. (NAIH/2018/4568/V.)

Egy másik ügyben a panaszos a Hatósághoz küldött levelében egy adótanácsadással, könyveléssel foglalkozó cég honlapjával kapcsolatos aggályait adta elő és kifogásolta a honlapon található adatvédelmi tájékoztató hiányát.

Ha az érintettre vonatkozó személyes adatokat az érintettől gyűjtik, az adatkezelőnek a személyes adatok megszerzésének időpontjában a tisztességes és átlátható adatkezelés érdekében az érintetteknek részletes tájékoztatást kell adni a GDPR 13. cikkébe meghatározottakról. A GDPR 5. cikk (2) bekezdése szerinti elszámoltathatóság elvéből fakadóan az adatkezelőnek képesnek kell lennie arra, hogy igazolja a személyes adatok kezelésére vonatkozó elveknek való megfelelést.

A Hatóság megállapította, hogy a GDPR rendelkezéseinek megfelelő adatvédelmi tájékoztatás akár az adatkezelő honlapján közzétéve, de akár más igazolható módon (pl. nyomtatványon, szerződésben, levelekben) is megtörténhet az adott adatkezelési tevékenység sajátosságaitól függően. (NAIH/2018/5407/V.)

II.1.2.4. Jogalapok

Az adatkezelés jogalapjait az általános adatvédelmi rendelet 6. cikk (1) bekezdése tartalmazza, melyek a következők:

– az érintett hozzájárulása;
– az érintettel létesített vagy létesítendő szerződéses viszony;
– az adatkezelőre vonatkozó jogi kötelezettség;
– az érintett vagy más természetes személy létfontosságú érdeke;
– közérdekű feladat ellátása és közhatalomi jogosítvány gyakorlása;
– az adtakezelő vagy harmadik fél jogos érdeke.

Pusztán ezen jogalapok közül valamelyik fennállása azonban nem elegendő a személyes adatok különleges kategóriáinak jogszerű kezeléséhez, ahhoz ugyanis az általános adatvédelmi rendelet 9. cikke további követelményeket ír elő. A főszabály az, hogy a különleges személyes adatok kezelése tilos. E főszabály alóli kivételeket a GDPR 9. cikk (2) bekezdése tartalmazza, mely kivételek fennállása esetén kezelhetők különleges személyes adatok, feltéve hogy az adatkezelő valamely, a GDPR 6. cikk (1) bekezdése szerinti jogalap fennállását is igazolni tudja.

1. A hozzájárulás jogalapja

A hozzájárulás fogalmát meghatározza az általános adatvédelmi rendelet. Az érintett hozzájárulása az érintett akaratának önkéntes, konkrét és megfelelő tájékoztatáson alapuló és egyértelmű kinyilvánítása, amellyel az érintett nyilatkozat vagy a megerősítést félreérthetetlenül kifejező cselekedet útján jelzi, hogy beleegyezését adja az őt érintő személyes adatok kezeléséhez. A hozzájárulás fogalmi elemei hasonlóan a korábbi – Infotv. szerinti – szabályoknak a megfelelő előzetes tájékoztatás, az önkéntesség, illetve a hozzájárulás akaratának konkrét és egyértelmű kinyilvánítása. Amennyiben e fogalmi elemek közül valamelyik nem felel meg a rájuk vonatkozó követelményeknek, a hozzájárulás jogalapjára nem hivatkozhat jogszerűen az adatkezelő.

A fogalmi elemek közül a megfelelő tájékoztatás az, amelyen keresztül az érintettek megismerik a személyes adataikra vonatkozó adatkezelést, nyomon tudják követni személyes adataik sorsát és az előzetes tájékoztatáson keresztül tud az információs önrendelkezési jog érvényesülni: az adatkezelés lehet jogszerű, amelynek körülményei az érintettek előtt maradéktalanul ismertek. A hozzájárulás érvényességének másik összetevője az érintett akaratának önkéntessége, külső befolyástól való mentessége, amely akkor valósul meg, ha valódi választási lehetőség áll az

érintett rendelkezésére. A hozzájárulás megadása nem tekinthető önkéntesnek, ha az érintett nem rendelkezik valós vagy szabad választási lehetőséggel és nem áll módjában a hozzájárulás anélküli megtagadása vagy visszavonása, hogy ez kárára válna. A hozzájárulás érvényességének további követelménye az érintett akaratának konkrét, egyértelmű, nyilatkozat vagy megerősítést félreérthetetlenül kifejező cselekedet útján történő kinyilvánítása, mely azt jelenti, hogy a hozzájárulásnak aktív magatartásnak kell lennie, egy tevőleges magatartás elmulasztása nem tekinthető határozott és félreérthetetlen hozzájárulásnak.

A hozzájárulás további feltételeit a GDPR 7. cikke tartalmazza. Ezek közül az egyik olyan új – az elszámoltathatóság elvéből is fakadó – követelmény, amelyet az Infotv. korábban ilyen formában nem rögzített az, hogyha az adatkezelés hozzájáruláson alapul, az adatkezelőnek képesnek kell lennie annak igazolására, hogy az érintett személyes adatainak kezeléséhez hozzájárult.

További – az átláthatóság elvéből is eredő – többlet-követelményként fogalmazza meg az általános adatvédelmi rendelet, hogy az írásbeli nyilatkozaton a hozzájárulás iránti kérelmet más ügyektől egyértelműen megkülönböztethető módon kell előadni, érthető és könnyen hozzáférhető formában, világos és egyszerű nyelvezettel. Ezen túlmenően az adatkezelőnek azt is biztosítania kell, hogy az érintett ugyanolyan módon vissza tudja vonni hozzájárulását, ahogyan azt megadta.

Az említett főbb követelményeken túl az 95/46/EK irányelv 29. cikke alapján létrehozott Adatvédelmi Munkacsoport (továbbiakban: 29-es Munkacsoport) a GDPR szerinti hozzájárulásról szóló iránymutatása részletesen foglalkozik azzal, hogy az adatkezelőket milyen további kötelezettségek terhelik, hogy jogszerűen hivatkozhassanak a hozzájárulás jogalapjára.

A Hatóság a NAIH/2018/3750/V. számú ügyben, melyben a bejelentő azt kifogásolta, hogy az adatkezelő egy futópályájára történő belépéshez minden sportolni szándékozó személy köteles a nevét, címét, illetve telefonszámát egy, a porta asztalán elhelyezett A4-es lapra felírni, megállapította, hogy az adatkezelő által hivatkozott jogalap, az érintett hozzájárulása nem volt alkalmazható egyrészt a megfelelő tájékoztatás, másrészt az önkéntesség hiánya miatt. Az adatkezelő ugyanis bár rendelkezett adatkezelési tájékoztatóval, az nem tartalmazta az általános adatvédelmi rendelet által előírt összes adatkezelési körülményt, információt, és az önkéntesség követelménye sem volt biztosított, tekintettel arra, hogy, aki nem iratkozott fel a lapra, nem vehette igénybe a sportpályát.

2. Szerződéses viszonyon alapuló adatkezelés

Az Infotv.-hez képest új, a hozzájárulástól elkülönülő, önálló jogalapként szabályozza a GDPR a szerződéses viszonyon alapuló adatkezelést akként, hogy jogszerű az az adatkezelés, amely olyan szerződés teljesítéséhez szükséges, amelyben az érintett az egyik fél, vagy az a szerződés megkötését megelőzően az érintett kérésére történő lépések megtételéhez szükséges. Ennek a jogalapnak tehát két esetköre van. Az egyik az, amikor az adatkezelés olyan szerződés teljesítéséhez szükséges, amelyben az érintett az egyik fél, míg a másik eset, amikor az adatkezelés a szerződés megkötését megelőzően bizonyos lépéseknek az érintett kérésére történő megtételéhez szükséges.

A szerződés teljesítéséhez szükséges adatkezelés előfeltétele egy olyan érvényes szerződés, amelyben az egyik szerződő fél az érintett. Erre az esetre példa többek között a munkaszerződés, amelyben a munkáltatónak a szerződés teljesítéséhez szükséges a munkavállalók adatait kezelnie. Fontos hangsúlyozni azonban azt, hogy a munkaviszonyból eredően további adatkezelések, adatkezelési célok is keletkeznek, keletkezhetnek, amelyek vonatkozásában azonban a szerződés jogalapja helyett más jogalapok, például a jogi kötelezettség vagy a jogos érdek jogalapja alkalmazható.

A szerződés megkötését megelőzően az érintett kérésére történő lépések megtételéhez szükséges adatkezelés azt az esetet jelenti, amikor a felek között még nem jött létre szerződés, azonban ahhoz, hogy ez megtörténjen, bizonyos olyan lépéseket kell megtenni, amelyekhez szükséges adatkezelés. Fontos kritérium azonban, hogy ezen – szerződés megkötését megelőző – lépésekre nem az adatkezelő vagy egy harmadik fél érdekében, illetve kezdeményezésére kerülhet sor, hanem az érintettére. Példa erre az adatkezelésre az árajánlat kérése. Ekkor ahhoz, hogy az adott szolgáltató meg tudja tenni az érintett felé az ajánlatát, szükséges lehet ideiglenesen kezelnie az érintett több személyes adatát is (például élet- vagy gépjármű-felelősségbiztosítás esetében meglehetősen széles adatkört).

3. Jogi kötelezettség jogalapja

A személyes adatok kezelése akkor is jogszerű, ha az adatkezelés az adatkezelőre vonatkozó jogi kötelezettség teljesítéséhez szükséges.

Ha az adatkezelésre az adatkezelőre vonatkozó jogi kötelezettség teljesítése keretében kerül sor, az adatkezelésnek az uniós jogban vagy valamely tagállam jogában foglalt jogalappal kell rendelkeznie. Az általános adatvédelmi rendelet

azonban nem követeli meg, hogy az egyes konkrét adatkezelési műveletekre külön-külön jogszabály vonatkozzon. Elegendő lehet az is, ha egyetlen jogszabály szolgál jogalapul több olyan adatkezelési művelethez is, amely az adatkezelőre vonatkozó jogi kötelezettségen alapul. Az adatkezelés célját is uniós vagy tagállami jogban kell meghatározni. Az általános adatvédelmi rendeletnek a személyes adatok kezelésének jogszerűségére vonatkozó általános feltételeit a tagállami jogi normák pontosíthatják, továbbá az adatkezelő megjelölésére vonatkozó pontos szabályokat, az adatkezelés tárgyát képező személyes adatok típusát, az érintetteket, azokat a szervezeteket, amelyekkel a személyes adatok közölhetők, az adatkezelés céljára vonatkozó korlátozásokat, az adattárolás időtartamát, valamint egyéb, a jogszerű és tisztességes adatkezelés biztosításához szükséges intézkedéseket is meghatározhatják. A Hatóság a jogbiztonság érdekében ezen feltételek jogalkotó általi meghatározását támogatja és szorgalmazza.

Olyan jogi kötelezettséget is előírhatnak jogszabályok, amely bár személyes adatok kezelésével járhat, az adott jogszabály nem határozza meg az adatkezelés körülményeit. Amennyiben az ilyen kötelező adatkezelést előíró jogszabály nem felel meg maradéktalanul az Infotv. 5. § (3) bekezdésének és nem tartalmazza az adatkezelés körülményeit, úgy az adatkezelőnek kell érvényre juttatnia a személyes adatok kezelésére irányadó általános szabályok szerinti alapelveket és garanciákat, amelyekről a jogalkotó elmulasztott rendelkezni.

Előfordulhat olyan eset is, amikor a jogszabály csak általános felhatalmazást tartalmaz meghatározott – személyes adatok kezelésével járó – tevékenység végzésére. Ilyen eset például az Mt. azon rendelkezése, amely alapján a munkáltató a munkavállalót a munkaviszonnyal összefüggő magatartása körében ellenőrizheti. Ekkor a törvény az ellenőrzés lehetőségét (és nem kötelezettségét) biztosítja, adatkezelést sem ír elő kötelezettségként, ezért az adatkezelésnek is eltérő a jogalapja (a munkáltató jogos érdeke).

4. Az érintett létfontosságú érdekén alapuló, úgynevezett „vis maior" jellegű adatkezelés

Az általános adatvédelmi rendelet szabályai értelmében jogszerű az az adatkezelés is, amely az érintett vagy egy másik természetes személy létfontosságú érdekeinek védelme miatt szükséges.

Más természetes személy létfontosságú érdekeire hivatkozással személyesadatkezelésre akkor kerülhet sor, ha a szóban forgó adatkezelés egyéb jogalapon nem végezhető. Ezen jogalap kapcsán hangsúlyozandó, hogy egyes adatke-

zelések esetén potenciálisan több jogalap alkalmazása is felmerülhet, ezek közül az adatkezelőnek kell kiválasztania azt, amelyre az adatkezelését alapozza (így pl. a személyesadat-kezelés néhány típusa szolgálhat egyszerre fontos közérdeket és az érintett létfontosságú érdekeit is, így olyan esetben, amikor az adatkezelésre humanitárius okokból – többek között járványok és terjedéseik nyomon követéséhez, vagy humanitárius vészhelyzetben, különösen természeti vagy ember által okozott katasztrófák esetében – van szükség.

5. Közérdekű feladat ellátásához és közhatalom gyakorlásához szükséges adatkezelés

A közérdekű feladat ellátásához és közhatalom gyakorlásához szükséges adatkezelés mint adatkezelési jogalap kapcsán, hasonlóan a 3. pontban vizsgált jogalaphoz, elmondható, hogy a hazai jogi környezet és az Alkotmánybíróság gyakorlata szerint az érintett alapvető jogait – így információs önrendelkezési jogát is – az állam csak a szükséges és arányos mértékben, valamely alapvető jog érvényesülése vagy valamely alkotmányos érték védelme érdekében, azaz közérdekből korlátozhatja. Ezért e jogalap alkalmazásához feltétel, hogy az adatkezelő közhatalmi feladat- és hatáskörének gyakorlásához, vagy egyéb közérdekből elvégzendő feladata végrehajtásához szükséges adatkezelési tevékenységét közérdeken alapuló célból jogszabály, vagy uniós norma alapozza meg. Ezen jogszabályi rendelkezés ugyanakkor sok esetben csak az adatkezelő közfeladatát, eljárási mozgásterét és kötelezettségét határozza meg, az ehhez kapcsolódó adatkezelési műveletek részletes szabályait nem.

Az adatkezelő közfeladatait meghatározó jogszabályi rendelkezéseken alapuló adatkezelések jogalapja tehát a GDPR 6. cikk (1) bekezdés e) pontja. Fontos kiemelnünk azt is, hogy egy közhatalmi tevékenységet vagy egyéb közfeladatot ellátó szerv – mint költségvetési szerv – minden közjogi és magánjogi jogviszonyának, és az ahhoz járulékosan kapcsolódó adatkezelési jogviszonyainak kizárólag közfeladatai ellátásával összefüggésben lehet alanya, ettől eltérő minősége fogalmilag kizárt. Ebből fakadóan e jogalap, mintegy magába olvasztja, elnyeli a további adatkezelési jogalapokat. E felfogást tükrözi – az általános adatvédelmi rendelettel szemben a magánszféra adatkezelésére tárgyi és szervi hatálya folytán egyáltalán nem alkalmazandó – bűnügyi adatvédelmi irányelv is, ahol az adatkezelés jogalapja kizárólag az irányelv hatálya alá tartozó tevékenység, mint közfeladat lehet [8. cikk].

Ha pedig a jogalkotó ezen adatkezelésekre vonatkozó részletes szabályokat az Infotv. 5. § (3) bekezdésének előírásait figyelmen kívül hagyva nem rögzítette,

az adatkezelő az általános adatvédelmi szabályok – így különösen az alapelvek és a jogalap szükségességi mércéje – szerint köteles adatkezelési tevékenységét végezni, és annak jogszerűségét az elszámoltathatóság elvének megfelelően igazolni.

6. Jogos érdek, érdekmérlegelés

Ha az adatkezelés jogalapja a jogos érdek, akkor az adatkezelőnek előzetesen érdekmérlegelési tesztet kell elvégeznie[3], továbbá a tájékoztatási kötelezettsége[4] keretében az érintettet a tiltakozáshoz való jogáról is külön tájékoztatnia kell. Az általános adatvédelmi rendelet példálózóan megemlít két esetet, melyeknél ennek a jogalapnak az alkalmazása gyakran előfordul, nevezetesen azokat, amikor az érintett az adatkezelő ügyfele vagy annak alkalmazásában áll[5].

Az adatkezelőnek az érdekmérlegelési teszt keretében többek között egyértelműen meg kell határoznia az adatkezelés alapjául szolgáló jogos érdeket, az érintettre gyakorolt hatást, továbbá azt, hogy az adatkezelés szükséges, illetve arányos-e, valamint mérlegelnie kell, hogy az adatkezelő vagy harmadik személy jogos érdeke az érintetti joghoz képest elsődleges-e. Az arányosság biztosítása érdekében az adatkezelő köteles ellenőrizni, hogy van-e alternatívája az adott adatkezelésnek, és az adott alternatíva ugyanolyan hatékony-e és esetlegesen kisebb beavatkozással járhat-e, mert amennyiben kisebb beavatkozással járó ugyanolyan hatékony adatkezelés is választható, abban az esetben az adatkezelőnek azt kell alkalmaznia.

A fentiekben említett szempontok mérlegelése alapján, az adatkezelés megkezdése előtt kell megállapítani azt, hogy kezelhető-e a személyes adat. Ha az érdekmérlegelés eredménye alapján az adatkezelő vagy harmadik személy jogszerű érdeke elsődleges, továbbá az adott intézkedés arányos is, és nincs kisebb beavatkozással járó ugyanolyan hatékony alternatívája az adatkezelésnek, abban az esetben a jogos érdekre hivatkozással jogszerű lehet az adatkezelés.

A Hatóság tapasztalatai alapján az adatkezelők a legtöbb esetben nem végzik el megfelelően az érdekmérlegelést. Az egyik legnagyobb hiba abból adódik, hogy az adatkezelők a saját érdekeik azonosításán túl – erre sem kerül minden esetben maradéktalanul sor –, valódi érdekmérlegelést nem végeznek, nem vezetik

3 Általános adatvédelmi rendelet (47) preambulum-bekezdés

4 Általános adatvédelmi rendelet 13. cikk (2) bekezdés b) pont, 14. cikk (2) bekezdés c) pont és 21. cikk (4) bekezdés

5 Általános adatvédelmi rendelet (47) preambulum-bekezdés

le következetes módon azt, hogy az érdekmérlegelésükben megnevezett érdekeik miért részesítendőek előnyben az érintett érdekeivel szemben.

További kifogásolható adatkezelési gyakorlat az érdekmérlegelésekkel összefüggésben az is, hogy az adatkezelők a személyes adatok védelméhez kapcsolódó érdekeket nem valamilyen jogos és valódi érdekkel vetik össze, hanem kényelmi szempontokat helyeznek előtérbe az érintett alapvető jogaival szemben, ami adatvédelmi szempontból nem elfogadható, tekintettel arra, hogy ezek nem lehetnek hangsúlyosabbak az adatalanyi érdekeknél.

Megfelelő, az adatkezelés szükségességét alátámasztó érveket nélkülöző érdekmérlegelési teszt hiányában az adatkezelők nem hivatkozhatnak a jogos érdekre, mint jogalapra, tehát ilyen esetekben megállapítható, hogy az adatkezelés jogellenes.

a) A Hatóság a NAIH/2018/6142/H. számú ügyben vizsgálta az eredetileg hozzájáruláson, majd jogos érdeken alapuló adatkezelés esetét. Ebben az ügyben az érintett telefonszám adatának nyilvántartásban való rögzítésére érintetti hozzájárulás alapján 10 évvel ezelőtt került sor. Az érintett az általános adatvédelmi rendelet hatályba lépése után tiltakozott a telefonszám adatának kezelése ellen és a törlését kérte.

Az adatkezelő a tiltakozás alapján nem törölte az érintett telefonszámát, mert az általános adatvédelmi rendelet 17. cikk (1) bekezdés b) pontja értelmében amennyiben az érintett visszavonja az adatkezelés alapját képező hozzájárulását, az adatkezelő nem köteles törölni az adatokat, ha másik jogalapja van az adatkezelésre és arra hivatkozott, hogy az általa elvégzett érdekmérlegelési teszt alapján a jogos érdek mint jogalap fennáll.

A Hatóság a jogos érdek alátámasztására készített adatkezelői érdekmérlegeléssel kapcsolatosan sok hiányosságot feltárt, így megállapította, hogy megfelelő és elfogadható érdekmérlegelés hiányában a személyes adat kezelését az adatkezelő jogos érdekre nem alapozhatja. Az érdekmérlegeléssel kapcsolatos hiányosságok közül példálózóan az alábbiak emelendők ki:

- az adatkezelő több adatkezelési célt is megjelölt, azonban nem célonként végezte el az érdekmérlegelést,
- az adatkezelés céljához viszonyított szükségesség nem volt bizonyított,
- az adatkezelő gazdasági érdeket és kényelmi szempontokat helyezett előtérbe az érintett érdekeivel és alapvető jogaival szemben, úgy, hogy

ezen érdekek elsődlegességét nem bizonyította és arányosítást lényegében nem végzett,
- az adatkezelő hiányosan és helytelenül azonosította az érintetti érdeket,
- az adatkezelés mellett olyan érvek kerültek felsorakoztatásra, melyek az érdekmérlegelés szempontjából irrelevánsak.

b) A NAIH/2018/2041/V. számú ügyben tett megállapítások szerint olyan személy adatait kezelte a pénzügyi intézmény, akivel nem állt szerződéses kapcsolatban. 2007-ben a panaszos férje kölcsönszerződést kötött, amit a bank felmondott. A követelés engedményezésre került, amiről csak a panaszos férjét értesítették. A pénzügyi intézmény a panaszos adatainak kezelésével kapcsolatban több jogalapot is megjelölt, hivatkozott szóbeli hozzájárulásra, Csjt.-re és Ptk.-ra, majd a Hatóságnak írt nyilatkozatában jogos érdekre. 2018. május 25. napjától az adatkezelő által hivatkozott jogalapok közül csak a jogos érdek lehetett volna elfogadható az adott esetben, amennyiben az adatkezelő megfelelő érdekmérlegelési teszttel rendelkezik a jogos érdekének alátámasztására.

A Hatóság megállapításai alapján az adatkezelő által becsatolt – dátum nélküli – érdekmérlegelési teszt nem volt megfelelő, mert az abban foglaltak szerint az adatkezelő ténylegesen semmilyen érdekmérlegelést nem végzett, mivel a Hatóság felhívására becsatolt dokumentum nem tartalmazta az arra irányuló vizsgálatot, hogy a panaszos adatainak kezelése az adott esetben elengedhetetlenül szükséges-e.

7. Az adatgyűjtés céljától eltérő célú adatkezelés

A GDPR lehetővé teszi, hogy az adatok az eredeti céltól eltérő céllal is hasznosíthatóak legyenek, ha a célok összeegyeztethetőek.

Az általános adatvédelmi rendelet példálózóan felsorolja azokat a szempontokat, melyeket figyelembe kell venni annak megállapításához, hogy az eltérő célú adatkezelés összeegyeztethető-e azzal a céllal, amelyből a személyes adatokat eredetileg gyűjtötték.

E szerint meg kell vizsgálni az adatgyűjtés eredeti célja és az adatkezelés új célja közötti kapcsolatot, továbbá azt, hogy a személyes adatok gyűjtése milyen körülmények között történt (érintett és az adatkezelő közötti kapcsolat), mi a személyes adatok jellege, milyen megfelelő garanciák kerülnek bevezetésre és azt is, hogy az érintettekre nézve a további adatkezelés milyen körülményekkel jár.

Az általános adatvédelmi rendelet által előírt tájékoztatási kötelezettségüknek eleget téve az érintetteket tájékoztatniuk kell az adatkezelőknek az adatkezelés jogalapjának változásáról, valamint az érintetti jogaik gyakorlása körében a tiltakozáshoz való jogukról.

A NAIH/2018/6142/H. számú ügyben a Hatóságnak az általános adatvédelmi rendelet 6. cikk (4) bekezdése alapján is vizsgálnia kellett a telefonszámmal kapcsolatos adatkezelést, tekintettel arra, hogy az adatkezelő új adatkezelési célra is hivatkozott.

Az általános adatvédelmi rendelet 6. cikk (4) bekezdése lehetővé teszi, hogy a személyes adatokat az adatkezelés eredeti céljától eltérő egyéb célból kezelje az adatkezelő, feltéve, hogy az adatkezelés összeegyeztethető az adatkezelés eredeti céljával, amelyekre a személyes adatokat eredetileg gyűjtötték. Ebben az esetben az adatkezelőnek több szempontot figyelembe kell vennie, melyek közül az általános adatvédelmi rendelet a 6. cikk (4) bekezdésében példálózó felsorolásban kiemeli azokat a körülményeket, amelyek mérlegelését a legfontosabbnak tartja.

Az ügyben megállapítható volt, hogy az adatkezelő az eredeti adatkezelési céltól (szerződés teljesítése) eltérő egyéb célból is kezelte a telefonszám adatot (ügyfélszolgálati tevékenység fejlesztése), ezért e cél tekintetében az adatkezelőnek alkalmaznia kellett volna az általános adatvédelmi rendelet 6. cikk (4) bekezdésében foglaltakat. A Hatóság megállapította, hogy az adatkezelő ezt a mérlegelést nem végezte el, ezért az adatkezelés jogalapja a telefonszám kezelése tekintetében az új adatkezelési cél vonatkozásban sem állt fenn.

II.1.2.5. Az érintetti jogok

Az általános adatvédelmi rendelet hatálybalépésével az érintetteket megillető jogosultságok köre szélesedett. Az érintetti kérelmek előterjesztését minden adatkezelőnek kötelessége elősegíteni, ennek megfelelően az adatkezelő által kialakított adatkezelési tájékoztatóban minden esetben ki kell térni e kérések intézésének módjára, menetére.

1. Tájékoztatáshoz való jog, átláthatóság

1.1. Fontos, hogy az adatkezelők előzetes, az adatkezelés minden lényeges körülményére kiterjedő, közérthető tájékoztatást nyújtsanak az érintettek részére a személyes adataik kezelésének útjával és körülményeivel kapcsolatban.

A Hatóság találkozott olyan esetekkel, ahol az adatkezelő egyáltalán nem tett közzé adatkezelési tájékoztatást a honlapján. A Hatóság több ügyben kimondta, hogy azáltal, hogy az érintetteket – a honlapon történő regisztráció során kért személyes adatok megadása előtt – nem tájékoztatták előzetesen az adatkezelés körülményeiről, sérültek a GDPR 12. cikkében foglalt rendelkezések (NAIH/2018/1549/V. és NAIH/2018/5300/V.).

Az adatkezelőknél leggyakrabban felmerülő kérdések a tájékoztatók elkészítésének szükségességére, formájára, nyelvezetére, közzétételére, tartalmára vonatkoztak, valamint arra, hogy 2018. május 25-e után a már folyamatban lévő adatkezelések tájékoztatóinak GDPR szerinti módosítását követően a változásokról az érintetteket tájékoztatni kell-e. A GDPR az elszámoltathatóság mérföldköveként nevesíti az adatkezelő tájékoztatási kötelezettségét. A rendelet által előírt, az érintett részére nyújtott tájékoztatás elkészítése során az adatkezelőnek minden adatkezelést illetően törekednie kell olyan tájékoztatás megadására, amely tömör, átlátható, érthető és könnyen hozzáférhető. A jogszabályi követelményeknek való megfelelő, kellően részletes tájékoztató nemcsak az adatkezelő kötelessége, hanem az érintettek jogainak érvényesülését szolgálja. Az adatkezelési tájékoztató elkészítése az adatkezelő feladata, nincsen Hatóság által készített formanyomtatvány, vagy mintasablon, minden adatkezelő önállóan gondoskodik a tartalom összeállításáról (NAIH/2018/5909/V.).

A tájékoztatók többsége formáját tekintve írásos, de lehetőség van szóbeli tájékoztatás nyújtására is. A szóbeli tájékoztatás alapulhat élő kapcsolaton (pl. telefonbeszélgetés), másrészről előre rögzített szóbeli tájékoztatáson, ez esetben az adatkezelők kötelesek az érintettek számára azt biztosítani, hogy azok az ilyen módon kapott tájékoztatást visszahallgathassák.

A GDPR rendelkezéseinek megfelelő adatvédelmi tájékoztatás az adott adatkezelési tevékenység sajátosságaitól függően akár az adatkezelő honlapján közzétéve, de akár más igazolható módon (pl. nyomtatványon, szerződésben, levelekben, stb.) is megtörténhet.

Tekintettel arra, hogy a GDPR nem írja elő az előzetes felvilágosítás közzétételének/közlésének pontos módját, ezért a Hatóság egy ügyben azt állapította meg, hogy pusztán abból a tényből, hogy a honlapon nem található részletes adatvédelmi tájékoztató, nem vonható le következtetés arra vonatkozóan, hogy az adatkezelő nem a hatályos törvényi előírásoknak megfelelően kezeli a személyes adatokat vagy nem ad megfelelő tájékoztatást az adatkezelési tevékenységéről (NAIH/2018/5407/V.).

A GDPR nem tartalmaz előírást arra vonatkozóan, hogy az adatvédelmi tájékoztatót milyen nyelven kell elkészíteniük az adatkezelőknek. A 29-es Munkacsoport az adatkezelési műveletek átláthatóságáról iránymutatást[6] adott ki, melyben tájékoztatást nyújt az adatkezelő fordítással kapcsolatos kötelezettségeit illetően. Az iránymutatás alapján az átlátható adatkezelés követelményeinek teljesítése érdekében mindazokon a nyelveken indokolt elkészíteni a tájékoztatást, amely anyanyelvű személyeket az adatkezelő az adott szolgáltatással meg kíván szólítani (NAIH/2018/3847/V.).

1.2. A GDPR az adatvédelmi reformot megelőzően alkalmazandó magyar előírásoktól eltérően különbséget tesz aszerint, hogy a személyes adatokat közvetlenül az érintettől, vagy nem az érintettől gyűjtik. Amennyiben a személyes adatokat az érintettől gyűjtik, akkor az adatkezelőnek a 13. cikkben felsoroltakat, úgymint – az adatkezelő(k) kiléte, elérhetősége, az adatvédelmi tisztviselő elérhetősége, az adatkezelés célja, jogalapja, adattovábbítás esetén a címzettek, illetve azok kategóriái – az adatok gyűjtésének időpontjában kell az érintett rendelkezésére bocsátania.

Az adatkezelő a 13. cikk (1) bekezdésében felsoroltakon túl a tisztességes és átlátható adatkezelés biztosítása érdekében a (2) bekezdésben felsorolt ún. kiegészítő információkról – a tárolás időtartamáról, az érintett hozzáférési jogáról, hozzájárulás visszavonásának feltételeiről, panasz benyújtásának jogáról, jogszabályon vagy szerződéses kötelezettségen alapuló adatkezelés tényéről, e jogalapok esetén a személyes adatok megadásának köztelezettségéről, valamint az e kötelezettség teljesítésének elmulasztása következményeiről, a profilalkotás, illetve automatizált döntéshozatal tényéről – is köteles tájékoztatni az érintetteket.

Ezen túlmenően a 29-es Munkacsoport az átláthatóságról szóló iránymutatásában[7] kifejtette mindazon szempontokat, melyeket javasol, hogy az adatkezelők előzetes tájékoztatásuk során figyelembe vegyenek.

Az adatkezelő a tájékoztatási kötelezettsége alól mentesül, ha az érintett az információk egy részével, vagy azok összességével már rendelkezik. A gyakorlatban igen nehéz azt eldönteni, hogy az érintett rendelkezik-e, és ha igen, akkor milyen mértékben a felsorolt információkkal, ezért az adatkezelő akkor jár el helyesen, ha a Rendeletben előírt, kötelezően nyújtandó információkon túl az adat-

6 WP 260 rev.01

7 https://www.naih.hu/files/wp260rev01_hu.pdf

kezeléssel kapcsolatos valamennyi releváns információt, bizonyítható módon (lehetőség szerint írásban) az érintett rendelkezésére bocsát. Ily módon eleget tesz a Rendelet másik fontos alappillérének, az elszámoltathatóság követelményének is.

Az adatkezelőnek az adatkezeléssel összefüggő információkat meg kell adnia az érintett számára abban az esetben is, amikor az adatkezelő a személyes adatokat nem az érintettől szerzi meg (14. cikk), hiszen az érintettet nem érheti joghátrány azért, mert adatait nem közvetlenül tőle szerezték meg. A Rendelet rugalmas határidőt biztosít az adatkezelőnek a tájékoztatási kötelezettségét illetően, amikor kimondja, hogy a tájékoztatást az adatok megszerzésétől számított észszerű határidőn, de legkésőbb egy hónapon belül kell megadnia. A rendelet az általános szabályozáson túl két speciális esetre vonatkozóan tartalmaz előírást. Az adatkezelőnek, ha a személyes adatok felvételére az érintettel való kapcsolattartás felhasználásának céljából került sor, akkor legalább az első kapcsolatfelvétel alkalmával, vagy ha az adatokat várhatóan más címzettekkel is közölni fogják, akkor a személyes adatoknak az első alkalommal való közlésekor kell tájékoztatnia az érintettet.

Az adatkezelőt ebben az esetben sem terheli a tájékoztatási kötelezettség akkor, ha érintett az információk egy részével, vagy azok összességével már rendelkezik, vagy a szóban forgó információk rendelkezésre bocsátása lehetetlen, vagy aránytalan erőfeszítéssel járna. A rendelet nem ír elő tájékoztatási kötelezettséget, ha az adat megszerzését vagy közlését az adatkezelőre vonatkozó az érintett jogos érdekeinek védelmét szolgáló megfelelő intézkedésről rendelkező uniós vagy tagállami jog írja elő, valamint abban az esetben sem, ha a személyes adatoknak valamely uniós illetve tagállami jogban előírt szakmai titoktartási kötelezettség (orvosi titok, ügyvédi titok) alapján bizalmasnak kell maradnia.

2018. május 25-ét követően az adatkezelő feladata a már meglévő, folyamatban lévő adatkezelésekre vonatkozó tájékoztatók GDPR-nak való megfeleltetése, mellyel kapcsolatban a Hatóság álláspontja az, hogy az adatkezelőnek a változásokról az érintetteket külön értesítenie nem szükséges.

Felülvizsgálatra kerültek a Hatóság adatvédelmi tájékoztatói is, amelyek közül a nem csak a munkatársakat érintő tájékoztatók elérhetőek a Hatóság honlapján.

1.3. A GDPR alapján a hozzáférési jog keretében jogosult az érintett arra, hogy az adatkezelőtől visszajelzést kapjon arra vonatkozóan, hogy személyes ada-

tainak kezelése folyamatban van-e, és ha ilyen adatkezelés folyamatban van, jogosult arra, hogy hozzáférést kapjon a személyes adatokhoz és különösen arra vonatkozóan, hogy milyen forrásból származik, amennyiben az adatokat nem az érintettől gyűjtötték.

A hozzáféréshez való jog tekintetében nyújtandó tájékoztatás a már folyamatban lévő adatkezelés esetén értelmezhető. Ez alapján az érintett hozzáférési jogának keretében az adatkezelő köteles tájékoztatást nyújtani az adatkezelés tényéről, céljáról, a személyes adatok kategóriájáról, az esetleges adattovábbításról, a panaszbenyújtás lehetőségéről és menetéről, a tiltakozási jogáról és a begyűjtött adatok forrásáról.

A Hatósághoz nagy számban érkeznek direkt marketing témájú üzenetek fogadásával kapcsolatos beadványok, amelyek szerint nem lehet leiratkozni a hírlevélről, és amikor a panaszos tájékoztatást kér az adatkezelőtől, akkor az adatkezelőtől nem kap választ a kérelmére.

Az érintett tájékoztatási kérelmének megtagadásának kivizsgálásakor az adatkezelők rendszeresen hivatkoznak üzleti titokra vagy más személy személyes adatainak megsértésére. A hozzáférési jog ebben az esetben korlátozható, azonban ekkor is törekedni kell arra, hogy az érintett megkaphassa a kellő tájékoztatást a személyes adataival kapcsolatban, és például a nem releváns adatokat kitakarva, adják ki neki a kért dokumentumokat.

1.4. A GDPR a hozzáférési jog keretén belül új, annak legteljesebb megvalósulását biztosító részjogosultságot nevesít, a másolat kiadásához való jogot. A másolat kiadásához való jog biztosítja az érintett számára a személyes adataihoz való tényleges hozzáférését.

A másolathoz való jognak a hozzáférési jog – az Infotv. korábbi terminológiája szerint tájékoztatáshoz való jog – részeként való elismerése nem abszolút újdonság, azt a Hatóság a GDPR alkalmazandóságát megelőzően is – bizonyos kivételekkel – a tájékoztatáshoz való jog egyik részelemének tekintette, például banki szerződések vonatkozásában.

A másolathoz való jog egyik speciális esete: a kamerafelvételek másolata. A Hatóság GDPR alkalmazandóvá válását megelőzően kialakított gyakorlata szerint a kamerafelvételek vonatkozásában a tájékoztatáshoz való jog a felvételbe való betekintés biztosításával volt a legszélesebb körben megvalósítható. Ennek egyik oka, hogy az Infotv. a tájékoztatáshoz való jog keretében nem

biztosította az érintettek számára azt a lehetőséget, hogy megválaszthassák a tájékoztatás formáját, csupán annyit írt elő az adatkezelők számára kötelezettségként, hogy a tájékoztatást közérthető formában kell megadniuk. A GDPR 15. cikk (3) bekezdése azonban kifejezetten rendelkezik az érintettek másolathoz való jogáról.

A NAIH/2018/5559/H. számú ügyben az adatkezelő az érintett kamerafelvétel másolatának kiadására vonatkozó kérelmét megtagadta arra hivatkozással, hogy az érintett nem igazolta a másolat kiadásához fűződő jogát vagy jogos érdekét, valamint úgy vélte, hogy a kamerafelvétel másolata nem alkalmas azon cél elérésére, amelyet az érintett a másolat kiadása iránti kérelmében megjelölt.

A Hatóság ennek kapcsán megállapította, hogy a GDPR a másolat kiadásához való jog gyakorlásához nem támaszt többletkövetelményeket, az feltétel nélkül gyakorolható, tehát az érintettnek nem kell igazolnia a másolat kiadásához való jogos érdekét, illetve nem kell indokolnia, hogy mi okból kíván élni ezzel a jogával. A hozzáférési jog – ideértve a másolat kiadásához való jogot – gyakorlására vonatkozó kérelem kizárólag a GDPR 12. cikk (5) bekezdése szerinti esetekben tagadható meg, a GDPR 15. cikke nem tartalmaz további korlátozásokat, ezért az ilyen kérelmeket további feltételek támasztása nélkül teljesítenie kell az adatkezelőknek.

Kiemelendő továbbá, hogy a másolat kiadásához való jog gyakorlása – összhangban a GDPR (63) preambulum-bekezdésével – továbbra sem érintheti hátrányosan mások jogait és szabadságait, ebből kifolyólag az érintett a másolathoz való joga alapján továbbra sem kaphatja meg a kamerafelvétel olyan másolatát, amelyen más érintettek kitakarás nélkül szerepelnek, azonban a GDPR 15. cikk (3) bekezdése alapján az adatkezelő már kötelezhető a kitakarás elvégzésére az érintetti jog érvényesülése érdekében.

2. A törléshez való jog („az elfeledtetéshez való jog")

A törléshez való jogot már a 95/46/EK irányelv is tartalmazta, azonban e jog gyakorlásának egyik módjaként az elfeledtetéshez való jogot az általános adatvédelmi rendelet a 17. cikkében kifejezetten nevesíti, melynek értelmében az érintett jogosult arra, hogy bizonyos feltételek fennállása esetén, kérésére az adatkezelő indokolatlan késedelem nélkül törölje a rá vonatkozó személyes adatokat.

Az elfeledtetéshez való jog jellemző aspektusa egyrészt, ha az érintett kérelme az adatkezelő által üzemeltetett honlapon megjelenő adatok törlésére vagy az

adatkezelő által kezelt, tárolt információk eltávolítására irányul, másrészt, ha az érintett egy keresőmotoron megjelenő találatot, linket szeretne eltávolítani.

Az általános adatvédelmi rendelet alapelvként rögzíti, hogy a személyes adatok kizárólag célhoz kötötten és meghatározott ideig kezelhetők. Ebből kifolyólag a kezelt személyes adatok törlését indukálhatja például az adatkezelésre vonatkozó cél megszűnése, illetve a megfelelő jogalap hiánya – különösen akkor, ha az érintett a korábbi hozzájárulását visszavonta –, egyébiránt az adatkezelőre alkalmazandó uniós vagy tagállami jogban előírt jogi kötelezettség teljesítése is.

A fentieken túl a személyes adatok törlését az érintett által az adatkezelőnek címzett kérelme esetén is teljesíteni kell. Az adatkezelő indokolatlan késedelem nélkül, de mindenféleképpen a kérelem beérkezésétől számított egy hónapon belül köteles tájékoztatni az érintettet a kérelemben foglalt információkról, továbbá az az alapján megtett intézkedésről (a törlésről)[8]. Kiemelendő, hogy ha elmarad az érintett törlési kérelmének teljesítése, akkor ennek okáról tájékoztatást kell nyújtani.

További kötelezettség terheli az adatkezelőt abban az esetben, ha a kezelt személyes adatokat nyilvánosságra hozta. Az adatkezelőnek figyelembe kell vennie az elérhető technológia és megvalósítás költségeit annak érdekében, hogy tájékoztassa az adatokat kezelő adatkezelőket, hogy az érintett kérelmezte tőlük a szóban forgó személyes adatokra mutató linkek vagy e személyes adatok másolatának, illetve másodpéldányának törlését.

A rendelet több esetkört is szabályoz, amikor az érintett nem élhet a törléshez és elfeledtetéshez való jogával. Ilyen például, ha a személyes adatok kezelését az adatkezelőre alkalmazandó uniós vagy tagállami jog írja elő, vagy az adatkezelés tudományos, közérdekű, történelmi kutatási, statisztikai célból történik. Megtagadható a törlési kérelem akkor is, ha az adatok kezelése jogi igények előterjesztéséhez, érvényesítéséhez, illetve védelméhez szükséges. Ebben az esetben az adatkezelő köteles igazolni, hogy az adatok kezelésére továbbra is szükség van.

A NAIH/2018/6093/H. számú hatósági eljárásban a kérelmező egy követeléskezelő társasággal szemben kívánt élni törléshez való jogával. A Kötelezettre 2011-ben egy lejárt követelést engedményeztek, azonban az ügy tisztázása érdekében a Kérelmező felvette a kapcsolatot a Kötelezettel, mert nem tartotta

8 GDPR 12. cikk (3) bekezdés

jogosnak a követelést, valamint vitatta az adatkezelés jogszerűségét is. A kapcsolatfelvétel során a Kötelezett arra kérte a Kérelmezőt, hogy természetes személyazonosító adataival azonosítsa magát, mivel csak így tud eleget tenni a kérelmének, ezt azonban a Kérelmező megtagadta, mivel álláspontja szerint az ügyszám és a neve elegendő az azonosításához. A Kötelezett álláspontja szerint nem volt sikeres az azonosítás, így a panasza kivizsgálására irányuló eljárást lezárta. A Kérelmező ezután postai levélben kérte személyes adatainak törlését. A Kötelezett azt a tájékoztatást nyújtotta, hogy a követelés visszavásárlásra került, így a Kérelmező személyes adatai törlése iránt intézkedik, azonban azok továbbra is fellelhetők a Társaság informatikai rendszeréről készített biztonsági másolatokban. Az ügyben a kérelemnek részben helyt adó határozat született, melynek során a Hatóság felszólította a Kötelezettet – többek között – arra, hogy tájékoztassa a Kérelmezőt a személyes adatait tartalmazó biztonsági mentések törlésének időpontjáról. A Hatóság elutasította azonban a kérelem azon részét, amely a létrejött engedményezési szerződés, valamint a Kérelmezővel szembeni követelés visszavásárlására vonatkozó szerződéssel kapcsolatos személyes adatai törlésére vonatkozik, mivel számviteli bizonylatnak minősülnek, amelyeket a Kötelezettnek a számvitelről szóló 2000. évi C. törvény (a továbbiakban: Sztv.) előírásai szerint nyolc évig meg kell őriznie. A számviteli bizonylatokban található személyes adatok kezelésének jogalapja a GDPR 6. cikk (1) bekezdés c) pontja, így azok a Kérelmező kérelmére sem törölhetők a GDPR 17. cikk (3) bekezdés b) pontjának megfelelően.

3. Az érintettek azonosítása

A GDPR 12. cikk (6) bekezdése szerint, ha az adatkezelőnek megalapozott kétsége merül fel az érintetti joggyakorlásra irányuló kérelmet benyújtó természetes személy kilétével kapcsolatban, további, az érintett személyazonosságának megerősítéséhez szükséges információk nyújtását kérheti.

Ha az érintett személyesen terjeszti elő az érintetti joggyakorlásra irányuló kérelmét, az azonosítás folyamata viszonylag egyszerű, mivel szükség esetén valamelyik személyazonosító okmánya bemutatásával az érintett azonosítani tudja magát.

Nagyobb nehézséget okoz a távollevők közti azonosítás, például, ha az érintetti joggyakorlásra irányuló kérelme postán vagy e-mailben érkezik az adatkezelőhöz. Ezen esetekben, ha az adatkezelőnek megalapozott kétsége merül fel az érintett kilétét illetően – korábban nem ismerte az érintett e-mail címét vagy az eltér az általa kezelttől –, el kell végeznie az azonosítást.

A személyazonosság igazolása és az azonosítás nem azonos fogalmak, ezért az azonosításhoz csak kivételes esetben szükséges mind a négy természetes személyazonosító adat megadása, a legtöbb esetben elegendő a név és a további három személyazonosító adat közül az egyik, amennyiben az az ügyfél azonosításához ténylegesen szükséges, tekintettel az adattakarékosság elvére. Ez természetesen nem zárja ki a név és ügyfélszám vagy a név, az ügyfélszám és a lakcím kombinációjával történő azonosítást sem. Az adatkezelőnek esetről esetre kell vizsgálnia, hogy az e-mailt küldő konkrét személy kilétével kapcsolatban van-e megalapozott kétsége, és annak eloszlatásához pontosan mely személyes adat – kivételesen személyes adatok – megadására van szüksége. Ezen mérlegelés során az adatkezelőnek különös figyelmet kell fordítania arra, hogy csak olyan személyes adat megadását kérje azonosítás céljából, amelyet már kezel, amelyet van mivel összevetnie, ellenkező esetben az azonosítás céljából kért adat nem alkalmas az érintett azonosítására, és annak kezelése a célhoz kötött adatkezelés elvébe ütközhet. (NAIH/2019/1841)

Megjegyzendő, hogy az azonosítási kötelezettség nem minden esetben áll fenn. Ha az érintett által benyújtott kérelem vagy egyéb megkeresés tartalmaz olyan információkat, amely alapján az érintett azonosítható, úgy további személyes adatok azonosítás céljából történő megadása nem kérhető az érintettől.

II.1.3. Egyes gyakori ügycsoportok

II.1.3.1. Egészségügyi dokumentáció első másolatának költségmentessége

Egészségügyi területen további fontos változást jelentett az érintetti jogok között a hozzáféréshez való jog megjelenése. Ennek keretein belül az adatkezelőt az Infotv. alapján terhelő tájékoztatási kötelezettséget felváltotta a GDPR 15. cikkének (3) bekezdése alapján a személyes adatokról történő másolat biztosításának kötelezettsége, amely főként az egészségügyi dokumentumokhoz való hozzáférés esetében jelentett változást a korábbiakhoz képest.

Az egészségügyi és a hozzájuk kapcsolódó személyes adatok kezeléséről és védelméről szóló 1997. évi XLVII. törvény (Eüak.) és az egészségügyről szóló 1997. évi CLIV. törvény (Eütv.) biztosítja az érintettnek az egészségügyi dokumentációba történő betekintés és az arról való másolat-kérés jogát. A GDPR alkalmazásától kezdődően e jogosultság az érintettet a GDPR-ból fakadóan közvetlenül illeti meg, az általános adatvédelmi rendelet az adatokhoz való hozzáférés és másolatkérés jogát a 15. cikkben részletezi.

Míg azonban az Eütv. és az Eüak. jelenleg hatályos szabályozása szerint az érintett saját költségére kaphat másolatot az egészségügyi dokumentációból, addig a GDPR a hozzáférési jog keretében az érintett által kért másolat költségmentességét rögzíti [15. cikk (3) bekezdés)], így ez vonatkozik az egészségügyi szolgáltatók által kezelt egészségügyi dokumentációra is.

A Hatóság az elmúlt években több ízben folytatott vizsgálatot azzal kapcsolatban, hogy az egészségügyi szolgáltató egyes esetekben irreálisan magas árat (50 ezer - 100 ezer Ft) szabott az érintett részére történő másolat szolgáltatásának ellenértékeként. Mivel jogszabály nem rendezte az intézmények által elkérhető díjat, a különböző egészségügyi szolgáltatók is rendkívül széles skálán mozogva szabták meg a másolatkészítés költségét. A Hatóság korábban ajánlásban részletezte a díjmegállapítás szempontjait, és ajánlást tett a költségtérítés mértékére.

A 2018-ban vizsgált ügyben egy kórház több mint 50 ezer forintban állapította meg a panaszos terhesgondozására és a gyermeke születésére vonatkozó dokumentumok kiadásának díját. Ez a vonatkozó ajánlásokban foglaltakat messze meghaladó összeg volt és a piaci árnak is többszörösét tette ki, amely a Hatóság álláspontja szerint az érintett információs önrendelkezési jogát súlyosan korlátozta, illetve annak gyakorlását anyagi okból lehetetlenné tette.

A GDPR alkalmazásától kezdve az egészségügyi szolgáltatók számára is kötelező szabály a hozzáférés jogának keretében az első másolat költségtérítés nélküli biztosítása.

A Hatóság ennek okán a vizsgált ügyben az adatkezelőt felszólította, hogy az uniós jog elsőbbsége alapján ingyenesen biztosítsa az érintettnek a dokumentáció első másolatát, és az Állami Egészségügyi Ellátó Központ vezetőjének figyelmét is felhívta, hogy az ÁEEK által fenntartott intézményekben az ismertetett gyakorlatot kövessék. Az adatkezelő a felszólításra adott válaszában arról adott tájékoztatást, hogy a másolat korábban elkért költségét az érintettnek visszafizették. (2018//262/V)

II.1.3.2. Igazságügyi szakértő vizsgálata során az érintett által megadott adatok másolata

A bírósági vagy hatósági eljárásban kirendelt igazságügyi szakértők a szakvélemény elkészítésekor az érintettektől különböző személyes adatokat rögzítenek, teszteket töltetnek ki, kérdésekre adott válaszokat jegyeznek le, rajzot készíttet-

nek a vizsgált személlyel stb. Ezek az adatok az érintett személyes adatainak minősülnek, amelyeket az érintett a vizsgálat során maga ad meg.

Ettől elkülönülnek azok az adatok és következtetések, amelyeket a szakértő állapít meg a vizsgálatok során felvett adatokból, ezek – bírósági ítélet alapján is – szakértői adatnak minősülnek, és a szakértő szakmai szempontok alapján maga ítéli meg, hogy ezen következtetéseket a szakvéleményben milyen formában szerepelteti.

A GDPR alkalmazását megelőző időszakban több vizsgálatban felmerült probléma volt az, hogy az érintett kérésére a szakértők a vizsgálatok során az érintettektől felvett személyes adatokat (pl. a kitöltött tesztek másolatát) az érintettek kérelmére nem adták át arra hivatkozva, hogy a másolatadási kötelezettséget az Infotv. nem írta elő.

A Hatóság eljárásaiban rendszeresen felmerülő, jogértelmezést igénylő kérdés volt az, hogy az Infotv. 2018. júliusáig hatályos 15. § (1) bekezdése alapján adott tájékoztatás nem írta elő az adatkezelő részére a kezelt személyes adatokat tartalmazó adathordozóról készített másolatnak az érintett részére történő átadására irányuló kötelezettséget. Ebből kifolyólag az adatkezelők rendre arra hivatkoztak, hogy a tájékoztatást a személyes adatok kezeléséről megadják, de mivel az Infotv. nem tartalmazott erre vonatkozó kötelezést, nem biztosították az adott – személyes adatot tartalmazó vagy annak minősülő – irat másolatban történő kiadását vagy az abba való betekintést. A Kúria Pfv. IV. 20.971/2013/5. számú döntése is ezt az érvelést erősítette meg.

A Hatóság álláspontja az volt, hogy az információs önrendelkezési jog lényegét tekintve az érintett a rá vonatkozó, sőt általa megadott adatok megismerése elől a jogszabályokban rögzített kivételektől eltekintve nem lehet elzárva, és arra ösztönözte az adatkezelőket is, hogy a tájékoztatás fogalmát kiterjesztően értelmezzék, és kérelemre azt másolatadás formájában teljesítsék, azonban kétségtelen, hogy jelen ügyben az adatkiadást nem rendelte el jogszabály, illetőleg ezzel ellentétes bírói gyakorlat született.

A GDPR az Infotv. az adatvédelmi reformot megelőzően alkalmazandó 15. §-ában foglalt tájékoztatással érdemét és funkcióját tekintve azonos jogintézményként szabályozza érintett hozzáférési jogát. Ezen jogot taglaló 15. cikkében a tájékoztatás mellett kifejezetten előírja a másolat-adás követelményét (15. cikk (3) bekezdés).

A GDPR 23. cikk (1) bekezdés i) pontja lehetőséget biztosít a tagállamoknak, hogy jogalkotás útján korlátozást vezessenek be a jogérvényesítésre vonatkozó szakaszok alkalmazása tekintetében az érintett vagy mások jogainak védelme érdekében[9].

Ezen korlátot jelenti az igazságügyi szakértőkről szóló 2016. évi XXIX. törvény (Szaktv.) 42. § (5) bekezdése, mely szerint *„a szakértő az információs önrendelkezési jogról és az információszabadságról szóló törvény szerint az érintettet megillető, a szakértő által kezelt adatokra vonatkozó tájékoztatás kiadását megtagadja a kirendelő vagy megbízó bűncselekmények megelőzése vagy üldözése, továbbá az érintett vagy mások jogainak védelmének érdekében tett utasítására”*. A tájékoztatás (hatályosan hozzáférés) korlátozását tehát a kirendelő, illetve megbízó bíróság vagy a hatóság rendelheti el.

Azon adatok, melyeket az érintett a vizsgálat során maga adott meg (kitöltött teszt, kérdőív, vizsgálati jegyzőkönyv adatai, stb.) – tehát nem a szakértő által levont szakmai következtetések nyomán létrejött adatok – egyértelműen az érintett személyes adatának minősülnek[10], és jellemzően ezek az adatok azok, amelyeket az érintettek az iratmegismerési kérelmek során igényelnek.

A GDPR-ral alkalmazandóvá vált megváltozott szabályrendszer a Hatóság álláspontja szerint a szakértők adatkezelését annyiban érinti, hogy amennyiben az érintett a szakértő által kezelt, a vizsgálat során saját maga által megadott adatok másolatát kéri, a másolatadást a szakértőnek biztosítania kell, és azt csak indokolt esetben, a kirendelő hatóság, bíróság utasítására tagadhatja meg, ahogyan azt a Szaktv. 42. § (5) bekezdése előírja.

---

9 GDPR 23. cikk (1) Az adatkezelőre vagy adatfeldolgozóra alkalmazandó uniós vagy tagállami jog jogalkotási intézkedésekkel korlátozhatja a 12-22. cikkben és a 34. cikkben foglalt, valamint a 12–22. cikkben meghatározott jogokkal és kötelezettségekkel összhangban lévő rendelkezései tekintetében az 5. cikkben foglalt jogok és kötelezettségek hatályát, ha a korlátozás tiszteletben tartja az alapvető jogok és szabadságok lényeges tartalmát, valamint az alábbiak védelméhez szükséges és arányos intézkedés egy demokratikus társadalomban: i) az érintett védelme vagy mások jogainak és szabadságainak védelme.

10 GDPR 4. cikk 1. „személyes adat”: azonosított vagy azonosítható természetes személyre („érintett”) vonatkozó bármely információ; azonosítható az a természetes személy, aki közvetlen vagy közvetett módon, különösen valamely azonosító, például név, szám, helymeghatározó adat, online azonosító vagy a természetes személy testi, fiziológiai, genetikai, szellemi, gazdasági, kulturális vagy szociális azonosságára vonatkozó egy vagy több tényező alapján azonosítható;

További fontos körülmény, hogy az érintett hozzáférési joga nem vonatkozik automatikusan harmadik személyek vizsgálati anyagának megismerésére, tipikusan a gyermek vizsgálati anyagának megismerésére a szülő által.

A pszichológiai vizsgálat során felvett adatok átadása azt jelentené, hogy a pszichológus olyan személynek adja át a gyermek biztonságát, pszichés integritását érintő adatokat, akinek se kompetenciája, se tapasztalata nincs, hogy felmérje az így előálló, a gyermeket további negatív hatásokkal károsító körülményeket. A vizsgálati adatoknak a szakvélemény elkészítéséhez történő felhasználásakor a szakértő ügyel arra is, hogy például a gyermek explorációjából csak a kirendelés szempontjából lényeges azon elemek kerüljenek, melyek nem váltják ki az ellenérdekű szülő esetleges retorzióját a gyermekkel szemben.

A szakmai indokok megalapozottságát a Hatóság is osztja, álláspontja szerint a szakértő kompetenciája eldönteni, hogy a vizsgálat tapasztalatai alapján kezdeményezi-e a törvényes képviselő tájékoztatásának megtagadását a gyermektől felvett adatok vonatkozásában, ahogyan erre a Szaktv. 42. § (5) bekezdése lehetőséget biztosít a GDPR 15. cikk (4) bekezdése alapján[11].

A szakértőknek tehát át kell alakítani a gyakorlatukat a tekintetben, hogy az adatkezelésről történő tájékoztatás helyett az érintettet a saját adatai vonatkozásában hozzáférési és ennek keretében másolatkérési jog illeti meg, tehát az érintett által megadott adatok másolatát az érintettnek át kell adniuk. A Hatóság a szakértői kamara elnökének figyelmét felhívta, hogy a szakértők a jövőben a fentieknek megfelelően alakítsák a gyakorlatot. (NAIH/2018/426/V)

II.1.3.3. Szülők jogai, szülői felügyeleti jog

Az utóbbi időben megszaporodtak a Hatósághoz érkezett azon panaszok, amelyekben a beadványozók iskolától, pedagógiai szakszolgálattól, bölcsődétől, egészségügyi intézménytől kértek kiskorú gyermek adatairól való tájékoztatást, és azt az intézmények megtagadták. Minden esetben kiderült, hogy az adatkérő személy szülői felügyeletet nem gyakorló szülő volt.

A Ptk. szerint különélő szülők esetében főszabály a szülői felügyelet közös gyakorlása. Azonban ha a szülők megállapodása vagy bíróság döntése alapján az egyik szülő gyakorolja a szülői felügyeleti jogot – és ennek részjogosítványaként

11 GDPR 15. cikk (4) bekezdés: A (3) bekezdésben említett, másolat igénylésére vonatkozó jog nem érintheti hátrányosan mások jogait és szabadságait.

a törvényes képviseletet – a másik szülőnek csak a Ptk.-ban felsorolt ún. lényeges kérdésekben van döntési joga.

Noha különélő szülők esetében a Ptk. előírja egymás tájékoztatását (Ptk. 4:174. §), ez azonban a sokszor elmérgesedett viszony miatt a gyakorlatban nem valósul meg. Így a másik szülő közvetlenül az intézménytől, egészségügyi szolgáltatótól stb. kér tájékoztatást, mert a különélő szülő a felügyeletet gyakorló szülő együttműködésének hiányában nem rendelkezik elegendő információval a gyermekről.

A személyes adatok védelme, mint személyiségi jog az érintett által gyakorolható, így a GDPR szerinti, az adatokhoz való hozzáférés jogát az érintett – tehát nagykorú cselekvőképes személy esetén maga, vagy kiskorú esetén a törvényes képviselője (Ptk. 2:14. §) – gyakorolhatja. A gyermek adatainak kezelésére vonatkozó tájékoztatási/hozzáférési kérelmeket tehát törvényes képviselőként a szülői felügyeletet gyakorló szülő nyújthatja be.

Egyes jogszabályok (a nemzeti köznevelésről szóló 2011. évi CXC. törvény (Knt.), a gyermekek védelméről és a gyámügyi igazgatásról szóló 1997. évi XXXI. törvény (Gyvt.)) a tájékoztatás címzettjeként a szülőt jelölik meg, nem rögzítik azonban, hogy azalatt a szülői felügyelet gyakorlóját kell érteni, vagy sem, illetve értelmezhető úgy, hogy ezáltal önálló, *sui generis* szülői tájékoztatásról van szó.

A Ptk. alapján a *„lényeges kérdésekben”* – így az iskola, életpálya megválasztása kérdésében – szülői felügyeletet gyakorol a másik szülő is (Ptk. 4:175. §), amely jog tartalma a fent kifejtettek szerint törvényes képviseletre, ezáltal az adatokhoz való hozzáférés gyakorlására is kiterjed. Ugyanis információ hiányában a különélő szülő a gyermek iskolájának, életpályájának megválasztásához szükséges közös döntést igénylő kérdésekben nem tud megalapozottan állást foglalni. E körben a Hatóság értelmezése szerint a szülői felügyeleti jogot egyébként nem gyakorló szülőnek a kezelt adatok tekintetében adandó tájékoztatás az iskola/életpálya megválasztása szempontjából releváns információkra terjed ki, és ő arra a Ptk. szabályozása alapján – törvényes képviseleti joggal eljárva – közvetlenül jogosult.

A Knt. mindemellett önálló szülői jogosítványként előírja *„a gyermek fejlődéséről, magaviseletéről, tanulmányi előmeneteléről”* való tájékoztatási kötelezettséget. A Gyvt. pedig a szülőnek biztosít az intézménynél (pl. bölcsőde) kezelt iratokba való betekintési és másolatkérési jogot (136/A. §).

Összefoglalva: a szülő és a törvényes képviselő fogalma különélő, és a szülői felügyeletet egyedül gyakorló szülők esetében nem fedi egymást, és míg az adatokról való tájékoztatásra/hozzáférésre, másolat formájában történő adatkérésre a GDPR és a Ptk. alapján a törvényes képviselő jogosult, addig adott esetben ugyanannak az adattartalomnak a megismerésére, iratmásolat formájában történő kérésére a Gyvt. a „*szülőt*" jogosítja fel – így a szülői felügyeletet nem gyakorló, tehát törvényes képviselőként el nem járó szülőt is. A Knt. sem rögzíti egyértelműen a tájékoztatás jogosultját és terjedelmét.

Ezen jogszabályok nem egyértelmű megfogalmazása miatt az adatkezelők gyakorlata sem egységes abban, hogy a jogszabályok szerinti tájékoztatás megilleti-e a szülői felügyeletet nem gyakorló szülőt, és ha igen, milyen terjedelemben, illetve az érintettek – a különélő, és felügyeletet nem gyakorló szülők – hivatkoznak az adatkezelők előtt is a törvényben megfogalmazott önálló tájékoztatási, irat-megismerési jogukra.

Az adatvédelmi szabályok szerint jogellenes adattovábbítást követ el, és az ezért fennálló felelősséggel tartozik az az adatkezelő, aki kérelemre nem az „érintett" – az adatalany, vagy kiskorú esetében a törvényes képviselő – részére szolgáltat adatot. Az adatkezelő nem mérlegelheti, hogy ha a felügyeletet gyakorló szülő a különélő szülő felé nem teljesíti a Ptk. szerinti tájékoztatási kötelezettségét, akkor ő kiadja az adatot. Az adatkezelők *„biztos, ami biztos"* alapon a jogosulatlan adattovábbítást elkerülve minél kevesebb információt adnak. Ugyanakkor a külön jogszabályokban előírt tájékoztatás nem teljesítése az adott intézmény részéről szintén jogsértő.

A gyermekre vonatkozó egészségügyi adatot a szülői felügyeletet nem gyakorló szülő jogszabály alapján nem kérhet. Az Eütv. 24. §-a biztosítja az egészségügyi adatokról történő tájékoztatás kérésének jogát, mivel azonban a gyermek sorsát érintő lényeges kérdések között nem szerepel a gyermek egészségi állapotára vonatkozó kérdés, így a szülői felügyeletet nem gyakorló szülő ebben a körben nem jogosult az adatokról való tájékoztatási/hozzáférési kérelmet benyújtani.

Például a gyermek háziorvosától nem kaphat közvetlen adatszolgáltatást arra vonatkozóan, hogy a gyermek milyen betegségekben szenvedett, milyen gyógyszerezést kapott, – amennyiben a másik szülő a gyermek háziorvosát nem nevezi meg, az egészségügyi közigazgatási szervtől azt az információt sem kaphatja meg, hogy ki a gyermek orvosa –, vagy példának okáért nem kaphat közvetlen tájékoztatást arról sem, hogy a gyermek milyen egészségügyi okból hiányzik

az óvodából/iskolából. Ez utóbbi adattartalom kiadását a Knt. az oktatási intézménynek sem rendeli el.

Azon adatkörben tehát nem jogosult a szülői felügyeletet nem gyakorló szülő informálódni a gyermekéről, amely esetekben döntési joggal nem rendelkezik, jognyilatkozatot nem tehet. Bár a döntési joga csak a lényeges kérdésekre korlátozódik, a Hatóság szerint vizsgálandó az, hogy van-e joga a különélő, szülői felügyeletet nem gyakorló szülőnek a gyermekről közvetlenül az intézményektől tájékoztatást kérni, pusztán információ-szerzési céllal. Tehát formailag nem jogosult a gyermek adatának kezeléséről tájékoztatást kapni a GDPR alapján – mert arra törvényes képviseleti minőségének hiányában sok esetben nem jogosult –, de mint szülő a saját jogán tájékoztatást kaphat a gyermekéről.

Mindezek figyelembevételével a Hatóság felkérte az alapvető jogok biztosát arra, hogy vizsgálja meg, megfelelő-e a különélő, szülői felügyeletet nem gyakorló szülők tájékoztatásának jogszabályi háttere és gyakorlata, illetve indokolt-e és biztosítható-e külön jogszabályban önálló szülői jogosítványként a szülő tájékoztatása, függetlenül a GDPR 15. cikkében foglalt, gyermek adatához való hozzáférési jogtól. (NAIH/2018/3844/V)

II.1.3.4. Honlapok adatkezelése

A NAIH 2018. évi gyakorlatában számos alkalommal felmerült a honlapok adatkezelésének kérdésköre. Az általános adatvédelmi rendelet 2. cikke alapján az általános adatvédelmi rendelet tárgyi hatálya az ott felsoroltakon kívül minden személyes adat kezelésére kiterjed függetlenül attól, hogy a honlap üzemeltetője nagyvállalat, kkv vagy magánszemély. Amennyiben egy honlap érintettek személyes adatát kezeli, akkor alkalmazni kell rá az általános adatvédelmi rendelet szabályait, többek között az általános adatvédelmi rendelet 13. és 14. cikk szerinti tájékoztatási kötelezettségre és az általános adatvédelmi rendelet 30. cikk (1) bekezdése szerinti nyilvántartások vezetésének kötelezettségére vonatkozó szabályokat is.

Az általános adatvédelmi rendelet 4. cikk 1. alpontja szerint személyes adat bármely olyan információ, amely akár közvetve akár közvetetten egy adott természetes személyhez köthető. Ebbe az úgynevezett „pszeudonim" vagy álnevesített személyes adatok is beletartoznak, mint a becenév vagy az e-mail cím akkor is, ha nem tartalmazza a természetes személy valódi nevét. A vissza nem fejthető hash-ek adott esetben lehet, hogy nem személyes adatok, de ezt csak az eset és az adatkezelés technikai megvalósításának összes körülménye alap-

ján lehet megállapítani, hogy bárki által összeköthetőek-e egy természetes személlyel. Az adatkezelés az általános adatvédelmi rendelet 5. cikke alapján nem terjedhet ki az adott adatkezelési cél elérésére alkalmatlan, ahhoz nem feltétlenül szükséges, aránytalanul sok személyes adatra, és csak a célhoz feltétlenül szükséges ideig tarthat.

Az olyan sütik, szerver naplók (pl. IP címek naplózása), vagy egyéb személyes adatok kezelését, amelyek az adott honlap alapvető működéséhez és az informatikai rendszer biztonságához szükségesek, általában az általános adatvédelmi rendelet 6. cikk (1) bekezdés f) pontja szerinti jogos érdekre célszerű alapozni, mivel ha a honlap alapvető működéséhez és az informatikai rendszer biztonságához szükséges az adatkezelés, akkor enélkül a honlap objektíven nem lehet elérhető, ezért nem lehet érvényes hozzájárulás tárgya.

Az általános adatvédelmi rendelet 6. cikk (1) bekezdésének f) pontjára történő hivatkozás esetén fontos annak előzetes dokumentálása, hogy az adott konkrét jogos érdek(ek) érvényesítése előnyt élvez az adott helyzetben a honlapot használó érintettek személyes adataihoz fűződő rendelkezési jogához képest, és milyen technikai, szervezeti, eljárási intézkedések biztosítják azt, hogy az érintettek személyes adatai biztonságban legyenek (érdekmérlegelési teszt).

Az olyan sütik, szerver naplók, vagy egyéb személyes adatok kezelésére, amelyek az adott honlap alapvető működéséhez és az informatikai rendszer biztonságához nem szükségesek (pl. csak statisztikai, kényelmi, marketing, stb. célokat szolgálnak) általában az általános adatvédelmi rendelet 6. cikk (1) bekezdés a) pontja szerinti hozzájárulás szolgálhat jogalapként.

Az általános adatvédelmi rendeletnek megfelelő hozzájárulás alapvető feltételeit a 29-es Munkacsoport WP259 számú iránymutatása részletezi. Eszerint minimum követelmény, hogy a hozzájárulás megfelelő tájékoztatáson alapuló, önkéntes (negatív következmény nélkül megtagadható vagy visszavonható), egyértelműen kifejezett, és konkrét legyen, és az adott érintett általi hozzájárulás megtörténtét az adatkezelő az általános adatvédelmi rendelet 5. cikk (2) bekezdése alapján bármikor igazolni tudja. Az egyértelműen kifejezettség feltételét nem teljesíti a hozzájárulás, ha azt „előre kitöltött jelölőnégyzetes” módszerrel gyűjtik, a passzív magatartás nem minősül megfelelőnek. A konkrétság feltételét nem teljesíti a hozzájárulás, ha az egyes egymástól független adatkezelési célokhoz, illetve egyes egymástól független, különböző adatkezelők által végzett adatkezelésekhez nem lehet külön is hozzájárulni, kizárólag mindenhez egy „csomagban”.

A honlapok adatkezelésével és a közvetlen üzletszerzéssel kapcsolatos speciális szabályokat a jelenleg még csak tagállami egyeztetés alatt lévő új, elektronikus hírközlési adatvédelmi rendelet (ePrivacy Rendelet) fogja tartalmazni, amely – a jogalkotói szándék szerint – a jelenleg hatályos 2002/58/EK elektronikus hírközlési adatvédelmi irányelvet váltja majd fel.

II.1.4. Egyes fontos ügyek

II.1.4.1. A Magyarországi Szcientológia Egyház és a Szcientológia Egyház XVIII. Misszió adatkezelése

1. Előzmények

A Magyarországi Szcientológia Egyház adatkezelését mind az adatvédelmi biztos, mind a Hatóság is több alkalommal vizsgálta. A Hatóság legutóbbi vizsgálata 2017 októberében zárult le, ebben a Magyarországi Szcientológia Egyház mellett, annak legmagasabb szintű hazai szervezetének, a Szcientológia Egyház Központi Szervezetének adatkezelési gyakorlatát vizsgálta meg a Hatóság. Ebben az eljárásban értékelte a munkavállalók adatainak kezelését, az Egyházba történő belépés során alkalmazott egyes formanyomtatványokat az azokon gyűjtött adatok köre és az általuk nyújtott tájékoztatás tekintetében, valamint a Szcientológia Egyház Központi Szervezet által nyújtott szolgáltatások során megvalósuló adatkezelések jogszabályoknak való megfelelését. A Hatóság határozatában több jogsértés megállapítása és a jogsértő adatkezelési gyakorlat megtiltása mellett maximális összegű, 20-20 millió forintos adatvédelmi bírsággal sújtotta mindkét szervezetet. A határozat bírósági felülvizsgálata jelenleg is folyamatban van.

A Hatóság annak érdekében, hogy a Magyarországi Szcientológia Egyház helyi szervezeteinek, úgynevezett misszióinak adatkezelési gyakorlatát is megismerje és értékelje, a fenti eljárással párhuzamosan hivatalból adatvédelmi hatósági eljárást indított a Szcientológia Egyház XVIII. Misszió (a továbbiakban: Misszió), azaz a Szcientológia Egyház nyíregyházi missziójának vizsgálatára. Ebben az ügyben a határozathozatalra 2018-ban került sor.

Ezen adatkezelések tekintetében a GDPR alkalmazandóvá válását megelőzően hatályos magyar jogi rendelkezések – így elsősorban az Infotv. korábbi rendelkezései – érvényesülését vizsgálta a Hatóság.

2. Az eljárás bemutatása

A Hatóság a tényállás tisztázása érdekében – előzetes értesítés mellőzésével – helyszíni szemlét tartott. A Hatóság a helyszíni szemle során lefoglalta a Misszió minden olyan iratát és elektronikus adathordozóját, amelyen személyes és különleges személyes adatok találhatóak. A Hatóság az eljárás során ügyfélként vonta be az eljárásba a Magyarországi Szcientológia Egyházat is (a két vizsgált adatkezelő a továbbiakban: Egyház).

Tekintettel arra, hogy a megalapozott döntéshez a Hatóságnak meg kellett ismernie a Misszió elektronikus úton kezelt nyilvántartásait, így számítástechnikai és informatikai igazságügyi szakértő vizsgálatát rendelte el. A Hatóság szükségesnek tartotta az adatkezelők által végzett speciális adatkezelési műveletek kihatásának vizsgálatát az érintettek döntésére, így pl. az adatok kezelésének jogalapjaként megjelölt hozzájárulás önkéntességére, ezért ennek tanulmányozására a Hatóság klinikai pszichológiai igazságügyi szakértő vizsgálatát is elrendelte.

3. Dossziék típusai

A vizsgált adatkezelés – tekintve hogy a Szcientológia Egyház teljes működése a Nemzetközi Szcientológia Egyház által szigorúan kontrollált, egységes elvek és gyakorlatok alapján működik – jórészt különböző, az előző eljárásban is megismert papír alapú dossziékban testesült meg. Ezek egy része az általuk nyújtott szolgáltatásokhoz, másik részük a Misszióban dolgozók foglalkoztatásához kapcsolódik.

Az Egyház által nyújtott különböző szolgáltatások célja, hogy elősegítse a hívő, avagy preclear útját a szellemi szabadság felé. Ezekhez a szolgáltatásokhoz kapcsolódóan rendkívül nagy mennyiségű személyes és különleges adat kezelése történik, ugyanis különböző dossziékat nyitnak a hívőknek. Ezekben a dossziékban sok esetben nem csak a hívők adatainak kezelését tapasztalta a Hatóság, hanem tipikusnak mondható harmadik személyek személyes adatainak a kezelése is.

A dossziék – a Szcientológia Egyház által lefektetett szabályoknak megfelelően – rendszerezve tartalmazzák a különböző formanyomtatványokat, jelentéseket, feljegyzéseket. Ilyen dosszié az úgynevezett PC dosszié, mely az Egyház legfőbb szolgáltatásai – az auditálás és a méregtelenítés – során keletkező feljegyzéseket, jegyzőkönyveket, jelentéseket tartalmazzák, az Etikai dosszié, melyben az Egyház által elvártaknak etikailag meg nem felelő cselekményekről gyűjtenek jelentéseket, valamint az Egyház saját belső igazságszolgáltatásának

iratai találhatóak bennük, a Levelezési dosszié, mely a hívőkkel való kapcsolattartás, levelezések leiratait tartalmazza, valamint a Munkatársi dosszié, melyben a munkatársi megállapodások, kvalifikációhoz szükséges nyomtatványok, interjúk, tesztek vannak összegyűjtve.

4. Adatkezelések azonosítása

A nyíregyházi misszió által folytatott adatkezelési folyamat három adatkezelési célhoz kötődik:

I. A hívőknek nyújtott szolgáltatásokhoz, a szellemi fejlődésük nyomon követéséhez kötődő adatkezelési cél → elsősorban a PC és Etikai dossziékhoz kötődik;
II. A munkatársak, munkavállalók jelentkezésével, alkalmasságának megállapításával, összefüggő adatkezelési cél → a Munkatársi dossziékban jelenik meg;
III. Direkt marketing cél → Levelező dosszié.

5. Auditálás és méregtelenítés

A PC dossziéban találhatóak az Egyház legfőbb szolgáltatásai, az auditálás és a méregtelenítés során keletkező feljegyzések, jegyzőkönyvek, munkalapok, jelentések, melyek nagy mennyiségben tartalmazzák a hívők és harmadik személyek személyes és különleges adatait.

Az auditálás egy meghatározott menetrend alapján folytatott eljárás, melyen az auditor (az egyház lelkésze) és a páciense (a hívő, vagy preclear) vesznek részt, az auditor kérdéseket intéz az egyénhez, aki arra választ ad, melyet az auditor nyugtáz és feljegyez. Az auditálást az E-méter nevű szerkezet segíti.

A hívők az auditálási ülések alkalmával rendkívül sok személyes, gyakran különösen érzékeny adatot is megosztanak az auditorral, melynek során sok esetben harmadik személyekkel kapcsolatos adatokat, harmadik személyek személyes és különleges adatait is rögzítik a munkalapon.

A PC aktákban helyeznek el több olyan dokumentumot is, melyek szintén kényes adatokat szolgáltatnak a PC-ről, így korábbi betegségeiről, operációiról, testi, lelki állapotáról, családi állapotáról, családtagjai személyes adatairól, stb.

A „méregtelenítés” szintén egy jellemző szolgáltatása az Egyháznak. A méregtelenítő program megkezdését megelőzi egy orvosi alkalmassági vizsgálat, és

ahhoz kapcsolódóan egy – az Egyház által tárolt – alkalmassági nyomtatvány kitöltése, melyen a hívő személyes és különleges adatai szerepelnek (pl. vérnyomás érték; van-e valamilyen tünete vérszegénységnek, szívbetegségnek, májbetegségnek, cukorbetegségnek, kábítószer fogyasztási szokások, szedett gyógyszerek, korábbi műtétek, stb.)

A Hatóság a PC dossziék esetében – a 2017 októberében kelt határozathoz hasonlóan – megállapította, hogy a szolgáltatások megkezdését megelőzően aláírattatott nyilatkozatokban található tájékoztatóban az Egyház nem nyújt megfelelő tájékoztatást, ugyanis nem jelölik meg egyértelműen az adatkezelő személyét, valamint nagyon szűkszavú ismertetés olvasható az adatkezelés céljáról is. A Hatóság álláspontja szerint azonban egy olyan összetett és rengeteg személyes adatot kezelő adatkezelés esetében, mint amilyen a vizsgált adatkezelés, sokkal pontosabban és követhetőbben kell megjelölni az adatkezelés célját és azt, hogy ahhoz kapcsolódóan milyen adatok kezelésére van szükség, azokat milyen módon veszik igénybe a megjelölt cél elérése érdekében, hiszen csak így tudja eldönteni az érintett, hogy hozzájárul-e az adatkezeléshez. A tájékoztatók nem jelölik meg, hogy mely egyházi személyek, tisztségviselők, munkatársak jogosultak megismerni az adatokat, nem nyújtanak teljes körű tájékoztatást az érintetti jogokról és a nyitva álló jogorvoslati lehetőségekről sem, valamint nem szereznek be külön hozzájárulást az adattovábbításokhoz.

Tekintve hogy, mint minden szolgáltatásuk, így a méregtelenítés is a Szcientológia Egyház szigorú iránymutatásai alapján történik, így a Misszióban folytatott méregtelenítő program esetében is megállapítható volt az első határozathoz hasonlóan az, hogy a felvett egészségügyi adatokat, állapotfelmérést és leleteket csak a vizsgáló orvos, egészségügyi szolgáltató kezelhette volna hozzájárulás alapján, és pusztán az arra vonatkozó információt továbbíthatta volna az orvos az Egyház felé, hogy az érintett megfelel-e vagy sem a programban való részvétel feltételeinek. Azonban a Hatóság álláspontja szerint a nyilatkozat teljes tartalma az érintett részletes egészségügyi állapotfelmérésével és leleteivel vallási szervezetnek nem adható át.

Mindezekből következően a Hatóság megállapította, hogy az Egyház megsértette az Infotv. 20. § (2) bekezdését, míg az elégtelen előzetes tájékoztatás miatt az Infotv. 3. § 7. pontja szerinti hozzájárulásra vonatkozó követelményeket is.

A Hatóság az első eljáráshoz hasonlóan megállapította azt is, hogy az Egyház az auditálás és méregtelenítés során különleges adatokat kezel, melynek jogalapjaként nem alkalmazható az Infotv. 5. § (2) bekezdés a) pontja, továbbá az

Infotv. 5. § (2) bekezdés c) pontja szerinti jogalap sem állapítható meg az Egyház adatkezelése során, figyelemmel arra, hogy az adatkezelés célját vallási szolgáltatásként jelölte meg az Egyház, és ez a cél nem illeszthető bele sem az Eüak. 4. § (1) bekezdésébe – amely az egészségügyi ellátó-hálózaton belüli adatkezelésre vonatkozik –, sem az Eüak. 4. § (2) bekezdésébe megjelölt egyéb célok közé. Az Eüak. 4. § (3) bekezdésében alapított hozzájárulás mint jogalap pedig a fent írtak miatt szintén nem támasztható alá.

A Hatóság kiemelkedő súlyú jogsértésként értékelte a harmadik személyek adatainak jogalap nélküli kezelését. Az Infotv. fogalom-meghatározásának figyelembevételével harmadik személynek, illetve harmadik személyre vonatkozó személyes adatnak minősül a dossziékban található dokumentumokban szereplő mindazon adat, amely a PC-n kívül bármely más személyre vonatkozik. Így ebbe a körbe tartozik például a PC hozzátartozóira, barátaira, ismerőseire, párkapcsolataira vonatkozó valamennyi adat. Több esetben előfordult, hogy a nyíregyházi missziótól lefoglalt dokumentumokban harmadik személyek különleges adatát azonosította a Hatóság, annak ellenére, hogy azok kezelésére a vizsgált adatkezelők nem rendelkeztek felhatalmazással az érintettektől.

Az Egyház azzal, hogy harmadik személyek személyes adatait kezeli, megsértette az Infotv. 4. § (1) bekezdés szerinti célhoz kötött adatkezelés elvét. A Hatóság álláspontja szerint a PC dossziékban tárolt dokumentumok kezelése során harmadik személyek személyes adatait az Egyház meghatározott cél, valamint megfelelő előzetes tájékoztatás nélkül kezeli.

Ha pedig az adatkezelésnek nincs jogszerű célja, úgy az a fentiek szerint jogellenesnek minősül. Ugyanakkor nem lehet figyelmen kívül hagyni, hogy ezen harmadik személyeknek az Egyház nemcsak, hogy nem nyújt tájékoztatást az adatkezelési körülményekről, hanem úgy kezeli ezen személyek személyes és különleges adatait, hogy ezen személyeknek semmilyen tudomása nincs arról, hogy egyáltalán az Egyház kezeli az adataikat.

Ezzel a tájékoztatás nélküli adatkezeléssel az adatkezelő, az Egyház oldalán olyan „információs erőfölény” alakul ki, mely rendkívüli módon sérti ezen harmadik személyek személyes adatok védelméhez és magánéletük tiszteletben tartásához fűződő jogát, nem tudják érvényesíteni információs önrendelkezési jogukat, mindemellett az adatkezelés tisztességtelennek is minősül. Az előzetes tájékoztatás hiányából fakadóan az önkéntesség és határozottság követelménye sem teljesül. A hozzájárulással kapcsolatban továbbá meg kell jegyezni, hogy az csak az adott érintettre – a PC-re – vonatkoztatva értelmezhető, más személy

helyetti hozzájárulásról nem beszélhetünk, így a PC hozzájárulása nem jelenti egyben a harmadik személy hozzájárulását.

Az Egyházzal jogviszonyban, tagi viszonyban nem álló adatalanynak minősülő harmadik személyek adatainak rögzítése, nyilvántartása azért is kifogásolható, mert nincs olyan jogszerű, elfogadható adatkezelési cél, amely ezen személyek adatainak, sok esetben különleges adatainak kezelését feltétlenül szükségessé, vagy akár csak elfogadhatóvá tenné. Bizonyos személyek adatainak rögzítése egy tőlük teljesen független adatkezelési cél, illetve egy rájuk semmilyen szempontból sem vonatkoztatható jogviszony miatt, hozzájárulás alapján nem indokolható és egyáltalán nem szükséges, továbbá indokolatlan beavatkozást jelent ezen érintettek magánszférájába.

Az Egyházzal jogviszonyban, tagi viszonyban nem álló adatalany magánéletének tiszteletben tartásához való joga előnyben részesítendő az Egyház vagy az azt egy eljárás során megosztó PC érdekével szemben. Az Egyház csak azokat a vallási szolgáltatások nyújtásával összefüggő adatokat rögzítheti és kezelheti, melyek tekintetében érvényes jogalappal rendelkezik.

A Hatóság ezért a nyíregyházi misszió esetében is megállapította, hogy a vele jogviszonyban, tagi viszonyban álló PC személyes adatait, különleges adatait nem kapcsolhatja össze a PC által elmondott, a PC környezetében élő más személyek személyes adataival, mivel az ilyen, a Szcientológia egyházzal jogviszonyban, tagi viszonyban nem álló személyek személyes adatainak kezelése a célhoz kötöttség és a szükségesség elvébe ütközik.

Mindemellett pedig azt is kimondta a Hatóság, hogy a Kötelezettek jogalap nélkül is kezelik a harmadik személyek személyes és különleges adatait, hiszen az adatkezelők által megjelölt jogalap, a hozzájárulás egyik fogalmi eleme sem teljesül, nem kapnak megfelelő előzetes tájékoztatást, nem önkéntesen, saját maguk járulnak hozzá személyes adataik kezeléséhez, és ebből következően a további fogalmi elem, a kifejezettség, határozottság sem tud érvényesülni. Mivel egyéb jogalap megléte sem állapítható meg – így a különleges adatok esetében olyan jogszabály, amely közérdeken alapuló célból elrendelné ezen adatok kezelését – az Egyház megsértette az Infotv. 3. § 7. pontját és az 5. § (1)-(2) bekezdését.

Mindezekre tekintettel a Hatóság a Határozat rendelkező részében megtiltotta az egészségügyi adatok kezelését, elrendelte a hívők megfelelő előzetes tájékoztatását, hozzájárulásuk ismételt beszerzését, valamint elrendelte azon hívők személyes adatainak törlését, akik nem erősítették meg hozzájárulásukat, vala-

mint a harmadik személyek személyes adatainak törlését és egyúttal megtiltotta a harmadik személyekre vonatkozó adatgyűjtési gyakorlatot.

A PC dossziékhoz kapcsolódó jogsértésként állapította meg ezen eljárásban is a Hatóság, hogy nem biztosítják az érintettek számára azon jogukat, hogy megismerjék a róluk kezelt személyes és különleges adatokat, ugyanis a hívők nem tekinthetnek bele a róluk készült PC dossziéba. Mivel azonban az érintett információs önrendelkezési jogának része, hogy követhetővé és ellenőrizhetővé kell számára tenni az adatkezelés útját, vagyis joga van tudni, hogy ki, mikor, milyen adatát és mire használja fel az adatkezelő, ezért a Hatóság megállapította, hogy az Egyház megsértette az Infotv. 14. § a) pontjában szabályozott érintetti jogot.

6. Etikai dossziék

A dossziéban találhatóak jelentések a hívőről vagy munkatársról, a személlyel lefolytatott etikai és igazságszolgáltatási eljárások feljegyzéseiről és eredményeiről, valamint különböző dicséretek. Az etikai dossziék legnagyobb részét az úgynevezett tudomásjelentések és más egyéb jelentések teszik ki. A hívők ezekben különböző jelentéseket írnak egymásról, melyekben valamilyen szabálytalanságra hívják fel a figyelmet egy másik hívővel annak életvitelével, munkájával, a Misszióban végzett feladataival, párkapcsolataival kapcsolatban. Ezek a szabálytalanságok a jelentéktelen „bűnöktől" egészen odáig terjedhetnek, hogy a másik személy egészségügyi, pénzügyi, vagy szexuális életéről tesznek jelentést, vagy akár egy hívő által elkövetett bűncselekményről is.

Ebben az aktatípusban szerepelnek az Egyház belső igazságszolgáltatásával kapcsolatos iratok is. Ahogy az több formanyomtatványukban, hívőkkel kitöltendő hozzájárulásban olvasható, a hívők lényegében lemondanak arról, hogy egymás közötti, illetve az Egyházzal szembeni vitájukat polgári bíróság előtt érvényesítsék, az ilyen vitás ügyek csakis a szcientológia vallási hatóságai által oldhatóak meg. Az etikai és egyéb bűnök kivizsgálására és szankcionálására különböző eljárásokat dolgoztak ki. A Hatóság ezen dosszié típus esetében is megállapíthatónak tartotta az előzőekben bemutatott jogsértéseket, vagyis a megfelelő jogalap nélküli adatkezelés mind a hívők, mind a harmadik személyek személyes és különleges adatai tekintetében.

7. Munkatársi dossziék

A Misszióban dolgozók alkalmazását megelőzően a jelentkezőknek többféle jelentkezési lapot, alkalmassági tesztet és kérdőívet kell kitölteniük, melyek rend-

kívül nagy mennyiségű személyes és különleges adatot szolgáltatnak az Egyház számára.

A Hatóság áttekintve az alkalmazáshoz kötődő formanyomtatványon keresztül nyújtott tájékoztatást, a PC dossziékban elmondottakhoz hasonlóan megállapította, hogy a Kötelezettek megsértették az előzetes tájékoztatás követelményét, illetve ebből adódóan, mivel az előzetes tájékoztatás a hozzájárulás egyik feltétele, megsértették az Infotv. 3. § 7. pontja szerinti hozzájárulásra vonatkozó követelményeket is, így megállapítható volt, hogy az Egyház jogalap nélkül kezeli a posztra jelentkezők személyes adatait, megsértve ezzel az Infotv. 5. § (1) bekezdés a) pontját.

8. Levelező dossziék és direkt marketing

A Hatóság ebben a témában a levelező dossziékban továbbá az elektronikus tagnyilvántartásnak tekinthető adatbázisban található személyes adatok kezelésének, valamint a különböző online felületeken – mint az Egyház egyik legfontosabb személyiségértékelő tesztjének, az „Oxfordi képességelemzésnek" az online kitöltésére szolgáló weboldalnak , illetve az online könyvértékesítő felületen – folytatott adatkezelési tevékenységnek a jogszerűségét vizsgálta.

A Hatóság két vonatkozásban találta jogsértőnek az Egyház marketing célú adatkezelését:

- a Kötelezettek nem szereztek be a gazdasági reklámtevékenység alapvető feltételeiről és egyes korlátairól szóló 2008. évi XLVIII. törvény (a továbbiakban: Grt.) 6. § (1)-(2) bekezdésének (illetve az Infotv. 3. § 7. pontjának) megfelelő hozzájárulást az érintettektől, tekintettel arra, hogy valamennyi fenti módon gyűjtött adat esetében ezen hozzájárulás beszerzése a marketing célú adatkezelés jogszerűségéhez mellőzhetetlen, valamint
- tekintettel arra, hogy a Kötelezettek által vezetett elektronikus nyilvántartásból nem állapítható meg az érintettek hozzájárulásának forrása, ezért megállapítható, hogy a Kötelezettek nem tettek eleget a Grt. 6. § (5) bekezdéséből fakadó, a hozzájárulások forrására vonatkozó nyilvántartási kötelezettségüknek.

9. Rendelkező rész és a bírságkiszabás

A Hatóság a fentiek miatt megtiltotta a Kötelezettek további jogellenes adatkezelését és felszólította őket arra, hogy a hatályos jogszabályi rendelkezéseknek

megfelelően alakítsák át előzetes tájékoztatási gyakorlatukat, adjanak megfelelő előzetes tájékoztatást és kérjék az összes érintett adatkezelési hozzájárulását, illetve hozzájárulásának megerősítését. Megerősített hozzájárulás hiányában felszólította a Kötelezetteket az érintett adatainak dokumentált törlésére. Megtiltotta a Hatóság a munkatársnak, munkatársi megbízásra jelentkezőnek és hívőnek nem minősülő harmadik személyek személyes adatainak megfelelő cél és jogalap hiányában történő gyűjtését és elrendelte az így kezelt személyes adatok törlését is. Felszólította továbbá a Kötelezetteket arra, hogy szüntessék meg az érintettek meghatározott személyes adatainak megfelelő jogalap nélküli továbbítását, illetve arra, hogy tegyenek eleget az adatbiztonsági elvárásoknak a személyes adatok külföldre történő továbbítása tekintetében.

A Hatóság mindezeken felül 12-12 millió forint adatvédelmi bírságot szabott ki az adatkezelőkre. A kiszabott bírság összegének megállapításakor figyelembe vette az ügy összes körülményét, így különösen az érintettek számát, a jogsértés súlyát és a jogsértés ismétlődő jellegét.

II.1.4.2. Google-ügyek

1. A NAIH 2018. október 29. napján hivatalból hatósági ellenőrzést indított, tekintettel arra, hogy a rendelkezésre álló adatok nem voltak elegendőek annak megítéléséhez, hogy a https://policies.google.com/privacy?hl=hu&gl=ZZ webcímen elérhető tájékoztatóban megjelölt szolgáltatások nyújtása során a Google LLC az egyetlen adatkezelő a tájékoztatásnak megfelelően, valamint annak eldöntéséhez, hogy a Google Kft. kapcsolódik-e, és ha igen, akkor milyen minőségben kapcsolódik a fenti szolgáltatásokkal kapcsolatos adatkezeléshez.

Az ellenőrzés keretében a NAIH adatszolgáltatásra és nyilatkozattételre hívta fel a Google LLC-t és a Google Kft-t, akik válaszukban mindketten úgy nyilatkoztak, hogy a Google LLC határon átnyúló adatkezelést folytat, amelynek tekintetében Írország az általános adatvédelmi rendelet 4. cikk 16. pontja értelmében vett uniós tevékenységi központja, mivel a Google Ireland Ltd. leányvállalata az uniós központi ügyintézésének helye, ezért az ír adatvédelmi hatóság minősül fő felügyeleti hatóságnak. Előadták továbbá, hogy az ellenőrzés tárgyát képező tájékoztatóval érintett, a Google LLC szolgáltatásával összefüggő személyes adat kezelések tekintetében az adatkezelő a Google LLC, ezzel kapcsolatban a Google Kft. adatkezelési tevékenységet jelenleg nem folytat. A Google LLC arról is beszámolt, hogy előkészületben van egyes adatkezelési tevékenységeinek a Google Ireland Ltd. részére történő átadása, amely azonban a válasz idején még nem valósult meg.

Az ír adatvédelmi hatóság a többi tagállam adatvédelmi hatósága részére több más tagállami panasz, illetve adatvédelmi incidens kapcsán az általános adatvédelmi rendelet 56. cikke szerint eljárni jogosult hatóság tisztázására irányuló egyeztetés során azt nyilatkozta, hogy jelenleg nem tekinthető a Google LLC adatkezelése tekintetében az általános adatvédelmi rendelet 56. cikk (1) bekezdése értelmében vett fő felügyeleti hatóságnak.

A fentiek miatt az eljárni jogosult hatóság tisztázása érdekében a NAIH az általános adatvédelmi rendelet 61. cikk (1) bekezdése szerinti eljárás során megkereste az ír adatvédelmi hatóságot, hogy adjon részletesebb tájékoztatást az álláspontja alátámasztására szolgáló, rendelkezésére álló körülményekről, információkról. Válaszában az ír adatvédelmi hatóság kifejtette, hogy értelmezése szerint a Google LLC jelenleg nem rendelkezik Uniós tevékenységi központtal az Unión belüli adatkezelés hiánya miatt, ezért az egyablakos ügyintézés (one-stop-shop) nem alkalmazható jelenleg. Amennyiben a Google LLC megfelelően átalakítja a működését és adatkezelési folyamatait, akkor 2019. január 22-től lehetséges, hogy az ír adatvédelmi hatóság az általános adatvédelmi rendelet 56. cikk (1) bekezdése értelmében vett fő felügyeleti hatósággá válik.

2. A NAIH-hoz érkezett kérelmében a magyar érintett előadta, hogy az általános adatvédelmi rendelet 15. cikke alapján a Google AdWords üzemeltetőjéhez, a Google Ireland Ltd-hez fordult elektronikus úton, és tájékoztatását kérte a név személyes adata hirdetésekhez kapcsolt keresési kulcsszóként történő kezelésével kapcsolatban a Google keresőben, ugyanakkor a Google Ireland Ltd. ezt az érintetti joggyakorlási kérelmét nem teljesítette.

Az általános adatvédelmi rendelet szabályai szerint a kérelem szerinti adatkezelés határon átnyúló adatkezelés, amely tekintetében a NAIH érintett hatóság, ezért a Google Ireland Ltd. tevékenységi központja szerinti ír adatvédelmi hatóságnak mint az általános adatvédelmi rendelet 56. cikke szerinti fő felügyeleti hatóságnak a megkeresése szükséges annak tisztázására, hogy az ügy az általános adatvédelmi rendelet 56. cikk (2) bekezdése szerint helyi ügyként kezelhető-e, vagy a tevékenységi központ szerinti főhatóság kíván eljárni. Az érintett kérelme a NAIH-hoz 2019. január 22. előtt érkezett, de a döntést az ügyben 2019. január 22. után kell meghozni, így az általános adatvédelmi rendelet erre vonatkozó egyéb részletszabálya hiányában a NAIH megkeresése alapján az ír adatvédelmi hatóság döntheti el, hogy melyik tagállami adatvédelmi hatóság fog eljárni ebben az ügyben.

3. Egy további ügyben a panaszos, egy köztiszteletben álló személy, azt kifogásolta, hogy a Google találati listájában olyan URL-ek szerepelnek, amelyek elhunyt házastársával és családi életével kapcsolatos bántó, kegyeletsértő információkat tartalmaznak. A Google korábban a kérést közérdekre hivatkozva elutasította, de a NAIH felszólításának eleget téve 2018-ban végre sor került a kegyeletsértő cikkekre mutató linkek találati listából való eltávolítására.

Ezzel kapcsolatban mindenképp megjegyzendő, hogy a listából való törlés csupán az elérési utat szünteti meg, azaz a keresőszolgáltatás nem fogja kilistázni az eltávolított URL-eket, de a szóban forgó weboldalakon továbbra is elérhető marad az információ. Amennyiben az érintett az adatok teljes törlését szeretné elérni, az adatkezelőhöz, illetve az adott weboldal üzemeltetőjéhez fordulhat az adatok törlésére irányuló kérelemmel.

4. Az előzőekben említetteken túl a Hatóság 2018-ban több ügyben is közvetlenül megkereste a Google-t. Ezek egy része az általános gyakorlat feltérképezésére irányult, de volt olyan ügy, amelyben a Hatóság a megváltozott jogszabályi környezetre (GDPR, Infotv. 25. §) tekintettel korábbi álláspontjának felülvizsgálatára szólította fel az adatkezelőt. Megkérdeztük, hogy a Google Search milyen alapon rangsorolja a keresési találatokat, hogyan működik a keresési algoritmus, mik a rangsorolási szempontok, valamint melyek a GDPR előírásainak való megfelelés érdekében tett intézkedések a keresőmotor szolgáltatással összefüggésben.

Az alábbi linkek segítenek a tájékozódásban:

- https://transparencyreport.google.com/eu-privacy/overview
- https://policies.google.com/privacy?hl=hu
- https://privacy.google.com/your-data.html.
- https://support.google.com/transparencyreport/answer/7347822/?hl=hu

II.1.4.3. Az ISZT-ügy

A NAIH/2018/3474/H számú, honlapján közzétett (https://www.naih.hu/files/NAIH-2018-3474-H-hatarozat.pdf) határozatában a NAIH megállapította, hogy az ISZT Nonprofit Korlátolt Felelősségű Társaság .hu legfelsőbb domain regisztrációval kapcsolatos adatkezelési gyakorlata a vizsgált 2012 és 2017 közötti időszakban nem felelt meg a hatályos jogszabályoknak. Emiatt figyelmeztetést alkalmazott és eltiltotta a kötelezettet a további jogsértéstől. Az ISZT Nonprofit Korlátolt Felelősségű Társaság vállalta, hogy a határozatnak megfelelően átalakítja a .hu domain regisztrációval kapcsolatos adatkezelési tevékenységét,

és megfelelő tájékoztatást nyújt az érintetteknek, az időközben alkalmazandóvá vált általános adatvédelmi rendelet figyelembevételével. A teljesítés nyomon követése és ellenőrzése folyamatban van a NAIH részéről.

II.2. Az incidens bejelentés és az előzetes hatásvizsgálat

II.2.1. Az adatvédelmi hatásvizsgálat Hatósággal történő előzetes konzultációja

A GDPR 35. cikk (1) bekezdése alapján az adatvédelmi hatásvizsgálatot akkor kell elvégezni, amikor az adatkezelés *„valószínűsíthetően magas kockázattal jár a természetes személyek jogaira és szabadságaira nézve”*. Az adatvédelmi hatásvizsgálat célja az adatkezelés jellegének feltárása, szükségességének és arányosságának vizsgálata, valamint a személyes adatok kezeléséből eredően a természetes személyek jogait és szabadságait érintő kockázatok kezelésének elősegítése e kockázatok értékelésével és a kezelésükre szolgáló intézkedések meghatározásával.

A 29-es Munkacsoport vonatkozó iránymutatása[12] (a továbbiakban: hatásvizsgálati iránymutatás) szerint, ha az adatvédelmi hatásvizsgálat azt jelzi, hogy a kockázat mérséklését célzó garanciák, biztonsági intézkedések és mechanizmusok hiányában az adatkezelés magas kockázattal járna a természetes személyek jogaira és szabadságaira nézve, és az adatkezelő véleménye alapján a kockázat nem mérsékelhető a rendelkezésre álló technológiák és a végrehajtási költségek szempontjából észszerű módon, akkor az adatkezelési tevékenység megkezdése előtt a felügyeleti hatósággal konzultálni kell (lásd: GDPR 36. cikk (1) bekezdés és (94) preambulum-bekezdés).

Az adatvédelmi hatásvizsgálat eredményéről a fentiek alapján tehát előzetesen konzultálni kell a felügyeleti hatósággal, ha az érintettek jogait és szabadságait érintő kockázatok adatkezelő által történt értékelését követően az adatkezelő nem tud megfelelő intézkedéseket hozni a kockázatok elfogadható szintre való csökkentésére, azaz a fennmaradó kockázatok továbbra is jelentősek.

12 Iránymutatás az adatvédelmi hatásvizsgálat elvégzéséhez és annak megállapításához, hogy az adatkezelés az (EU) 2016/679 rendelet alkalmazásában *„valószínűsíthetően magas kockázattal jár”*-e [WP 248 rev.01]

Az elfogadhatatlanul magas fennmaradó kockázatra példa, ha az érintettek olyan jelentős vagy akár visszafordíthatatlan következményekkel szembesülnek, amelyeket nem tudnak leküzdeni (például adatokhoz való jogosulatlan hozzáférés, amely az érintettek életét fenyegető veszélyt, elbocsátást vagy pénzügyi nehézséget eredményez). A Hatóság – mint az Alaptörvény VI. cikk (4) bekezdése és az Infotv. 38. § (2a) bekezdése szerint az általános adatvédelmi rendelet szerinti felügyeleti hatóság, ebből következően az adatvédelmi hatásvizsgálatra vonatkozó előzetes konzultációt a Hatóság végzi el.

A Hatóság az előzetes konzultáció keretében a szervezet által már lefolytatott hatásvizsgálat dokumentációjából azt állapítja meg, hogy az adatvédelmi hatásvizsgálat lefolytatása a GDPR vonatkozó rendelkezései, illetve a hatásvizsgálati iránymutatás előírásai szerint történt-e. Továbbá azt vizsgálja, hogy a fennmaradó kockázatok mérséklésében tud-e segítséget nyújtani.

A GDPR 36. cikkének (3) bekezdése tartalmazza azokat az információkat, amelyeket az adatkezelőnek a konzultáció során ismertetnie kell a Hatósággal. A Hatóság a konzultáció során az adatkezelés tényleges folyamatát vizsgálja, így a benyújtott adatkezelési folyamatok vonatkozásában elsősorban azt nézi, hogy az adatkezelő pontosan azonosítja-e az adatkezelési tevékenységeket, illetve az adatkezelések kockázatait, valamint sikerül-e a kockázatok kezelésére irányuló intézkedéseket meghozni. Továbbá a Hatóság vizsgálja, hogy az adatkezelésben érintett adatok körének vizsgálatánál pontosan szét van-e választva a személyes adatok és a különleges adatok kezelése az adatkezelés folyamatában, az adatkezelések jogszerűek és az adatkezelő lefolytatta-e az érdekmérlegelési tesztet. Az adatvédelmi hatásvizsgálatot többfajta, különböző módszertan segítségével el lehet végezni, de a hatásvizsgálatnál figyelembe veendő szempontok azonosak, hiszen a GDPR meghatározza az adatvédelmi hatásvizsgálat alapvető jellemzőit. Az adatvédelmi hatásvizsgálat alapvető szempontjainak meghatározásával kapcsolatosan a Hatóság kiemeli a hatásvizsgálati iránymutatás 2. mellékletét, amelyben az adatvédelmi hatóságok által közös szempontok kerültek kidolgozásra annak érdekében, hogy lehetővé váljon a választás a különböző adatvédelmi hatásvizsgálati módszertanok alkalmazása során, egyúttal az adatkezelők be tudják tartani a GDPR rendelkezéseit. A Hatóság az előzetes konzultáció során mindig hangsúlyozza, hogy a kockázatelemzés a személyes adatok kezelésével összefüggő folyamatokra, adatkezelési műveletekre vonatkozik, amelyek a hatásvizsgálat lefolytatásának eredményeként az érintett jogait és szabadságait érintő kockázatot jelentenek. Az adatvédelmi hatásvizsgálat lényege az adatkezelés előzetes kontrollja a kockázatok feltárása és a kockázatok mérséklésére teendő intézkedések értékelése révén. A kockázatnak egyértel-

műnek, konkrétnak kell lennie, és ahhoz, hogy az adatkezelő azonosítani tudjon kockázatokat, meg kell előznie egy kockázatelemzési folyamatnak.

Az adatvédelmi hatásvizsgálat alapvetően két nagy részből áll. Egyrészről az adatkezelő értékeli az adatvédelmi alapelveknek történő megfelelést, kvázi egy jogi megfelelőségi elemzést végez. Másrészről azonban az adatkezelőnek értékelnie kell az adatbiztonsági intézkedéseket, azaz egy informatikai biztonsági elemzést is el kell végeznie. Az adatvédelmi hatásvizsgálatban kiemelten az adatbiztonsági intézkedések nyújtanak a legnagyobb mozgásteret a kockázatok csökkentésére. Ennek megfelelően a Hatóság a magasabb szintű megfelelőség érdekében olyan módszertan kiválasztását javasolja, amelyet az adott adatvédelmi hatóság már összhangba hozott a GDPR rendelkezéseivel. Ilyen például a francia adatvédelmi hatóság (CNIL) által a saját honlapján is közzétett módszertan, amely alkalmazását tovább erősíti az a tény, hogy a CNIL közzétett egy nyílt forráskódú szoftvert is, amellyel az adatkezelők könnyen elkészíthetik a módszertannak megfelelő adatvédelmi hatásvizsgálatot. A CNIL szoftvert főleg olyan adatkezelőknek fejlesztették ki, amelyek némileg jártasak a hatásvizsgálat elvégzésében. Az adatkezelők könnyen le tudják tölteni és elindítani a számítógépre az önálló verziót. A szoftvert egy szervezet a szerverére is telepítheti, hogy más eszközökkel és rendszerekkel integrálva együtt tudja használni a cégen belül. A fenti szoftver magyar nyelvű verzióval is rendelkezik és elérhető a Hatóság honlapjáról.

Amennyiben az előzetes konzultáció során a Hatóság véleménye szerint a tervezett adatkezelés megsértené a GDPR-t, különösen, ha az adatkezelő a kockázatot nem elégséges módon azonosította vagy csökkentette, úgy gyakorolhatja a GDPR 58. cikkében említett hatásköreit, így többek között azt megtilthatja (GDPR 36. cikk (2) bekezdése).

II.2.2. Előzetes konzultáció a Hatósággal a jogszabálytervezetek adatvédelmi hatásvizsgálatával összefüggésben

A GDPR 36. cikk (4) bekezdése a felügyeleti hatósággal való előzetes konzultációt kötelezővé teszi a személyes adatok kezeléséhez kapcsolódó, a nemzeti parlament által elfogadandó jogalkotási intézkedésre – vagy ilyen jogalkotási intézkedésen alapuló szabályozási intézkedésre – irányuló javaslat előkészítése során.

Magyarországon a jogszabálytervezetek adatvédelmi hatásvizsgálatára vonatkozó részletes szabályokat a Módtv. hatálybalépését követően az Infotv. tartal-

mazza. Az Infotv. 25/G. § (6) bekezdése mondja ki, hogy kötelező adatkezelés esetén az adatvédelmi hatásvizsgálatot az adatkezelést előíró jogszabály előkészítője folytatja le. Kötelező adatkezelések alatt a törvény a jogszabály előírásain alapuló adatkezeléseket (így a GDPR 6. cikk (1) bekezdés c) és e) pontjában meghatározott adatkezeléseket) érti. A fentiek alapján tehát egy személyes adatok kezelését is érintő, azt előíró jogszabály előkészítése során a jogszabály előkészítőjének adatvédelmi hatásvizsgálatot kell készítenie.

A hatásvizsgálati iránymutatás alapján az adatvédelmi hatásvizsgálat eredményéről akkor kell előzetesen konzultálni a Hatósággal, ha az érintettek jogait és szabadságait érintő kockázatok adatkezelő által történt értékelését követően az adatkezelő nem tud megfelelő intézkedéseket hozni a kockázatok elfogadható szintre való csökkentésére (tehát a fennmaradó kockázatok továbbra is jelentősek).

A Hatóság az ajánlásra tekintettel csak azokban az esetekben tartja szükségesnek az előzetes konzultáció lefolytatását, ha a hatóságvizsgálat megállapítja, hogy a kockázatok továbbra is jelentősek és az adatkezelő nem képes azokat csökkenteni. A Hatóság ezt az előírást a jogalkotás során elkészítendő adatvédelmi hatásvizsgálatokkal kapcsolatban is irányadónak tekinti, amennyiben a tervezett adatkezeléssel kapcsolatban a GDPR alkalmazandó. Amennyiben a jogszabálytervezet előkészítése során az előkészítő által lefolytatott adatvédelmi hatásvizsgálat eredménye alapján megállapítható, hogy a tervezett adatkezelés magas kockázatú és az adatkezelő nem képes azokat csökkenteni, úgy a jogszabály előkészítője konzultációt kezdeményez a Hatósággal. Ez az előírás a GDPR tárgyi hatálya alá tartozó adatkezelésekre irányadó. Így a GDPR hatálya szerinti adatkezelések jogszabályban történő előkészítése esetén csak a fennmaradó, az adatkezelő által nem csökkentett kockázatot jelentő adatkezelések esetén van szükség előzetes konzultációra.

Más a helyzet a GDPR hatálya alá nem tartozó, így kizárólagos magyar joghatóság alá tartozó adatkezelésekkel összefüggésben. Ezekkel kapcsolatban az Infotv. 25/H. § (1) és (2) bekezdésében foglaltak határozzák meg az előzetes konzultáció kezdeményezésének feltételeit. A magas kockázatot és ennek megfelelően az előzetes konzultáció szükségességét a kivett adatkezelések közül a bűnüldözési, nemzetbiztonsági és honvédelmi célú adatkezelések esetén vélelmezni kell a törvény alapján. Ezek szerint valamennyi bűnüldözési, nemzetbiztonsági és honvédelmi célú adatkezelést szabályozó jogszabály előkészítése során hatásvizsgálatot kell készítenie az előkészítőnek és konzultálni is kell a Hatósággal.

Mind a GDPR hatálya, mind a kizárólag magyar joghatóság alá tartozó adatkezelésekkel kapcsolatos jogszabályok előkészítése során fontos, hogy amennyiben előzetes konzultációra kerül sor, úgy azt a Hatóság a jogszabály előkészítőjével (ez legtöbbször az illetékes minisztérium) folytatja le. Amennyiben az előkészítés folyamata már lezárult, és a jogszabálytervezet már benyújtásra került a parlamentnek elfogadásra, vagy azt esetleg már ki is hirdették, úgy a konzultációs eljárás is lezárul, annak tovább folytatására az elfogadást követően nincs lehetőség.

II.2.3. A jogszabály előkészítése során készített adatvédelmi hatásvizsgálat tartalmi kritériumai

A jogszabálytervezet szövegéhez mellékelt adatvédelmi hatásvizsgálati dokumentációval kapcsolatban a törvény csupán annyit ír elő, hogy annak tartalmaznia kell a tervezett adatkezelési műveletek általános leírását, az érintettek alapvető jogainak érvényesülését fenyegető, az adatkezelő által azonosított kockázatok leírását és jellegét, az e kockázatok kezelése céljából tervezett, valamint a személyes adatokhoz fűződő jog érvényesülésének biztosítására irányuló, az adatkezelő által alkalmazott intézkedéseket. A jogszabályok előkészítése során elkészített adatvédelmi hatásvizsgálati dokumentációnak tehát elvileg pontosan ugyanazokat az elemeket kell tartalmaznia, mint az adatkezelők által lefolytatott hatásvizsgálatnak.

A hatásvizsgálati dokumentációnak a jogszabály tervezetében meghatározott, előrelátható, konkrét adatkezeléseket kell leírnia (pl. az adatkezeléshez használt rendszerek működése, használata stb.) valamint azt, hogy az ezzel kapcsolatban kialakult konkrét és beazonosított kockázatokat hogyan kívánja az adatkezelő mérsékelni. Nem elég tehát például, ha a hatásvizsgálatban leírják általánosságban, hogy *„személyiséglopás kockázata fennáll”*, hanem le kell írni pontosan, hogy az adott adatkezelés kapcsán ez hogyan következhet be (pl. jogosulatlan külső támadó hozzáférhet a rendszergazda jelszavához). Az azonosított kockázatok elhárítására tett intézkedéseket is konkrétan le kell írni a hatásvizsgálati dokumentációban (pl. havonta megváltoztatandó, szoftveresen kikényszerített erős jelszavak használata a bejelentkezéseknél).

A konkrét kockázatok beazonosítására természetesen a jogszabály előkészítője saját hatáskörben a legtöbbször nem képes, mivel nincsen minden információ birtokában az adatkezeléssel kapcsolatban. Ennek feloldására a majdani adatkezelővel való konzultációra lehet szükség és adott esetben fel kell kérnie arra, hogy egészítse ki észrevételeivel a hatásvizsgálati dokumentációt.

Természetesen az is előfordulhat, hogy a jogalkotás adott szakaszában még az adatkezelésből eredő konkrét kockázatok nem azonosíthatóak be (pl. a jogszabályszöveg csak egy általános felhatalmazást tartalmaz az adatkezeléssel kapcsolatban). Amennyiben ez a helyzet, úgy erre egyértelműen utalnia kell a jogalkotónak a hatásvizsgálati dokumentációban és a hatásvizsgálat kiegészítésének jövőbeli kötelezettségéről kell döntenie (pl. az adatkezelő megbízásával a teljes értékű hatásvizsgálat lefolytatására a rendszer beüzemelése és a technikai paraméterek kialakítása előtt).

II.2.4. Hatásvizsgálati lista

A GDPR 35. cikkének (4) bekezdése a felügyeleti hatóságok kötelezettségei közzé sorolja azon adatkezelési műveletek listájának összeállítását és nyilvánosságra hozatalát, amelyre nézve az adatkezelőt hatásvizsgálat elvégzésére kötelezi. A Hatóság a lista összeállítását követően azt megküldi az Európai Adatvédelmi Testület részére. A Testület a megküldött listával kapcsolatban a 2018. szeptember 25-26-án tartott ülés szavazási eredményének megfelelően a 10/2018 számú véleményében javasolt módosításokat és kiegészítéseket. A Hatóság a véleményben foglalt javaslatokat elfogadta, és az annak megfelelően módosított lista 2018. október 11. napján az IMI rendszerbe feltöltésre került, illetve a Hatóság a magyar és az angol nyelvű listát a honlapján nyilvánosságra hozta. A lista a közzétételt követően a Technológia Alcsoport 2018. december 19. napján tartott ülésen meghozott döntés szerint módosult, azaz a listán szereplő biometrikus adat a GDPR 4. cikk szerinti fogalmát a 9. cikk szerinti kiegészítéssel kell használni. A kiegészítéssel a GDPR 9. cikk (1) bekezdéssel való összhang valósul meg, valamint az adatkezelőknek is nagyobb bizonyosságot ad afelől, hogy mely adatkezelések esnek a lista hatálya alá.

A lista a következő adatkezelési műveleteket tartalmazza:

1. Ha egy természetes személy egyedi azonosítását célzó biometrikus adatának kezelése módszeres megfigyelésre irányul.
2. Ha kiszolgáltatott helyzetben lévő érintettekkel – különös tekintettel a gyermekekre, munkavállalókra, idős, mentális betegségben szenvedőkre – kapcsolatos egyedi azonosítását célzó biometrikus adat kezelése történik.
3. Ha az adatkezelés egy természetes személy genetikai adatainak egyéb különleges adatokhoz vagy fokozottan személyes jellegű adatokhoz történő hozzákapcsolásával jár.

4. Ha egy természetes személy genetikai adatai kezelésének célja a természetes személy értékelése vagy pontozása.
5. Pontozás. Az adatkezelés célja, hogy az érintett bizonyos tulajdonságait felmérje, és annak eredménye kihatással van az érintett részére nyújtott, illetve nyújtandó szolgáltatás létrejöttére vagy minőségére.
6. Hitelképesség értékelése. Az adatkezelés célja, hogy az érintett hitelképességét felmérje a személyes adatok nagyszámú, illetve módszeres értékelése útján.
7. Fizetőképesség értékelése. Az adatkezelés célja, hogy az érintett fizetőképességét felmérje a személyes adatok nagyszámú, illetve módszeres értékelése útján.
8. Harmadik személytől gyűjtött adatok további felhasználása. Az adatkezelés célja, hogy a harmadik személytől begyűjtött személyes adatokat felhasználják az érintettre vonatkozó szolgáltatás visszautasítására vagy megszüntetésére vonatkozó döntés meghozatalánál.
9. Diákok, hallgatók személyes adatainak értékelésre való felhasználása. Az adatkezelés célja a diákok, hallgatók felkészültségének, teljesítményének, alkalmasságának, illetve mentális állapotának rögzítése, valamint vizsgálata és az adatkezelés nem jogszabályon alapul, függetlenül attól, hogy az oktatás alap-, közép- vagy felsőfokú.
10. Profilozás. Az adatkezelés célja személyes adatok nagy számú, illetve módszeres értékelése révén végzett profilozás, különösen ha az az érintett munkahelyi teljesítményére, gazdasági helyzetére, egészségi állapotára, személyes preferenciáira vagy érdeklődési körére, megbízhatóságra vagy viselkedésre, tartózkodási helyére vagy mozgására vonatkozó jellemzők alapján történik.
11. Csalás elleni fellépés. Az adatkezelés célja hitelreferencia-, pénzmosás és a terrorizmus finanszírozása elleni vagy csalásellenes adatbázis felhasználása ügyfelek szűrésére.
12. Okosmérők. Az adatkezelés célja közműszolgáltatók által telepített „okosmérők” alkalmazása (fogyasztási szokások nyomon követése).
13. Joghatással vagy hasonló jelentős hatással járó automatizált döntéshozatal. Az adatkezelés célja a természetes személy tekintetében joghatással bíró vagy a természetes személyt hasonlóképpen jelentős mértékben érintő döntések meghozatala, amely adatkezelés adott esetben egyének kirekesztését vagy hátrányos megkülönböztetését eredményezheti.
14. Módszeres megfigyelés. Érintettek nagyszámú és módszeres megfigyelése jellemzően közterületeken vagy nyilvános helyeken történő kamerarendszerek, drónok felhasználásával, illetve bármely más új technológia használatával (Wi-Fi tracking, Bluetooth tracking, testkamera).

15. Helymeghatározási adatok kezelése, ha az módszeres megfigyelésre vagy profilalkotásra utal.
16. Munkavállalók munkájának megfigyelése. Az adatkezelés célja a munkavállaló munkájának megfigyelése során a munkavállaló személyes adatainak nagyszámú és módszeres feldolgozása, illetve értékelése. Például GPS megfigyelő autóban történő elhelyezése, kamerás megfigyelés lopás vagy csalás elleni fellépés céljából.
17. Különleges adatok nagy számban való kezelése. A GDPR (91) preambulumbekezdése alapján a személyes adatok kezelése nem tekinthető nagymértékűnek, ha az adatkezelés egy adott szakorvos, egészségügyi szakember betegei vagy egy adott ügyvéd ügyfelei személyes adataira vonatkozik.
18. Nagyszámú személyes adatok kezelése bűnüldözési célból
19. Kiszolgáltatott helyzetben lévő érintettekkel kapcsolatos, nagy számban kezelt adatok eredeti céltól eltérő kezelése: pl. gyermekek, idősek, mentális betegségben szenvedők esetében.
20. Gyermekek személyes adatainak kezelése profilozás, automatikus döntéshozatal, vagy marketing céljából, vagy közvetlenül részükre kínált, információs társadalommal összefüggő szolgáltatások ajánlása vonatkozásában.
21. Új technológiai megoldások használata az adatkezelés során. Ideértve az érzékelővel ellátott eszközök által előállított adatok interneten vagy más csatornán keresztül történő nagyszámú kezelése (pl.: okos televízió, okos háztartási eszközök, okos játékok stb.), és amelyek adatokat szolgáltatnak a természetes személy fizetőképességére, egészségére, személyes érdeklődési körére, megbízhatóságára vagy viselkedésére, tartózkodási helyére és amelyek alapján profilalkotás történik.
22. Egészségügyi adatokra vonatkozó adatkezelések. Nagy számban kezelt adatok tekintetében a kórházak, egészségügyi ellátó intézmények, magán-egészségügyi szolgáltatók vagy nagyszámú páciensi körrel rendelkező természetgyógyászok által kezelt különleges adatok vonatkozásában. Ideértve a nagyobb sportlétesítmények, edzőtermek által a tagoktól felvett egészségügyi adatok kezelése.
23. Amikor több adatkezelő egy egész ágazat által közösen használt alkalmazást, rendszert, eszközt, illetve platformot tervez létrehozni, amelyben különleges adatokat is kezelnek.
24. Az adatkezelés célja a különböző forrásokból származó adatok összevonása, egymással való megfeleltetése vagy összehasonlítása.

A listán szereplő adatkezelések nem jelentik azt, hogy csak ezekben az esetekben kell az adatkezelőnek hatásvizsgálatot lefolytatnia. Ha az adatkezelés a GDPR 35. cikkének (1), illetve (3) bekezdésében található feltételeknek megfelel, úgy az adatkezelő köteles hatásvizsgálatot lefolytatni.

II.2.5. Az adatvédelmi incidensek

Az adatvédelmi incidens a GDPR 4. cikk 12. pontja értelmében a biztonság olyan sérülése, amely a továbbított, tárolt vagy más módon kezelt személyes adatok véletlen vagy jogellenes megsemmisítését, elvesztését (rendelkezésre állás sérülése), megváltoztatását (integritás sérülése), jogosulatlan közlését vagy az azokhoz való jogosulatlan hozzáférést (bizalmas jelleg sérülése) eredményezi.

Az adatvédelmi incidenst az adatkezelő köteles indokolatlan késedelem nélkül, és ha lehetséges, legkésőbb 72 órával azután, hogy az adatvédelmi incidens a tudomására jutott, bejelenteni az illetékes felügyeleti hatóságnak, kivéve, ha az adatvédelmi incidens valószínűsíthetően nem jár kockázattal a természetes személyek jogaira és szabadságaira nézve. Ha a bejelentés nem történik meg 72 órán belül, mellékelni kell hozzá a késedelem igazolására szolgáló indokokat is. Amennyiben az incidens az adatfeldolgozó tevékenységi körén belül valósul meg, az adatfeldolgozó azt az arról való tudomásszerzését követően indokolatlan késedelem nélkül bejelenti az adatkezelőnek.

Ha az adatkezelő már észszerű mértékű bizonyossággal bír az incidens bekövetkeztéről, de még nem rendelkezik minden információval azzal kapcsolatban, érdemes – a 72 órás határidő betartása érdekében – a szakaszos bejelentés lehetőségével élni. Az ilyen jellegű bejelentések az annak pillanatában nem ismert információkkal később kiegészíthetők, helyesbíthetők, módosíthatók.

Az incidens bejelentése történhet a Hatóságnak címzett postai, vagy az ugyfelszolgalat@naih.hu címre küldött elektronikus levélben, melyhez a Hatóság honlapjáról (http://naih.hu/adatvedelmi-incidensbejelent--rendszer.html) letölthető a bejelentő nyomtatvány több formátumban; illetve a Hatóság által erre a célra létrehozott, szintén a Hatóság honlapjáról elérhető bejelentő felületen (https://dbn-online.naih.hu/public/login). Az incidensbejelentő portál célja kizárólag annak elősegítése, hogy az adatkezelők számára az incidensbejelentés folyamatát megkönnyítse, az panaszbenyújtásra nem szolgál.

A Hatóság a bejelentés vizsgálata során kiemelt figyelmet fordít arra, hogy az tartalmazza-e legalább a GDPR 33. cikk (3) bekezdésében foglaltakat:

a) az adatvédelmi incidens jellege, beleértve – ha lehetséges – az érintettek kategóriáit és hozzávetőleges számát, valamint az incidenssel érintett adatok kategóriáit és hozzávetőleges számát;

b) az adatvédelmi tisztviselő vagy a további tájékoztatást nyújtó egyéb kapcsolattartó nevét és elérhetőségeit;
c) az adatvédelmi incidensből eredő, valószínűsíthető következményeket;
d) az adatkezelő által az adatvédelmi incidens orvoslására tett vagy tervezett intézkedéseket, beleértve adott esetben az adatvédelmi incidensből eredő esetleges hátrányos következmények enyhítését célzó intézkedéseket.

Az adatkezelő által vezetett adatvédelmi incidens-nyilvántartás szóban forgó incidensre vonatkozó részének másolata is a bejelentés (illetve adott esetben a tényállás tisztázó végzésre adott válasz) fontos eleme.

A GDPR hatálybalépésétől 2018. december 31. napjáig 244 incidens-bejelentés érkezett a Hatósághoz. Az incidensekkel kapcsolatos kötelezettségek adatkezelő általi teljesítésének vizsgálatát a Hatóság az általános közigazgatási rendtartásról szóló 2016. évi CL. törvény (a továbbiakban: Ákr.) által szabályozott hatósági ellenőrzés keretében végzi. Ha a bejelentés, illetve annak kiegészítései nem tartalmaznak minden szükséges információt, a Hatóság a tényállás tisztázása érdekében felveszi a kapcsolatot az adatkezelővel.

Amennyiben a Hatóság a hatósági ellenőrzés során a GDPR 33-34. cikkében foglalt kötelezettségek betartásával kapcsolatban jogsértést tár fel, hatósági eljárást indít; ellenkező esetben a hatósági ellenőrzést lezárja. Adatvédelmi incidensekkel kapcsolatban a hatósági ellenőrzésben feltárt körülmények alapján hatósági eljárás indítására 2018-ban összesen 7 esetben került sor, bírságkiszabás azonban az eddig lezárt ügyekben nem történt.

Az alábbiakban felsorolásra kerülnek a gyakorlatban tipikusan előforduló incidenstípusok, a Hatóság által az adatkezelőtől jellemzően elvárt kockázatcsökkentő intézkedésekkel együtt.

a) A bejelentések legjelentősebb részét a téves címzés miatti félrepostázások, illetve téves címzett részére küldött elektronikus levelek adták. Az adatkezelőnek ilyenkor mindent meg kell tennie, hogy a téves címzett a birtokába jutott, személyes adatokat tartalmazó dokumentumot, üzenetet megsemmisítse/törölje. Postai küldemény esetén az adatkezelő válaszborítékkal együtt küldött újabb levélben is kérheti a téves címzettet a nem neki szóló küldemény visszaküldésére. Gondoskodnia kell továbbá az adatkezelőnek arról, hogy a tényleges címzett is megkapja az üzenetet, valamint, amennyiben például az érintett személyes

adatok jellege alapján az incidens kockázatát valószínűsíthetően magasnak értékeli, tájékoztatnia kell az incidensről az érintettet. Az ilyen tájékoztatás másolatát is célszerű megküldeni a Hatóságnak. Hasonló magatartás várható el az adatkezelőtől akkor is, ha a címzettnek az egyébként neki szóló üzenettel együtt téves, személyes adatokat tartalmazó csatolmány is kiküldésre került, akár postán, akár elektronikus üzenetben.

b) E-mailek küldése több címzett részére olyan módon, hogy a címzettek nem a „Titkos másolat", hanem a „Másolatot kap" mezőben vannak felsorolva, tehát a címzettek látják, jogosulatlanul megismerik egymás e-mail címeit. Ilyenkor az incidens által a személyes adatokra jelentett kockázat csökkentése érdekében mindenképpen elvárható az adatkezelőtől, hogy a címzettekkel ismét felvéve a kapcsolatot, őket felkérje az üzenet törlésére.

c) Az adatkezelőt ért hackertámadás következtében kiszivárgott adatok. Ilyen esetben fontos az incidens által érintett adatok mihamarabbi azonosítása, az informatikai biztonsági rendszerek felülvizsgálata. Abban az esetben, ha az adatkezelőnek szakértelem hiányában nem sikerül azonosítani a támadás folyamatát, illetve részletesen feltárni az incidenshez vezető körülményeket, érdemes külső szakértőt felkérni. Amennyiben a támadás emberi tényező kihasználásával történt (pl. phising), az elhárítás folyamatából kihagyhatatlan a munkavállalók oktatása. Abban az esetben, ha informatikai hibából adódott a sérülékenység, a teljes rendszer felülvizsgálata lehet indokolt. Minden esetben elvárható az adatkezelő információbiztonsági szabályzatának felülvizsgálata.

d) Ellopott/elvesztett számítástechnikai eszközök, telefonok. Ilyen esetekben kiemelt szereppel bír az is, hogy az adatkezelő az incidenst megelőzően megfelelő figyelmet biztosított-e eszközei védelmének (jelszó, titkosítás), mellyel megakadályozható, hogy az adott eszközön tárolt adatokat illetéktelen személyek megismerhessék. Távoli hozzáférés lehetősége esetén utólag is elképzelhető az adatok eszközről való törlése. Fontos, hogy az incidensről való tudomásszerzést követően az adatkezelő azonnal azonosítsa, hogy az adott kliens milyen adatokhoz, szerverekhez fért hozzá, és milyen jogosultság került kiosztásra számára, azok pedig azonnal kerüljenek megvonásra, az érintett szervereket, szolgáltatásokat vonják vissza, illetve változtassák meg azok hozzáféréseit.

Általánosságban elmondható, hogy egy adatvédelmi incidens után, a feltárt hiányosságokat kiértékelve, az adatkezelő részéről indokolt lehet a belső folyamatok felülvizsgálata, további szűrők, ellenőrzések beiktatása a munkafolyamatba, illetve a munkatársak adatvédelmi tudatosságának növelése.

II.2.6. Határon átnyúló adatkezeléssel kapcsolatos incidensek

A GDPR 56. cikke értelmében az adatkezelő vagy az adatfeldolgozó tevékenységi központja vagy egyetlen tevékenységi helye szerinti felügyeleti hatóság jogosult fő felügyeleti hatóságként eljárni az említett adatkezelő vagy az adatfeldolgozó által végzett határokon átnyúló adatkezelés tekintetében, a 60. cikk szerinti eljárással összhangban („one-stop-shop" mechanizmus).

Tehát a Hatóság eljárása határon átnyúló adatkezeléssel kapcsolatos incidenseknél attól függ, hogy az adatkezelő vagy az adatfeldolgozó tevékenységi központja Magyarországon található-e, vagy sem.

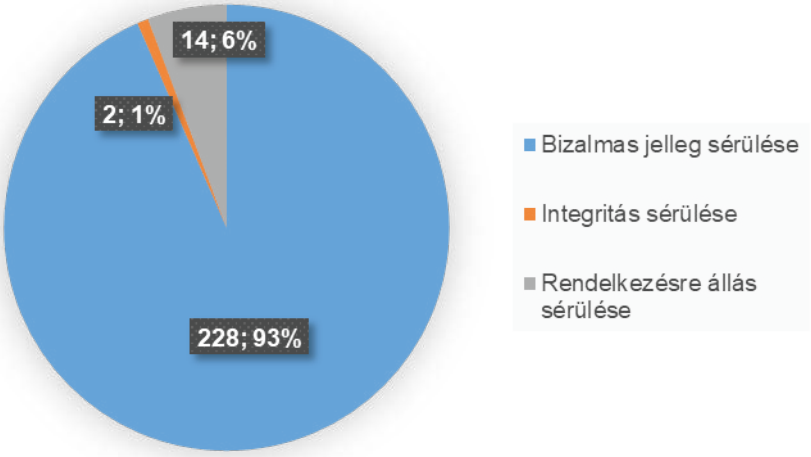
Határon átnyúló adatkezeléssel kapcsolatos incidensre példa a Marriott Hotels Limited-nél történt adatvédelmi incidens, miszerint 2014 óta illetéktelen személyek hozzáfértek a cég egy leányvállalata, a Starwood Hotels adatbázisához. Mivel az incidens határon átnyúló adatkezelést érintett, és a cég központi tevékenységi helye az Egyesült Királyságban, Londonban található, ezért az Egyesült Királyság adatvédelmi hatósága, az Information Commissioner's Office (ICO) 2018. november 30. napján a GDPR 56. cikke szerinti, a fő-, illetve érintett felügyeleti hatóságok meghatározására irányuló eljárást kezdeményezett.

Az ICO önmagát tekinti fő felügyeleti hatóságnak az ügyben, mellyel a Hatóság (és a többi érintett felügyeleti hatóság is) egyetértett, valamint jelezte az ICO felé, hogy a Hatóság is érintettnek tekinti magát, tekintettel arra, hogy az adatkezelés jelentős mértékben érinti vagy valószínűsíthetően jelentős mértékben érinti a Magyarországon lakóhellyel rendelkező érintetteket.

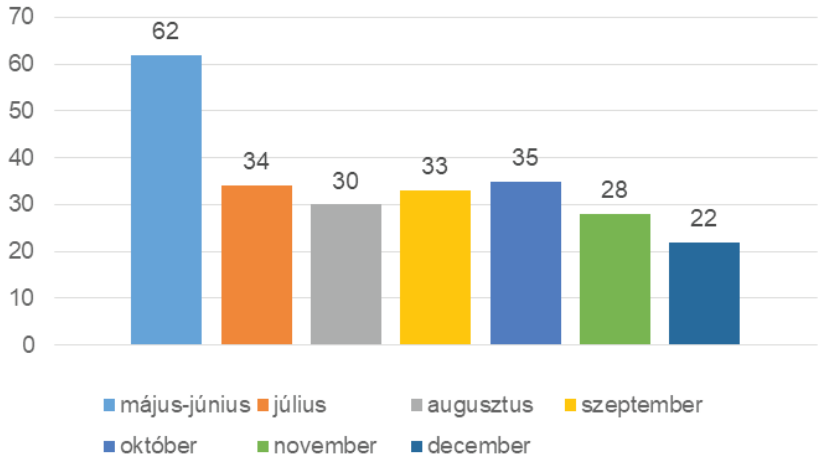
A gyakorlatban ez azt jelenti, hogy az ICO az adatkezelő egyetlen kapcsolattartója az általa végzett, határokon átnyúló adatkezeléssel kapcsolatban, ő folytatja le az incidenssel kapcsolatos vizsgálatot, de az érintett hatóságok – így a Nemzeti Adatvédelmi és Információszabadság Hatóság is – véleményezhetik az ügyben készült döntés tervezetet, ahhoz megjegyzéseket, vagy kifogásokat fűzhetnek.

Fordított a helyzet abban az ügyben, melyben az incidenssel érintett, határon átnyúló adatkezelést folytató adatkezelő tevékenységi központja Magyarországon van, ilyenkor ugyanis a Hatóság jár el fő felügyeleti hatóságként: a GDPR 56. cikke szerinti eljárásban azonosítja az érintett felügyeleti hatóságokat, melyek a Hatóság által készített döntéstervezetet véleményezhetik.

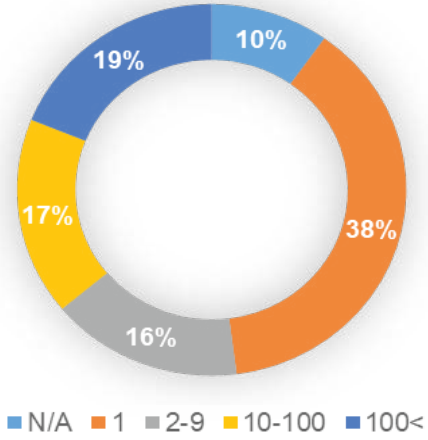
Incidensek jellege



Incidensek hónapok szerinti bontásban



Incidensek megoszlása az érintettek száma alapján



II.2.7. A GDPR alkalmazása előtt történt adatvédelmi incidensek

A Hatósághoz számos bejelentés érkezett a BKK Budapesti Közlekedési Központ Zrt. (a továbbiakban: BKK) által üzemeltett online jegyértékesítési rendszerrel összefüggő adatkezeléssel kapcsolatban. A bejelentők azt kifogásolták, hogy a BKK online jegyértékesítési rendszere nem felel meg az Infotv. 7. §-ában foglalt adatbiztonsági követelményeknek, emellett több panaszban kifogásolták, hogy a sajtóban megjelent hírek[13] alapján valószínűsíthető, hogy a regisztráció során megadott személyes adataikhoz harmadik személyek jogosulatlanul hozzáférhettek.

A Hatóság a panaszok nyomán vizsgálati eljárást folytatott le, majd – tekintettel arra, hogy a bejelentésekben szereplő, valószínűsített jogsértéseket a vizsgálati

13 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/

eljárás alapján megalapozottnak látta – 2017. július 31-én hivatalból adatvédelmi hatósági eljárást indított. Az adatvédelmi hatósági eljárás tárgya a BKK online értékesítési rendszerével összefüggő adatkezelése, különös tekintettel az adatbiztonsági követelményekre és az érintettek előzetes tájékoztatására.

A Hatóság az előzetes tájékoztatással kapcsolatban megállapította, hogy a BKK által az érintettek rendelkezésére bocsátott adatkezelési tájékoztató nem tartalmaz az adatkezeléssel kapcsolatos minden 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 BKK az adatkezelésről nem adott megfelelő tájékoztatást az érintettek számára, és ezzel megsértette az Infotv. 20. § (1)-(2) bekezdéseit. A Hatóság a BKK-t ezért felszólította arra, hogy az adatkezelési tájékoztatási gyakorlatát az Infotv. rendelkezéseire figyelemmel módosítsa, és a jövőben adjon megfelelő tájékoztatást az érintettek részére.

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 BKK által üzemeltetett online jegyértékesítési rendszer adatbázisából kigyűjtött, a regisztrált felhasználók személyes adatait tartalmazó adatbázishoz arra jogosulatlan személyek is hozzáférhetnek. A Hatóság a tényállás tisztázása során megállapította, hogy ez, a részére megküldött adatbázis megegyezik a BKK online jegyértékesítési felületével összefüggésben kezelt adatbázissal, ezért sor került az adatbiztonság olyan sérülésére, amely a BKK által kezelt adatokhoz való jogosulatlan hozzáférést eredményezte, vagyis az Infotv. 3. § 26. pontja szerinti adatvédelmi incidens történt.

A Hatóság az eljárás során megvizsgálta, hogy a BKK eleget tett-e az Infotv. 7. §-ában foglalt adatbiztonsággal kapcsolatos kötelezettségeinek és ezzel kapcsolatban az alábbiakat állapította meg:

– A BKK 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, hogy a BKK nem tudta megállapítani azt, hogy az általa végzett adatkezelés vonatkozásában adatvédelmi incidensre került sor, illetve annak körülményeit, így különösen az érintettekre gyakorolt hatását sem tudta megállapítani. A BKK-nak az adatbiztonsági intézkedések körében gon-

doskodnia kellett volna arról is, hogy megállapítsa az esetleges adatvédelmi incidens bekövetkezésekor alkalmazandó eljárásrendet is, amelyre a BKK nyilatkozatai, valamint a rendelkezésre bocsátott dokumentumok alapján nem került sor.

– A BKK az adatfeldolgozóval kötött szerződésben nem tért ki az adatkezeléssel kapcsolatos kérdésekre, így abban nem rögzítettek adatbiztonsági előírásokat, követelményeket sem. A BKK emellett a szerződés megkötését követően sem adott utasításokat az általa igénybe vett adatfeldolgozónak az adatbiztonsági intézkedések vonatkozásában.
– A BKK az adatvédelmi incidensekkel kapcsolatosan általánosságban nem alkotott meg előzetesen olyan belső eljárásrendet, szabályzatot, amelynek alkalmazásával egy esetleges incidens feltárható és kezelhető. Emellett a BKK 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 fentiek alapján a Hatóság 2018. január 22-én hozott határozatában a BKK-t tízmillió forint adatvédelmi bírság megfizetésére kötelezte, valamint arra, hogy 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. Kötelezte továbbá arra, hogy 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.

A Fővárosi Törvényszék a határozat bírósági felülvizsgálata iránti perben a BKK keresetét 2018. július 4-én elutasította. A BKK e döntés ellen fellebbezést nyújtott be a Kúriánál, melynek eljárása a beszámoló lezárásának időpontjában folyamatban van.

II.2.8. Engedélyezési eljárások

A GDPR alapján a Hatóság feladatköre bővült az 58. cikk (3) bekezdése szerinti engedélyezési hatáskörökkel, melyeknek részletszabályait a nemzeti jogsza-

bályok tartalmazzák. A Hatóság esetében a Módtv. rendelkezéseivel módosított Infotv. alkalmazandó, amelynek 64/A-64/C §-ai úgy rendelkeznek, hogy az ilyen hatáskörök gyakorlása során adatkezelési engedélyezési eljárás lefolytatására kerül sor.

Adatkezelési engedélyezési eljárás lefolytatására az alábbi ügycsoportok esetén kerül sor:

I. Magatartási kódex jóváhagyása és a magatartási kódexnek való megfelelést ellenőrző szervezet tevékenységének engedélyezése
II. Tanúsítási szempontok jóváhagyása
III. Harmadik országba történő adattovábbítással kapcsolatos engedélyezési eljárások

II.2.8.1. Magatartási kódex jóváhagyása és a magatartási kódexnek való megfelelést ellenőrző szervezet tevékenységének engedélyezése

1. Magatartási kódex

Az Infotv. 64/A. § (1) bekezdés a) pontja alapján, a Hatóság a GDPR szerinti magatartási kódexek tervezetének, kiegészítésének vagy módosításának jóváhagyása iránti kérelmek benyújtása esetén adatkezelési engedélyezési eljárást folytat le.

Az adatkezelők vagy adatfeldolgozók kategóriáit képviselő egyesületek és egyéb szervezetek magatartási kódexeket dolgozhatnak ki, hogy pontosítsák a GDPR alkalmazását. A magatartási kódex a GDPR által megnevezett olyan eszköz, amelynek önkéntes alkalmazása segít az adatkezelőknek abban, hogy a GDPR-nak való megfelelést biztosítsák. A GDPR példálózó felsorolást tartalmaz arról, hogy melyek azok a kérdések, amelyekre vonatkozóan egy magatartási kódex pontosíthatja a GDPR alkalmazását. Az Ákr.-ben meghatározottakon túl, a kérelemnek tartalmaznia kell a kódex, illetve annak kiegészítése vagy módosítása tervezetét.

Az alábbi tartalmi elemeknek szerepelnie kell a kódexben vagy a kérelemben:

– A kódexnek egy konkrét szektor vagy tevékenységi kör adatkezeléssel kapcsolatos kérdéseire kell fókuszálni, és megoldásokat kínálni a kódexet alkalmazó adatkezelők és adatfeldolgozók számára ezekkel a kérdésekkel kapcsolatban. A jóváhagyásra irányuló eljárás során ezért

a kérelmezőnek be kell mutatnia azt, hogy a magatartási kódex elegendő hozzáadott értéket képvisel.
- A kérelmezőnek ismertetnie kell, hogy az általa képviselt szektornak milyen sajátos kérdései, problémái vannak, melyek indokolják a magatartási kódex kidolgozását.
- Ennek előkérdéseként arról is biztosítania kell a felügyeleti hatóságot, hogy van „felhatalmazása" egy kódex kidolgozására, vagyis azt, hogy az adott szervezet megfelelő arra, hogy egy szektort érintő szabályrendszert kidolgozzon, és annak betartatására hatékony eszközöket hozzon létre.
- A kódexből pontosan ki kell derülnie, hogy milyen tárgyi és földrajzi hatálya van, vagyis a kérelmezőnek meg kell határoznia egyrészt azt, hogy mely adatkezelési tevékenységekre, mely adatkezelőkre vonatkozik a kódex, másrészt azt, hogy mely tagállam(ok)ban lesz alkalmazható.
- A kérelemben, illetve a mellékletét képező tervezetben be kell mutatni, hogy a kódex milyen mechanizmusokat hoz létre, amelyek lehetővé teszik a kódex ellenőrzését végző szervezetnek, hogy ellenőrizze, hogy a kódex alkalmazását vállaló adatkezelők vagy adatfeldolgozók megfelelnek-e a kódex rendelkezéseinek, illetve hogy azt kikényszerítse.
- Ha a magatartási kódex több tagállamot érintő adatkezelési tevékenységre vonatkozik, akkor a kérelmezőnek indokolnia kell, hogy mi alapozza meg a Hatóság illetékességét. Ennek során a következőket veheti figyelembe például: a szektor vagy adatkezelési tevékenység leggyakoribb előfordulásának helye; a kérelmező egyesület vagy a javasolt ellenőrző szervezet székhelye.

A tervezet összeállítása során figyelembe kell venni az Európai Adatvédelmi Testület készülő iránymutatásában foglaltakat, amelyet a véglegesítését követően a Hatóság is közzé fog tenni honlapján.

A Hatóság a GDPR 40. cikk (5) bekezdése alapján véleményt bocsát ki arról, hogy a tervezet összhangban van-e a GDPR-ral, és amennyiben igen, akkor azt adatkezelési engedélyezési eljárásban jóváhagyja.

Előfordulhat, hogy a magatartási kódex több tagállamot is érintő adatkezelési tevékenységekre is vonatkozik, ebben az esetben az illetékes hatóság a jóváhagyást megelőzően a GDPR szerinti egységességi mechanizmus keretében benyújtja azt az Európai Adatvédelmi Testületnek is. Ilyen esetekben a Testület is véleményt bocsát ki arról, hogy a tervezet összhangban van-e a GDPR-ral. Amennyiben a Testület úgy ítéli meg, hogy a tervezet megfelelő, benyújtja azt

a Bizottságnak, amely végrehajtási aktusok útján határozhat úgy, hogy a hozzá benyújtott, jóváhagyott magatartási kódex az Unió területén általános érvénnyel rendelkezik.

A felügyeleti hatóság feladatai közé tartozik még az, hogy a jóváhagyott magatartási kódexet nyilvántartásba veszi és közzéteszi, amennyiben az érintett kódex nem vonatkozik több tagállamot érintő adatkezelési tevékenységre. Amennyiben egy kódex a Bizottság döntése alapján általános érvényű, akkor a nyilvánosságáról is a Bizottság gondoskodik. Emellett az Európai Adatvédelmi Testület valamennyi jóváhagyott magatartási kódexet egy nyilvántartásban állítja össze, és megfelelő módon nyilvánosan elérhetővé teszi őket.

2. A magatartási kódexnek való megfelelést ellenőrző szervezet tevékenységének engedélyezése

A magatartási kódexeknek olyan mechanizmusokat kell meghatározni, amelyek lehetővé teszik, hogy az erre akkreditált szervezet ellenőrizze, hogy a kódex alkalmazását vállaló adatkezelők vagy adatfeldolgozók megfelelnek-e a kódex rendelkezéseinek. A GDPR 41. cikk (1) és (6) bekezdése alapján, a felügyeleti hatóság feladat- és hatásköreinek sérelme nélkül, a magatartási kódexnek való megfelelés ellenőrzését olyan szervezet végezheti, amely a kódex tárgya tekintetében megfelelő szakértelemmel rendelkezik, és amelyet az illetékes felügyeleti hatóság erre akkreditál. Ez a rendelkezés nem alkalmazandó a közhatalmi szervek és közfeladatot ellátó egyéb szervek által végzett adatkezelésre.

Az Infotv. 64/A. § (1) bekezdés b) pontja alapján a Hatóság adatkezelési engedélyezési eljárást folytat le a magatartási kódexnek való megfelelést ellenőrző tevékenység engedélyezése iránti kérelmek benyújtása esetén.

A GDPR 41. cikk (2) bekezdése alapján egy magatartási kódexnek való megfelelés ellenőrzésére abban az esetben lehet akkreditálni egy szervezetet, amennyiben az:

– az illetékes felügyeleti hatóság számára kielégítő bizonyítékot szolgáltatott arra nézve, hogy független, és a kódex tárgyában szakértelemmel bír;
– létrehozott olyan eljárásokat, amelyek révén meg tudja állapítani, hogy az érintett adatkezelők és adatfeldolgozók alkalmasak-e a kódex alkalmazására, ellenőrizni tudja, hogy az érintett adatkezelők és adatfeldolgozók betartják-e a kódex rendelkezéseit és rendszeres időközönként felül tudja vizsgálni a kódex működését;

– létrehozott olyan eljárásokat és struktúrákat, amelyek révén kezelni tudja a kódex megsértésével vagy a kódex adatkezelő vagy adatfeldolgozó általi alkalmazásával kapcsolatos panaszokat, és ezeket az eljárásokat és struktúrákat az érintettek és a nyilvánosság számára átláthatóvá teszi; valamint
– az illetékes felügyeleti hatóság számára kielégítő bizonyítékot szolgáltat arra nézve, hogy feladataival kapcsolatban nem áll fenn összeférhetetlenség.

A GDPR alapján a NAIH-nak közzé kell tennie a honlapján az ellenőrző szervezet akkreditációjával kapcsolatos szempontokat, melyre azt követően fog sor kerülni, hogy arról az Európai Adatvédelmi Testület egységességi mechanizmus keretében véleményt bocsát ki.

Az ilyen tevékenység engedélyezésére irányuló kérelemnek tartalmaznia kell annak igazolását, hogy a szervezet milyen módon teljesíti a GDPR 41. cikk (2) bekezdésében foglalt, illetve a NAIH által közzétett engedélyezési szempontokban meghatározott feltételek fennállását.

II.2.8.2. Tanúsítási szempontok jóváhagyása

A tanúsítás a GDPR által létrehozott, az adatkezelők és adatfeldolgozók által önkéntesen alkalmazható eszköz, amely felhasználható annak bizonyítása során, hogy az adatkezelő teljesíti a GDPR-ban meghatározott kötelezettségeit.

A tanúsítás meghatározott követelmények – a tanúsítási szempontok – szerint folytatott megfelelőség-értékelés, amelyet egy harmadik személy végez el és igazol. A követelmények szabványokból vagy jogszabályokból erednek, az adatvédelmi tanúsítás esetében a GDPR jelenti a normatív szabályrendszert, amely a követelmények értékelésének alapját képezi. Ahhoz, hogy megfeleljen a tanúsítás céljának, a GDPR rendelkezéseit azonban tanúsítási szempontokban, illetve tanúsítási mechanizmusban kell pontosítani, konkretizálni a tanúsítás tárgyára. A sikeres tanúsítás eredménye a tanúsítvány, bélyegző vagy jelölés, amely igazolja, hogy az adott szervezet megfelelt a tanúsítási mechanizmusban található tartalmi és eljárási követelményeknek.

A GDPR szerinti tanúsítással kapcsolatban további információkat tartalmaz az Európai Adatvédelmi Testület által elfogadott, 1/2018. számú iránymutatásra, amely megtalálható a https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-12018-certification-and-identifying-certification_en elérési úton.

Az Európai Adatvédelmi Testület álláspontja szerint a GDPR szerinti tanúsítás tárgya adatkezelési művelet vagy műveletek összessége lehet. Ez jelenthet például irányítási folyamatokat is, amelyek szervezési intézkedésnek tekinthetők, és ezáltal egy adatkezelési műveletnek szerves részét képezik.

A tanúsítványt akkreditált tanúsító szervezetek vagy az illetékes felügyeleti hatóságok állítják ki. Amennyiben tanúsító szervezet kíván tanúsítványt kiállítani, akkor arra az illetékes felügyeleti hatóság által jóváhagyott tanúsítási szempontok, illetve mechanizmus alapján kerülhet sor. A tanúsító szervezet akkreditációjának tehát előfeltétele, hogy a tanúsítás alapjául szolgáló tanúsítási szempontokat, illetve mechanizmust a Hatóság adatkezelési engedélyezési eljárás keretében jóváhagyja.

Az Infotv. 64/A. § (1) bekezdés c) pontja alapján a Hatóság a tanúsítási szempontok jóváhagyása iránti kérelmek benyújtása esetén adatkezelési engedélyezési eljárást folytat le. A kérelemnek az Ákr.-ben meghatározottakon túl tartalmaznia kell a tanúsítási mechanizmus általános leírását és a tanúsítási szempontok tervezetét. A tanúsítási szempontokkal, illetve mechanizmussal kapcsolatos minimum elvárásokat a Hatóság az Európai Adatvédelmi Testület iránymutatásának véglegesítését követően fogja közzétenni.

II.2.8.3. Harmadik országba történő adattovábbítással kapcsolatos engedélyezési eljárások

A GDPR rendelkezései alapján vannak olyan eszközök, amelyek akkor jelentenek megfelelő garanciákat a harmadik országba történő adattovábbítás során, amennyiben azt az illetékes felügyeleti hatóság jóváhagyja, engedélyezi.
Az adattovábbításra az illetékes felügyeleti hatóság külön engedélye nélkül sor kerülhet, azonban az alapjául szolgáló eszközt az illetékes hatóságnak jóvá kell hagynia:

1. kötelező erejű vállalati szabályok (BCR),
2. magatartási kódex,
3. tanúsítás.

Az illetékes felügyeleti hatóság engedélyével az alábbiak is megfelelő garanciákat jelentenek:

1. az adatkezelő vagy adatfeldolgozó és a harmadik országbeli adatkezelő vagy adatfeldolgozó vagy a személyes adatok címzettje között létrejött szerződéses rendelkezések,

2. közhatalmi vagy egyéb közfeladatot ellátó szervek között létrejött, közigazgatási megállapodásba beillesztendő rendelkezések, köztük az érintettek érvényesíthető és tényleges jogaira vonatkozó rendelkezések.

1. BCR jóváhagyása

Amennyiben egy vállalkozáscsoport vagy közös gazdasági tevékenységet folytató vállalkozások csoportja („Csoport", vagy „kérelmező") BCR-t kíván megalkotni, akkor figyelembe kell vennie a GDPR 47. cikkében előírt kötelező tartalmi elemeket, valamint az Európai Adatvédelmi Testület által kiadott iránymutatásokat, munkadokumentumokat[14]. A jóváhagyás során az illetékes felügyeleti hatóság, az érintett felügyeleti hatóságok, illetve a Testület az ezekben előírt tartalmi követelmények meglétét vizsgálja.

A GDPR úgy rendelkezik, hogy a BCR jóváhagyását az illetékes felügyeleti hatóság az egységességi mechanizmusnak megfelelően folytatja le, így biztosítva az Unió egész területén az egységességet. Amennyiben tehát egy illetékes felügyeleti hatóság BCR jóváhagyására irányuló eljárást folytat le, akkor a döntéstervezetet, illetve minden releváns információt – ideértve például más érintett felügyeleti hatóságok véleményét – közölnie kell az Európai Adatvédelmi Testülettel, amely ezt követően véleményt bocsát ki róla.

A Testületnek benyújtandó döntéstervezet előkészítésére, vagyis az érintett hatóságok közötti, a BCR megfelelőségének vizsgálatára vonatkozó egyeztetésre vonatkozóan a GDPR nem állapít meg pontos eljárásrendet. A GDPR arra sem ad pontos előírást, hogy milyen módon kell kijelölni a 47. cikk alapján a BCR vonatkozásában „illetékes" hatóságot, vagyis azt, hogy egy konkrét BCR jóváhagyását melyik felügyeleti hatóságnál kell kezdeményezni.

A fentiek orvoslására az Európai Adatvédelmi Testület elfogadta a WP 263 rev. 01 számú munkadokumentumot,[15] melyben a Testület lefekteti a BCR jóváhagyása iránti eljárások hatékony lefolytatását célzó, felülvizsgált együttműködési eljárás alapjait. Egyrészt meghatározza, hogy milyen módon kell megállapítani azt,

14 WP 256 rev. 01: Munkadokumentum a kötelező erejű vállalati szabályokba belefoglalandó elemeket és elveket tartalmazó táblázat meghatározásáról (https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=614109);
WP 257 rev. 01: Az adatfeldolgozókra vonatkozó kötelező erejű vállalati szabályok elemeit és elveit tartalmazó táblázatot létrehozó munkadokumentum (https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=614110)

15 https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=623056

hogy egy adott BCR vonatkozásában mely felügyeleti hatóság tekinthető „illetékesnek", vagyis ún. „vezető hatóságnak", másrészt azt is, hogy milyen módon zajlik az egyeztetés az érintett tagállami felügyeleti hatóságok között a BCR jóváhagyását megelőzően a tartalmának elemzése, vizsgálata érdekében.

2. Az adatkezelő vagy adatfeldolgozó és a harmadik országbeli adatkezelő vagy adatfeldolgozó vagy a személyes adatok címzettje között létrejött szerződéses rendelkezések engedélyezése

Harmadik országba történő adattovábbításra sor kerülhet akkor is, ha az adatkezelő vagy adatfeldolgozó az illetékes felügyeleti hatóság engedélyével a megfelelő garanciákat a közötte és a harmadik országbeli adatkezelő, adatfeldolgozó vagy a személyes adatok címzettje között létrejött szerződéses rendelkezések útján biztosítja. Az ilyen szerződéses rendelkezések engedélyezésére azon tagállam felügyeleti hatósága rendelkezik a GDPR szerinti „illetékességgel", amelyből a személyes adatok továbbítására sor kerül.
Az ilyen szerződéses rendelkezésekkel kapcsolatban az Európai Adatvédelmi Testület még nem adott ki iránymutatást, további információk a későbbiekben lesznek elérhetők.

3. Közhatalmi vagy egyéb közfeladatot ellátó szervek között létrejött, közigazgatási megállapodásba beillesztendő rendelkezések, köztük az érintettek érvényesíthető és tényleges jogaira vonatkozó rendelkezések engedélyezése

Harmadik országba történő adattovábbításra sor kerülhet akkor is, ha a megfelelő garanciákat az illetékes felügyeleti hatóság által engedélyezett közhatalmi vagy egyéb közfeladatot ellátó szervek között létrejött, közigazgatási megállapodásba beillesztendő rendelkezésekkel biztosítják. Az ilyen rendelkezéseknek ki kell terjedniük az érintettek érvényesíthető és tényleges jogaira is. Az engedélyezésre azon tagállam felügyeleti hatósága rendelkezik a GDPR szerinti „illetékességgel", amelyből a személyes adatok továbbítására sor kerül.

Ez az eszköz tehát közhatalmi vagy közfeladatot ellátó szervek által alkalmazható, amely harmadik országban található közhatalmi vagy közfeladatot ellátó szerv(ek) részére kíván személyes adatokat továbbítani, abban az esetben, ha a szervek valamelyikének nincs lehetősége, hatásköre más módon megfelelő garanciákat biztosítani (például nem tud jogilag kötelező erejű megállapodást kötni). Ez az eszköz nem alkalmas arra, hogy egy közhatalmi vagy közfeladatot ellátó szerv és egy magánjogi szerv közötti adattovábbításhoz teremtse meg a megfelelő garanciákat.

II.3. Az adatvédelmi tanúsítás

A GDPR alkalmazandóvá válását követően megszűnt a Hatóság számára az adatvédelmi audit szolgáltatás nyújtásának lehetősége. A Módtv. azonban a GDPR 42. cikk (5) bekezdésére tekintettel megállapította az adatkezelő vagy adatfeldolgozó kezdeményezésére induló adatvédelmi tanúsítási eljárásra vonatkozó alapvető rendelkezéseket, amely előírásokat – a két jogintézmény hasonló jellegére tekintettel – az Infotv. korábbi, az adatvédelmi auditra vonatkozó eljárásrendre alkalmazandó szabályainak helyén, azokkal hasonló tartalommal alakította ki a magyar jogalkotó.

Az adatvédelmi tanúsítás azonban a hasonlóságok ellenére közelebb áll a szabványoknak történő megfelelés értékelésére és igazolására szolgáló tevékenységhez, e tekintetben lényegében különbözik az általános felülvizsgálati eszközként értelmezhető adatvédelmi audittól. Az adatvédelmi audit az adatkezelő által végzett vagy tervezett adatkezelési műveletek – a Hatóság által meghatározott és közzétett szakmai szempontok szerinti – értékelésén keresztül a jogszabályi követelményeknek történő megfelelés felmérésére, majd a vizsgálat időpontjában hatályos elvárások és biztosítékok kialakítására törekedett, az adatkezelőnek pedig lehetősége volt az audit céljának és hatókörének meghatározására. Ezzel szemben az adatvédelmi tanúsítás során az adatkezelő feladata dokumentált módon alátámasztani a Hatóság által előre meghatározott és közzétett – csak az adatvédelmi műveletek egy jóval szűkebb köre esetében elérhető – szempontrendszernek történő megfelelést.

Az adatvédelmi tanúsítás során a Hatóság kizárólag az általa nyújtott tanúsítási körbe eső adatkezelési művelethez kapcsolódóan vizsgálja az adatkezelő kérelmében megjelölt adatkezelési gyakorlatát, ennek keretében értékeli az adatvédelmi alapelveknek történő megfelelést, az adatkezelő érintetti jogok biztosításával kapcsolatos kötelezettségeinek teljesítését, dokumentált belső és külső eljárásait, szabályzatait, tájékoztatóit, kockázatelemzési és kockázatkezelési tevékenységét és esetleges adatfeldolgozási vagy adattovábbítási tevékenységéhez kapcsolódó követelmények teljesülését. A Hatóság az egyedi adatkezelésre vonatkozó bélyegző közzétételével kizárólag az előre rögzített követelmények megvalósulását igazolhatja, az új jogintézményből már hiányzik a megfelelés kialakítását segítő konzultációs tevékenység, tágabb értelemben vett felkészítés. Emellett a GDPR 42. cikk (4) bekezdése rögzíti, hogy a tanúsítás nem csökkenti az adatkezelő vagy adatfeldolgozó adatvédelmi követelmények betartásáért való felelősségét, és nem sérti a felügyeleti hatóságok feladat- és hatáskörét, tehát egy folyamatban lévő tanúsítási eljárásban részt

vevő, vagy már bélyegzővel rendelkező adatkezelési művelettel kapcsolatban a Hatósághoz érkező érintetti panasz elbírálására, az eljárás megindítására a tanúsítás nem lehet kihatással.

A tanúsítás és a bélyegző Hatóság általi kiállítását fontos elhatárolnunk az Infotv. 64/A. § c) pontban meghatározott hatósági eljárási szabályok szerint lefolytatandó adatkezelési engedélyezési eljárástól (ld. a fentiekben), továbbá a GDPR 43. cikkében meghatározottak szerint tanúsító szervezetek akkreditációjára irányuló, a Nemzeti Akkreditáló Hatóság által lefolytatott eljárástól is, amelyben a NAIH szakhatóságként vesz részt.

A Hatóság az Infotv. 69. § alapján nyújtott tanúsítási tevékenysége emellett az engedélyezési eljárástól eltérően nincs a magyar akkreditációs előírások, illetve az ISO/IEC 17065/2012 szabvány követelményeihez kötve, tekintettel arra, hogy a felhatalmazást közvetlenül a GDPR jelenti számára a tanúsítási mechanizmusok kidolgozására. Ilyen tanúsítási tevékenységet korábban több uniós tagállam adatvédelmi hatósága is folytatott (ld. pl. a francia felügyeleti hatóság (CNIL) 2015. január 13-án közzétett tanúsítási mechanizmusa a digitális széf, adatvédelmi képzések és az adatvédelmi auditokra vonatkozóan).

A Hatóság szervezetén belül a tanúsítással kapcsolatos feladatokat az e célra létrehozott szervezeti egység, az Elnöki Kabinet Adatvédelmi Tanúsítási Osztálya látja el, amelynek munkatársai információbiztonsági és adatvédelmi jogi kompetenciákkal egyaránt rendelkeznek.

A Hatóság tanúsítási mechanizmusa, szempontrendszere és az annak eredményeként a kezdeményező részére kiállítható adatvédelmi bélyegzőre vonatkozó részletszabályok jelenleg kidolgozás alatt állnak, annak érdekében, hogy az adatkezelők, illetve adatfeldolgozók számára elérhetővé tegyen egy olyan rugalmas és magas színvonalú tanúsítási mechanizmust, amely megfelel a GDPR 42. és 43. cikkében foglalt követelményeknek, valamint az Európai Adatvédelmi Testület azokhoz kapcsolódó 1/2018.[16] és 4/2018.[17] számú iránymutatásának. A Hatóság tanúsítási termékei körének meghatározására az Európai Adatvédelmi Testületi iránymutatások végleges változatának közzétételét követően, más tagállamok felügyeleti hatóságainak tanúsítási gyakorlatára figyelemmel a jövőben kerül sor.

16 Guidelines 1/2018 on certification and identifying certification criteria in accordance with Articles 42 and 43 of the Regulation 2016/679 - version for public consultation.

17 Guidelines 4/2018 on the accreditation of certification bodies under Article 43 of the General Data Protection Regulation (2016/679).

III. A személyes adatok bűnüldözési, honvédelmi és nemzetbiztonsági célú kezelésével kapcsolatos eljárások

A címben említett három adatkezelési cél és az azokhoz tartozó adatkezelések külön fejezetben való tárgyalását az indokolja, hogy ezekre nem alkalmazandók a GDPR szabályai, hanem továbbra is tagállami jogalkotási hatáskörben maradnak, vagyis ezen tárgykörökben a Módtv. hatálybalépését követően is az Infotv. határozza meg a személyes adatok védelmének alapvető szabályait. A GDPR és az Infotv. egyaránt a személyes adatok védelmének magas szintjét célozza meg és az általuk szabályozott elvek és jogintézmények sok tekintetben hasonlóak, ám az Infotv. hatálya alá tartozó tárgykörök olyan alapvető állámérdekekkel állnak kapcsolatban, amelyeket nem lehet teljesen a (főként a piaci, vállalati, transznacionális adatkezelés adatvédelmi szabályozási igényeire reflektáló) GDPR-al paralel módon szabályozni. Ennek megfelelően az Infotv.-ben szabályozott tárgykörökben az adatkezelés lehetséges jogalapjai közül nagyobb szerep jut például a kötelező adatkezelésnek, de az is megemlíthető, hogy más feltételek vonatkoznak az érintett jogainak korlátozására, mint azon adatkezelések esetében, amelyek adatvédelmi kereteit a GDPR határozza meg.

2018. folyamán mindhárom tárgykörben, valamint a bűnügyi célú nemzetközi és európai adattovábbítások és információs rendszerek adatvédelmi ellenőrzésével kapcsolatban is keletkezett beszámolásra érdemes adatvédelmi tapasztalat; a továbbiakban ezeket vesszük sorra.

III.1. Bűnüldözési célú adatkezelésekkel kapcsolatos eljárások

III.1.1. A közösségi hálózati profilok és a felhőszolgáltatások ellenőrzése büntetőeljárás során

Egy állampolgár azért fordult a Hatósághoz, mert miután a rendőrség informatikai, távközlési eszközöket foglalt le tőle és a közeli hozzátartozóitól, azt tapasztalták, hogy lányuk, illetve a saját Facebook-fiókjukba, Gmail-fiókjuba és egyéb alkalmazásaikba valaki belépett és azokhoz új jelszót igényelt. Mikor az eszközöket az igazságügyi szakértői vizsgálat után visszakapták, azt találták, hogy azokról SMS-üzeneteket és adatokat töltöttek le, illetve egy mobiltelefonra telepítettek egy, vélhetően az igazságügyi szakértőhöz tartozó Gmail-fiókot.

A Hatóság a vizsgálat során megkereste az igazságügyi szakértőt és az őt megbízó rendőrségi szervet is. A vizsgálat során nem merült fel olyan adat, amely arra engedne következtetni, hogy az igazságügyi szakértő eljárása során megbízásának kereteit átlépte volna, és a szakértői tevékenységének végzéséhez szükségesen túl a bejelentők személyes adatait kezelte volna.

III.1.2. Képfelvétel készítése rendőri intézkedésről

Az alapvető jogok biztosa egy általa vizsgált ügyben kért véleményt a Hatóságtól, mert az általa megállapított tényállás több alapvető jogot érintett és ezek között információs alapjogok érintettsége is felmerült. A kérdés lényegében arra irányult, hogy egy körözött személy elfogása közben eljáró, közfeladatot ellátó rendőr képmása, személyes adatai kezelhetőek-e oly módon, hogy az intézkedés alá vont személy a nála lévő mobiltelefonnal képfelvételt készít az intézkedéséről és az intézkedést foganatosító rendőrökről.

A Hatóság az eset ismert körülményeinek megvizsgálása után arra jutott, hogy egy ilyen helyzetben két érdekkör áll egymással szemben: egyrészt a jogszerű intézkedés hatékonyságának érdeke, amely végső soron önmaga is a demokratikus rend fenntartását szolgálja, másrészt a közhatalmi szervek működése ellenőrzésének érdeke, amely ellenőrizhetőségnek előfeltétele, hogy az állampolgárok rendelkezésére álljanak a szükséges információk, amelyek alapján megalapozott vélemény alkotható arról, hogy a közhatalmi szerv, jelen esetben a rendőrség, a jogállamiság keretei között, a vonatkozó jogszabályoknak megfelelően látta-e el a feladatait.

Az intézkedő rendőr közfeladatot ellátó szerv feladat- és hatáskörében eljáró személynek minősül, ezért a feladatellátással kapcsolatban a személyes adatai közül az Infotv.-ben meghatározott adatkörbe tartozók közérdekből nyilvános személyes adatok. A közérdekből nyilvános személyes adatok a célhoz kötött adatkezelés elvének tiszteletben tartásával terjeszthetőek. Az adatok terjesztéséhez való jog gyakorlásának alkotmányos kereteit az Alkotmánybíróság több határozata érintette. Fontos ugyanakkor megjegyezni, hogy a rendőrök arcképmása az Infotv. szerint nem tartozik a közérdekből nyilvános adatok közé.

Az adatok terjesztéséhez való jog gyakorlásának előfeltétele az információk megismerése, illetve a nyilvánosságra hozható, terjeszthető adatok (másolatának) birtokbavétele. A közérdekű vagy közérdekből nyilvános adatok megismerése tipikusan adatigénylés útján, az adatot kezelő szervtől vagy személytől kapott tájékoztatással vagy iratmásolat megküldésével történik, de ezek nem

kizárólagos módozatai az adatok megszerzéséhez való jog gyakorlásának. A rendőri intézkedésről rendszerint nem készül rendőrségi képi dokumentáció, vagyis az ilyen adatok formális, utólagos adatigényléssel történő megismerésére nincs mód, ezért az állampolgári jogérvényesítés más, a jog által nem tiltott módjait is elfogadhatónak kell tekinteni. A Hatóság álláspontja szerint e körbe tartozik az, ha az intézkedés alá vont személy képfelvételt készít az intézkedésről. Azonban a joggyakorlás ezen módozata nem akadályozhatja a jogszerű intézkedés végrehajtását. Ugyanakkor az intézkedő rendőrnek tartózkodnia kell attól, hogy az intézkedés képfelvétellel történő dokumentálását szükségtelenül, mondvacsinált indokokkal akadályozza. A rögzített felvétel – mivel a rendőrök arcképmása nem közérdekből nyilvános adat – nyilvánosságra nem hozható, de felhasználható pl. egy a rendőri intézkedés jogszerűségét vizsgáló eljárásban.

III.1.3. A terheltek és a sértettek személyazonosító adatainak feltüntetése nyomozóhatóságok által küldött megkeresésekben

A Hatósághoz forduló bejelentő, aki egy cég vezetője, azt kifogásolta, hogy cége több alkalommal kapott olyan, adatközlésre vonatkozó megkeresést a rendőrségtől, az ügyészségtől, illetve egyes esetekben bíróságtól, amely megkeresés az alapjául szolgáló büntetőeljárás azonosító adatai között a büntetőeljárásban érintett személyek (a terhelt, illetve a sértett) számos személyes adatát is tartalmazta. A megkeresésben közölt személyes adatokra nem volt szükség a megkeresés teljesítéséhez.

A Hatóságnak más forrásból is tudomása van hasonló gyakorlatról, így például az egyik esetben a nyomozóhatóság szükségtelenül tüntette fel a megkeresésben a büntetőügy azonosító adatai között olyan kiskorúak személyes adatait, akik szexuális jellegű bűncselekmény áldozatai voltak. A Hatóság álláspontja szerint az ismertetett adatkezelési gyakorlat nincs összhangban a személyes adatok célhoz kötött kezelésének követelményével. Továbbá az adatok szükségtelen közlése tetézheti a bűncselekmények sértettjeinek sérelmét, szenvedését. De nemcsak a sértettek, hanem a terheltek esetében sem fogadható el az adataik szükségtelen továbbításának fentiekben vázolt gyakorlata, hiszen a gyanúsítottat megilleti az ártatlanság vélelme és a gyanúsított személyes adatainak kezelésére is kiterjed a személyes adatok védelme.

A Hatóság a bejelentés alapján a Belügyminisztériumot és az Igazságügyi Minisztériumot megkeresve intézkedést kezdeményezett a kifogásolt adatkezelési gyakorlat megszüntetése érdekében.

III.1.4. A Rendőrség által kezelt adatok lehetséges szivárgása

Egy bejelentő azért fordult a Hatósághoz, mert az ismerősi köréből olyan információ jutott el hozzá, amelyből arra lehetett következtetni, hogy olyan személyek is tudomással bírnak egy bírsággal végződött gyorshajtási ügyéről, akik erről jogszerűen nem tudhatnának. A Hatóság vizsgálata során megkereste az érintett szerveket, de nem került elő olyan adat, amely bizonyította volna a bejelentő Rendőrség által kezelt személyes adataival történt visszaélést, ezért a Hatóság a vizsgálatot lezárta. Ennek kapcsán érdemes megjegyezni, hogy az Infotv. széleskörű vizsgálati jogosultságokat biztosít a Hatóság számára az adatkezeléssel kapcsolatos tényállás megismeréséhez, ám a Hatóság nyomozati jogkörrel nem rendelkezik.

III.2. Honvédelmi célú adatkezelésekkel kapcsolatos eljárások

2018. őszén ellentmondásos sajtóhíradások jelentek meg arról, hogy Demeter Márta országgyűlési képviselő a Magyar Honvédség egyik légi szállítási feladatával kapcsolatban a repülőgépen utazó utasokra vonatkozó adatokat hozott nyilvánosságra, ezért a Hatóság hivatalból eljárva megkísérelte a tényállás tisztázását. A Hatóság által az MH. 59. Szentgyörgyi Dezső Repülőbázison tartott helyszíni vizsgálaton megállapítást nyert, hogy az országgyűlési képviselő asszony a törvényi előírásoknak megfelelően tájékoztatást kapott a számára bemutatott dokumentumok kezeléséről és azok „nem nyilvános” minőségéről. A Hatóság megállapította, hogy Demeter Márta az iratbetekintése során, a megtekintett dokumentumokból nem szerezhetett arra utaló információt, melyet a 2018. október 16-i interpellációiban tényként közölt. A kérdéseivel összefüggésbe hozható dokumentumok nem tartalmaztak a nyilvánosságra hozott, miniszterelnök lányára utaló személyes adatokat. A képviselő által nyilvánosságra hozott adatokra, illetve a kérdésében megnevezett természetes személyre (a miniszterelnök lányára) vonatkozó információ – a névazonosságot kivéve – nem szerepelt a dokumentumokban. A vizsgálat alapján a Hatóság megállapította, hogy a miniszterelnök kiskorú lányára vonatkozóan személyes adatokat Demeter Márta, országgyűlési képviselő hozott nyilvánosságra az Országgyűlésben a nyílt, írásbeli választ igénylő kérdésében.

III.3. Nemzetbiztonsági célú adatkezelésekkel kapcsolatos eljárások

III.3.1. A nemzetbiztonsági szolgálatok közvetlen adatelérése

A nemzetbiztonsági szolgálatokról szóló 1995. évi CXXV. törvény (a továbbiakban: Nbtv.) lehetőséget biztosít a nemzetbiztonsági szolgálatok számára, hogy az állami szervektől, a többségi állami tulajdonú gazdasági társaságoktól, valamint a hitelintézetekről és pénzügyi vállalkozásokról szóló törvényben meghatározott pénzügyi intézményektől közvetlen adatelérés útján igényeljenek adatokat. Ezen túl a Terrorelhárítási Információs és Bűnügyi Elemző Központ a rá vonatkozó különös szabályok szerint jogosult az együttműködő szervekkel való on-line kapcsolattartásra és a közvetlen adatelérést biztosító adatkapcsolatok kiépítésére.

A közvetlen elektronikus adateléréssel történő adatigénylés kapcsán mind technikai, mind jogi téren számos megoldandó kérdés merül föl. Az adatot igénylő nemzetbiztonsági szolgálatnál és az adatszolgáltatásra kötelezett szervezeteknél is rendelkezésre kell állnia a közvetlen adatelérést biztosító informatikai rendszereknek, valamint az azok működéséhez szükséges munkaszervezetnek, belső normáknak stb. Az Nbtv. sajátos szabályokat határoz meg például az elektronikus csatlakozási felület létrehozására és az adatszolgáltatások dokumentálására. Az Nbtv. közvetlen adatelérésre vonatkozó szabályai több éve hatályban vannak, ám az informatikai rendszerek megvalósításának kezdeti lépéseire ismereteink szerint 2018-ban, az igények és a lehetőségek felmérését követően került sor.

A Magyar Bankszövetség 2018-ban többoldalú egyeztetést kezdeményezett a hitelintézetek által közvetlen adatkapcsolat útján történő adatszolgáltatással kapcsolatban felmerülő kérdések tisztázása céljából, amelyen a Bankszövetségen, a Magyar Nemzeti Bankon és a kereskedelmi hitelintézeteken kívül a Hatóság, a Belügyminisztérium, az Igazságügyi Minisztérium és a Nemzetbiztonsági Szakszolgálat (a továbbiakban: NBSZ) magas szintű vezetői vettek részt. Az egyeztetésen elhangzottak konklúziója szerint adottak a törvényi szabályozási feltételek a közvetlen adatkapcsolat létrehozásához az NBSZ és a hitelintézetek között. A résztvevők felkérték a Hatóságot, hogy vizsgálja meg az NBSZ és egy hitelintézet viszonylatában kialakított, közvetlen adatelérést biztosító pilotrendszert abból a szempontból, hogy annak működése összhangban van-e a személyes adatok védelmének szabályaival, különös tekintettel a hitelintézetekre vonatkozó banktitok-védelmi kötelezettségekre. A felkérés alapján a Hatóság több alkalommal vizsgálta a pilotrendszer működését az NBSZ-nél, illetve a fej-

lesztésben résztvevő hitelintézetnél. A pilotrendszer fejlesztése – beleértve az informatikai rendszeren kívül a munkaszervezetet, a hitelintézeti workflow rendszert, a belső normák előkészítését stb. – még folyamatban van. A Hatóság figyelemmel kíséri, és a személyes adatok védelmének érdekében észrevételek, javaslatok tételével segíti a fejlesztések előrehaladását.

III.3.2. A leplezett eszközök alkalmazásának szabályozása

A titkos információgyűjtés a személyes adatok védelmének, valamint a magánélet és (a magánélet kitüntetett helyszíneként) a lakásnak a tiszteletben tartásához való jog drasztikus korlátozását teszi lehetővé, ráadásul úgy, hogy a beavatkozás titkossága miatt az egyénnek a gyakorlatban vajmi kevés esélye van arra, hogy az adatkezeléssel kapcsolatban a jogait érvényesítse, illetve az esetleges jogsértéssel szemben jogorvoslattal éljen, ezért a titkos információgyűjtés szabályozásának és tényleges gyakorlatának ellenőrzése mindenkor ott van a magyar adatvédelmi hatóság fő prioritásai között. 2018-ban lényeges változást hozott e terület újraszabályozása az új büntetőeljárási szabályok rendszerében. Még nem telt el elég idő az új joganyag információs alapjogi hatásainak részleteiben és összefüggéseiben történő értékeléséhez, ezért egyelőre csak az első tapasztalatokról tudunk beszámolni. A személyes adatok védelme szempontjából üdvözlendő, hogy a leplezett eszközökre vonatkozó törvényi szabályozás a korábbiaknál pontosabban definiálja az egyes eszközök és módszerek mibenlétét. A tárgykör újraszabályozása szerencsés módon túllépte a büntető eljárásjog határait, mert az új szabályok megalkotásával párhuzamosan a nemzetbiztonsági célú titkos információgyűjtés korrekciójára is sor került. A titkos információgyűjtés eszközeinek és módszereinek megjelölése immár kitér azokra az úgynevezett eszközcselekményekre, amelyek szükségesek a titkos információgyűjtés végrehajtásához (például az információs rendszer ellenőrzése során a technikai eszköz, illetve elektronikus adat elhelyezése), ám korábban törvényi szabályozás hiányában nem volt egyértelmű az alkalmazásuk jogszerűsége.

III.3.3. Az érintett tájékoztatási joga a rá vonatkozó nemzetbiztonsági ellenőrzési eljárással kapcsolatban

Egy érintett arra vonatkozó panaszt nyújtott be Hatóságunkhoz, hogy a nemzetbiztonsági ellenőrzésre irányuló eljárás állására vonatkozó tájékoztatási kérelmét az ellenőrzést kezdeményező szerv (Honvédelmi Minisztérium Védelemgazdasági Hivatal) nem teljesítette. A Hatóság által feltárt tényállás szerint az érintett nemzetbiztonsági ellenőrzését kezdeményező szerv jogutódlással megszűnt, ezért a nemzetbiztonsági szolgálat főigazgatója nem rendelte el

a nemzetbiztonsági ellenőrzést a törvényben meghatározott határidőn belül, hanem megkereste a kezdeményező szerv jogutódját annak közlése végett, hogy a szervezeti változásokra tekintettel továbbra is szükséges-e az érintett nemzetbiztonsági ellenőrzésének végrehajtása. A kezdeményező szerv jogutódja nem nyilatkozott egyértelműen, ezért az ellenőrzés továbbra sem került elrendelésre. Az érintett eközben abban a hiszemben volt, hogy folyamatban van a nemzetbiztonsági ellenőrzése, noha időközben kérdésessé vált az a jogviszonya, amiatt korábban a nemzetbiztonsági ellenőrzését kezdeményezték.

A Hatóság a vizsgálat során a következőket állapította meg:
Az információs önrendelkezési jog részeként mindenkinek joga van tudni, ki, mikor, milyen célra használhatja fel az ő személyes adatát. E jogosultság gyakorlása csak az Infotv.-ben meghatározottak szerint korlátozható. Az Infotv. – a Módtv.-t megelőzően hatályos – 15. § (1) bekezdése szerint az érintettet megillető tájékoztatási jog része volt az adatkezelés tényéről való tájékoztatás is. Az eljárást kezdeményező szerv jogutódja tudomással bírt arról, hogy sor került-e az érintett nemzetbiztonsági ellenőrzésének lefolytatására, ezért – bár nem a kezdeményező szerv végezte a nemzetbiztonsági ellenőrzést –, a birtokában lévő, az érintettel kapcsolatba hozható információkat illetően az adatkezelő kötelezettségei terhelték, beleértve az érintett tájékoztatásával kapcsolatban az Infotv.-ben előírt kötelezettségeket is. A Hatóság megállapította, hogy az érintettől származó, a személyes adatai kezelésével járó eljárás állására vonatkozó tájékoztatás iránti igényt az érintett Infotv.-ben meghatározott tájékoztatási jogára vonatkozó szabályok keretei között kell elbírálni.

A Hatóság felhívta a nemzetbiztonsági ellenőrzést kezdeményező jogutód szervet, hogy az olyan tájékoztatás iránti kérelmeket, melyek a kérelmező személyes adatának kezelésére vonatkoztathatók, és megválaszolásuk teszi az érintett számára követhetővé személyes adatai felhasználásának útját, az Infotv. szabályai szerint válaszolja meg. Az érintett tájékoztatási jogának érvényesülése csak annyiban korlátozható, amennyiben azt a minősített adatok védelme, illetve a nemzetbiztonsági érdek szükségessé teszi. Az ellenőrzést kezdeményező szerv jogutódja a Hatóság felhívására adott válasza szerint adatkezelési gyakorlatát a Hatóság megállapításainak és felhívásának figyelembevételével fogja folytatni.

A Hatóság a nemzetbiztonsági ellenőrzést végző Katonai Nemzetbiztonsági Szolgálat (a továbbiakban: KNBSZ) eljárását is vizsgálta. Ennek során nem kifogásolta az adatkezelő szerv azon döntését, hogy az ellenőrzés elrendelése helyett óvatosságból megerősítést kért az ellenőrzést kezdeményező szerv jogutódjától az ellenőrzés kezdeményezésének fenntartásáról (noha szigorúan

véve az Nbtv. nem ad lehetőséget az ellenőrzés megkezdésének ilyen indokkal történő késleltetésére), hiszen csak ilyen módon zárhatta ki azt a lehetőséget, hogy esetleg feleslegesen folytasson le egy utóbb feleslegesnek bizonyuló nemzetbiztonsági ellenőrzést. Ez az intézkedés összhangban van az adatminimalizálás elvének érvényesülésével. Ugyanakkor a nemzetbiztonsági ellenőrzés elrendelésének fenti okból történő késedelme a törvényes adatkezelési időkeretek túllépése miatt sértette az érintett tájékoztatási jogának érvényesülését, hiszen a törvényi időkeretektől való eltérés miatt bizonytalanná vált az érintett számára az adatkezelés ténye és az ellenőrzések végrehajtásának időszaka. Ezért a Hatóság felhívta a nemzetbiztonsági ellenőrzés lefolytatására jogosult szervet, hogy ha a jövőben egy nemzetbiztonsági ellenőrzés megkezdésére valamilyen okból a törvényben meghatározott határidőn túl kerül sor, úgy az információs önrendelkezési jog sérelmét elkerülendő a nemzetbiztonsági ellenőrzés megkezdésének tényleges időpontjáról az érintettet hivatalból tájékoztassák. A KNBSZ egyetértett a Hatóság felhívásában foglaltakkal.

III.3.4. Országgyűlési képviselő nemzetbiztonsági ellenőrzésének felülvizsgálata során keletkezett adatok kezelése

Az Országgyűlés Hivatala főigazgató-helyettese arról kért állásfoglalást, hogy közérdekből nyilvános adat-e az a tény, hogy egy országgyűlési képviselő esetében a nemzetbiztonsági ellenőrzéshez kapcsolódó felülvizsgálati eljárás megállapított-e nemzetbiztonsági kockázati tényezőt, vagy sem.

A Hatóság szerint a felülvizsgálati eljárást lefolytató nemzetbiztonsági szolgálat az Nbtv.-ben meghatározott feladat- és hatáskörében eljárva nemzetbiztonsági célú adatkezelést végez, amelyre az Infotv. és az Nbtv. adatvédelmi szabályai vonatkoznak, azonban a felülvizsgálati eljárás eredményét tartalmazó, az Országgyűlés elnökének átadott irat adatkezelője nem a nemzetbiztonsági szolgálat, hanem az Országgyűlés elnöke, ezért az általa végzett adatkezelésre (például a szakvéleményben foglaltak esetleges ismertetése egy országgyűlési bizottsággal, illetve az irat egyes adatainak esetleges nyilvánosságra hozatala) nem az Infotv. hatálya alá tartozó nemzetbiztonsági adatkezelésnek minősül, hanem a GDPR szabályai alkalmazandók rá. A GDPR 6. cikk (1) bekezdés c) és e) pontjai értelmében az adatkezelés jogszerű, ha az az adatkezelőre vonatkozó jogi kötelezettség teljesítéséhez szükséges, illetve ha az közérdekű vagy az adatkezelőre ruházott közhatalmi jogosítvány gyakorlásának keretében végzett feladat végrehajtásához szükséges. A GDPR 6. cikk (2) bekezdése szerint az e rendeletben foglalt, adatkezelésre vonatkozó szabályok alkalmazásának kiigazítása érdekében, a tagállamok az (1) bekezdés c) és e) pontjának való megfelelés

céljából fenntarthatnak vagy bevezethetnek konkrétabb rendelkezéseket, amelyekben pontosabban meghatározzák az adatkezelésre vonatkozó konkrét követelményeket, és amelyekben további intézkedéseket tesznek az adatkezelés jogszerűségének és tisztességességének biztosítására, ideértve a IX. fejezetben meghatározott egyéb konkrét adatkezelési helyzeteket is. A magyar jogrendszerben az Nbtv. 19. § (1) és (7)-(10) bekezdései, valamint a 72/B. § (8) bekezdése tartalmazza azokat a közhatalmi jogosítvány gyakorlásának keretében végzett feladatokat, amelyekhez a nemzetbiztonsági ellenőrzésről, illetve a felülvizsgálatról készült szakvéleményben rögzített, a kockázati tényezőre vonatkozó adat felhasználható a hivatkozott törvényi szabályoknak megfelelően. (Minősített adat esetében a vonatkozó titokvédelmi szabályok betartása mellett.) A GDPR. 85. cikk (1) és (2) bekezdései szerint a tagállamok jogszabályban összeegyeztetik a személyes adatok e rendelet szerinti védelméhez való jogot a véleménynyilvánítás szabadságához és a tájékozódáshoz való joggal, ideértve a személyes adatok újságírási célból, illetve tudományos, művészi vagy irodalmi kifejezés céljából végzett kezelését is. A személyes adatok újságírási célból, illetve tudományos, művészi vagy irodalmi kifejezés céljából végzett kezelésére vonatkozóan a tagállamok kivételeket vagy eltéréseket határoznak meg [...], ha e kivételek vagy eltérések szükségesek ahhoz, hogy a személyes adatok védelméhez való jogot össze lehessen egyeztetni a véleménynyilvánítás szabadságához és a tájékozódáshoz való joggal. A GDPR 86. cikke szerint a közérdekű feladat teljesítése céljából közhatalmi szervek, vagy egyéb, közfeladatot ellátó szervek, illetve magánfél szervezetek birtokában lévő hivatalos dokumentumokban szereplő személyes adatokat az adott szerv vagy szervezet az uniós joggal vagy a szervre vagy szervezetre alkalmazandó tagállami joggal összhangban nyilvánosságra hozhatja annak érdekében, hogy a hivatalos dokumentumokhoz való nyilvános hozzáférést összeegyeztesse a személyes adatok e rendelet szerinti védelméhez való joggal.

A Hatóság szerint a GDPR hivatkozott cikkeivel összhangban van az Infotv. 3. § 6. pontja, amely szerint közérdekből nyilvános adat: a közérdekű adat fogalma alá nem tartozó minden olyan adat, amelynek nyilvánosságra hozatalát, megismerhetőségét vagy hozzáférhetővé tételét törvény közérdekből elrendeli. Az Infotv. 26. § (2) bekezdése szerint közérdekből nyilvános adat a közfeladatot ellátó szerv feladat- és hatáskörében eljáró személy neve, feladatköre, munkaköre, vezetői megbízása, a közfeladat ellátásával összefüggő egyéb személyes adata, valamint azok a személyes adatai, amelyek megismerhetőségét törvény előírja. Ami a nemzetbiztonsági kockázat tényére vagy a kockázatmentességre vonatkozó adatot illeti, olyan országgyűlési képviselő esetében, akinek nemzetbiztonsági ellenőrzését az Nbtv. előírja, ezen adat kétségtelenül az országgyű-

lési képviselő közfeladatának ellátásával összefüggő személyes adat, amely az Infotv. előbb hivatkozott szabályai szerint közérdekből nyilvános.

III.4. Részvétel az adatvédelmi hatóságok közös felügyeleti tevékenységében

III.4.1. A Privacy Shield Egyezmény második éves felülvizsgálata

Az Európai Unió és az Amerikai Egyesült Államok között 2016. július 12-én megkötött adatvédelmi keretegyezmény, az ún. Adatvédelmi Pajzs Egyezmény (Privacy Shield Agreement) második éves felülvizsgálatában a NAIH munkatársa is részt vett. Az Európai Bizottság munkatársaiból és az Európai Adatvédelmi Testület által delegált szakértőkből álló uniós vizsgálócsoport és az Egyesült Államok delegációja Brüsszelben találkozott 2018 októberében, hogy az egyezmény első éves felülvizsgálata óta eltelt időben történt fejleményekről tárgyaljanak és megvitassák a keretegyezményben vállalt kötelezettségekkel kapcsolatban felmerülő kérdéseket.

A felülvizsgálat során a gazdasági és kereskedelmi célú adatkezelésekkel összefüggésben megtárgyalták a felek a tanúsítással és újratanúsítással, megfelelőséggel, a panaszkezeléssel, valamint a fogyasztók tudatosságnövelésével kapcsolatos kérdéseket. A nemzetbiztonsági és bűnüldözési célú adatkezelésekkel összefüggésben pedig megvitatták a jogorvoslati lehetőségekkel, valamint az uniós állampolgárok adatvédelmi panaszainak kivizsgálására létrehozott ombudsmani eljárással kapcsolatos kérdéseket.

A Bizottság és az Európai Adatvédelmi Testület is jelentést készített az egyezmény második éves felülvizsgálatának eredményéről. A Testület jelentésében hangsúlyozta a keretegyezmény fontosságát, ugyanakkor megjegyezte, hogy egy állandó Ombudsman kinevezése nélkül nem garantálható az Európai Uniós állampolgárok számára a hatékony jogorvoslat.

III.4.2. Határok, Utazás és Bűnüldözés szakértői alcsoport (Borders, Travel and Law Enforcement Expert Group – BTLE)

A csoport véleményt készített az elektronikus bizonyítékokhoz való hozzáférésről szóló javaslatcsomagról. Az új szabályok célja, hogy egyszerűbbé és gyorsabbá váljon a rendőri és igazságügyi hatóságok számára a szükséges elektro-

nikus bizonyítékok, például az e-mailek vagy a felhőben tárolt dokumentumok beszerzése, a bűnözőkkel és terroristákkal szembeni nyomozás és büntetőeljárás lefolytatása, valamint azok elítélése céljából. Az új szabályok lehetővé teszik, hogy az uniós tagállamok online és határokon túl is kövessék a nyomravezető információkat, miközben elegendő biztosítékot nyújtanak az összes érintett jogai és szabadságai számára. A javaslatcsomag két részből áll, a közlésre és megőrzésre kötelező európai határozatból, illetve a jogi képviselők a büntetőeljárásban bizonyítékok összegyűjtése céljából történő kinevezéséről szóló határozatból.

A közlésre kötelező európai határozat lehetővé teszi, hogy egy tagállam igazságügyi hatósága – az adatok helyétől függetlenül – közvetlenül igényeljen elektronikus bizonyítékot bármely, az Unióban szolgáltatásokat kínáló és más tagállamban letelepedett vagy képviselettel rendelkező szolgáltatótól, amely köteles 10 napon belül, veszélyhelyzet esetén pedig 6 órán belül válaszolni. A megőrzésre kötelező európai határozat lehetővé teszi, hogy valamely tagállam igazságügyi hatósága konkrét adatok megőrzésére kötelezzen bármely, az Unión belül szolgáltatásokat kínáló és egy másik tagállamban letelepedett vagy képviselettel rendelkező szolgáltatót, annak érekében, hogy a hatóság ezt az információt később kölcsönös jogsegély, európai nyomozási határozat vagy közlésre kötelező európai határozat útján kikérhesse. A határozatok kizárólag büntetőeljárás keretében bocsáthatók ki, és azokra valamennyi büntetőjogi eljárási biztosíték alkalmazandó. Az új szabályok garantálják az alapvető jogok erőteljes védelmét és jogbiztonságot nyújtanak a vállalkozásoknak és szolgáltatóknak.

A csoport kidolgozta a szabadságon, biztonságon és jog érvényesülésén alapuló térség nagyméretű IT-rendszereinek ellenőrzési módszereiről szóló tanulmányt, amely a feladatkörök tekintetében három csoportra osztja az IT-rendszereket:

1. határok, menedékjog, migráció (SIS II, VIS, Eurodac, EES, ETIAS)
2. rendőri és igazságügyi együttműködés (TCN-ECRIS, Eurojust, EPPO, Customs, Europol)
3. belső piac (IMI)

Az így létrejövő koordinált ellenőrzés keretei között a tagállamoknak és az Európai Adatvédelmi Biztosnak évente legalább két alkalommal kellene ülést tartania és évente jelentést készítenie az elvégzett munkáról. A feladatok nagyrészt megegyeznének a már működő ellenőrző csoportok feladataival.

A csoport elkészítette a Privacy Shield Egyezmény második éves felülvizsgálatáról szóló, az Európai Adatvédelmi Testület által írt jelentésnek a nemzetbiz-

tonsági és bűnüldözési célú adatkezeléssel kapcsolatos részét, amely egyebek mellett a független Ombudsman kinevezésének fontosságát hangsúlyozza (tekintettel arra, hogy az uniós állampolgárok adatvédelmi panaszait kivizsgálni hivatott ombudsmani tisztséget továbbra is egy megbízott Ombudsman látja el).

Az Európai Unió és Japán közötti, személyes adatok védelméről szóló tárgyalások lezárását követően a Bizottság elindította a megfelelőségi határozat elfogadásának eljárását, melynek részeként a Bizottság a Testülettől kért véleményt. Ennek a GDPR 70. cikk (1) s) szerinti véleménynek a kidolgozására a Bizottság a Nemzetközi Adattovábbítási Szakértői Csoportot (ITS) és a Határok, Utazás és Bűnüldözés Szakértői Csoportot (BTLE) kérte fel. A testületi vélemény kibocsátását követően 2019 elején az Európai Bizottság elfogadta Japán vonatkozásában a megfelelő védelmi szintről szóló határozatát.

III.4.3. A Schengeni Információs Rendszer Adatvédelmét felügyelő munkacsoport (SIS II SCG)

A Schengeni Információs Rendszer (SIS II) Európa legnagyobb informatikai rendszere, amely a térség belső határainak eltörléséből eredő kockázatokat hivatott kezelni. A SIS II rendszer fejlesztésének, és új adatkategóriák bevezetésének köszönhetően a rendszer hatékonyan veszi fel a harcot a terrorizmus veszélyeivel és megfelelő eszköznek bizonyul a határon átnyúló bűnüldözést illetően. A Schengeni Információs Rendszert érintően a Bizottság módosította rendeletét a rendőrségi és igazságügyi együttműködés, a határellenőrzés és a harmadik országbeli állampolgárok illegális tartózkodásának visszaszorítása érdekében, új adatkategóriákat vezetett be, valamint kiterjesztette a tárgyakra vonatkozó figyelmeztető jelzések alapjául szolgáló tárgyak körét a hamis okmányokra, nagy értékű azonosítható tárgyakra és informatikai eszközökre. A beutazási és tartózkodási tilalmat elrendelő figyelmeztető jelzések SIS II-be való rögzítése kötelezővé vált.

A 2013. április 9-én hatályba lépett Schengeni Információs Rendszer második generációjának (SIS II) létrehozásáról, működtetéséről és használatáról szóló 1987/2006/EK számú európai parlamenti és tanácsi rendelet alapján működő koordinációs ellenőrző csoport (Supervision Coordination Group) 2018-ban is folytatta munkáját. A SIS SCG elfogadta a rendszerhez történő hozzáférések nemzeti szintű naplózásával kapcsolatban készített munkaanyagot. A munkacsoport ajánlásokat fogalmazott meg a kötelező naplózással, a logok teljességével és minimalizálásával, a felhasználók beazonosításával, a naplóbejegyzésekhez való hozzáférések szabályozásával, képzések tartásával, a megőrzési idők ér-

vényesítésével, a naplóbejegyzések automatikus törlésével, a távoli hozzáféréssel, a biztonsággal és a biztonsági másolatokkal összefüggésben.

Az Európai Bizottság által közzétett, az EU nagyméretű IT rendszereinek interoperabilitását megteremteni kívánó javaslatcsomaggal kapcsolatban az Európai Adatvédelmi Biztos véleményt adott ki, a munkacsoport pedig megfogalmazott egy levelet, amelyben egyetértett a véleményben foglaltakkal, valamint kiemelte, hogy a javaslatok nem a rendszerek interoperabilitásáról, hanem sokkal inkább a rendszerek összekapcsolásáról szóltak. A munkacsoport álláspontja szerint nem lehet megfelelően véleményt alkotni egy javaslatcsomagról úgy, hogy az általa érintett rendszerek átalakítás előtt/alatt állnak.

A Schengeni Információs Rendszert üzemeltető eu-LISA képviselője a központi rendszer fejlesztése kapcsán beszámolt arról, hogy a központi rendszer kapacitását folyamatosan növelik. 2018 elején több, mint 76 millió jelzés volt a rendszerben, ami 7%-os emelkedést jelent az előző évhez viszonyítva.

A Hatósághoz 2018-ban 17 alkalommal fordultak a SIS II-ben tárolt személyes adatok kezelésével kapcsolatban. Ezen megkeresések többsége az érintetti jogok gyakorlásával kapcsolatos kérdés volt (tájékoztatás kérés, törlés), amely esetekben a Hatóság általános tájékoztatást nyújtott a beadványozónak a SIRENE Irodához fordulás jogáról és menetéről, valamint a Hatóság által indítható felülvizsgálati eljárásról. A SIRENE Iroda (Supplementary Information Request at National Entry) feladata, hogy összehangolja a SIS-ben a figyelmeztető jelzésekkel kapcsolatos válaszokat, és biztosítsa, hogy megtörténjen a megfelelő intézkedés, ha egy személy, akinek a schengeni térségbe való belépését elutasították, ismételten megpróbál belépni a térségbe, vagy ha lopott gépjárművet vagy azonosító okmányt foglalnak le.

III.4.4. A Vízuminformációs Rendszer Adatvédelmét felügyelő munkacsoport (VIS SCG)

A Vízuminformációs Rendszert – a Schengeni Információs rendszer és az Eurodac adatbázisokkal együtt – a szabadságon, biztonságon és jogérvényesülésen alapuló térség nagyméretű IT-rendszereinek üzemeltetési igazgatását ellátó európai ügynökség, az eu-LISA kezeli. A Vízuminformációs Rendszer célja, hogy elősegítse a közös vízumpolitika végrehajtását, a konzuli együttműködést és a központi vízumhatóságok közötti konzultációt. A Vízuminformációs Rendszert használják a schengeni térség konzulátusain, ahol vízumot állítanak ki, valamint a határátkelőhelyeken, ahol a határőrök ellenőrzik a biometri-

kus vízummal rendelkező személyek személyazonosságát. A VIS célja, hogy segítségével beazonosíthatóak legyenek az olyan személyek, akik nem teljesítik a tagállamok területére történő beutazás, az ott tartózkodás vagy a letelepedés feltételeit. A Vízuminformációs Rendszerhez hozzáférnek ezért a bűnüldöző hatóságok, menekültügyi hatóságok, valamint az Europol is.

A Vízuminformációs Rendszer adatvédelmét felügyelő munkacsoport (VIS SCG) 2018-ban elkészítette a véleményét a 767/2008/EK rendelet (VIS rendelet), a 810/2009/EK rendelet (Vízumkódex), a 2017/2226/EU rendelet (határregisztrációs rendszer létrehozásáról szóló rendelet), a 2016/399/EU rendelet (a Schengeni határellenőrzési kódex), a 2004/512/EK határozat (a VIS létrehozásáról szóló határozat) módosításáról, valamint a 2008/633/IB határozat (VIS hozzáférésről szóló határozat) hatályon kívül helyezéséről szóló javaslatról. A közös uniós vízumpolitika új célkitűzései között szerepel a rövid távú tartózkodásra jogosító vízumkérelmek feldolgozásának javítása, a VIS adatkategóriák kiterjesztése, a menekültügyi hatóságok VIS adatokhoz való hozzáférésének kiterjesztése, a VIS adatok harmadik országok és nemzetközi szervezetek részére történő továbbításának megkönnyítése, az ujjlenyomatvétel alsó korhatárának 6 évre csökkentése, kötelező arckép készítés a kérelem benyújtásakor, valamint a VIS-hez való bűnüldözési célú hozzáférés kiterjesztése.

A Hatósághoz 2018-ban 5 alkalommal érkezett megkeresés a Vízuminformációs Rendszerrel kapcsolatban, amelyek általános tájékoztatás keretein belül kerültek megválaszolásra, felülvizsgálati eljárást a Hatóság egyetlen esetben sem indított.

III.4.5. Europol Cooperation Board

A 2018-ban tárgyalt egyik ügy az European Tracking Solution (ETS) elnevezésű, kidolgozás, megvitatás alatt álló projekt, amely közel valós idejű, határon átnyúló helymeghatározásra vonatkozó adatcserét tenne lehetővé a tagállamok között titkosított csatornán keresztül.

III.4.6. Eurodac Rendszer Adatvédelmét felügyelő munkacsoport (Eurodac SCG)

A 603/2013/EU rendelettel létrejött az Eurodac rendszer, amely lehetővé teszi a Dublini rendeletet alkalmazó országok számára, hogy az Eurodac rendszerben tárolt ujjlenyomatok összehasonlításával megállapítsák, hogy az egyik tag-

államban illegálisan tartózkodó és menedékjogot kérő külföldi állampolgár kért-e korábban menedékjogot másik tagállamban. Az Eurodac rendszer segítségével a tagállamok megállapítják, hogy melyik tagállam köteles a menekültügyi eljárás lefolytatására. Az Eurodac rendszerbe adatokat küldő tagállamoknak a személyes adatok védelme érdekében biztosítaniuk kell, hogy az ujjlenyomatok levétele, valamint az adatok feldolgozásával, továbbításával, tárolásával vagy törlésével kapcsolatos műveletek jogszerűek legyenek. Az Eurodac adatkezeléseket az Európai Adatvédelmi Biztos felügyeli, együttműködve a nemzeti felügyeleti hatóságokkal (Eurodac SCG).

Az Eurodac Rendszer adatvédelmét felügyelő munkacsoport elkészítette az állampolgárságot szerzett személyek ujjlenyomatainak Eurodac-ból való törlésével kapcsolatos munkaanyagot, amely kapcsán elmondható, hogy nem egységes a tagállamok gyakorlata a törlést illetően, szükséges az egységes alkalmazás érdekében további követelményeket megfogalmazni. Az eu-LISA képviselője az Eurodac SCG ülésén beszámolt az informatikai rendszert érintő legújabb fejleményekről. 2018 első félévében körülbelül 5,2 millió ujjnyomatot tárolt a rendszer, melynek kapacitása 7 millió (de tervezik a növelését 10 millióra). A tranzakciós hibák fő oka jellemzően az ujjnyomatok rossz minősége. A menedékkérők és a tagállamok külső határainak illegális átlépése miatt elfogott személyektől levett ujjlenyomatok száma csökkent, a valamely tagállam területén illegálisan tartózkodó személyektől levett ujjlenyomatok száma nőtt.

IV. Információszabadság

A fejezet elején – a legfontosabb alkotmánybírósági döntések mellett – több információszabadságot érintő jelenségről, fejleményről szeretnénk hírt adni. A tavalyi beszámolóban már történt utalás arra, hogy az információszabadság ügyekre is hatással van a GDPR. Az Infotv. vonatkozó szabályait a 2018-as módosítás ugyan közvetlenül nem érintette, de egyre nagyobb számban fordulnak elő olyan ügyek, panaszok, melyek a két információs jog „közös halmazába" tartoznak. Különösen igaz ez az interneten szabadon terjedő megnyilvánulások esetében. Amennyiben ugyanis a személyes adatok védelméhez való jog mellett valamely más, az adatok nyilvánosságával összefüggő alapvető jog – általában a közérdekű vagy közérdekből nyilvános adatok nyilvánosságához vagy a sajtó és véleménynyilvánítás szabadságához fűződő alapvető jogok – együttes vagy egymásra figyelemmel történő érvényesüléséről van szó, akkor az alkotmányos jogok esetleges kollízióját valamilyen módon fel kell oldani. Döntést kell hozni arról, hogy melyik érdek védelme szolgálja jobban a közérdeket, és ez a döntés milyen konkrét jogi rendelkezésekre, illetve jogelvekre vezethető vissza. Előfordulhat, hogy a jogaikban sértett személyek közszereplők (akik pozíciójuk, a helyi vagy országos közéletben betöltött funkciójuk vagy önkéntes szerepvállalásuk okán közvélemény-formáló szereplővé lépnek elő, ugyanakkor személyes adataikat, magánszférájukat mások által veszélyeztetve érzik). Egyes esetekben azonban éppen a közszereplőnek minősülő közfeladatot betöltő személyek (például polgármesterek) választanak helytelen eszközt a jogsértések – jellemző módon az internet nyilvánossága előtt történő – „leleplezésére", mások pellengérre állítására.

A Hatósághoz 2018 végén több beadvány is érkezett a közösségi oldalakon, illetve a különböző sajtóorgánumokban megjelent, tömegdemonstrációkon készült és az azokon megvalósított cselekményeket dokumentáló képfelvételek nyilvánosságra hozatalával összefüggésben. Tömegrendezvényeken természetesen magánszemélyek, országgyűlési képviselők és sajtónak nem minősülő szervezetek is készíthetnek fényképfelvételeket, és bár rájuk nem vonatkoznak a „sajtótörvény" rendelkezései, a képfelvételek készítése és felhasználása során nekik is be kell tartaniuk a GDPR, az Infotv. és a Polgári Törvénykönyv rendelkezéseit. A képfelvételek nem személyes célokra történő felhasználásának mint adatkezelésnek a jogszerűségét e jogi rendelkezések számos követelményhez kötik, így kiemelendő a jogszerű adatkezelési cél és az ehhez kapcsolódó megfelelő jogalap meghatározása. (NAIH/2018/7556/V, NAIH/2018/7547/V)

A NAIH nemzetközi szerepvállalása 2018-ban az információszabadság területén is intenzívebbé vált, ennek legfontosabb eredménye, hogy 2018. november

26-27-én Budapesten került megrendezésre először az az „esetjogi gyakorlatok" bemutatását célzó nemzetközi találkozó („FOI Case Handling Workshop"), mely a közérdekű adatok nyilvánosságát felügyelő nemzeti intézmények munkatársait gyűjtötte egybe 11 országból (Dél-Afrikai Köztársaság, Marokkó, Németország, Egyesült Királyság, Albánia stb.). 16 prezentáció adta az alapját a megbeszéléseknek, kifejtve például a felügyeleti szervek számára rendelkezésre álló hatásköri elemeket, a bírósági jogérvényesítés eszközeit, a közzétételi listák rendszerét és a más alkotmányos jogokkal való kollízió eseteit.

A bírósági jogalkalmazás egységességének, a jogbiztonság erősítésének céljával a Kúrián 2018 végén megszületett *„A közérdekű adatok kiadásával kapcsolatos perek"* bírósági gyakorlatával foglalkozó joggyakorlat-elemző csoport összefoglaló véleménye. Az elemző csoportok vezetői és tagjai a Kúria bírái, de külső szakértőként a NAIH is meghívást kapott. A két éves elemző munka eredményeként az összefoglaló vélemény a bíróságok által a Kúria részére megküldött határozatok elemzését tartalmazza, külön tárgyalva az anyagi jogi és eljárásjogi észrevételeket, javaslatokat. (e megállapítások pl.: bank- és adótitokra való hivatkozás esetében a bírói gyakorlat nem fogadja el a kiterjesztő értelmezéseket, vagy, ha az adatigénylő nem tudja kellő pontossággal meghatározni az igényelt adatok körét – az áttekintett ítéletek tanúsága szerint – a bíróságok az adatigénylő irányába jóhiszeműen járnak el, hiszen ennek oka éppen a per tárgyát képező információk hiánya.)

2018-ban megkezdődött a közszféra információinak további felhasználásáról szóló 2003/98/EK európai parlamenti és tanácsi irányelv (a továbbiakban: PSI irányelv) felülvizsgálata. A közszféra hatalmas adatmennyiséget állít elő (pl.: meteorológiai adatok, digitális térképek, jogszabályok stb.), ezek az adatok értékes forrásai a digitális gazdaságnak. Az Európai Bizottság értékelő jelentésében megállapította, hogy számos területen további intézkedés szükséges: ezek közé tartozik a dinamikus adatokhoz történő valós idejű hozzáférés biztosítása megfelelő technikai eszközök révén, a nagy értékű nyilvános adatok további felhasználás céljából való rendelkezésre bocsátásának növelése, a kizárólagosságot biztosító megállapodások új formáinak visszaszorítása, a határköltség szerinti díjszámítás elve alóli kivételek korlátozása. A NAIH is részt vesz a PSI irányelv módosításával kapcsolatos magyar álláspont kialakításában. A Hatóság tapasztalatai szerint Magyarország felkészültsége a nyílt hozzáférésű adatok *(„open data")* tekintetében a múltban nem minősült sikeresnek; annak ellenére, hogy az irányelv átültetése a hazai jogrendbe megtörtént, annak végrehajtása tekintetében számos hiányosság merül fel.

IV.1. Alkotmánybírósági joggyakorlat

2018-ban az Alkotmánybíróság több jelentős döntést hozott információszabadság tárgykörben, ezeket röviden az alábbiakban ismertetjük:

- 3077/2017. (IV. 28.) AB határozat (a négy éven túli peres ügyek listája): Az Alkotmánybíróság az alkotmányjogi panaszt elutasította, mert a polgári peres eljárásban félként (alperes vagy felperes) résztvevő jogi személy neve nem közérdekű adat, így az adatkezelő (bíróság) nem kötelezhető az adat kiadására.
- 3/2018. (IV. 20.) AB határozat (az MNB által létrehozott alapítványok részéről természetes személyek számára nyújtott támogatások átláthatósága): A kétséget kizáróan közpénzzel gazdálkodó és közfeladatot ellátó alapítványok pályázatán nyertes pályázók nevének nyilvánosságtól való elzárása jogalkotói mulasztásra vezethető vissza, mert a közpénzekből nyújtott támogatások átláthatóságáról szóló 2007. évi CLXXXI. törvény személyi hatálya nem terjedt ki az adatkezelőre, konkrét törvényi felhatalmazás hiányában pedig a személyes adatok nem ismerhetők meg.
- 3133/2018. (IV. 19.) AB határozat (széleskörű adatigény teljesítésének szempontjai): A Nemzeti Egészségfejlesztési Intézet az ún. pszichoaktív anyaggá minősítés során keletkezett vizsgálati dokumentációk kikérését elutasította az Infotv. 27. § (5) bekezdésére hivatkozva. A Kúria hangsúlyozta ítéletében, hogy *„a kiadni kért adatok speciális mivoltára figyelemmel valóban indokolt az egyébként kivételes nyilvánosság-korlátozás. A Kúria szerint is fennáll annak reális lehetősége (veszélye), hogy a kibontakozó nyilvános szakmai vita az adott igen érzékeny területen óhatatlanul külső nyomás alá helyezi a szakmai vélemények kidolgozásában érintett személyeket és ez valóban alkalmas lehet arra, hogy az alperesi közfeladatot ellátó szerv törvényes működési rendjét vagy feladat- és hatáskörének illetéktelen külső befolyástól mentes ellátását, így különösen az adatot keletkeztető álláspontjának a döntések előkészítése során történő szabad kifejtését veszélyeztesse. A kábítószerek, illetve az azzal azonosan minősülő pszichotróp, vagy pszichoaktív anyagok megítélése olyan kivételesen speciális terület, amelyek nemcsak legális érdekek ütközésével járhatnak, valamint figyelemmel kell lenni arra is, hogy a döntést előkészítő munka eredménye rendszeresen nyilvános jogszabályi rendelkezésekben egyébként is manifesztálódik, továbbá az érintett anyagok listája folyamatosan változik, bővül, átalakul.”*

  Az Alkotmánybíróság az alkotmányjogi panaszt elutasította és kiemelte, hogy az indítványozó által előterjesztett adatigény voltaképpen határtalan mennyiségű, pontosan nem behatárolható, s alapvetően döntés-elő-

készítő iratokba foglalt információ megszerzésére irányult, így helyes volt az a bírói jogértelmezés, amely az adatigény által lefedett teljes döntés-előkészítő folyamatra egészében az ún. automatikus nyilvánosságkorlátozás szabályát alkalmazta.

- 3254/2018. (VII. 17.) AB határozat (minisztériumi államtitkár külföldi útjainak nyilvánossága): a Miniszterelnökséget vezető államtitkár két konkrét külföldi kiküldetése kapcsán az adatigénylő a tárgyalások tárgya (mely közérdekű adatként kiadásra került) mellett rákérdezett a tárgyalópartnerek nevére is.

  Az Alkotmánybíróság az alkotmányjogi panaszt elutasította arra való hivatkozással, hogy itt személyes adatokról van szó, melyek nyilvánossága csak akkor merülhet fel, ha ezeket konkrét törvényi rendelkezés közérdekből nyilvánosnak minősíti (ide nem értve az Infotv. 26. § (2) és 27. § (3a) bekezdését), vagy az érintett a személyes adatai nyilvánosságra hozatalához hozzájárul.

IV.2. Helyi közügyek – az önkormányzati széles körű nyilvánosság megteremtésének kérdései

A Magyarország helyi önkormányzatairól szóló 2011. évi CLXXXIX. törvény (a továbbiakban: Mötv.) 2. §-a a helyi önkormányzás alapvető feltételeként tekint a nyilvánosság valós és hatékony megvalósulására. Az önkormányzati működés során tehát elsődleges szempont, hogy a széles körű nyilvánosság alapelve mindenkor megfelelően érvényesüljön és azt a közösség tagjai egyaránt szem előtt tartsák. A gyakorlatban azonban az önkormányzatok információszabadsághoz való viszonya igen változatos képet mutat. Egyes települések hivatalai naprakészen és „alapjogi szemlélettel" viszonyulnak az adatigénylésekhez, sok helyen azonban nem kellően felkészültek és esetleg még mindig zaklatásként élik meg az állampolgári adatigényléseket.

A NAIH a vizsgálatai, illetve a konzultációk során igyekszik egyfajta mediátorként is eljárni a felek között és számos esetben segíti a polgármesterek, helyi képviselők, jegyzők, igazgatási ügyintézők, önkormányzati tulajdonú társaságok tisztségviselőinek munkáját a jogszabályok helyes értelmezésében. (2018. április 20-án a Miniszterelnökség Területi Közigazgatásért Felelős Államtitkárságának felkérésére a Megyei Kormányhivatalok belső adatvédelmi felelősei részére megtartott szakmai értekezleten, 2018. november 21-én a Hajdú-Bihar Megyei Kormányhivatal által jegyzőknek szervezett szakmai napon munkatársunk előadást tartott az önkormányzati nyilvánosság kérdéseiről.)

IV.2.1. Az adatigénylések teljesítése

2019-ben általános önkormányzati választások lesznek hazánkban, nyilvánvaló, hogy az önkormányzatok által végzett tevékenység és az arra vonatkozó közadatok még inkább az érdeklődés középpontjába kerülnek, melyre az adatkezelőknek előre fel kell készülniük. Az információszabadság biztosításának elengedhetetlen feltétele, hogy a szerv vezetője időszakonként áttekintse a rendelkezésre álló erőforrásokat és azok átszervezésével, racionalizálásával, bővítésével felkészítse a szervezetet a megváltozott igények által támasztott követelményeknek való megfelelésre.

A Hatóság joggyakorlata szerint az információszabadság biztosítása szempontjából a *képviselőtestület szervei* egységet alkotnak, vagyis nem tekinthetőek külön-külön is közfeladatot ellátó szerveknek és nem hivatkozhatnak alappal arra, hogy az önkormányzatot érintő adatigénylést nem hozzájuk kellett volna benyújtani (például: vagyonnyilatkozatok megismerése, európai uniós pályázatok adatai tárgykörben). Ha az adatigénylés teljesítésének kötelezettségéről belső szabályzat rendelkezik, akkor az annak elbírálására és teljesítésére köteles és jogosult személyhez az adatigénylést belső eljárás keretében rövid úton továbbítani kell. Emellett a jegyzőnek kitüntetett szerepe van a kérelmek koordinálásában, jogszerű és szakszerű teljesítésében, illetve a megalapozott, a törvényesség talaján álló elutasításában.

IV.2.2. A helyi képviselők jogai

Régóta fennálló és kifejezetten gyakori értelmezési dilemma kapcsolódik az *önkormányzati képviselőket megillető tájékozódási jog* hatályának kérdésköréhez, mely csak az Mötv.-Infotv.-GDPR rendelkezéseinek együttes értelmezésével oldható fel. Az önkormányzati képviselő önálló feladat- és hatáskörrel nem rendelkezik, *„képviselői munkája”* elsősorban a képviselő-testület és bizottságai döntési kompetenciájába tartozó egyes ügyek döntéseinek előkészítésében, végrehajtásuk szervezésében és ellenőrzésében való részvételt jelenti. Amennyiben a képviselő nem az Mötv. szerinti képviselői tájékoztatáshoz való jogával, hanem a közérdekű adatok megismerésének jogával kíván élni, akkor az Infotv. szabályai alkalmazandóak az adatkérés teljesítésénél, itt azonban semmilyen plusz jogosítvány nem illeti meg a képviselőt más állampolgárhoz képest, így ebben a jogviszonyban ők sem ismerhetnek meg adótitkot, a szociális nyilvántartás adatait, köztisztviselők, önkormányzati cégek munkavállalóinak személyi anyagait vagy egyéb védett adatot. Kivétel: ha külön törvényi rendelkezés ezeket az adatokat közérdekből nyilvánosnak minősíti

vagy törvény, illetve törvény felhatalmazása alapján megalkotott önkormányzati rendelet felhatalmazza a képviselőt valamely adatfajta megismerésére közfeladatának ellátása érdekében, illetve az önkormányzat képviselő testülete megbízza valamely önkormányzati hatáskörbe tartozó feladat tervezésével, szervezésével, ellenőrzésével valamely bizottság tagjaként, esetleg egyénileg (például tanácsnoki feladatok ellátásával). Ilyen esetben a célhoz kötött adatkezelés és az adattakarékosság elvének betartásával szükségessé válhat, hogy a jogszabályban felsorolt személyes adatokat (adatfajtákat) kezelje a képviselő.

IV.2.3. A foglalkoztatottak közérdekből nyilvános adatai

Az *önkormányzattal foglalkoztatási jogviszonyban állók közérdekből nyilvános* adataival szintén sokat foglalkozunk. A nyilvánosság szempontjából különböző foglalkoztatási kategóriákat kell megkülönböztetni azzal, hogy a szerv feladat- és hatáskörében eljáró személynek a közfeladat ellátásával összefüggő egyéb személyes adata is nyilvános, ahogy ezt több NAIH állásfoglalás, alkotmánybírósági határozat, a Kúria és a Fővárosi Ítélőtábla ítéletei is egybehangzóan megállapítják (ez alapján például az adott adatigényt mérlegelve a feladatkörrel összefüggő és ezért közérdekből nyilvános személyes adat lehet az iskolai végzettség vagy a túlórára vonatkozó információ is annak ellenére, hogy a konkrét törvényi felsorolás nem tartalmazza ezeket).

Legtágabb a kör a *köztisztviselők* esetében. A közszolgálati tisztviselőkről szóló 2011. évi CXCIX. törvény (a továbbiakban: Kttv.) 179. §-a alapján közérdekből nyilvános adat a név, állampolgárság, a foglalkoztató államigazgatási szerv neve, a szolgálati jogviszony kezdete, a besorolási adatok, a munkakör, a vezetői kinevezés időpontjai, a címadományozás és az illetmény. Fontos, hogy az Infotv. a közérdekből nyilvános személyes adatok esetében különbséget tesz az adatok megismerhetősége és az adatok terjesztése, illetve nyilvánosságra hozatala között, így például legfeljebb egy évig lehet az elektronikus közzétételi felületként szolgáló internetes honlapon közzé tenni a közérdekből nyilvános személyes adatokat tartalmazó nyilvános testületi ülésre benyújtott képviselő-testületi előterjesztéseket.

Az önkormányzati intézményeknél foglalkoztatott közalkalmazottaknál a közalkalmazottak jogállásáról szóló 1992. évi XXXIII. törvény (a továbbiakban: Kjt.) értelmében közérdekből nyilvános adat a munkáltató megnevezése, a közalkalmazott neve, beosztása, továbbá a besorolására vonatkozó adat (vagyis a számszerű illetmény nem).

A *munkavállalók* adatai ugyanakkor nem közérdekből nyilvános, hanem védendő személyes adatok. A munkaszerződések anonimizálva (személyazonosításra alkalmatlan módon), illetve a munkavállalók adatai összesített formában, statisztikai adatként adhatók ki. A Munka Törvénykönyve nem teszi lehetővé, hogy az önkormányzat tulajdonában álló gazdasági társaság munkavállalóinak személyes adatait akár a képviselőtestülethez továbbítsák, mivel a munkaviszony fennállása tekintetében a képviselőtestület harmadik személynek minősül. Helytelen az az adatkezelési gyakorlat, hogy a bérjegyzéket a munkavállalók adatainak továbbításával, személyazonosításra alkalmas módon adják át a közpénzből nyújtott támogatás elszámolása érdekében. Meg kell azonban jegyezni, hogy a köztulajdonban álló gazdasági társaságok takarékosabb működéséről szóló 2009. évi CXXII. törvény 2. §-a e társaságok tisztségviselői esetében konkrét adatnyilvánossági és elektronikus közzétételi kötelezettségeket ír elő.

IV.2.4. Közpénzek, költségvetési támogatások átláthatósága

A közpénzből finanszírozott megbízási szerződések, költségvetési támogatások átláthatóságát szolgálja az Infotv. 27. § (3) bekezdése, nevesítve a helyi önkormányzatokat is és *ex lege* közérdekből nyilvános adatnak minősítve a költségvetési, illetve az európai uniós támogatás felhasználásával, az önkormányzati vagyon kezelésével kapcsolatos adatokat. Az ilyen jogviszonyba belépő másik (nem állami) szerződő felet pedig a törvény alapján – erre irányuló igény esetén – bárki felé tájékoztatási kötelezettség terheli. Így a költségvetési támogatások kedvezményezettjeinek a nevére, a támogatási program megvalósítási helyére vonatkozó adatok, illetve az államháztartás pénzeszközei felhasználásával, az államháztartáshoz tartozó vagyonnal történő gazdálkodással összefüggő, ötmillió forintot elérő vagy azt meghaladó értékű árubeszerzésre, építési beruházásra, szolgáltatás megrendelésre, stb. vonatkozó szerződések megnevezése (típusa), tárgya, a szerződést kötő felek neve és az ott felsorolt további adatok közérdekből nyilvánosak és kötelezően közzéteendőek. A természetes személyek neve a fenti jogviszonyok tekintetében közérdekből nyilvános adatnak minősül. A költségvetési támogatásnak nem minősülő adatok esetében a természetes személyre vonatkozó adatok védelmet élveznek. (NAIH/2018/3091/2/V)

IV.2.5. Vagyonnyilatkozatok

A *polgármesterek, alpolgármesterek, önkormányzati képviselők vagyonnyilatkozat*ának tartalma 2018-ban is jelentős közérdeklődésre tartott számot. Az Mötv. 39. § (3) bekezdése alapján a vagyonnyilatkozatot a szervezeti és működési szabályzatban erre kijelölt bizottság (vagyonnyilatkozat-vizsgáló bizottság) tart-

ja nyilván és ellenőrzi. Az önkormányzati képviselő vagyonnyilatkozata – az ellenőrzéshez szolgáltatott azonosító adatok kivételével – közérdekből nyilvános információ, ugyanakkor ismét fel kell hívnunk a figyelmet arra, hogy ezek az adatok a célhoz kötött adatkezelés elvének tiszteletben tartásával terjeszthetőek, illetve a honlapon történő közzétételre külön rendelkezések irányadóak. Az Infotv. 1. számú melléklete jelenleg nem rendelkezik arról, hogy az önkormányzati képviselők vagyonnyilatkozatát elektronikus úton kötelezően közzé kellene tenni, de semmilyen rendelkezés nem tiltja, hogy a helyi önkormányzatok ezt egyedi közzétételi lista útján mégis megtegyék. (NAIH/2018/4196/V, NAIH/2018/1256/V).

IV.2.6. A helyi önkormányzatok és a digitális nyilvánosság

A széleskörű nyilvánosság megteremtése a XXI. században, digitális formában, az internetes közzététellel valósulhat meg a legköltséghatékonyabban és leginkább polgárbarát módon *(elektronikus információszabadság)*. *A „helyben szokásos közzétételi mód"* tartalma és követelménye véglegesen átalakult. Az „*analóg*", hagyományos közzétételi formák, mint a hirdetőtábla, hivatalos lap, helyi televízió stb. közlési módjaival párhuzamossá vált az internetes közzététel, mely néhány évtizeden belül bizonyosan szinte kizárólagossá válik majd. Az önkormányzatoknak az információszabadság szempontjából talán ez a legnagyobb kihívás, amely a Hatósághoz tett bejelentések jelentős részében is megmutatkozik.

Az Állami Számvevőszék *„Az önkormányzatok gazdasági társaságai — Az önkormányzatok többségi tulajdonában lévő gazdasági társaságok gazdálkodásának ellenőrzése"* program keretében több alkalommal is bejelentéssel fordult a Hatósághoz egyes önkormányzatok, illetve önkormányzati tulajdonban lévő gazdasági társaságok elektronikus közzétételi kötelezettségének hiányos teljesítése miatt, hiszen a köztulajdonban álló gazdasági társaságok takarékosabb működéséről szóló 2009. évi CXXII. törvény értelmében közérdekből nyilvános adatok a vezető tisztségviselők, felügyelő bizottsági tagok, valamint az önálló cégjegyzésre vagy a bankszámla feletti rendelkezésre jogosult munkavállalók adatai. Az önkormányzati társaságok a NAIH felszólításának megfelelően kivétel nélkül pótolták a mulasztást. (NAIH/2018/1224/V, NAIH/2018/1394/V, NAIH/2018/1597/V, NAIH/2018/1644/V)

Az önkormányzatoknak nincs kötelezettsége arra, hogy saját honlapot tartsanak fenn, de arra igen, hogy az általuk választott módon és helyen a közérdekű adataikat az Infotv.-nek megfelelően interneten közzé tegyék (kozadat.hu, kozadattar.hu). A Hatóság gyakorlata alapján, amennyiben az önkormányzat rendelkezik

saját honlappal is, úgy az állampolgárok tájékozódását úgy szolgálják megfelelően, ha ott is közzéteszi az Infotv. szerint kötelezően közzéteendő adatokat. Az Infotv. 1. számú melléklete szerinti közzétételi lista, továbbá a közadattár adattartalmának összeállításához *„segítséget nyújt”* a 305/2005. (XII. 25.) kormányrendelet és a 18/2005. (XII. 27.) IHM rendelet. Fontos, hogy a központi honlapra az általános közzétételi lista leíró adatait minden esetben fel kell tölteni.

Számos beadvány érkezik a Hatósághoz a *közzétételi listák* hiányosságai, vagy éppen a rajtuk keresztül megvalósuló adatvédelmi jogsértések miatt. Az állampolgárok figyelemmel kísérik a helyi döntéshozók munkáját, az adatigénylők az önkormányzat képviselő-testületi üléseinek jegyzőkönyveiről, rendeleteiről, előterjesztésekről, napirendjéről, valamint a különböző bizottsági ülések meghívóiról, jegyzőkönyveiről rendszeresen érdeklődnek, ha az önkormányzat hivatalos honlapján ezek az információk nem találhatóak meg. Ez vonatkozik a gazdálkodási adatokra, a helyi költségvetés helyzetére, az önkormányzat rendelkezésére álló közpénzek elköltésének részleteire. „*Népszerű*” tárgyai az információigénynek az önkormányzatok által szervezett rendezvények költségeivel kapcsolatos adatok, valamint ezen események lebonyolítására vállalkozó cégekkel kötött szerződések, a helyi fesztivál bevételei. (NAIH/2018/2124/V)

IV.2.7. A képviselőtestületi ülések nyilvánossága, közvetítése

A képviselőtestületi ülések nyilvánossága, közvetítése, felvételek készítése számos gyakorlati kérdést vet fel. A képviselőtestületi és bizottsági ülések meghívói, előterjesztései, napirendje, a jegyzőkönyvek és határozatok kötelezően közzéteendő adatok. A képviselőtestületi ülés főszabályként nyilvános, azon bárki megfigyelőként jelen lehet. A hazai adatvédelmi gyakorlat alapján a nyilvános ülést az SzMSz-ben meghatározottak szerint az önkormányzat vagy megbízottja a nyilvánosság felé közvetítheti – például interneten vagy a helyi közösségi televízió útján, illetve sok helyen hangfelvétel is készül – erre azonban minden esetben előzetesen az érintettek figyelmét fel kell hívni (a tájékoztatás megtörténhet az ülés helyszínén szóban, valamint a kihelyezett tájékoztató útján, a városi televízió honlapján, közösségi oldalain, és/vagy az önkormányzat honlapján is.) Az ülésen megjelenteknek is joga van ahhoz, hogy a nyilvános ülést közvetítsék, arról kép- és hangfelvételt készítsenek a személyiségi jogot és az emberi méltóságot tiszteletben tartó módon. A nyilvános ülésekről készített felvételeknek a nyilvánosság széleskörű tájékoztatásának céljából történő közzététele nem jogellenes, de a korábban már kifejtettek szerint a felvételen szereplő közérdekből nyilvános személyes adatokat nem jogszerű a célhoz kötöttség és adattakarékosság elvének megsértésével terjeszteni. (NAIH/2018/6137/2/V).

A választópolgárok – a zárt ülés kivételével – betekinthetnek a képviselő-testület előterjesztésébe és ülésének jegyzőkönyvébe. A *zárt ülésen* hozott képviselő-testületi döntés is nyilvános és az Infotv. alapján elektronikusan, az interneten közzéteendő adat. A közérdekű adat és közérdekből nyilvános adat megismerésének lehetőségét zárt ülés tartása esetén is biztosítani kell. Ez az információszabadság szempontjából azt jelenti, hogy a közérdekű adat nem veszíti el a nyilvános jellegét amiatt, mert az zárt ülésen keletkezik, illetve a zárt ülésen hozott személyi döntések esetében is figyelemmel kell lenni arra, hogy az ott kezelt adatok, adatfajták valamely törvény rendelkezése folytán közérdekből nyilvánosak-e. Ellenkező esetben az adatokat védeni kell a jogosulatlan hozzáféréstől, illetve nyilvánosságra hozataltól, így a nyilvános határozatok megszövegezése nem utalhat természetes személlyel kapcsolatba hozható adatra. Egy konkrét (megalapozott) panasz tárgya pontosan az volt, hogy a panaszos volt munkáltatója, egy nagyközség polgármesteri hivatala a weboldalán olyan zárt képviselő-testületi üléseken hozott döntésekről szóló polgármesteri beszámolókat tett közzé, amelyekből bárki tudomást szerezhetett arról, hogy a bejelentő munkaügyi perben áll volt munkáltatójával. (NAIH/2018/7429/2/V).

IV.2.8. A közösségi média és a helyi közügyek

A kommunikáció és tájékoztatás napjainkban jelentős mértékben az interneten, azon belül is elsősorban a *közösségi médiumokon* keresztül zajlik, így nem meglepő, hogy egyre több település és polgármester üzemeltet oldalt a legnagyobb közösségi oldalon (is). A Hatósághoz több panasz érkezett ebben a körben:

Az egyik ügyben a Hatóság megállapította, hogy a városi (és polgármesteri) *„hivatalos”* Facebook oldal szerkesztőjének, adminisztrátorának, moderátorának neve az Infotv. 26. § (2) bekezdése értelmében közérdekből nyilvános adatnak minősül és felszólította a polgármesteri hivatalt, hogy küldje meg az adatigénylőnek a kért adatokat.(NAIH/2018/7338/V)

Egy másik ügyben egy város polgármestere a saját Facebook oldalán közzétette az egyik önkormányzati képviselő képviselői megbízatásáról lemondó levelét. A levélíró kérésére a bejegyzés ideiglenesen eltávolításra, majd az érintett képviselő adatainak kitakarásával ismét közzétételre került. A vizsgálat megállapítása szerint a választott önkormányzati képviselő közfeladatot ellátó személynek, a képviselői tisztségről való lemondás ténye közérdekű adatnak, a képviselő neve pedig közérdekből nyilvános adatnak minősül, de a személyazonosító adatok (születési hely, idő, anyja neve) mindenképpen felismerhetetlenné tételre szoruló személyes adatok. (NAIH/2018/3394/2/V)

Egy község polgármestere saját Facebook oldalán a település hulladékgyűjtő szigeteit nem rendeltetésszerűen használó személyekről készült felvételeket tett közzé. A Hatóság álláspontja szerint a polgármester akkor járt volna el helyesen, ha a fokozatosság elve alapján elsősorban a szabálysértések, illetve bűncselekmények felderítésére hatáskörrel rendelkező szervhez fordul a képfelvételen szereplő személyek beazonosítása érdekében. (NAIH/2018/2866/5/V)

IV.3. Ákr. kontra Infotv. avagy közadatok a közigazgatási eljárásban

2018-ban több olyan ügyben is érkezett a NAIH-hoz panasz, ahol folyamatban lévő közigazgatósági hatósági eljárások iratanyagát kívánták a betekintők megismerni (jellemzően helyi rádiós médiaszolgáltatási jogosultság hasznosítására irányuló pályázati eljárások iratairól volt szó). A közfeladatot ellátó szerv álláspontja szerint a hatósági eljárás közérdekű adatainak (eljárási iratok és az abban született döntések) megismerhetőségére, nyilvánosságára *lex specialis*-ként az Ákr. és a médiaszolgáltatásokról és a tömegkommunikációról szóló 2010. évi CLXXXV. törvény (a továbbiakban: Mttv.) irányadó, ezért alkalmazható az Infotv. 27. § (2) bekezdésének g) pontjában szereplő korlátozás *(„a közérdekű és közérdekből nyilvános adatok megismeréséhez való jogot törvény bírósági vagy közigazgatási eljárásra tekintettel korlátozhatja”).*

Az Ákr. eljárási, iratbetekintési szabályainak értelmezése, illetve az ezzel kapcsolatos kérdések megválaszolása csak annyiban tartozik a Hatóság hatáskörébe, amennyiben az a két információs alapjogot érinti, a közérdekű adatok megismerésével kapcsolatos alapjog-korlátozás lehetőségét azonban minden esetben megszorítóan kell értelmezni (ráadásul a rádiós frekvencia pályáztatás szakasza ezekben az ügyekben már lezárult). Önmagában az a tény, hogy a kiadni kért közérdekű adatokat egyébként közigazgatási hatósági eljárásban felhasználják, ezen adatokat nem fosztja meg közérdekű adat jellegüktől. Az, hogy a közigazgatási hatósági eljárásra tekintettel indokolt-e a nyilvánosságkorlátozás, kizárólag a konkrét esetre vonatkoztatva ítélhető meg. A NAIH nem foglalhat állást arról, hogy a vizsgálat alapjául szolgáló adatigénylés során az Ákr. szerint megindult hatósági eljárásban az adatigénylő ügyfélnek is, vagy általánosságban úgynevezett harmadik személynek minősül. Az ügyfél az eljárás bármely szakaszában betekinthet az eljárás során keletkezett iratba és ez a jog akkor is megilleti, ha korábban nem vett részt az eljárásban. Ügyféli minőség hiányában azonban a kérelmezőnek a személyes adatot tartalmazó irat megtekintéséhez fűződő jogalapját megfelelően igazolnia kell – ennek hiányában vagy sikertelensége esetén a NAIH álláspontja szerint a közfeladatot ellátó szerv akkor jár el helyesen, ha elutasítja az iratbetekintési kérelem teljesítését.

A harmadik személy csak akkor tekinthet be a személyes adatot vagy védett adatot tartalmazó iratba, ha igazolja, hogy az adat megismerése joga érvényesítéséhez, illetve jogszabályon, bírósági vagy hatósági határozaton alapuló kötelezettsége teljesítéséhez szükséges. Az Ákr. tehát itt is csak azon adattípusokat jelöli meg, amelyek megismerhetősége feltételhez kötött. A NAIH álláspontja alapján a közérdekű és közérdekből nyilvános adatok tekintetében ezen szakasz nem tartalmaz korlátozást, annak értelmezése során egyedül a személyes adatok, vagy egyéb védett adatok felismerhetetlenné tétele az, amit a jogszabály előír.

A már jogerőssé vált döntés megismerhetősége ugyanakkor a Hatóság álláspontja szerint nem zárható el a panaszostól arra hivatkozással, hogy a (személyes adatok felismerhetetlenné tétele mellett kiadott) határozat kivonatából következtetések vonhatóak le az ügyfél személyére nézve.

Az Mttv. alapján az állami tulajdonban lévő, korlátos erőforrásokat igénybe vevő lineáris médiaszolgáltatási jogosultság pályázat útján történő elnyerésével kapcsolatos eljárásokra az Ákr. szabályait az Mttv.-ben foglalt rendelkezésekkel kell alkalmazni, így a pályázati ajánlatban szereplő adatokról a Médiatanács harmadik személynek csak a szerződés megkötését követően adhat tájékoztatást. Ezzel kapcsolatban különbséget kell tenni már lezárt, valamint még folyamatban lévő hatósági eljárások között. Amennyiben egy hatósági eljárás lezárult és annak iratanyagát valaki meg kívánja ismerni, úgy a NAIH álláspontja szerint ez főszabályként megismerhető.

Az Infotv. 27. § g) pontja szerinti korlátozás rendeltetése a Hatóság álláspontja értelmében tehát nem a már lezárult közigazgatási hatósági eljárásokra vonatkozik. Megemlítendő továbbá, hogy mind az Ákr., mind pedig az Mttv. a személyes, valamint minősített adatok esetén ír elő korlátozást, a közérdekű és közérdekből nyilvános adatok anonimizálását egyetlen jogszabály sem rendelte el. A Hatóság a hozzá benyújtott panaszügyekben elérte a közérdekű adatigénylések megfelelő teljesítését. (NAIH/2018/291/V, NAIH/2018/819/V, NAIH/2018/1646/V)

IV.4. Az adatigénylés teljesítéséért megállapítható költségtérítés szabályai – legújabb fejlemények

A előző évi beszámolóban már részletesen ismertettük a költségtérítés alapvető szabályait (Infotv. 29. § és a közérdekű adat iránti igény teljesítéséért megállapítható költségtérítés mértékéről szóló 301/2016. (IX. 30.) Korm. rendelet – továbbiakban: Korm. rendelet alapján). Az elmúlt év tapasztalatai lényegében

hasonlóak, de a Hatóság néhány újszerű, a gyakorlatban eddig elő nem forduló esetben is állásfoglalást bocsátott ki, továbbra is szem előtt tartva azt, hogy a közfeladatot ellátó szervek a közérdekű adatigénylések teljesítésekor nem szolgáltatást nyújtanak, hanem az Alaptörvényben meghatározott alapvető jogból eredő kötelezettségeiket teljesítik.

2018-ban is az információszabadság ügyeink jelentős részét tették ki a költségtérítés jogalapját, és/vagy annak összegszerűségét vitató panaszok (39 db). Az adatkezelők között érintettek voltak minisztériumok (Pénzügyminisztérium, Agrárminisztérium, Emberi Erőforrások Minisztériuma), önkormányzatok, valamint állami és önkormányzati tulajdonú gazdasági társaságok, közintézmények. A megállapított költségtérítési összegek tág határok között mozogtak: a pár tízezer forintos tétel volt a leggyakoribb, de előfordult több százezer forintos összeg, illetve néhány kirívó esetben milliós nagyságrendekről is beszélhetünk (Magyar Államkincstár: 5.414.856,– forint; Magyar Rögbi Szövetség: 1.972.666,– forint; Szegedi Szabadtéri Nonprofit Kft: 891.540,– forint + ÁFA). A legmagasabb költségtérítést a XIX. kerületi Rendőrkapitányság állapította meg 11.482.319,– forint összegben, oly módon, hogy sem az adatigénylő, sem pedig a Hatóság kérésére nem részletezte a felmerülő költségelemeket. (Ebben az ügyben a Hatóság az országos rendőrfőkapitányhoz fordult.)

A NAIH mint felügyeleti szerv hatékonyságát és eredményességét igazolja, hogy a lezárt ügyek jelentős hányadában a vizsgálat következtében az adatigénylést az adatkezelő végül költségtérítés megfizetése nélkül teljesítette, vagy a hibás kalkuláción alapuló költségtérítés összegét mérsékelte, illetve a már befizetett költségtérítést az adatkezelő az igénylő részére visszautalta. Ilyen módon zárultak le például a Magyar Rögbi Szövetséggel, az Agrárminisztériummal, a BRFK-val, a Radioaktív Hulladékokat Kezelő Közhasznú Nonprofit Kft.-vel, a Barcika Park Nonprofit Zrt.-vel, illetve Budaörs Város Önkormányzatával kapcsolatban indult vizsgálataink. Ugyanakkor tény, hogy az elmúlt évben több olyan vizsgálat is indult, mely a beszámoló készítésének időszakában is folyamatban van, tekintettel arra, hogy az álláspontok többszöri levélváltást követően sem közeledtek egymáshoz.

A téma kapcsán hangsúlyozandó, hogy költségtérítés megállapítása sohasem kötelező. Minden esetben az adott közfeladatot ellátó szerv dönti el, hogy a törvényi keretek között él-e ezzel a lehetőséggel vagy sem. Amennyiben igen, a teljesítés során kizárólag a felhasznált adathordozó, a kézbesítés, valamint a munkaerőforrás ráfordítás költségeinek megtérítését lehet jogszerűen igényelni, ezen túlmenően más költségelem nem vehető figyelembe.

A legtöbb probléma az adatigénylések teljesítéséhez szükséges munkaerőforrás-ráfordítás költségének megtérítésével kapcsolatban merült fel, különösen azért, mert az adatigénylőkkel kifizetendő összegnek általában ez a legnagyobb hányada.

Az adatigénylés teljesítése bizonyos mértékű munkaerő-ráfordítást szükségképpen igényel, ez a közérdekű adatok megismeréséhez fűződő alapjog intézményi biztosításának velejárója. A Korm. rendelet értelmében figyelembe vehető az igényelt adat felkutatásához, összesítéséhez és rendszerezéséhez, az igényelt adat adathordozójáról másolat készítéséhez, valamint a másolaton a meg nem ismerhető adatok felismerhetetlenné tételéhez szükséges időtartam. Amennyiben ez meghaladja a 4 munkaórát, akkor a költségelemet úgy kell számítani, hogy a közreműködő személy által teljesített munkaórák számát meg kell szorozni az egy munkaórára eső tényleges munkaerő költségével. Utóbbi az adott személyt megillető rendszeres személyi juttatások összegét, de – a Korm. rendelet értelmében – jelenleg legfeljebb 4400 Ft-ot jelent. A járulékok, prémiumok, jutalmak és egyéb juttatások, például a béren kívüli juttatások, nem vehetőek figyelembe. Fontos, hogy a költségtérítésnek a valós költségekhez kell igazodnia, melyek akár lehetnek a Korm. rendeletben meghatározott összegeknél alacsonyabbak is.

A NAIH következetes álláspontja, hogy a közérdekű adatok megismerése iránti igény teljesítése nem tartozik ÁFA körbe. Ezt az álláspontot támasztja alá *„a közérdekű adatigénylés kapcsán fizetendő költségtérítés ÁFA-rendszerbeli megítéléséről szóló 2016/25. adózási kérdés”*, melyet az NGM szakmai főosztálya bocsátott ki 2016-ban.

A munkaerő-ráfordításért abban az esetben lehet költségtérítést felszámolni, ha az a közfeladatot ellátó szerv

1. alaptevékenységének ellátásához szükséges munkaerőforrás,
2. aránytalan mértékű igénybevételével jár, továbbá
3. a szükséges munkaerő-ráfordítás időtartama meghaladja a 4 munkaórát.

A fentiek értelmében tehát nem attól minősül aránytalannak a munkaerőforrás-ráfordítás időtartama, ha az meghaladja a 4 munkaórát, az említett három feltételnek együttesen kell érvényesülnie.

A NAIH által kidolgozott szempontrendszer alapján szükség szerint a vizsgálat során rákérdezünk arra, hogy hány fő dolgozik a közfeladatot ellátó szervnél, az adatigénylés teljesítésében résztvevő alkalmazottak milyen munkakörben dol-

goznak, illetve az adatigénylés teljesítésében résztvevő alkalmazottak munkaköre hogyan viszonyul a közfeladatot ellátó szerv alaptevékenységéhez és mely alaptevékenységét nem tudta ellátni a szerv az adatigénylés teljesítése miatt. Bekérjük az adatkezelő álláspontját arról, hogy miért vélik úgy, hogy az alaptevékenység ellátásához szükséges munkaerőforrás igénybevétele aránytalan mértékű. Emellett figyelembe vesszük a szerv rendelkezésére álló technikai infrastruktúrát is (pl. hány nyomtató és szkenner működik az adott intézményben, és ezeket milyen időtartamban kellett az adatigénylés teljesítéséhez igénybe venni).

Tipikus kérdésként merül fel továbbá, hogy az adatigénylő által igényelt adatok az általa kívánt formában rendelkezésre állnak-e. Ha nem, akkor az igénylő által megkívánt forma előállításának mekkora a becsült munkaóra igénye (a már meglévő adatok migrálása szerkeszthető excel táblázatba stb.). Az adatigénylésben érintett adatoknak nem csak a mértéke, de az adatokhoz való hozzáférés módja is meghatározó lehet (például archivált adatok esetében).

Vizsgálandó, hogy az igényelt adatok szerepelnek-e az Infotv. 1. melléklet szerinti általános közzétételi listában, tehát olyan adatokról van-e szó, amelyeket a közfeladatot ellátó szervnek elektronikusan már hozzáférhetővé kellett volna tennie. Ezen adatok esetében egyáltalán nem merülhet fel költségigény, tekintettel arra, hogy az Infotv. 30. § (2) bekezdése szerint az adatok pontos internetes elérési útvonalának megadásával teljesíthető az adatigénylés.

A NAIH a vizsgálat során arra is rákérdez egyes esetekben, hogy az adatok adatbázisba rendezése milyen módon lehetséges (pl. digitalizált dokumentumokból manuális kigyűjtéssel vagy egyszerű szűréssel). Ez a tény ugyanis lényegesen befolyásolhatja annak megítélését, hogy a munkaerőforrás aránytalan mértékű igénybevételéről beszélünk-e.

Munkaerő-ráfordításra tekintettel igényelt költségtérítés esetében a NAIH olyan kimutatást is kért az adatkezelőktől, hogy hány fő, hány munkaóráját számolták el és munkakörhöz kapcsolódó személyenkénti bontásban munkaóránként mekkora összeget vettek figyelembe, továbbá annak bemutatását is kérte, hogy melyek azok a munkafolyamatok, amelyek szükségessé válnak/vagy váltak az adatigénylés teljesítéséhez, illetve mennyire komplex feladat az adatigénylés teljesítése (pl.: hány szervezeti egység bevonására van szükség).

Amennyiben a költségtérítés megállapításának az indoka a dokumentum jelentős terjedelme, a NAIH azt is figyelembe vette, hogy mekkora iratmennyiség

felkutatására, rendszerezésére vagy másolására van szükség az adatigénylés teljesítéséhez.

Ha az adatigénylés teljesítésére elektronikus úton kerül sor, a munkaerő-ráfordítás időtartama csak akkor vehető figyelembe, ha:

– az adat elektronikus formában nem áll rendelkezésre (szkennelni kell) vagy
– szkennelni/másolni gyorsabb lenne, mint az elektronikus fájl-t előkeresni.

A költségtérítéses ügyek vizsgálata során igyekszünk felhívni az adatkezelők figyelmét a költséghatékonyabb adatigénylés teljesítésének lehetőségére is. Egy konkrét ügyben például, ahol az adott szervezet az adatigénylés időpontjában már sem humán erőforrással, sem pedig technikai eszközökkel nem rendelkezett ahhoz, hogy az adatigényléssel érintett nagymennyiségű dokumentumot elő tudják készíteni, a NAIH mediátorként sikeresen javasolta, hogy az adatok megismerését betekintés, jegyzet és képfelvétel készítés biztosításával valósítsák meg. (NAIH/2018/436/V)

A NAIH jogértelmezése szerint, amennyiben egy közfeladatot ellátó szerv az Infotv. 29. § (4) bekezdését kívánja alkalmazni (vagyis a költségtérítés előzetes megfizetésétől teszi függővé az adatigénylés teljesítését), akkor köteles az igénylés beérkezését követő 15 napon belül tájékoztatni erről a bejelentőt. Ha az adott szerv elmulasztja ezt a határidőt, akkor költségtérítést a határidőn túl már nem állapíthat meg. Kétségtelen tény azonban, hogy a jogszabály nem rendelkezik egyértelműen arról, hogy a 15 napos, költségtérítésről szóló tájékoztatásra vonatkozó határidő abszolút jogvesztő-e. Ez a jogszabályi hiányosság ugyanakkor több ügyben is konkrétan jelentkezett, melynek megoldása nem egyértelmű sem a bíróságok, sem pedig a NAIH számára. Amikor ugyanis az adatot kezelő közfeladatot ellátó szerv jogi kérdésben elfoglalt álláspontja alapján elutasítja az adatigénylés teljesítését – például arra hivatkozik, hogy ő az igényelt adat vonatkozásában nem adatkezelő, vagy az adat nem közérdekű/közérdekből nyilvános adat – értelemszerűen még a költségtérítés vonatkozásában nem hoz döntést. A költségtérítés a közérdekű adat kiadásához kapcsolódik, az erről való döntés jogi megállapításához kötődik egyfajta járulékos kérdésként. A Hatóság a joggyakorlat orientálása érdekében úgy foglalt állást, hogy amennyiben a jogvita lezárásakor akár a NAIH, akár az eljáró bíróság döntésében megállapítja, hogy az adatkezelő jogi álláspontja helytelen volt, és ezért a kért adatot ki kell adni, a 15 napos, költségtérítés megállapítására szolgáló határidő a hatósági döntésről szóló tudomásszerzéstől újra indul. A fenti jogértelmezési, jogalkalmazási probléma megnyugtató módon jogalkotás útján rendezhető. A NAIH a fenti álláspontjáról tájékoztatta a Kúriát.

A Hatóság fontosnak tartja kiemelni azt is, hogy az Infotv. 29. § (4) bekezdésében foglalt 15 napos tájékoztatási határidő független attól, hogy az adott szerv meghosszabbította-e a teljesítésre nyitva álló határidőt vagy sem. A tájékoztatási kötelezettség ugyanis ebben az esetben nem a meghosszabbított teljesítési határidőhöz kapcsolódik.

Végezetül hangsúlyozni szükséges a költségtérítés megállapításával kapcsolatos eljárás átláthatóságának követelményét. A transzparenciát leginkább a megfelelő tájékoztatás szolgálja. Minél részletesebb a tájékoztatás, annál hatékonyabban tölti be szerepét. Sajnálatos módon továbbra is nagy számban jutnak tudomásunkra helytelen gyakorlatok: például „*az adatigénylés teljesítésével kapcsolatban költségtérítéssel él*"; „*az adat igénylésének költsége X forint*", melyből egyáltalán nem állapítható meg a költségtérítés ténybeli és jogi indoka. A NAIH ezért minimális tartalmi követelményként elvárja a költségelemenkénti bontást, a munkaerő ráfordítás esetében annak kimutatását, hogy hány fő, hány munkaóráját számolták el, és munkakörhöz kapcsolódó személyenkénti bontásban munkaóránként mekkora összeget vettek figyelembe. Mind a jogorvoslati lehetőségek igénybevételét, mind pedig a NAIH vizsgálati eljárását megkönnyíti, ha az adatkezelő pontosan leírja azokat a munkafolyamatokat, amelyek szükségessé válnak/vagy váltak az adatigénylés teljesítéséhez. Jelentős terjedelmű másolat készítésénél a tájékoztatásnak az erre vonatkozó információkra is ki kell terjednie, például az adatigénylés mekkora iratmennyiséget ölel fel. Közölni kell az adatigénylővel az adatigénylés teljesítésének a másolatkészítést nem igénylő lehetőségeit is. Itt kell beszámolnunk a Pénzügyminisztérium által követett gyakorlatról, mely szerint az adatigénylők kifejezett kérésére sem adnak tájékoztatást arról, hogy milyen költségelemekből tevődik össze az előzetesen kalkulált költségtérítés, noha ez a NAIH álláspontja szerint valóban olyan információ, melyre a minisztériumnak már az összeg megállapításakor ki kellene térnie.

A NAIH a fentiek összefoglalójaként *„Tájékoztatót"* tett közzé a honlapján, mely a költségtérítés vonatkozásában is hasznos információkkal szolgál: http://www.naih.hu/files/Infoszab_tajekoztato_2018_06_30.pdf

IV.5. Felsőoktatási publikálási és nyilvánossági ügyek

A Hatóság gyakorlatában következetesen érvényesül az a megállapítás, miszerint az állami felsőoktatási intézmények mindenképp közfeladatot ellátó szervek, a nem állami felsőoktatási intézmények pedig a közpénzekkel való gazdálkodásra vonatkozóan kötelesek a nyilvánosság előtt az adatigények teljesítésével és

a külön törvényi rendelkezések szerint a közzététellel számot adni. Ennek alapja a felsőoktatási intézmények alaptevékenységének finanszírozásáról szóló 389/2016. (XII.2.) Korm. rendelet alapján a Kormánnyal megkötött éves finanszírozási megállapodás, melynek listáját a NAIH kikérte az illetékes minisztériumtól. (NAIH/2015/6179/V, NAIH/2018/2301/V)

A közpénzekből finanszírozott egyetemi publikációk tartalma vonatkozásában is érvényesülnek a szerzői jogi oltalomra vonatkozó szabályok [Infotv. 27. § (2) bekezdés h) pont]. Ebből következően főszabályként mindaddig, amíg egy egyetemi kéziratot (akár szakdolgozat, akár más tudományos értekezés, cikk esetében) a szerzője nem hoz nyilvánosságra, nem alkalmazhatóak a műre a szabad felhasználás szabályai, az alkotás továbbra is szerzői jogi oltalom alatt áll, annak tartalma nyilvánosságra hozataláról kizárólag a szerző dönthet. A munkaviszonyban vagy más hasonló jogviszonyban létrehozott művekre azonban eltérő szabályok vonatkoznak. Ha a mű elkészítése a szerzőnek munkaviszonyból folyó kötelessége, a mű átadása a nyilvánosságra hozatalhoz való hozzájárulásnak minősül. A mű visszavonására irányuló szerzői nyilatkozat esetén a munkáltató köteles a szerző nevének feltüntetését mellőzni. Ugyancsak mellőzni kell a szerző kérésére nevének feltüntetését akkor is, ha a művön a munkáltató a munkaviszonyból eredő jogaival élve változtat, de a változtatással a szerző nem ért egyet.

Más megítélés alá esnek azonban az egyetemi hallgatók által hallgatói jogviszonyuk alatt készített szakdolgozatok, disszertációk, vagy más egyéb egyéni, eredeti szellemi alkotások. Erre vonatkozó eltérő megállapodás hiányában az egyetemi könyvtár gyűjteményének részét képező művek tartalma az egyetem könyvtárában üzembe állított számítógépek képernyőjén a tudományos kutatás vagy az egyéni tanulás céljából az egyetemi hallgatók, illetve egyéb könyvtárlátogatók számára szabadon megjeleníthetők, illetve a nyilvánosság számára hozzáférhetővé tehetők, feltéve, hogy a művek tartalmát ez utóbbi személyek nem jövedelemszerzési célzattal kívánják megismerni, illetve felhasználni, hiszen a hallgatók tanulását, tudományos kutatását, szakmai fejlődését gátolná az, ha az egyetemi könyvtári állomány részét képező, illetve a jövőben abba bekerülő tudományos szellemi termékek nem lennének legalább helyben, a könyvtárban – minél szélesebb körben – kutathatóak és megismerhetőek. A szerző által már nyilvánosságra hozott egyetemi publikációkkal kapcsolatban pedig alapvetően a szabad felhasználásra vonatkozó szabályok érvényesülnek.

A közfinanszírozású, nyilvánosságra hozott egyetemi publikációk vonatkozásában további kérdésként merül fel a közpénzek felhasználásával készült, nyílt

hozzáférésű kutatási közadatok további felhasználásának, illetve újrahasznosításának kérdése is. A közadatok újrahasznosításáról szóló 2012. évi LXIII. törvény 3. § (1) bekezdés e) pontja alapján azonban nem bocsátható rendelkezésre újrahasznosítás céljából és jogszabályban sem határozható meg kötelezően rendelkezésre bocsátandó közadatként vagy kulturális közadatként az oktatási és kutató intézmények, iskolák, felsőoktatási intézmények, valamint kutatási eredmények továbbítására létrehozott szervezetek kezelésében lévő közadat. A fentiek alapján az egyetemek kezelésében lévő közadatok a jelenleg hatályos magyar jogszabályok szerint kivételt képeznek az újrahasznosításra vonatkozó szabályok alól.

Fontos azonban megemlíteni, hogy a tudományos publikációk nyílt hozzáférése az Európai Unióban is évek óta napirenden lévő, aktuális kérdés. Az Európai Bizottság és a felelős uniós biztos sajtóközleményeiben kiáll a nyílt hozzáférés mellett.

Sok egyetemi oktató továbbra sem tud megbékélni a MarkMyProfessor weboldalon (www.markmyprofessor.com) található oktatói adatlapokkal, kifogásolva az oktatókra vonatkozó hozzászólások, értékelések tartalmát és stílusát. A Hatóság álláspontja változatlan: a felsőoktatási rendszer működtetése állami feladat, következésképpen minden államilag elismert felsőoktatási intézmény – fenntartójától függetlenül – közfeladatot ellátó intézménynek, az oktatással összefüggő feladatokat oktatói és tanári munkakörben ellátó foglalkoztatottak pedig közfeladatot ellátó, egyfajta tudományos közszereplést vállaló személynek minősülnek. Tekintettel arra, hogy a weboldalon elérhető adatbázis célja az, hogy a hallgatók tájékozódhassanak az adott oktató által nyújtott oktatás színvonaláról, valamint az éppen aktuális követelményekről, az oktatói tevékenységgel összefüggésben az eredetileg megfogalmazott céllal összhangban megnevezhető az oktató, amennyiben él az oktatói jogviszonya. (A weboldal üzemeltetője köteles törölni azoknak az oktatóknak az adatlapját, akik az oktatói jogviszony megszűnését követően törlés iránti kérelemmel fordulnak az adatkezelőhöz.)

A közfeladatot ellátó személyeknek (csakúgy, mint a közéleti szereplőknek) többet kell eltűrniük a rovásukra elhangzott negatív értékítéletek és szakmai tevékenységükkel kapcsolatos bírálatok vonatkozásában, ez azonban természetesen nem eredményezheti az emberi méltóság semmibevételét. Ezért a honlap üzemeltetője is felelősséggel tartozik.

IV.6. Környezeti információk

Az egészséges környezethez való jog biztosításához elengedhetetlen, hogy a nyilvánosság a környezeti információkhoz hozzáférhessen. Ezen információk hiánya megakadályozhatja a nyilvánosságot a döntéshozatalban való részvételben környezeti ügyekben. A hozzáférés jogalapja többszörösen biztosított: az Infotv. mellett a környezet védelmének általános szabályairól szóló 1995. évi LIII. törvény 12. § (2) bekezdése kimondja, hogy a környezeti információk közérdekű adatok, másrészt az ún. Aarhusi Egyezmény (kihirdette a 2001. évi LXXXI. törvény) 4. cikk 1. bekezdése írja elő a hatóságok részére, hogy *„környezeti információ kérése esetén a nyilvánosság rendelkezésére bocsátják a kért információt a nemzeti szabályozás keretében."*

A törvény ugyan enged kivételeket a nyilvánosság alól, például a hatósági eljárások titkosságára vagy a személyes adatok védelmére tekintettel, de a kivételek *„szűken értelmezendők, figyelembe véve az információ feltárásához fűződő közérdeket."*

Azt, hogy mely adatok minősülnek környezeti információnak, a nyilvánosság környezeti információkhoz való hozzáférésének rendjéről szóló 311/2005. (XII.25.) Korm. rendelet határozza meg (például: a környezeti elemek állapotára, továbbá a környezetterhelésre vonatkozó adatok, a környezettel összefüggő intézkedésekre vonatkozó adatok, a környezet védelmére hozott intézkedésekre vonatkozó adatok).

A Hatósághoz 2018-ban több ilyen tárgyú panasz is érkezett, főleg fakivágási engedélyekkel kapcsolatban. Az utcában hirtelen eltűnő, az utcakép részévé váló nagy fák kivágása az érzelmekre is kiható esemény.

Emellett a beszámolóval érintett időszakban érkezett a Duna nagyvízi mederkezelési tervére, a Városligetben tervezett beruházásokra, egy város közösségi közlekedésének fejlesztésére, hulladéklerakóba szállított hulladék mennyiségére, szaghatással összefüggő hatósági ellenőrzés iratanyagára, egy akkumulátorgyártó üzem zajszennyezésével, működésével kapcsolatos vizsgálatokra vonatkozó panasz is.

A megtagadott környezeti információk széles spektrumának ellenére bizonyos hasonlóságokat fel lehet fedezni az adatkezelők által hivatkozott elutasítási indokok terén.

Az Aarhusi Egyezmény néhány esetre leszűkítve megengedi a környezeti információkra vonatkozó kérés elutasítását, azonban a kivételek szűken értelmezendők, figyelembe véve az információ feltárásához fűződő közérdeket. Az egyik lehetséges elutasítási ok, ha a kérés a hatóságok belső kommunikációjára vonatkozik. Az Egyezményhez készült végrehajtási útmutató[18] elemzése szerint a *„hatóságok azon véleményei, álláspontjai, melyeket egy döntéshozatali eljárásban bocsátanak ki erre vonatkozó jogszabályi kötelezettség alapján, nem tekinthetők a hatóságok belső kommunikációjának. […] Továbbá onnantól kezdve, hogy a hatóság megoszt egy bizonyos információt harmadik személyekkel, az az információ nem tekinthető belső kommunikációnak."*

Azonban jogilag helytelen, de a gyakorlatban mégis többször előforduló érvelés, hogy az adatot igénylő nem ügyfél abban az eljárásban, melyben az igényelt határozat született. A korábban, az Ákr. rendelkezéseiről szóló fejezetrészben kifejtettek alapján az ügyféli jogosultság a végleges hatósági határozatokhoz való hozzáférést nem érintő tényező.

A másik hasonló elutasítási indok a döntést megalapozó adatokra vonatkozó nyilvánosságkorlátozás. Ezeket a döntéseket minden esetben körültekintő mérlegelés alapján kell meghozni és az Alkotmánybíróság által több határozatban is lefektetett szempontok alapján indokolni kell – ennek az adatkezelők több ügyben nem tettek eleget. A Duna nagyvízi mederkezelési tervdokumentációjának részét képező önkormányzati vélemény és az UNESCO Világörökség Bizottság részére készült Világörökségi Hatástanulmány nyilvánosságtól való elzárását nem indokolták megfelelően az adatkezelők, így ezekben az esetekben a Hatóság közérdekű adatok megismeréséhez fűződő jog sérelmét állapította meg. (NAIH/2018/7054/2/V)

Végezetül meg kell jegyezni, hogy amikor a közfeladatot ellátó szervnek mérlegelési lehetősége van a közérdekű adatok nyilvánosságával kapcsolatban, akkor mindig felhívjuk a szerv figyelmét arra, hogy az egészséges környezethez való jog biztosításához elengedhetetlen a környezeti információkhoz való hozzáférés.

18 The Aarhus Convention: An implementation guide http://www.unece.org/fileadmin/DAM/env/pp/Publications/Aarhus_Implementation_Guide_interactive_eng.pdf

IV.7. Nagy érdeklődést kiváltó egyéb ügyek

A Magyar Labdarúgó Szövetség (a továbbiakban: MLSZ) állásfoglalást kért arról, hogy a játékvezetői és játékvezető ellenőri keretek közérdekű adatnak minősülnek-e. Az Infotv. és a sportról szóló 2004. évi I. törvény rendelkezései, valamint az MLSZ Alapszabályában, Szervezeti és Működési Szabályzatában és 2018. július 1-jétől hatályos *„Labdarúgás versenyszabályzata nagypályára és csökkentett pályára"* című szabályzatában foglaltak alapján az MLSZ e tevékenysége során közfeladatot ellátó szervnek minősül, így a játékvezetők és játékvezető ellenőrök mint az MLSZ feladat- és hatáskörében eljáró személyek neve, feladatköre, valamint közfeladata gyakorlásával összefüggő egyéb személyes adata – a védendő személyes adatok – kivételével közérdekből nyilvános. Ugyanakkor a játékvezetők és játékvezető-ellenőrök nevének az adott bajnoki fordulót megelőző napon történő nyilvánosságra hozatala megfelelő gyakorlat, amellyel az MLSZ nem okoz jelentős érdeksérelmet az adott játékvezető és játékvezető-ellenőr számára, megfelelően eleget tesz tájékoztatási kötelezettségének, valamint hatékonyabbá teszi a mérkőzések kimenetelének tisztességtelen befolyásolása (például a futballbírók megvesztegetése) elleni védekezést is. (NAIH/2018/5631/V)

Az adatigénylő az Emberi Erőforrások Minisztériumától (a továbbiakban: EMMI) a bárányhimlő elleni védőoltás vakcináival kapcsolatos – elsősorban üzleti információkat – kívánt megismerni. Az EMMI az adatokat döntés-előkészítő adatnak minősítette és arra hivatkozott, hogy a vakcinát gyártó cég üzleti érdekeit sértené, ha a versenytársak megtudhatnák, pontosan milyen áron kínálja fel termékét az állami egészségügynek. A Hatóság az érvelést megalapozottnak találta és elfogadta. (NAIH/2018/3256/V)

A panaszos szülő kifogásolta, hogy egy online hírportálon megjelent, a Magyar Cserkészszövetséggel (a továbbiakban: MCSSZ) összefüggő politikai témájú cikk borítóképén kiskorú lánya felismerhető módon szerepel. A vizsgálat során kiderült, hogy a szóban forgó cikket egy, az MTI (MTVA) által készített és Fotóbankjából letöltött képpel illusztrálták, az eredeti, készítésekor zajlott eseményről szóló tudósítástól eltérő tartalom mellett. Felszólításunkra a képillusztrációt törölték, megállapítást nyert, hogy más médiumok az írást nem vették át, emellett az internetes keresőmotorok üzemeltetőit (Google, Bing) is értesítette a Hatóság, hogy a korábban indexelt tartalmat töröljék és indexeljék újra a cikket az új illusztrációval.

Figyelemmel arra, hogy a cserkészek jelentős része kiskorú gyermek, akiknek személyes adatai a GDPR szerint is különös védelmet érdemelnek, fontos, hogy a gyermekek, illetve törvényes képviselőik megfelelő tájékoztatást kapjanak az adatkezelésekről. Az MCSSZ arról tájékoztatta a Hatóságot, hogy nyilvános rendezvényein a regisztrációkor és a helyszínen kihelyezett hirdetőtáblák útján is felhívja a résztvevők figyelmét, hogy az eseményen video-, kép- és hangfelvétel készül, melyeken adott esetben felismerhető lehet az adott résztvevő személy. A Hatóság emellett javasolta egy ezzel kapcsolatos általános tájékoztatás beemelését az MCSSZ Szervezeti és Működési Szabályzatába is. (NAIH/2018/4601/V)

V. A Hatóság jogalkotással kapcsolatos tevékenysége

V.1. A jogi szabályozással kapcsolatos ügyek statisztikai adatai

2018-ban a korábbi évekhez viszonyítva csökkent a véleményezett tervezetek száma. Ez nem a Hatóság elhatározása miatt alakult így, hiszen alapvetően *„hozott anyagból dolgozunk”*, vagyis a kormányzat jogszabály előkészítési tevékenységének volumene határozza meg a Hatóság jogszabály véleményezés ügystatisztika adatait. (Amit kiegészít az évente hozzávetőleg tucatnyi olyan ügy, amelyben a Hatóság hivatalból eljárva tesz észrevételeket, illetve javaslatokat valamely korábban meg nem küldött előterjesztés, törvényjavaslat, vagy jogszabály ügyében, amely a személyes adatok védelme vagy a közérdekű adatok nyilvánossága szempontjából korrigálandó.)

A 2018-as visszaesés, amely elsősorban a kormányrendeleti és a miniszteri jogforrási szintű tervezeteket érintette, feltehetőleg a legutóbbi országgyűlési képviselőválasztásnak tudható be. Ezt az valószínűsíti, hogy a véleményezésre bocsátott előterjesztések számát a korábbi évek statisztikáival összevetve a tavaszi hónapokban volt kimutatható a csökkenés.

A jogi szabályozással kapcsolatos ügyek száma évenként és jogforrási szintenként			
Jogforrás/év	**2016**	**2017**	**2018**
Törvény	85	82	72
Kormányrendelet	98	89	47
Miniszteri rendelet	83	94	55
Kormányhatározat	29	33	40
Közjogi szervezet-szabályozó eszközök	20	23	17
Összesen	**315**	**321**	**231**

Az ügyszám csökkenése ellenére a Hatóság által tett érdemi észrevételek és javaslatok száma összességében nem csökkent, vagyis kevesebb tervezettel foglalkoztunk ugyan, de azok több munkát igényeltek. Ez azzal magyarázható, hogy

2018-ban az év közben került sor a GDPR alkalmazandóvá válására, vagyis az adatvédelem jogi kereteinek jelentős átalakulására, amely számos új elvet és szabályt hozott magával, amelyet a jogszabály-előkészítőknek éppúgy meg kell ismerniük, mint az adatalanyoknak és az adatkezelőknek, hiszen ettől kezdve az adatkezelésre vonatkozó magyar jogszabályok jó részét a GDPR-ra tekintettel, azzal összhangban kell megalkotni, ami különösen a kezdeti időkben sok tisztázandó kérdést vetett fel a jogszabály-előkészítési eljárások folyamán.

A jogszabály-véleményezésekben tett érdemi észrevételek statisztikája			
	2016	**2017**	**2018**
Adatvédelemmel kapcsolatos	222	461	487
Információszabadsággal kapcsolatos	101	28	22
Egyéb	127	92	79
Összesen	**450**	**581**	**588**

A GDPR alkalmazandóvá válása, valamint az Infotv. 2018-as módosítása a korábbiaknál több feladatot ró a Hatóságra a jogszabályok előkészítésével kapcsolatban. Elsősorban az előzetes adatvédelmi hatásvizsgálatot érintő konzultáció emelendő ki. Kötelező adatkezelés esetén az adatvédelmi hatásvizsgálatot az adatkezelést előíró jogszabály előkészítője folytatja le, és az adatvédelmi hatásvizsgálat eredménye alapján magas kockázatú adatkezelések esetében előzetes konzultációt kell kezdeményeznie a Hatósággal a kockázatok csökkentéséről. Az előzetes konzultációt a jogszabály előkészítésének szakaszában kell lefolytatni.

V.2. Az Európai Unió adatvédelmi reformjához kapcsolódó szektorális törvénymódosítások

Az Európai Unió többi tagállamához hasonlóan Magyarországnak is hozzá kell igazítania a jogrendjét az Európai Unió adatvédelmi reformja keretében megalkotott jogi aktusokhoz, vagyis a GDPR-hoz és a bűnügyi adatvédelmi irányelvhez. Ennek első lépése az Infotv. módosítása volt, amely előkészítésében való részvételről a 2017-es beszámoló adott számot. Az Infotv. módosításának hatályba lépésére 2018-ban került sor, de ezzel korántsem ért véget a jogszabály-mó-

dosítások sora. A következő lépés az úgynevezett „GDPR saláta" előkészítése volt, vagyis azé a törvényjavaslaté, amely számos szektorális törvénymódosítást irányzott elő. A törvényjavaslat tervezetének véleményezése során a Hatóság a részletes észrevételei megtétele mellett a következőkre hívta fel a figyelmet.

1. Noha a hazai jogharmonizációs kötelezettségek egy részének az Országgyűlés 2018. tavaszi ülésszakán megalkotott törvényi szabályok hatályba lépésével Magyarország eleget tett, az ágazati adatkezelési normáknak az általános adatvédelmi rendeletet, valamint a bűnügyi adatvédelmi irányelvet átültető rendelkezésekkel való összhangjának megteremtése további jogalkotói lépéseket tesz szükségessé. Ezeknek elsősorban a deregulációra szükséges irányulniuk, azaz azon magyar törvényi szabályok hatályon kívül helyezéséről kell rendelkezni, amelyek tekintetében az uniós jogi környezet szabályozása vált közvetlenül alkalmazandóvá, illetve amelyek tekintetében az uniós szabályozás nem biztosít a tagállami jogalkotó számára szabályozási mozgásteret az uniós szabályokat kiegészítő vagy azoktól eltérő rendelkezések megalkotására.

2. Az uniós szabályozás az adatkezelők elszámoltathatóságának elvét alapelvi szinten tartalmazza. Sem az uniós, sem a tagállami jogalkotónak nem áll módjában mérsékelni az adatkezelő ezen alapelvből fakadó felelősségét azzal, hogy az alkalmazandó uniós szabályozásban kifejezetten lehetővé tett körön túl egyes ágazati adatkezelési jogviszonyok kereteit és tartalmát normatív módon meghatározza.

3. Az általános adatvédelmi rendelet közvetlenül alkalmazandó a tagállami jogrendszerekben. Ebből fakadóan annak rendelkezéseit a magyar jogban megismételni nem szükséges és nem lehetséges. A rendelet szabályaitól eltérni pedig kizárólag azon jogviszonyokban lehetséges, ahol arra a rendelet kifejezetten, tételesen felhatalmazza a tagállami jogalkotót. Ezen, ún. rugalmassági klauzulák hiányában a tagállami jogi norma nem tartható hatályban, nem alkotható meg.

4. Az adatkezelés jogalapjait, valamint a különleges adatok kezelése jogszerűségének további, különös feltételeit az általános adatvédelmi rendelet a hatálya alá tartozó jogviszonyok vonatkozásában taxatív módon határozza meg. Ezen jogalapok köre és tartalma a korábbi magyar szabályozástól egyes elemeiben eltér. Ennek egyrészt az a következménye, hogy a tagállami jogalkotó jogalkotási lehetősége (ld. 6. cikk (3) bekezdés) tipikusan az ún. kötelező adatkezelések (6. cikk (1) bekezdés c) és e) pont) szabályozására korlátozódik, mely szabályozás tekintetében (a korábbi szabályozáshoz hasonlóan) az Infotv. 5. § (3) bekezdésében meghatározott elemeket szükséges tartalmaznia a kötelező adatkezelést

előíró rendelkezéseknek. A jogalapok változásának másik következménye, hogy a kötelező adatkezelésen kívüli jogalapok tekintetében (6. cikk (1) bekezdés a), b), d), f) pontok) a tagállami jogalkotó – főszabály szerint – az adatkezelésre vonatkozó további feltételeket és jogokat nem állapíthat meg.

5. A megváltozott uniós jogi szabályozási környezet, továbbá az adatkezelési jogviszonyok sokszínűsége és a szabályozás összetettsége miatt az érintett szakmai érdekképviseletekkel történő, valamint általános társadalmi egyeztetésének kiemelt jelentősége van. Az ágazati jogi rendelkezések jogalkalmazói ugyanis olyan ismeretekkel és tapasztalatokkal segíthetik a jogszabály-előkészítők munkáját, amelyek új szabályozási szükségletekre is rávilágíthatnak.

V.3. Az adatkezelések rendszerét érintő nagy állami informatikai fejlesztési tervezetek

V.3.1. A „Szitakötő projekt”

Már az előző évről szóló beszámoló is érintette a Belügyminisztérium terveit, amelyek a közterületi kamerák által rögzített képfolyamok központi, kormányzati tárolásának előírására irányultak. A 2017-ben még csak vázlatosan és egyes részleteiben ismert elképzelések konkretizálására és törvényszövegbe foglalására 2018-ban került sor. (Ekkor vált közismertté a tervezett informatikai rendszer minisztériumi munkaanyagokban használt megnevezése is, vagyis a „Szitakötő”.) A Hatóság ekkor szembesült azzal, hogy a Szitakötő projekt egy az ország valamennyi településén jelen lévő, egységes központosított rendszerbe szervezett, a közterületeken tartózkodók, a közlekedők és a tömegközlekedési eszközökön utazók intenzív és tömeges megfigyelést lehetővé tevő képi megfigyelő rendszer létrehozására vonatkozik. A következő adatok érzékeltetik a tervezett megfigyelőrendszer nagyságrendjét: 35 000 kamera képfolyamainak folyamatos gyűjtése a Kormányzati Adatközpontban, 25 000 TByte megfigyelési adat folyamatos kezelése és (a településeknél megjelenő további költségeket leszámítva) központi szinten legalább 50 milliárd forint közpénz elköltése mindennek megvalósítása érdekében.

A tervezet értelmében a központi tárhelyre feltöltött adatokhoz közvetlenül, egy informatikai alkalmazáson keresztül férnének hozzá az arra jogosult szervezetek. A Hatóság rámutatott, hogy e koncepció szerint a képállományok feltöltésére kötelezett szervezetek megszűnnek a központi tárhelyre feltöltött képállományok

adatkezelői lenni, hiszen nem lesz érdemi ráhatásuk arra, hogy mikor, mely adatigénylő szervezet mely kameráik képeihez férhet hozzá, sőt valószínűleg nem is szereznek majd tudomást pl. az általuk feltöltött képállományok felhasználásáról. A véleményezett normaszöveg szerint a központi tárhely-szolgáltató sem lenne a képállományok adatkezelője, hanem csak adatfeldolgozó. Ez összességében azt eredményezné, hogy létrejönne egy hatalmas, megfigyelésre szolgáló képi adattömeg, amely kiszolgálná az adathozzáférésre jogosult szervezetek igényeit, de ténylegesen nem lenne olyan gazdája, amelyet jogsértés esetén felelősségre lehetne vonni. A törvényszövegből nagyrészt hiányoztak az adatvédelmi garanciák, sőt, az egyeztetés közben módosított változatból törlésre kerültek azok a részek, amelyek az adathozzáférések jogosultságának ellenőrzését, valamint a képfolyamokhoz való hozzáférések naplózását és ellenőrzését írták elő.

A Hatóság kifogásolta, hogy a normaszöveg a lehető legáltalánosabb módon a gyűjtött adatok „felhasználására" ad lehetőséget, amibe a mindenkori technikai lehetőségek függvényében bármely felhasználási mód beleérthető a képfolyam egyidejű, ember általi megfigyelésétől kezdve a képállományok lementésén vagy más rendszerbe való áttöltésén keresztül akár a megfigyelt személyek automatikus biometrikus azonosításáig, mozgásának követéséig, továbbá viselkedési, valamint kapcsolati profiljának feltérképezéséig. Egy ilyen hatalmas léptékű technikai megfigyelőrendszer nagyon erős adatvédelmi garanciákat kíván, ám ezek szinte teljesen hiányoztak a törvénytervezetből. Annak sem volt írásos nyoma, hogy a projekt koncepcionális tervezésekor vizsgálták-e azt, hogy a tervezett adatkezelési műveletek milyen adatvédelmi kockázatokkal járnak és milyen jogi szabályozási, valamint igazgatási és technikai intézkedésekkel lehetne azokat csökkenteni.

A Hatóság az egyeztetések során számos részletes adatvédelmi észrevétellel és javaslattal élt, továbbá azt szorgalmazta, hogy a Belügyminisztérium csak akkor engedjen utat a Szitakötő projekt folytatásának, ha felelősséggel garantálni tudják azt, hogy az állampolgárok jogainak korlátozása nem lépi túl azt a mértéket, ami egy demokratikus társadalomban elfogadható. Az egyeztetések során megvitatott javaslatok egy részénél sikerült előrehaladást elérni, így például a Hatóság javaslatának megfelelően belekerült a törvénytervezetbe az, hogy továbbra is az adatokat feltöltő adatkezelők lesznek jogosultak a központi tárhelyre feltöltött képállományaik sorsáról dönteni.

V.3.2. Az „okos város" projekt

A Hatóság 2018. februárjában egy kormányhatározat tervezetéből értesült egy fontos kormányzati kezdeményezésről, amely egy olyan központi szolgáltatás-

platform létrehozását irányozta elő, amely a leendő magyarországi okos városokat fogja kiszolgálni. A fejlesztések megvalósítására és kipróbálására Monoron, egy pilot projekt keretében fog sor kerülni. A tervezett fejlesztések szinte mindegyike közvetlenül befolyásolja az ott élők és dolgozók információs jogainak érvényesülését, továbbá a projektben tesztelendő szolgáltatások mintaként fognak szolgálni a későbbi magyarországi okos város fejlesztések számára, ezért a Hatóság jelezte, hogy hivatalból figyelemmel kívánja kísérni a tervezett fejlesztések előkészítését és megvalósítását. Ezt követően a Belügyminisztérium 2018. októberében küldte meg véleményezésre azt az előterjesztést, amely tartalmazta a tervezett okos város fejlesztések listáját és funkcionális leírását, valamint a szolgáltatások bevezetéséhez kapcsolódó, kormányrendeleti jogforrási szintű jogi szabályozás tervezetét. A Hatóság a részleteket megismerve következőkre hívta fel a figyelmet:

1. Az Alaptörvény I. cikk (3) bekezdés alapján az alapvető jogokra és kötelezettségekre vonatkozó szabályokat törvény állapítja meg. Az Alaptörvény VI. cikk (3) bekezdés ilyen alapvető jogként határozza meg a személyes adatok védelméhez, valamint a közérdekű adatok megismeréséhez és terjesztéséhez való jogot. Az általános adatvédelmi rendelet szabályait az Alaptörvénnyel összhangban kell alkalmazni, ezért Magyarországon a GDPR 6. cikk (1) bekezdés c) pont szerinti adatkezelési jogalapot törvényben kell szabályozni. Az Infotv.) 5. § (3) bekezdése határozza meg az adatkezelést elrendelő törvényben minimálisan szabályozandó tárgyköröket. Ebből adódóan az okos város működéséhez kapcsolódóan szükséges kötelező adatkezelések törvényi szabályozást igényelnek.

2. A pilot projekt megvalósíthatósági tanulmánya a személyes adatok védelmének fontosságának elismerése mellett azt is fontosnak tartotta, hogy „*[a személyes adatok védelme] ne hátráltassa a projekt eredményességét, a megvalósuló rendszerek, alkalmazások széleskörű használatát. Meg kell vizsgálni, hogy a fenti szabályzók tekintetében szükséges-e jogszabályi korrekciók elvégzése akár állami, akár helyi szinten [...]*" A Hatóság ezzel kapcsolatban hangsúlyozta, hogy az általános adatvédelmi rendelet számos területen szűkítette a tagállami jogalkotó mozgásterét és a tagállami jogszabályok az abban foglaltaktól csak annyiban térhetnek el, amennyiben arra az általános adatvédelmi rendelet kifejezetten lehetőséget ad. A pilot projekt hosszú távra előretekintő fejlesztéseket tartalmaz, ezért célszerű lenne azt is figyelembe kell venni, hogy uniós tagállami szintű egyeztetés folyik az elektronikus hírközlési irányelvet felváltani hivatott ePrivacy Rendeletről. Ez tovább szűkíti majd a tagállami jogalkotó mozgásterét, ezért a hosszú távra irányuló döntéseket célszerű lenne az ePrivacy Rendelet szabályozási tartalmának véglegessé válása után meghozni.

3. A Hatóság hangsúlyozta az általános adatvédelmi rendelet 25. cikk szerinti beépített és alapértelmezett adatvédelem elvét, amely minden adatkezelőre kötelezően irányadó. Egy ilyen volumenű projektnél a lehető legkorábbi fázisban szükséges elvégezni az adatvédelmi hatásvizsgálatot. Ennek elmaradása miatt előfordulhat, hogy a rendszert jelentős anyagi pluszköltségekkel utólag kell majd átalakítani ahhoz, hogy a jogszabályokkal összhangban tudjon működni.

4. A tervezett szabályok a Kormányzati Adatközpont (KAK) kizárólagos feladatkörébe kívánják utalni az okos városok számára nyújtandó platform-szolgáltatások egy részének nyújtását és ezzel összefüggésben megtiltják a települési önkormányzatok számára, hogy ezekkel párhuzamos vagy alternatív szolgáltatásokat tartsanak fenn. A platformszolgáltatások kötelező igénybevétele az adatkezelés kormányzati centralizációjával járna, hiszen elvonná a polgárok helyi közösségeitől azt az önkormányzati autonómiából levezethető jogot, hogy eldöntsék, vállalják-e a központi platformszolgáltatásoktól való függőséget, valamint az adataik KAK-ban történő kezelését, vagy inkább maguk kívánnak gondoskodni a település működésével és a helyi ügyekkel összefüggő adataikról. A Hatóság széleskörű társadalmi vitát javasolt annak tisztázása érdekében, hogy elfogadhatónak tartják-e az állampolgárok és a helyi közösségeik a centralizált kormányzati platformszolgáltatások *ex lege* monopolizált bevezetését.

5. Ha az okos városok adatainak kezelése bekerül a KAK-ba, úgy egy országosan uniformizált és centralizált informatikai infrastruktúra fog létrejönni, illetve tovább épülni. Az egységesítésnek és a centralizációnak számos előnye mellett vannak árnyoldalai is, így például az, hogy a központtal való kapcsolat megszűnése esetén, illetve a központ bármilyen módon történő kiiktatásával (pl. üzemzavar, természeti katasztrófa, szabotázs stb.) megbénítható a rendszer működése. A Hatóság ezzel összefüggésben javasolta a monolitikus, centralizált architektúra alternatíváit, így különösen a decentralizált, heterogén és osztott információs rendszermodelleket is számításba venni az okos városok informatikai infrastruktúrájának koncepcionális tervezése során.

6. A Hatóság véleménye szerint rendkívül problematikusak a biometrikus arcképadatok kezelésére vonatkozó tervek, ugyanis a biometrikus személyazonosítás és ellenőrzés azon technológiák közé tartozik, amelyek jellegüknél fogva különösképp veszélyesek az állampolgárok alapvető jogaira. Az automatikus arcfelismerésen alapuló azonosítás és személyazonosság ellenőrzés nem igényli az érintett közreműködését, ezért rejtett megfigyelést tesz lehetővé. Az arcfelismerési és hasonló jellegű biometrikus technológiák kiterjedt, tömeges alkalmazása ahhoz vezethet, hogy a települési közterületek, a nyilvánosság

számára nyitva álló egyéb közterületek és a tömegközlekedési eszközök megszűnnek a magánélet színterei lenni. A biometrikus azonosításra épülő szolgáltatások alkalmazásának kiterjesztése ellentétbe kerülhet a magyar alkotmányos jogfejlődés már elért eredményeivel, így különösen azzal, hogy az Alaptörvény a magán- és családi élet, az otthon és kapcsolattartás tiszteletben tartását egyaránt alapvető jogokként ismeri el, továbbá a magánélet védelméről szóló 2018. évi LIII. törvényben a magánélet fokozottabb védelme érdekében deklarált elvekkel és szabályokkal. A helyi „okos városi" önkormányzati feladatkörben nem merülhet fel olyan biometrikus adat-felhasználási igény, amely alkotmányos keretek között megvalósítható lenne. Tovább fokozza az aggodalmat, hogy az okos városok közterületi megfigyelő rendszereit integrálnák a KAK-ban létrehozandó, az ország valamennyi településén, valamint a tömegközlekedési eszközökön és a közutakon jelenlévő, több tízezer közterületi kamera képfolyamatit folyamatosan gyűjtő és tároló, biometrikus azonosítást is alkalmazó, titkos megfigyelést lehetővé tevő képi megfigyelőrendszerbe. Jelenleg még beláthatatlan, hogy hosszabb távon milyen hatásai lennének egy ilyen totális megfigyelőrendszer létrehozásának az állam működésére és a társadalomra.

Az egyeztetések eredményeként számos kérdésben sikerült eredményt elérni, például a Belügyminisztérium törölte a tervezett okos város alkalmazások közül a rendezvényekre történő beléptetés során alkalmazandó biometrikus személyazonosság ellenőrzést.

V.3.3. A „honvédelmi salátatörvény"

A biometrikus adatok kötelező kezelésének adatvédelmi problematikája az egyes törvények honvédelmi kérdésekkel összefüggő módosításáról szóló törvényjavaslat tervezete esetében is megjelent. A törvénymódosítás tervezete szerint a Honvédség erői és a KNBSZ külföldi műveletei során az ujj- vagy tenyérnyomat, DNS minta, íriszkép, arckép, kéz érhálózat, hangminta, egyéni íráskép, egyéni mozgáskép biometrikus adatokként kezelhetők. A Hatóság elvben elfogadhatónak tartotta a biometrikus adatok kezelését a Honvédség külföldi missziói során, ám több korrekciós javaslattal élt az adatkezelés szabályait illetően:

Elengedhetetlen az adatkezelés céljának kellően pontos meghatározása. A tervezetben rögzített egyik adatkezelési cél, a *„Honvédség külföldi szerepvállalásának támogatása"* túl általános célmegjelölés, hiszen abba olyan feladatok ellátása is beleérthető, amely nem indokolja kényszerítően a biometrikus adatok kezelését. Ugyanakkor nem lenne kifogásolandó, ha a törvény ehelyett például a külföldi katonai szerepvállalásban érintett magyar katonák életének és bizton-

ságának védelmére, valamint a külföldi művelet során használt katonai objektumok védelmére utalna.

Az adatkezelés céljának meghatározásán túl a kötelező adatkezelés érintetti körének meghatározása is törvényi szabályozást igényel. Ennek hiányában nem lenne garantálható, hogy a tervezett szabályozás csak a szükséges mértékben és az adatkezelés céljával arányosan korlátozná az érintettek információs önrendelkezési jogát.

A biometrikus azonosító adatok kötelező kezelésére vonatkozó törvényi szabályok megalkotása azért igényel különös körültekintést, mert a biometrikus azonosítás céljára szolgáló adatok olyan egyedi azonosító adatok, amelyek megváltoztathatatlanok, letagadhatatlanok és az egyéntől elválaszthatatlanok, ezért potenciális univerzális azonosítók. Az Alkotmánybíróság következetes gyakorlata szerint egységes és univerzális azonosító kód nem egyeztethető össze az információs önrendelkezési joggal, ezért a magyar jogi szabályozásnak gondoskodnia kell arról, hogy a biometrikus azonosítók se válhassanak egységes és univerzális azonosító kóddá. Ebből következően a törvénynek egyebek mellett korlátoznia kell a biometrikus azonosítók felhasználását és továbbítását. Különösen problematikus a biometrikus azonosító adatok külföldre továbbításának lehetővé tétele, mert ha az adatok kikerülnek a magyar joghatóság alól, akkor a továbbiakban a magyar állam és a magyar jog csak korlátozottan képes azok védelmére. Ezért a Hatóság javasolta pontosítani és differenciálni a normaszövegben azt, hogy milyen feltételekkel továbbíthatók a Magyar Honvédség kezelésében lévő biometrikus azonosító adatok külföldi és nemzetközi partnerszervezetek számára. Példaként említhető, hogy nyilvánvalóan nem lenne szabad a magyar katonák biometrikus adatainak külföldi szervezetek számára történő átadására ugyanazokat a jogi feltételeket támasztani, mint az ellenséges hadviselők vagy az elfogott terroristák biometrikus adatainak átadására. A Hatóság javasolta, hogy a törvény minimálisan a magyar katonák, valamint a velük együttműködő személyek esetében kifejezetten tiltsa, vagy legalábbis szigorú feltételekhez kösse és korlátozza a biometrikus adatok gyűjtését, illetve a külföldi szervezetnek történő átadását.

Kötelező adatkezelés esetében az adatkezelés időtartama az információs önrendelkezési jog korlátozásának mértékét meghatározó paraméterek egyike. A kötelező adatkezelés időtartama nem haladhatja meg a szükséges mértéket. A véleményezett törvénytervezet egységesen ötven éves megőrzési időtartamot kívánt előírni a Magyar Honvédség és a KNBSZ által kötelezően kezelt biometrikus adatok esetében. A Hatóság ezzel szemben arra mutatott rá, hogy biometri-

kus adatok ilyen kirívóan hosszú idejű megőrzéséhez nem járul olyan indokolás, amely igazolná annak szükségességét, ezért javasolta az adatok megőrzését a célhoz kötött adatkezelés és az adatminimalizálás követelményére tekintettel annak függvényében meghatározni, hogy adott biometrikus adatot milyen célból kezelnek. Továbbá a Hatóság szerint a törvényjavaslat indokolásának olyan lényegre törőnek és részletesnek kell lennie, hogy kellő eligazítást nyújtson a törvényjavaslatot tárgyaló Országgyűlésnek, valamint a társadalmi egyeztetésében résztvevő állampolgároknak arról, hogy az előterjesztő véleménye szerint miért szükséges a biometrikus adatok egy emberöltőnyi idejű megőrzése.

A Hatóság a fentiekben ismertetetteken túl javasolta kiegészíteni a törvényben azoknak a helyszíneknek a listáját, ahol nem alkalmazható képfelvétel rögzítésére alkalmas megfigyelőrendszer. A Hatóság szerint a Magyar Honvédség személyi állományának pihenésére rendelt helyiségekben sem szabad képi megfigyelőrendszert alkalmazni, mert a helyszín képi megfigyelése óhatatlanul személyekre, emberi magatartásokra, szokásokra, megnyilvánulásokra, illetőleg magára az emberi testre is irányulhat. Amint arra az Alkotmánybíróság 36/2005. (X. 5.) AB határozata rámutatott, az elektronikus úton történő megfigyelés alkalmas arra, hogy a magánszférába behatoljon, intim (szenzitív) élethelyzeteket rögzítsen akár úgy is, hogy az érintett nem is tud a felvételről. A megfigyelés a magánélethez való jog sérelmén túl az emberi méltósághoz való jogot általában is érintheti. A magánszféra lényegi fogalmi eleme éppen az, hogy az érintett akarata ellenére mások oda ne hatolhassanak be, illetőleg be se tekinthessenek. Ha a nem kívánt betekintés mégis megtörténik, akkor nemcsak önmagában a magánélethez való jog, hanem az emberi méltóság körébe tartozó egyéb jogosultsági elemek, mint pl. az önrendelkezési szabadság vagy a testi-személyi integritáshoz való jog is sérülhet.

V.3.4. A biometrikus hazugságvizsgálat szabályozása

Nemcsak a biometrikus azonosítás és személyazonosság ellenőrzés területén tapasztalható a technológiák fejlődésének hatása, hanem olyan további új módszerek és alkalmazási lehetőségek is létrejöhetnek, amelyek jogi szabályozást igényelnek. Az egyes sarkalatos törvényi rendelkezéseknek a büntetőeljárásról szóló 2017. évi XC. törvénnyel összefüggő módosításáról szóló törvény tervezete a rendőrségről szóló törvény poligráfos vizsgálatra vonatkozó szabályai helyett a műszeres vizsgálat alkalmazására vonatkozó szabályokat léptetett. A módosítás deklarált célja az, hogy a poligráfos vizsgálaton túl további, közelebbről meg nem határozott módszereken alapuló műszeres vizsgálatok elvégzése is lehetségessé váljon. A Hatóság ezzel kapcsolatban arra hívta fel a figyelmet, hogy

a műszeres vizsgálatok elvégzéséhez felhasználható módszerek gyorsan fejlődnek, ám éppen emiatt előfordulhat, hogy az új fejlesztésű, új módszeren alapuló mérőeszközök pontosságáról, megbízhatóságáról és az alkotmányos alapjogvédelmi követelményeknek való megfeleléséről még nem áll rendelkezésre elég információ. A műszeres vizsgálat törvényességéhez az érintett hozzájárulásán túl az is szükséges, hogy az alkalmazni kívánt eszköz igazoltan alkalmas legyen a műszeres vizsgálat céljára; a műszeres vizsgálat során alkalmazott módszer ne sértse az érintett emberi méltóságát, továbbá az adatok kezelése és felvétele tisztességesen történjen. E szempontok érvényre juttatása megfelelő törvényi garanciákat kíván.

V.4. Adatvédelmi problémák, amelyek több tervezetben visszaköszöntek

V.4.1. A hallgatózás joga?

A Hatóság valamennyi 2018-ban véleményezett, kamerás megfigyelésre vonatkozó törvénytervezet esetében kifogásolta, hogy azok a kép- és hangfelvétel készítést, illetve a megfigyelést bármiféle megkülönböztetés nélkül, azonos feltételekkel tegyenek lehetővé. A Hatóság véleménye szerint azért lenne szükséges a szabályozás differenciálása, mert amíg a képi megfigyelés elsősorban egy adott helyszínen történtek megfigyelésére alkalmas – beleértve a helyszínen tartózkodók magatartását is –, az akusztikus megfigyelés és a hanginformációk rögzítése révén további érzékeny adatok, így különösen a helyszínen jelen lévők beszélgetése és egyéb magánjellegű közlései is megismerhetővé válnak. Ezek olyan többletinformációk, amelyek jellemzően semmiféle kapcsolatban nincsenek azzal az adatkezelési céllal, amely miatt a képi megfigyelőeszközt az adott helyszínen elhelyezték. Ezért a Hatóság szerint nem felelnek meg a célhoz kötött adatkezelés és az adatminimalizálás követelményének azok a törvényi szabályok, amelyek a közterületi képi megfigyelés mellett azonos feltételekkel a „hallgatózásra" és a hangfelvételek megőrzésére is felhatalmazást adnak.

A fentiek jegyében a Hatóság a „Szitakötő" projekttel kapcsolatos törvénymódosítás véleményezésekor javasolta, hogy a törvényi újraszabályozás által nyújtott alkalmat kihasználva vizsgálják felül azt, hogy mely adatkezelési célok és adatkezelők esetében engedhető meg a képi megfigyelés mellett a „hallgatózás" is. Hasonló javaslattal éltünk az egyes törvények honvédelmi kérdésekkel összefüggő módosításáról szóló törvény tervezetének, valamint a személyszál-

lítási szolgáltatásokról szóló 2012. évi XLI. törvény módosításának véleményezésekor. Végül, de nem utolsó sorban megemlítendő, hogy az Országgyűlési Őrség által végzett adatkezelés törvényi kiegészítésének véleményezésekor is hangsúlyos szempontként jelent meg, hogy az Országgyűlési Őrség által az Országgyűlés épületében működtetett képi megfigyelőrendszer mikrofonjaival ne lehessen észrevétlenül belehallgatni az Országgyűlés folyosóin elhangzó beszélgetésekbe.

V.4.2. Az objektumokba belépők adatainak kezelése

A Hatóság több olyan törvénymódosítást véleményezett, amelyek hosszú, éves vagy évtizedes nagyságrendbe eső adatmegőrzési időtartamot kívántak előírni az objektumba belépők azonosító adatai, valamint a be- és kilépés időpontját illetően. Ilyen szabályokat tartalmazott az egyes törvények honvédelmi kérdésekkel összefüggő módosításáról szóló törvény tervezete, valamint az az Országgyűlésről szóló 2012. évi XXXVI. törvény (a továbbiakban: Ogytv.) módosításának a tervezete. A Hatóság elismeri, hogy mind az Országgyűlés, mind a Magyar Honvédség objektumai olyan fontos létesítmények, amelyek védelméhez és ezen belül a be- és kilépések ellenőrzéséhez erős közérdek fűződik, ám a Hatóság szerint a legitim biztonsági igények nem teszik szükségessé a több éves vagy évtizedes adattárolási időtartamot, ezért azt javasolta, hogy az adatok megőrzésére csak hat hónapig kerüljön sor.

V.5. Az információs önrendelkezési jog és az információszabadság szabályozási kereteivel kapcsolatos törvénymódosítások

V.5.1. A magánélet védelméről szóló törvény

A Hatóság az Igazságügyi Minisztérium felkérésére véleményezte a T/706. számú törvényjavaslatot. A vélemény megállapította, hogy a törvényjavaslat a magánélet tiszteletben tartásához való jog részeként utal a személyes adatok védelmére. E szabály változatlan elfogadása esetén valamelyest módosul a személyes adatok védelméhez való jog jogrendszerben való elhelyezése, hiszen az alapjogok alkotmányos rendszerében a magánélet tiszteletben tartásához való jog, a családi élet tiszteletben tartásához való jog, az otthon tiszteletben tartásához való jog és a kapcsolattartás tiszteletben tartásához való jog a személyes adatok védelmével együtt alkotja a magánszférajogok együttesét. Az Infotv. szabályozás célját megjelölő 1. §-a sem a magánélet védelméhez való jog ré-

szeként határozza meg a személyes adatok védelmét, hanem a magánszféra tiszteletben tartását jelöli meg a törvény céljaként.

A személyes adatok védelme a törvényjavaslat szabályozási tárgykörébe tartozik, ezért vizsgálandó, hogy a törvényjavaslat összhangban van-e a személyes adatok védelmének az Infotv.-ben és az általános adatvédelmi rendeletben meghatározott alapvető szabályaival. A törvényjavaslat az uniós jog elsőbbségéből következően nem határozhat meg az általános adatvédelmi rendelet értelmezésére vonatkozó szabályt és csak annyiban szabályozhat e rendelet hatálya alá tartozó szabályozási tárgyat, amennyiben arra az általános adatvédelmi rendelet lehetőséget biztosít a tagállami jogalkotás számára. A törvényjavaslat szerint magánélethez való jogot érintő jogszabályokat az Alaptörvénnyel, valamint a magánélet hatékonyabb védelme céljából e törvény rendelkezéseivel összhangban kell értelmezni. A Hatóság szerint e szabály nem kifogásolandó, ugyanis nem vonatkozik az általános adatvédelmi rendelet értelmezésére, hiszen az nem tartozik az Alaptörvény T) cikk (2) bekezdésében felsorolt jogszabályok közé.

A törvényjavaslat érintette a közéleti szereplő személyiségi joga védelmének, versus a közügyek szabad megvitatásához, illetve a véleménynyilvánítás szabadságához való jog érvényesülésének viszonyát, ennek körében olyan anyagi jogi szabályokat megállapítva, amelyek az általános adatvédelmi rendelet szabályozási tárgykörébe tartoznak. Ezzel összefüggésben kiemelendő, hogy az általános adatvédelmi rendelet 153. preambulumbekezdése szerint „*A tagállamok jogának össze kell egyeztetnie a véleménynyilvánítás és a tájékozódás – ideértve az újságírói, a tudományos, a művészi, illetve az irodalmi kifejezés – szabadságára vonatkozó szabályokat a személyes adatok védelmére vonatkozó, e rendelet szerinti joggal. […] A tagállamok kivételeket és eltéréseket fogadnak el az általános elvek, az érintett jogai, az adatkezelő és adatfeldolgozó, a személyes adatoknak harmadik országokba vagy nemzetközi szervezetek részére történő továbbítása, a független felügyeleti hatóságok, az együttműködés és az egységes alkalmazás, illetve az egyedi adatkezelési helyzetek tekintetében. […] A véleménynyilvánítás szabadságához való jog minden demokratikus társadalomban fennálló jelentőségének figyelembevétele érdekében az e szabadsághoz tartozó olyan fogalmakat, mint az újságírás, tágan kell értelmezni.*” Az idézetteknek megfelelően a magyar törvény megállapíthat olyan szabályokat, amelyek határvonalat húznak a közéleti szereplők magánszférájának védelme és a közügyek szabad megvitatásához és a véleménynyilvánításhoz való jog érvényesülése között. A törvényjavaslat vonatkozó szabályai a személyes adatok védelme szempontjából nem kifogásolandók. A másik oldalról, a véleménynyil-

vánítás szabadságának érvényesülése szempontjából nem vizsgáltuk a tervezett szabályok alkotmányosságát, mert ez kívül esne a Hatóság Infotv. 38. § (2) bekezdése szerinti feladat- és hatáskörén.

V.5.2. A jogalkotásról szóló törvény módosítása

A Hatóság az Országgyűlés munkájának figyelemmel kísérése során értesült a jogalkotásról szóló 2010. évi CXXX. törvénynek az Alaptörvény hetedik módosításával összefüggő módosítását tartalmazó T/2939. számú törvényjavaslatról, melynek 2. §-a a jogalkotásról szóló 2010. évi CXXX. törvény törvényalkotási tárgykörre vonatkozó szabályainak pontosítását tartalmazta. A jogalkotás törvényi szabályozása képes az információs alapjogok szabályozási környezetének befolyásolására, ezért a Hatóság hivatalból eljárva áttekintette a törvényjavaslatot.

A tervezett módosítás szerint „*törvénynek kell rendelkeznie alapvető jog közvetlen és jelentős korlátozásáról, illetve érvényesülésének lényeges garanciáiról*", amihez az előterjesztő a következő indokolást fűzte: „*A szabályozás jogforrási szintjének leszállítása. A jogforrási szint szempontjából ‚felülértékelt' jogszabályalkotás ugyanis a változó körülményekhez igazodó, ésszerűen rugalmas jogalkotás gátját képezi: az Országgyűlést szükségtelenül technikai részletszabályok jogalkotójává teszi. A cél, hogy a törvények kizárólag olyan rendelkezéseket tartalmazzanak, amelyek feltétlenül törvényi szintű szabályozást igényelnek*."

Az Alkotmánybíróság több határozata is érintette az alapvető jogokra vonatkozó szabályozás jogforrási szintjének kérdéskörét, és a jogforrási szint leszállítását illetően szigorúbb követelményeket határozott meg, mint a törvényjavaslat. Így például a 34/1994. (VI. 24.) AB határozat indoklása szerint „*[…] nem mindenfajta összefüggés az alapjogokkal követeli meg, hogy a szabályozandó kérdésekről törvény rendelkezzen. Az alapjogokkal való közvetett és távoli összefüggések szabályozására elegendő a rendeleti szint is.[…]*". A Hatóság ezzel összefüggésben annak fontosságára hívta fel a figyelmet, hogy a jogalkotás törvényi szabályainak maradéktalanul összhangban kell lenniük az Alkotmánybíróság vonatkozó határozataival.

Végül a köztársasági elnök adta meg a döntő impulzust a vitatott szabályozás további sorsának megnyugtató rendezéséhez, ugyanis 2018. december 7-én megfontolás céljából visszaküldte a törvényjavaslatot az Országgyűlésnek. A köztársasági elnök állásfoglalása rámutatott arra, hogy a normaszöveg lényegében taxatív felsorolást ad arról, hogy az alapjogok szabályozása során mi mi-

nősül törvényalkotási tárgynak. A kifogásolt szövegből az következik, hogy az alapvető jogok tekintetében kizárólag két tárgykör, nevezetesen a közvetlen és jelentős korlátozás, valamint az érvényesülés garanciája követel törvényi szabályozási szintet. Azonban az Alaptörvény I. cikk (3) bekezdés első mondata értelmében az alapvető jogokra és kötelezettségekre vonatkozó szabályokat törvény állapítja meg, ami – az Alkotmánybíróság gyakorlatára is figyelemmel – lényegesen szélesebb kört ölel fel.

Ezt követően az Országgyűlés a köztársasági elnök észrevételeit figyelembe véve a vitatott § nélkül fogadta el a jogalkotási törvény módosításáról szóló törvényt.

VI. Titokfelügyelet, a minősített, illetve korlátozott nyilvánosságú közérdekű adatok

Az adatvédelem jogi kereteinek mélyreható megváltozása, vagyis a GDPR alkalmazandóvá válása és az Infotv. 2018-as módosításának hatályba lépése viszonylag kevéssé érintette a Hatóság minősített adatokhoz kapcsolódó ügykörét. Ennek két nyilvánvaló oka van. Az egyik az, hogy az adatok minősítése a minősítési eljárások egy részében (és talán megkockáztatható, hogy a nagyobb részében) nem a személyes adatok védelméhez való jog érvényesülését korlátozza, hanem a közérdekű adatok megismerését, márpedig a közérdekű adatokra vonatkozó jogi szabályozás érdemben nem változott a beszámoló tárgyévében. Másrészt, ami a személyes adatok védelmét illeti, az ilyen adatok minősítésére rendszerint bűnüldözési, nemzetbiztonsági és esetleg honvédelmi érdekből kerül sor, vagyis olyan jellegű adatkezelésekről van szó, amelyek továbbra is az Infotv. hatálya alá esnek. Ezért a Hatóság minősített adatokkal kapcsolatos ügyeire 2018-ban a folyamatosság, a korábban kialakított joggyakorlat továbbvitele volt jellemző.

VI.1. A megismételt minősítésű adatok problematikája

Egy titokfelügyeleti hatósági eljárás kapcsán, de általános érvénnyel merült fel az a kérdés, hogy miképpen lehetséges az adatnyilvánosság jogsértő korlátozása elleni fellépés olyankor, amikor a Hatóság eljárásának tárgya nem az adat minősítése, hanem a minősítési jelölés megismétlése. [A minősített adat védelméről szóló 2009. évi CLV. törvény (a továbbiakban: Mavtv.) 7. § (1) bekezdése szerint „*nem kell új minősítési eljárást lefolytatni, ha a készített adatba saját vagy más minősítő által korábban készített minősített adatot is belefoglalnak, és ennek során további, saját minősítést igénylő adat nem keletkezik. Ebben az esetben a korábban készített minősített adat minősítési jelölését meg kell ismételni, kivéve ha azt a megismételni kívánt adat minősítője megtiltotta[...]*”.]

Az említett ügyben a Hatóság által megállapított tényállás szerint a Központi Nyomozó Főügyészségen folyamatban lévő büntetőeljárás nyílt szakaszában keletkezett iratokat megismételt minősítéssel látták el. A minősített adatok a megelőző titkos információszerzés során keletkeztek. A Központi Nyomozó Főügyészség tájékoztatása szerint a minősítés megismétlésének indoka az volt, hogy a felsorolt iratok olyan minősített adatokat tartalmaznak, amelyek a Nemzeti Védelmi Szolgálat által végzett, bíró által engedélyezett titkos információgyűjtés során alkalmazott eszközre, módszerekre utalnak. A nyomozás során a Nemzeti Védelmi

Szolgálat kifejezetten kérte a Központi Nyomozó Főügyészséget az eljárásban alkalmazott eszközök és módszerek védelme érdekében, hogy a büntetőeljárás az átadott bizonyítékok minősítésének fenntartása mellett kerüljön lefolytatásra. A Központi Nyomozó Főügyészség kezdeményezte az általuk alkalmazott minősítés megszüntetését, azt a minősítő azonban megtagadta. A Hatóság bekérte a megismételt minősítést tartalmazó okiratokat. A Hatóság eljárásának folyamán a minősítő arról adott tájékoztatást, hogy az iratokban szereplő adatok minősítése tekintetében a minősítés megszüntetéséről döntött. Tekintettel arra, hogy a bejelentéssel érintett adatok minősítését a minősítő a vizsgálat folyamán megszüntette, így a vizsgálat folytatására okot adó körülmény a továbbiakban nem állt fenn, ezért a Hatóság a vizsgálati eljárást megszüntette.

Jóllehet, ebben az ügyben a minősítés megszüntetése miatt nem volt mód annak megállapítására, hogy jogszerűen történt-e az adatok minősítése, illetve a minősítés megismétlése, ám elvi síkon felmerült a kérdés, hogy vajon milyen jogi eszközök állnak rendelkezésre a nyilvánosság jogsértő korlátozása elleni fellépésre olyankor, ha az állapítható meg, hogy adott adat minősítése jogszerű volt, ám a minősítési jelölés megismétlése sértette a személyes adatok védelméhez vagy a közérdekű adatok megismeréséhez való jog érvényesülését. (Például olyankor kerülhet sor ilyesféle jogsérelemre, ha a minősítési jelölés megismétlésekor olyan adatokra is alkalmazzák a minősítési jelölést, amelyeket az eredeti minősítés nem tartalmazott és egyébként sem állnak fenn a minősítésük Mavtv.-ben meghatározott feltételei.)

A problémát az okozza, hogy az Infotv. 63. § (1) bekezdés a) pontja alapján a Hatóság a titokfelügyeleti hatósági eljárásban hozott határozatában a nemzeti minősített adat minősítésére vonatkozó jogszabályok megsértésének megállapítása esetén a minősítőt hívhatja fel a nemzeti minősített adat minősítési szintjének, illetve érvényességi idejének a jogszabályoknak megfelelő megváltoztatására vagy a minősítés megszüntetésére, ám e szabály nem vonatkozik arra az esetre, amikor nem az adat minősítése, hanem a minősítési jelölés megismétlése volt jogszerűtlen. A minősítési jelölést jogszerűtlenül megismétlővel szemben azért sem lehet a titokfelügyeleti hatósági eljárás keretei között fellépni, mert az Infotv. 63. § (4) bekezdése szerint a titokfelügyeleti hatósági eljárásban az ügyfél a minősítő. Ebből az következik, hogy a minősítési jelölés megismétlője nem ügyféli pozícióban van a titokfelügyeleti hatósági eljárásban, hanem tanúként, vagy szemletárgy birtokosaként vesz részt az eljárásban, így esetében az Infotv. 63. § (1) bekezdés a) pontja szerinti szankció nem alkalmazható. Ezért megállapítható, hogy a Hatóság a hatályos Infotv. alapján nem titokfelügyeleti hatósági eljárásban, hanem vizsgálati eljárásban tud fellépni a minősítés jogszerűtlen megismétlése ellen.

VI.2. A kémperben kezelt további adatok minősítése

A Hatóság tavalyi beszámolója kitért az úgynevezett kémper adatai minősítésének ellenőrzésére. A 2017-ben folytatott eljárás során a Hatóság titokfelügyeleti hatósági eljárásban hozott határozatában kötelezte a minősítőt egyes, a Nemzeti Védelmi Szolgálatnál keletkezett adatok minősítésének megszüntetésére. Azonban a 2017-es eljárásunk során kiderült, hogy a Fővárosi Ítélőtábla előtt folyó per iratanyagában olyan adatok is voltak, amelyek minősítése nem a Nemzeti Védelmi Szolgálatnál történt, hanem a Nemzetbiztonsági Hivatalnál (a továbbiakban: NBH, az utódszervezet neve: Alkotmányvédelmi Hivatal). Ezen további adatok minősítésének jogszerűségét a Hatóság 2018-ban egy újabb titokfelügyeleti hatósági eljárásban ellenőrizte. Az eljárás tárgyát képező iratanyag poligráfos vizsgálatok kapcsán keletkezett információkat tartalmazott. A megvizsgált iratok a büntetőügy történeti tényállásának néhány kis részletéről tartalmaznak meglehetősen részletes és érzékeny információkat, mint például az NBH különböző szervezeti egységeinél készült jelentéseket és feljegyzéseket. A dokumentumok tartalmának ennél részletesebb ismertetésére nincs mód, mert a Hatóság által vizsgált tényállás egyes részleteinek nyilvánosságra kerülése hátrányosan érintené Magyarország külpolitikai-diplomáciai kapcsolatait, továbbá következtetni lehetne a magyar nemzetbiztonsági szervek tevékenységére és ezáltal negatívan befolyásolná Magyarország hírszerző és elhárító képességeinek folyamatos hatékonyságát. A dokumentumokban olyan információk szerepelnek, melyek nyilvánvalóan továbbra is védendő adattartalma különösen az alábbi tárgykörökre terjed ki.

- A nemzetbiztonsági szolgálat felépítésével és a titkos információgyűjtés műveleti szabályaival kapcsolatos technikai adatok.
- A poligráf vizsgálati metodika részletei, valamint nemzetbiztonsági szolgálathoz tartozó személyekre vonatkozó poligráfos vizsgálatok körülményei és eredménye, beleértve rendkívül szenzitív módszertani információkat is, amelyek nyilvánosságra kerülése veszélyeztetné a későbbi poligráfos vizsgálatok megbízhatóságát, eredményességét.
- Az iratokban szereplő információk felhasználása révén megkísérelhető lenne a magyar nemzetbiztonsági szerv munkatársainak beazonosítása és esetleg illetéktelen befolyásolásuk.
- A nemzetbiztonsági információk kiértékelésének módjával és intézkedések konkrét részleteivel kapcsolatos ismeretek.
- Más állam hírszerző szervezetével kapcsolatos nem publikus információk és nem publikus témában tartott diplomáciai megbeszélés tartalma.
- Magyar nemzetbiztonsági szolgálat információforrására vonatkozó adat.

Mindezek figyelembe vételével a Hatóság megállapította, hogy a 2018-ban vizsgált adatok minősítése jogszerű volt, és azok „Szigorúan titkos!” minősítési szintjének fenntartása továbbra is indokolt.

VI.3. A Paks II. beruházás végrehajtási megállapodásainak minősítése

A Hatósághoz több bejelentés érkezett az MVM Paks II. Atomerőmű Fejlesztő Zrt. és az orosz Joint-Stock Company Nizhny Novgorod Engineering Company Atomenergoproekt által aláírt három megvalósítási megállapodás minősítésének jogszerűsége kapcsán.

A Hatóság vizsgálati eljárást indított annak megállapítására, hogy az ügy tárgyát képező iratok tartalmának minősítése sérti-e a közérdekű, illetve a közérdekből nyilvános adatok megismeréséhez fűződő jogok gyakorlását, vagy ennek közvetlen veszélye fennáll-e. A Hatóság kérte a minősítőtől a minősítés részletes indoklását, valamint iratbetekintést tartott és a helyszínen vizsgálta a vizsgálat tárgyát képező iratanyagot. Az iratok tanulmányozását nehezítette az iratanyag nagy terjedelme és bonyolult tárgyköre, valamint az iratanyag angol nyelve. Mivel a minősítő időközben felülvizsgálta az adatok minősítését, a Hatóság kérte a minősítőt, hogy küldje meg a felülvizsgálati döntéseket és a felülvizsgálatra vonatkozó javaslatokat tartalmazó iratok másolatát. Noha a minősítő megszüntette a Paks II és az orosz fél közötti megvalósítási szerződések jelentős részének minősítését, a Hatóság a fennmaradó tartalmi egységekre vonatkozóan a minősítés indokoltságát szakértői szintű konzultáció keretében kívánta tisztázni. A minősítő a továbbra is „Korlátozott terjesztésű” minősítés alatt álló részekkel kapcsolatban megküldte álláspontját a Hatóságnak.

A vizsgálat megállapította, hogy a megvalósítási megállapodásokban található adatok minősítése formai és eljárási szempontból megfelel a Mavtv. előírásainak. A minősítési eljárás lefolytatására a Mavtv.-ben meghatározott minősítési javaslatnak megfelelően, a törvényben előírt határidőn belül került sor. A minősítő az adatok minősítésére vonatkozó döntését írásba foglalta és az iratokon feltüntették a Mavtv.-ben meghatározott minősítési jelöléseket. Ami a minősítés szükségességét illeti, a Hatóság a vizsgálata során többször kérte a minősítőtől a minősítés részletes indokolását, amely alapján eldönthető, hogy a minősített adattartalom esetében szükséges-e a minősítés szintjének, illetve a minősítés érvényességi idejének fenntartása, tekintettel arra, hogy közérdekű adat nyilvánosságához fűződő jogot minősítéssel korlátozni csak a Mavtv.-ben meghatá-

rozott feltételek fennállása esetén a védelemhez szükséges minősítési szinttel és a feltétlenül szükséges ideig lehet.

A minősítés tartalmával kapcsolatban, a nyilvános és védendő adattartalom elhatárolását illetően több nehézség merült fel, amelyek jelentősen hátráltatták a tényállás megállapítását. Először is, rendkívül nagy terjedelmű, több ezer oldalas iratanyagot kellett átvizsgálni. Másodszor, a végrehajtási megállapodások rendkívül sokféle részkérdést szabályoztak, megnehezítve annak megválaszolását, hogy szükséges-e az adott adat nyilvánosságát korlátozni. Az adatok minősítésekor a minősítő a megállapodások teljes szövegére tekintettel minősítette az adatokat, vagyis nem az adatelv, hanem az iratelv érvényesült. A minősítés ezzel szemben konkrét adattartalomra kell, hogy vonatkozzon az adatelvnek megfelelően, és időről időre szükséges felülvizsgálni az adott részek minősítéssel történő védelmének indokoltságát. A Hatóság munkatársaival történő egyeztetést követően a minősítő, összhangban az adatelvvel, a megvalósítási megállapodások jelentős részének minősítését megszüntette, a fennmaradó tartalmi egységek „Korlátozott terjesztésű" minősítésének vonatkozásában pedig megküldte az indokolását a Hatóságnak.

VI.4. A Paks II. Zrt. szerződéseinek megismerhetősége

Bár szigorúan véve nem titokügy, a tárgyi összefüggésekre tekintettel itt ismertetjük a Paks II. Atomerőmű Zártkörűen Működő Részvénytársaság tájékoztatási költségkalkulációs gyakorlata miatt folytatott vizsgálatot.

A Hatósághoz érkezett bejelentés szerint a panaszos adatigénylést nyújtott be a Paks II. Atomerőmű Zártkörűen Működő Részvénytársasághoz, amelyben 2017. január 1-től az adatigénylése napjáig a Társaság által megkötött, egymillió forint értékhatár fölötti szolgáltatási és beszerzési szerződések megküldését kérte. A Társaság az adatigénylés teljesítésével összefüggésben 176.000 forint költségtérítést állapított meg a panaszos részére, arra hivatkozva, hogy az adatigénylés teljesítése a közfeladatot ellátó szerv alaptevékenységének ellátásához szükséges munkaerőforrás aránytalan mértékű igénybevételével jár.

A Hatóság a Társaság költségszámítása kapcsán felhívta a Társaság figyelmét arra, hogy a munkaerő-ráfordítás költségének számításakor a személyi alapbér összegét kell alapul venni, a 13. havi bért, a választható béren kívüli juttatások és a C tarifa kompenzáció összegét, az önkéntes nyugdíjpénztári, az önkéntes

egészségpénztári, és az önsegélyező pénztári hozzájárulás, továbbá a szociális, a szakképzési és az egészségügyi hozzájárulás valamint a személyi jövedelemadó összegét nem lehet felszámolni. A Hatóság emlékeztette a Társaságot arra, hogy a közfeladatot ellátó szervek a közérdekű és közérdekből nyilvános adatok megismerésére irányuló igények teljesítése során nem szolgáltatást nyújtanak, hanem egy alapvető jogból eredő kötelezettségüknek tesznek eleget.

A Hatóság javasolta a Társaságnak a költségtérítési igény további csökkentését, tekintettel arra, hogy a kért közérdekű adatok megismeréséhez kiemelt közérdek fűződik. Bár az Infotv. 29. § (3)-(5) bekezdésében megteremti a jogalapot arra, hogy a közfeladatot ellátó szervek az adatigénylés teljesítéséért költségtérítést állapítsanak meg, a közfeladatot ellátó szerv csökkentheti, vagy akár teljes egészében mellőzheti is a költségtérítést.

VI.5. Az országgyűlési képviselő minősített adatra vonatkozó adatmegismerési jogköre

A Miniszterelnökség közigazgatási államtitkára arról kért állásfoglalást, hogy az országgyűlési képviselő, illetve az európai parlamenti képviselő az Ogytv. 98. § (2) bekezdésével összhangban felhasználói engedély birtokában megismerheti-e azon minősített adatokat, amelyek esetében a minősítés jogszerűségének ellenőrzésére irányuló titokfelügyeleti hatósági eljárás van folyamatban.

A közérdekű adatok megismerésének joga az Alaptörvényben meghatározott alapvető jogok közé tartozik. Az Alaptörvény alapján az állampolgárokat vagy mindenkit megillető alapvető jogok az állam és az egyén viszonylatában értelmezhetők. A közérdekű adatok megismerésére és terjesztésére vonatkozó, az Alaptörvény VI. cikk (2) bekezdésében megnevezett alapvető jog az egyént illeti meg az állammal szemben. E jog azonban nem azonos a demokratikus közhatalmi testületek tagjainak a demokratikus jogállamiság követelményeiből levezethető, az Ogytv.-ben meghatározott tájékozódási és adatmegismerési jogával. A Hatóság következetes joggyakorlata az, hogy a demokratikus közhatalom választott testületei tagjai számára külön törvényben biztosított adatmegismerési jog értelmezése, valamint a külön törvényben szabályozott jog gyakorlásával kapcsolatos beadványok kivizsgálása kívül esik a Hatóság törvényben meghatározott feladat- és hatáskörén.

VI.6. „Szigorúan titkos!" minősítési szintre vonatkozó minősítői jogkör átruházás jogszerűségének ellenőrzése

Demeter Márta országgyűlési képviselő bejelentéssel fordult a Hatósághoz amiatt, mert a Miniszterelnöki Kabinetiroda Szervezeti és Működési Szabályzatának 2018. december 1-jén hatályba lépett módosítása szerint a miniszter „Szigorúan titkos!" minősítési szintre vonatkozó minősítői jogkörét a miniszter kabinetfőnöke is gyakorolhatta. A Mavtv. 4. § (2) bekezdés a) pontja értelmében a minősítők minősítői jogkörüket „Szigorúan titkos!" minősítési szintű adat esetén írásban a helyettesükre, valamint a Kormány tagja a közigazgatási államtitkárra, az államtitkárra és a helyettes államtitkárra ruházhatják át. A Miniszterelnöki Kabinetiroda kabinetfőnöke nem tartozik azon beosztást betöltő személyek közé, akikre a Mavtv. 4. § (2) bekezdés a) pontja szerint a miniszter minősítői jogköre „Szigorúan titkos!" minősítési szintű adat esetében átruházható, ezért a Hatóság vizsgálatot indított annak megállapítására, hogy okozott-e a személyes adatok védelmével vagy a közérdekű és a közérdekből nyilvános adatok megismeréséhez való jog gyakorlásával összefüggésben jogsérelmet a Miniszterelnöki Kabinetirodát vezető minisztert megillető minősítési jogkör átruházása a miniszter kabinetfőnökére. A vizsgálat során megállapítást nyert, hogy a miniszter kabinetfőnöke ténylegesen nem járt el a rá átruházott minősítői jogkörben, továbbá a Miniszterelnöki Kabinetirodát vezető miniszter még 2018. december folyamán megszüntette a „Szigorúan titkos!" adatokra vonatkozó minősítői jogkör átruházást, ezért a Hatóság az ügyben folytatott vizsgálatot lezárta.

VI.7. Ingatlannal kapcsolatos jogvita adatainak minősítése

Közérdekű adat kiadása iránti pert kezdeményeztek a Magyar Nemzeti Vagyonkezelő Zrt.-vel (a továbbiakban: MNV Zrt.) szemben, mert az elutasította azt a közérdekű adatigénylést, amely a Csillebérci Úttörőtáborral, vagyis egy olyan ingatlan tulajdonjogával kapcsolatos jogvita irataira vonatkozott, amelyben a Magyar Állam részéről az MNV Zrt. járt el. A Fővárosi Törvényszék titokfelügyeleti hatósági eljárást kezdeményezett a Hatóságnál a minősítés jogszerűségének ellenőrzése érdekében.

A titokfelügyeleti hatósági eljárás során a minősítő arra hivatkozott, hogy az ingatlan tulajdonjogi helyzetének rendezése érdekében kötendő egyezség előre meghatározott pénzügyi és jogi kereteinek nyilvánosságra kerülése, vagyis az adatok akár a szerződő fél, akár a vele szerződéses jogviszonyban álló harmadik felek, vagy a közvélemény részéről történő idő előtti megismerése olyan tárgya-

lási helyzetet teremthetett volna, mely az állam számára jogilag és pénzügyileg előnytelenebb egyezség megkötéséhez vezethetett volna, a Magyar Államnak pénzügyi veszteséget, esetleg tulajdonszerzésének meghiúsulását okozva, továbbá állampolgárok vagy gazdálkodó szervezetek részére jogtalan nyereséget vagy előnyszerzést tett volna lehetővé. A minősítő szerint a „Korlátozott terjesztésű!" minősítés maximális érvényességi idővel történő meghatározásának az volt az indoka, hogy a szerződő felek közötti megállapodást követően az esetlegesen érintett harmadik személyek részéről ne történhessen jogtalan nyereség vagy előnyszerzés, illetve ezek a személyek a Magyar Állam kárára ne okozhassanak pénzügyi veszteséget azzal, hogy a birtokukba jutott információ alapján esetlegesen valamilyen követeléssel éljenek.

Az eljárás során a Hatóság a minősítés érvényességi idejének meghatározását alátámasztó indokokat nem tartotta megfelelőnek. Ezzel összefüggésben tisztázandó volt, hogy a felek közötti jogvitát lezáró megállapodás megkötését és az ebből eredő kötelezettségek teljesítését követően mi indokolja a minősítés további fenntartását, illetve azt hogy összhangban vannak-e a polgári jog alapelveivel a minősítés fenntartásának indokai. A minősítő nem konkretizálta, hogy az *„esetlegesen érintett harmadik személyek"* kik lehetnek, milyen jellegű követeléssel élhetnek és e követelések miképpen vezethetnek jogtalan nyereség vagy előnyszerzéshez. A Hatóság kérte az indokolás további, részletes kifejtését, ha volt konkrétan felmerült követelés, annak részletezését.

Ezt követően a minősítő úgy nyilatkozott, hogy a tulajdonjoghoz, birtokláshoz kapcsolódó vitás kérdés az egyezségre tekintettel az egyezséget kötő felek között nem maradt. További indokkal nem támasztotta alá a maximális időtartamú érvényességi idő fenntartását, vagyis azt, hogy a megállapodás megkötését és az abban foglalt kötelezettségek teljesítését követően miképpen befolyásolná az adatok nyilvánosságra kerülése a védhető közérdeket.

A Hatóság az alábbi megállapításokat tette:

Tekintettel arra, hogy a minősítő nyilatkozata szerint a szóban forgó jogvita az egyezség megkötése által jogerősen lezárult, a tulajdonszerzés és a birtokba lépés a megállapodásnak megfelelően megtörtént a Hatóság megállapította, hogy a továbbiakban nem indokolt a minősítés fenntartása. A megállapodás megkötését követően ugyanis annak tartalmát, feltételeit, valamint az alkupozíciókat az adatok nyilvánosságra kerülése már nem befolyásolhatja, e tekintetben az állam számára nem okozhat pénzügyi veszteséget. Az adatok nyilvánosságra kerülése ilyen módon már nem befolyásolhatja a védeni kívánt közérdeket.

Egy jogvita lezárását célzó megállapodás esetében harmadik személyek esetleges követeléseinek kizárását a megállapodásban rögzítendő jogi garanciáknak kell biztosítaniuk, ezek alapján az érintett feleknek szavatolniuk. Az adatok minősítése nem szolgálhatja azt a célt, hogy az adatok nyilvánosságtól való elzárásával harmadik személyeket tartsanak vissza igényeik érvényesítésétől, mely esetleges igények jogszerűségéről bíróság jogosult dönteni. A megállapodás megkötését követően, azzal nem érintett, későbbiekben esetleg felmerülő igények, követelések jogos vagy jogszerűtlen voltának megítélésére a megállapodást megkötő felek nem jogosultak és erre a minősítő sem hivatott.

Az iratokból kitűnt, hogy a szerződésekben részes felek jog- és kellékszavatosságot vállaltak az ingatlan tulajdonba és birtokba adására, szavatossággal tartoznak az ingatlan per-, igény- és tehermentességért, stb. A felek tehát, a polgári jog szabályainak keretei között intézkedtek az ingatlanra vonatkozó vagy ahhoz kapcsolódó esetleges követelések jogszerű kizárásáról.

Alkotmányos követelmény, hogy a minősítő a közérdekű vagy közérdekből nyilvános adat minősítése felőli döntés során a minősítéshez fűződő közérdek mellett a minősítendő adat nyilvánosságához fűződő közérdeket is vegye figyelembe, és csak akkor döntsön az adat minősítéséről, ha a minősítéssel elérni kívánt cél arányban áll a minősített adat nyilvánosságához fűződő közérdekkel. Magyarország Alaptörvényének 38. cikke és 39. cikk (2) bekezdése a közpénzekkel való gazdálkodás átláthatóságának követelményét, valamint a közpénzekre és a nemzeti vagyonra vonatkozó adatok közérdekű adattá minősítését alkotmányos rangra emelte. A közpénzekre és a nemzeti vagyonra vonatkozó adatok esetében az átláthatóság és a közélet tisztaságának elvére tekintettel a minősítésnél figyelembe veendő az adatok megismerhetőségéhez fűződő közérdek jelentős súlya.

Az adatok nyilvánosságához fűződő érdeket támasztják alá az alábbi indokok.

- Az ingatlan tulajdonjogával kapcsolatos jogvita évtizedek óta tart, melynek bizonyos részletei széleskörű nyilvánosság előtt ismertek, közérdeklődésre tartanak számot.
- Az érintettek közötti jogvita perbeli egyezség révén jogerősen lezárult, az ingatlannal kapcsolatos igények rendeződtek.
- Az adatok egy részének minősítését a minősítő már megszüntette, tekintettel arra, hogy a peres egyezség és az adásvételi szerződések megkötésére, valamint az ingatlan-nyilvántartásba történő bejegyzésre csak így volt lehetőség.

– Az ingatlan hasznosításával kapcsolatosan is bizonyos információk már a sajtó révén nyilvánosságra kerültek, melyek szintén közérdeklődésre tartanak számot.
– A megállapodásban meghatározott jogi tények bekövetkezése okán a minősítéssel védhető közérdeket az adatok nyilvánosságra kerülése már nem befolyásolja. Az adatok nyilvánosságához fűződő érdekkel szemben megszűntek a minősítés eddigi indokai.

A Hatóság egyetértett a minősítő azon álláspontjával, miszerint a Magyar Államnak pénzügyi veszteséget okozhatott volna a minősítéssel érintett adatok nyilvánosságra kerülése. Az egyezség megkötéséhez meghatározott pénzügyi és jogi keretek nyilvánosságra kerülése ugyanis olyan tárgyalási helyzetet teremthetett volna, hogy a szerződő félnek, vagy – az ingatlanra tekintettel – vele jogviszonyban álló harmadik személyeknek módja lett volna a Magyar Állam számára hátrányosabb, nagyobb költségvetési kiadású egyezség megkötését kialkudni. A megállapodás megkötése érdekében minősítéssel védett pénzügyi és jogi keretekre vonatkozó adatok nyilvánosságra kerülése tehát az állam számára előnytelenebb egyezség megkötését eredményezhette volna, ezáltal pénzügyi veszteséget okozva az állam számára. A Hatóság azonban azt is megállapította, hogy a közérdekű adatok megismeréshez való jog korlátozása a jövőre nézve nem indokolt, mivel a Mavtv.-ben meghatározott valamennyi feltétel fennállása esetén is csak a legszükségesebb ideig védhetőek minősítéssel az adatok. Ezért a Hatóság megállapította a minősítésre vonatkozó jogszabályok megsértését és felhívta a minősítőt a minősítés haladéktalan megszüntetésére. A minősítő a Hatóság határozatát a közlésétől számított hatvan napon belül nem támadta meg bíróságon, ezért az adatok minősítése e határidőt követően a törvény erejénél fogva megszűnt.

VII. Nemzetközi ügyek és társadalmi kapcsolatok

Ebben a fejezetben áttekintjük a Hatóság nemzetközi tevékenységét. Részletesen szólunk az Európai Unió újonnan létrejött szervében, az Európai Adatvédelmi Testületben végzett tevékenységünkről.

Külön kiemeljük az Európa Tanács ún. 108-as Egyezményének korszerűsítését, amely a GDPR alkalmazandóvá válását követően szintén a nemzetközi adatvédelem egyik fontos fejleménye.

Bemutatjuk azokat a nemzetközi tanácskozásokat, így a Berlini Munkacsoport és az adatvédelmi hatóságok panaszkezelő kollégáinak részvételével tartott workshopot is, amelynek 2018-ban házigazdája a Hatóság volt.

VII.1. Részvétel az Európai Adatvédelmi Testület munkájában

A GDPR alkalmazandóvá válásával létrejött az Európai Adatvédelmi Testület. A Testületnek önálló jogi személyisége van. Kötelező döntéseket hoz, szemben a korábbi adatvédelmi irányelv alapján, csupán tanácsadó szervként működött a 29-es Munkacsoporttal. A Testület tagja a Hatóság is. A testületi munka döntéshozatali fóruma a plenáris ülés, azonban a munka legnagyobb része az ún. szakértői alcsoportokban zajlik. Ezt a munkát részletesen mutatjuk be alcsoporti bontásban.

VII.1.1. Technológiai szakértői alcsoport

A Testület Technológiai Szakértői Csoportja a 2018-as évben kivételesen sok munkával szembesült. A korábbi években megkezdett, a GDPR egyes rendelkezéseihez kapcsolódó iránymutatásainak elkészítése és társadalmi egyeztetése a csoport egész évét végigkísérte. Az év elején fejeződött be az adatvédelmi incidensekhez kapcsolódó iránymutatás társadalmi vitája, így a csoport a plenáris ülés elé tudta bocsátani annak végleges tervezetét.

Az év folyamán lezárult a tanúsításról szóló iránymutatás szövegezése is, amely dokumentum az év végén kiegészült azzal a melléklettel, amely a tanúsítási szempontrendszerekhez kapcsolódó kritériumokhoz is tartalmazott ajánlást. Ugyancsak így alakult a tanúsító szervezetek akkreditációjáról szóló iránymutatás is, amely szövegezéséhez az év elején a csoport egy közös workshop ke-

retében fogadta az akkreditáló hatóságok képviselőit. A tanúsító szervezetek akkreditációjáról szóló iránymutatás az év közben elnyerte végleges formáját, majd év végén kiegészült egy melléklettel, amely az akkreditációhoz kapcsolódó kiegészítő adatvédelmi követelményekhez tartozó kritériumokat tartalmazta.

A szakértői csoport másik jelentős feladata a felügyeleti hatóságok által a GDPR 35. cikk (4) bekezdése alapján benyújtott, adatvédelmi hatásvizsgálat alá vonandó adatkezelési műveletek listájának egységességi elemzése volt. Az év folyamán valamennyi tagállami felügyeleti hatóság benyújtotta a fenti listáját, amelyeket a szakértői csoport megvizsgált és a Testület korábbi iránymutatásával összevetett. A listák tartalmát az egységes jogalkalmazás szempontjából elemezte és véleménytervezetet készített valamennyi listáról, amelyeket a plenáris ülés elé terjesztett. Ezen vélemények végrehajtásának az utánkövetését is a Technológiai Szakértői Csoport fogja ellátni.

A fent említett két nagy feladat mellett tovább folyt a munka számos ajánlás és iránymutatás szövegezésével kapcsolatosan, amelyek közül kiemelendő a kamerás megfigyelés új technológiájáról, illetve a beépített és alapértelmezett adatvédelemről, valamint az ePrivacy Irányelv és a GDPR közös alkalmazásának kérdéseiről szóló vélemény tervezetek szövegezése.

VII.1.2. A jogi megfeleléssel, e-kormányzattal és egészségügyi kérdésekkel foglalkozó szakértői alcsoport (Compliance, eGovernment and Health)

A 29-es Munkacsoport korábbi eGovernment elnevezésű alcsoportja a Testület létrejöttével átnevezésre került Compliance, eGovernment and Health szakértői csoportra. A szakértői csoport hatáskörébe a GDPR szerinti magatartási kódexek, tanúsítás, adatvédelmi hatásvizsgálat, beépített és alapértelmezett adatvédelem elvének való jogi megfelelés tartozik, ezek mellett az elektronikus közigazgatással összefüggő és az egészségügyi adatkezelések problémái is a csoport hatáskörébe tartoznak.

A 2018-as évben a szakértői csoport fő feladata a GDPR magatartási kódexekre és az elfogadott magatartási kódexnek való megfelelést ellenőrző szervezetekre vonatkozó szabályainak értelmezése volt és ennek keretében egy iránymutatás megszövegezése. Az iránymutatást a szakértői csoport elkészítette és annak nyilvánosságra hozatala előtt benyújtotta a Testületnek jóváhagyásra. A nyilvános kihirdetésre annak a Testület általi elfogadása után kerülhet sor, amely 2019 első negyedévében várható.

A fentieken túl a szakértői csoport a GDPR és az 536/2014/EU rendelet (az emberi felhasználásra szánt gyógyszerek klinikai vizsgálatáról szóló rendelet) közötti összefüggésekről az Európai Bizottság által készített dokumentumot véleményezte. A véleményezett dokumentumot a Bizottság *„Kérdések és válaszok a klinikai vizsgálatokról szóló rendelet (CTR) és az általános adatvédelmi rendelet (GDPR) kapcsolatáról"* elnevezéssel kívánja később nyilvánosságra hozni. A szakértői csoport által a dokumentumról elkészített vélemény jellemzően a hozzájárulás és a többi lehetséges adatkezelési jogalap elemzésére koncentrál. A vélemény szerint a hozzájárulás megfelelő jogalap lehet, azonban csak néhány viszonylag szűk esetben, így nem ez az előnyben részesített megoldás. A dokumentum nyilvánosságra hozatala 2019 első negyedévében várható.

VII.1.3. Végrehajtási ügyekkel (enforcement) foglalkozó szakértői alcsoport

Az Enforcement Expert Subgroup a GDPR alkalmazásával, így különösen az egyes rendelkezéseknek a tagállami felügyeleti hatóságok által történő végrehajtásával, illetőleg végrehajtatásával foglalkozó szakértői csoport, melynek feladata kisebb részben anyagi jogi, döntően azonban eljárásjogi kérdések értelmezése, megoldási javaslatok kidolgozása a felmerült konkrét problémák tekintetében.

A 2018. évben a GDPR alkalmazására történő felkészülés keretében tovább folytatódott az egyes felügyeleti hatóságok eljárásjogának, eljárási gyakorlatának felmérése egyes, sarokpontnak tekinthető témakörökben (pl. az alkalmazandó anyagi jog és eljárásjog a GDPR alkalmazásának kezdetén folyamatban lévő ügyekben; az érintettek által benyújtott panaszok befogadhatósági kritériumai; a felügyeleti hatóságok vizsgálati hatáskörével kapcsolatos rendelkezések a GDPR 62. cikke szerinti eljárás esetén; tagállami titokvédelmi szabályok az egyes felügyeleti hatóságokra vonatkozó eljárásjogban), ennek távlati célja a felügyeleti hatóságok jogértelmezésének, eljárásrendjének közelítése.

A szakértői alcsoportban már a GDPR alkalmazásának kezdete előtti időkben is volt hagyománya a hatóságok közötti információcserének, összehangolt fellépésnek a több tagállamot érintő, jelentős adatkezelési tevékenységek esetében, így például népszerű online közösségi médiafelületek kapcsán.

Az alcsoport 2018. évi tevékenysége során napirendjére vette a felejtés jogára vonatkozó iránymutatás, valamint a keresőmotorok találati listájáról történő eltá-

volítás kritériumainak GDPR-ra tekintettel történő átdolgozását, mely feladatok teljesítése jelenleg is folyamatban van.

VII.1.4. A Testület bírságügyekkel foglalkozó szakértői csoportja (Fining taskforce)

A Fining Taskforce lényegében az EDPB Enforcement szakértői alcsoportjából vált ki, elsődleges feladata a GDPR 58. cikk (2) bekezdés i) pontja, illetőleg 83. cikke alapján kiszabható közigazgatási bírság kiszabása vonatkozásában a felügyeleti hatóságok gyakorlatának felmérése, majd ennek fokozatos közelítése, lehetőleg összehangolása.

Mivel ez a szakmai fórum érdemi tevékenységét csak 2017 decemberében kezdte meg, jelenleg az említett feladat elvégzéshez szükséges hatósági eszköztár első elemeinek kidolgozását végzi. Emellett a GDPR hivatkozott rendelkezéseinek gyakorlati értelmezésével kapcsolatos kérdésekben is álláspont tervezetet készít elő (pl. a vállalkozás EUMSZ 101. és 102. cikke szerinti fogalmának értelmezése adatvédelmi jogi tárgyú jogesetekben).

VII.1.5. A nemzetközi adattovábbítással foglalkozó szakértői alcsoport (International Transfers)

A Testület nemzetközi adattovábbítás alcsoportja (a továbbiakban ITS) a 2018-as évben nyolc alkalommal tartott ülést. A 2018-as évet a GDPR V. fejezetében szabályozott, személyes adatok harmadik országba vagy nemzetközi szervezetek részére történő továbbítására vonatkozó rendelkezések értelmezésével, illetve az Európai Bizottság megfelelőségi határozataival kapcsolatos munka határozta meg.

Az alcsoportban került kidolgozásra a GDPR 49. cikkéről szóló iránymutatás. Ez a cikk tartalmazza azokat a különös helyzetekben biztosított eltéréseket, amelyek esetében megfelelőségi határozat és az adatkezelő által biztosított megfelelő garanciák hiányában is sor kerülhet személyes adatok harmadik országba vagy nemzetközi szervezet részére történő továbbítására. Az iránymutatás segítséget nyújt a személyes adatokat továbbító adatkezelők vagy adatfeldolgozók számára az ilyen kivételes, különös helyzetek értelmezésében és azonosításában, valamint ezek alkalmazásában.

Az ITS a 2018-as év során befejezte a kötelező erejű vállalati szabályokkal (a továbbiakban: BCR) kapcsolatos munkadokumentumoknak a GDPR fényében

történő felülvizsgálatát, melynek eredményeként a Testület elfogadta a BCR jóváhagyására irányuló eljárás során alkalmazandó együttműködési eljárással kapcsolatos munkadokumentumot (WP 263 rev.01.), illetve a GDPR szerint felülvizsgált adatkezelői és adatfeldolgozói BCR jóváhagyására irányuló kérelemformanyomtatványt.

Az alcsoport emellett elkezdett kidolgozni egy iránymutatást a közhatalmi vagy egyéb közfeladatot ellátó szervek általi harmadik országba történő adattovábbítás garanciáit megteremtő eszközökről [GDPR 46. cikk (2) bekezdés a) pont és (3) bekezdés b) pont], amelyet várhatóan a 2019-es év során fog a Testület elfogadni.

Az EU–USA adatvédelmi pajzs („Privacy Shield") felülvizsgálatában az alcsoport az ún. kereskedelmi vonatkozású kérdések vonatkozásában vett részt. Ennek kapcsán a 2018 októberében lezajlott felülvizsgálatot megelőzően a vizsgálat során alkalmazott dokumentumok előkészítése zajlott, a felülvizsgálatot követően pedig a Testület jelentésének összeállításában is közreműködött.

Az alcsoport 2018-as munkájában emellett meghatározó téma volt a Japánra vonatkozó megfelelőségi határozat Testület általi véleményezésének előkészítése. Az alcsoport tagjaiból alakult szakértői csoport mélyrehatóan elemezte a Japán adatvédelmi jogával kapcsolatos megállapításokat, illetve a 2017-es év során elfogadott WP 254 számú munkadokumentum alapján azt, hogy Japán adatvédelmi szintje valóban lényegében azonos-e az Európai Unióban nyújtott szinttel.

Az alcsoportban számos, BCR jóváhagyásával, és egyéb adattovábbítással kapcsolatos konkrét kérdésről is zajlott szakmai egyeztetés és tapasztalatcsere a szakértők között.

VII.1.6. A GDPR kulcsfontosságú rendelkezéseivel foglalkozó szakértői alcsoport (Key provisions)

A 29-es Munkacsoport Key Provisions alcsoportja folytatta munkáját a Testület felállítását követően is, „Key Provisions" szakértői alcsoport néven. Az alcsoport kiemelt feladata általános útmutatások kidolgozása az európai adatvédelmi jogszabályok, különösen pedig a GDPR és a bűnügyi adatvédelmi irányelv egységes értelmezésének és alkalmazásának előmozdítása érdekében. Munkájába bevonja a jogalkalmazókat és más szakértőket is nyilvános konzultációk formájában.

Kiemelendő a GDPR területi hatályáról (3. cikk) szóló 3/2018. számú testületi iránymutatás. A dokumentum tárgya a GDPR területi hatályával kapcsolatos rendelkezésének értelmezése, gyakorlati útmutatás az annak alkalmazása során felmerülő kérdésekkel kapcsolatban. Az iránymutatás, amelyet szintén nyilvános konzultációra bocsátottak, megtalálható a Testület honlapján.

VII.1.7. Együttműködési szakértői alcsoport (Cooperation)

A szakértői alcsoport tevékenysége nem látványos a külvilág számára, hiszen olyan ügyekkel foglalkozik, amelyek a hatóságok egymás közötti együttműködésével állnak összefüggésben, az általa előkészített dokumentumok címzettje nem az érintett polgár vagy az adatkezelő. Az alcsoportnak fontos szerepe van abban, hogy a GDPR alkalmazása a hatóságok között olajozottan, az eljárási szabályok közös megközelítése alapján folyhasson.

VII.1.8. A közösségi médiával foglalkozó szakértői alcsoport (Social Media)

A GDPR alkalmazandóvá válása előtt a 29-es Munkacsoport a közösségi médiával foglalkozó új alcsoportot hozott létre, azzal a céllal, hogy iránymutatásokat dolgozzon ki és stratégiai prioritásokat javasoljon a személyes adatoknak a közösségi média által nyújtott funkciókból eredő kezelésével és feldolgozásával kapcsolatban. A Social Media alcsoport (SMSG) mandátuma az alábbiakra terjed ki:

- a közösségi média meglévő és új funkcióinak – beleértve az adatkezelési tevékenységeket és az ezekből fakadó kockázatokat is – elemzése;
- a közösségi média által nyújtott funkciókkal, illetve azok – különösen gazdasági vagy politikai célokból való – felhasználásával kapcsolatos iránymutatások, ajánlások és legjobb gyakorlatok kidolgozása; és
- más alcsoportokkal való közreműködés, elsősorban a felügyelettel, valamint új EDPB iránymutatások kidolgozásával és WP29-es iránymutatások aktualizálásával összefüggő stratégiai prioritásokra való javaslattétel formájában.

Az ülések visszatérő napirendi pontja az ún. „*tour de table*”, amikor is a nemzeti szakértők röviden beszámolhatnak az online közösségi média platformok funkcióit (célzott hirdetés, személyre szabás, applikációk integrálása, közösségi plug-inek, felhasználók azonosítása/hitelesítése, elemzések, stb.) érintő, nemzeti szinten folyó tevékenységeikről (pl. iránymutatások kiadása, folyamatban lévő vizsgálatok, beérkezett panaszok típusai, állásfoglalás-kérések, stb.). A cél

nem konkrét esetek megoldása és megvitatása, hanem az alcsoport munkája szempontjából releváns információk összegyűjtése.

A 2018-as üléseken szintén visszatérő napirendi pont volt a brit adatvédelmi hatóság (Information Commissioner's Office – ICO) által indított vizsgálat a nagy port kavart Facebook-Cambridge Analytica incidens kapcsán. Az ICO minden ülésen beszámolt a legfrissebb fejleményekről és a vizsgálattal kapcsolatban kiadott aktuális jelentéseiről, amelyek megtalálhatóak az ICO honlapján is: https://ico.org.uk/action-weve-taken/investigation-into-data-analytics-for-political-purposes/.

VII.1.9. Az új informatikai rendszert használók szakértői alcsoportja (IT user)

Az IT User szakértői alcsoport a Testület legfiatalabb alcsoportja. A Future User csoport utódjaként jött létre, melynek feladata a tagállami hatóságok szakértőinek felkészítése volt a Testület elektronikus ügykezelő rendszerének, a Belső Piaci Információs Rendszer (IMI) használatára.

A 2018. októberében tartott első ülésével megalakuló IT User szakértői alcsoport elsősorban az IMI rendszer fejlesztésével és a rendszer fennálló problémáinak felszámolásának nyomon követésével foglalkozik. Az Alcsoport tagjai visszajelzéseket és javaslatokat fogalmaznak meg a Testület felé annak érdekében, hogy a rendszert a felhasználói igényeknek megfelelően fejleszthessék.

Továbbá az Alcsoport lehetőséget biztosít arra, hogy a tagállami szakértők megosszák egymással ügykezelési gyakorlatukat, illetve a Testület Titkársága is intézhet felhívásokat a tagok felé. Mindez elősegíti az IMI rendszerrel egységes felhasználói gyakorlatának kialakulását.

Habár fókuszában az IMI rendszer áll, az Alcsoport foglalkozik más informatikai rendszerekkel melyeket a Testület üzemeltet. Ilyen például a Testület videokonferencia rendszere, valamint a tagállami hatóságok közti együttműködést segítő tudásbázis, az EBPD Confluence.

VII.2. Az Európa Tanács Adatvédelmi Egyezményének korszerűsítése

Az Európa Tanács 1981-ben elfogadott, a személyes adatok gépi feldolgozása során az egyének védelméről szóló úgynevezett 108-as Egyezménye (Magyarországon kihirdette az 1998. évi VI. törvény) az első jelentős, az egyezményben részes államokra nézve kötelező erejű nemzetközi jogi dokumentum az adatvédelem terén. Ez az egyezmény négy évtizeden át biztosította az adatvédelem kereteit és szolgált alapul a nemzeti és nemzetközi szabályozásokhoz. Hét év előkészítés után 2018. május 18-án elfogadták a 108-as Egyezményt Módosító Jegyzőkönyvet (ETS 223), melyet 2018. október 10-én nyitottak meg aláírásra ünnepélyes keretek között. Magyarország 2019. január 9-én írta alá a dokumentumot. Thorbjørn Jagland főtitkár szerint a korszerűsített egyezmény, amelyet az adatvédelmi szakértők „108+ Egyezménynek" is neveznek, globális szinten egy egyedülálló eszközt biztosít az együttműködésre a személyes adatok védelmére vonatkozó szabályozás területén.

A 108-as egyezmény modernizálása két fő célt tűzött ki:

- egyrészt az új információs és kommunikációs technológiák használatából eredő kihívások kezelését,
- másrészt az egyezmény még hatékonyabb és szigorúbb alkalmazását.

A korszerűsített egyezmény célja annak biztosítása, hogy a személyes adatok határokon átnyúló továbbítása megfelelő biztosítékokkal történjen, valamint, hogy egységességet teremtsen a nemzetközi normatív keretekkel, ideértve az európai uniós szabályozást is. A felülvizsgált szerződés lehetőséget nyújt az Európa Tanács valamennyi tagállamának és nemzetközi szervezeteknek is a csatlakozásra.

Az Egyezmény legfontosabb újításai:

- szigorúbb követelmények az adatkezelés folyamatában az arányosság és az adattakarékosság elvének alkalmazásával;
- a különleges adatok fogalmának kiterjesztése (genetikai és biometrikus adatok, szakszervezeti tagság, etnikai származás);
- az adatvédelmi incidensek bejelentésére vonatkozó kötelezettség;
- nagyobb átláthatóság az adatkezelés során;
- új jogosultságok a természetes személyek részére az automatizált döntéshozatali rendszerek alkalmazása során, melyek különös fontossággal bírnak a mesterséges intelligenciára vonatkozó fejlesztések kapcsán;
- az adatkezelők szigorúbb elszámoltathatósága;

- a határokon átnyúló adattovábbítások világos rendszerének kialakítása;
- az adatvédelmi hatóságok megerősített hatásköre és függetlensége, valamint a nemzetközi együttműködés jogalapjának erősítése.

VII.3. Nemzetközi tanácskozások Budapesten

VII.3.1. A Berlini Munkacsoport 63. budapesti ülése

A Berlini Munkacsoport 63. ülésére a Hatóság rendezésében Budapesten került sor 2018. április 9-10-én, a Grand Hotel Margitszigetben, 53 fő részvételével. Az ülést visszajelzések alapján sikeresnek és szakmai szempontból tartalmasnak ítélték meg a résztvevők. A két nap során a következő napirendi pontok kerültek megtárgyalásra: közös álláspont megszövegezése adatvédelmi standardok kialakítására a határokon átnyúló bűnüldözési célú adatkérések során; vélemény megszövegezése az okosautók és intelligens közlekedési rendszerek adatvédelmi kihívásairól; intelligens infrastruktúra/városok adatvédelmi aggályainak áttekintése; vélemény megszövegezése mesterséges intelligencia adatvédelmi kihívásairól; intelligens játékok okozta adatvédelmi aggályok áttekintése; a szülői hozzájárulás beszerzésének kérdése a gyerekek felé irányuló adatkezelések során; intelligens TV és a magánszféra védelme. A találkozón két dokumentum is elfogadásra került: *„Az okos autókról/összekapcsolt járművekről”*, valamint az *„Adatvédelmi standardok kialakítása a határokon átnyúló bűnüldözési célú adatkérések során”*.

VII.3.2. Data Protection Case Handling Workshop – 2018. november 27-29.

A 2012-es workshopot követően 2018 novemberében ismételten a magyar hatóság volt a házigazdája az európai adatvédelmi hatóságok munkatársainak rendszeresen szervezett, kifejezetten gyakorlati esetekre koncentráló találkozójának (Data Protection Case Handling Workshop, 27-29 November, 2018).

A találkozón több, mint 50 adatvédelmi szakember vett részt 14 Európai Uniós és 7 Európai Unión kívüli ország hatóságának képviseletében. Az előzetes felmérés és javaslatok alapján összeállított napirendi témák a hatósági eljárásokra, az aktuális adatvédelmi kérdésekre koncentráltak, különös tekintettel a GDPR hatályba lépése következtében felmerülő, országhatárokon átnyúló adatvédelmi kérdésekre. A rövid előadásokat követő kerekasztal tanácskozások keretében

olyan aktuális témák kerültek megvitatásra, mint a 3. országokba történő adattovábbítás, az EU-s és EU-n kívüli nemzeti hatóságok közötti 50. cikk szerinti együttműködése, a nyilvánosan elérhető személyes adatok felhasználása, a kamerás megfigyelés és a hozzáférési jog gyakorlásának kérdésköre.

A résztvevők visszajelzése a találkozó eredményességéről igen pozitív volt. A magyar hatóság javaslatára a jövőben megrendezendő találkozóknál a korábbi házigazda hatóság egyfajta titkárság szerepét tölti majd be, ezzel segítve a nemzeti hatóságok közötti kapcsolattartást és együttműködést.

2018. november 26-27-én Budapesten került megrendezésre első alkalommal az az „esetjogi gyakorlatok" bemutatását célzó nemzetközi találkozó, mely a közérdekű adatok nyilvánosságát felügyelő nemzeti intézmények munkatársait gyűjtötte egybe 11 országból. Erről az eseményről a beszámoló „Információszabadság" fejezetében bővebben is írtunk.

VII.4. Fogyasztóvédelmi és adatvédelmi hatóságok közös workshopja

A közösségi média platformokkal kapcsolatban számos olyan probléma és aggály merül fel, amelynek fogyasztóvédelmi és adatvédelmi vonatkozása is van, ennek megfelelően a fogyasztóvédelmi és adatvédelmi hatóságok közötti együttműködésre különös hangsúlyt kell fektetni. Ennek keretében, az Európai Bizottság Jogérvényesítési és Fogyasztópolitikai Főigazgatóságának (DG JUST) szervezésében, a fogyasztóvédelmi és adatvédelmi hatóságok képviselőinek részvételével, 2018. november 23-án Brüsszelben került megrendezésre a fogyasztóvédelmi és adatvédelmi hatóságok második közös workshopja, melyen a NAIH delegált szakértője és a Gazdasági Versenyhivatal is képviseltette magát. A workshop az adatvédelem és a fogyasztóvédelem közötti szinergia témakörét érintő előadások és esettanulmányok köré épült, és konklúzióként a Bizottság a fogyasztóvédelmi és adatvédelmi hatóságok közötti tényleges együttműködés elősegítése és erősítése érdekében az alábbi lehetőségeket vázolta fel:

– Egy közös „wiki" felület létrehozása, amelyen a két szakterület egyrészt kommunikálhat, másrészt tapasztalatokat és jó gyakorlatokat oszthat meg egymással. A felület elkészült, a hozzáférés a workshopon részt vevők számára biztosított.
– Egy olyan munkacsoport létrehozása (önkéntes alapon), amely a nemzeti hatóságok közötti gyakorlati együttműködéssel és végrehajtással

kapcsolatban dolgozna ki iránymutatást. A workshop során folytatott beszélgetésekből egyértelműen kiderült, hogy hasznos lenne az együttműködéssel kapcsolatos jó gyakorlatok megosztása és/vagy olyan minták, sablonok kidolgozása, amelyeket felhasználva a hatóságok könnyebben tudnának együttműködési/egyetértési megállapodásokat kötni.

– Bizonyos szolgáltató szektorokban működő vállalkozások számára közös iránymutatások kidolgozása a fogyasztóvédelmi és adatvédelmi követelményeknek való megfelelésről
– Fogyasztóvédelem és adatvédelmi szempontból egyaránt releváns alapvető jogi fogalmak (mint pl. a tisztességesség elve) egységes értelmezése a koherens jogalkalmazás és végrehajtás érdekében.

VIII. A NAIH projektjei

VIII.1. A STAR I. és a STAR II. Projekt

A NAIH a brüsszeli Vrije Egyetemmel és egy brit-ír tanácsadó és kutató-fejlesztő céggel, a Trilateral Research Ltd.-del partnerségben két egymáshoz kapcsolódó, az Európai Unió társfinanszírozásában futó adatvédelmi tárgyú projekt megvalósításában is részt vesz.

A 2017. november 1. – 2019. október 31. közötti REC-RDAT-TRAI-AG-2016 programba tartozó, 769138 azonosítószámú, 357.968,50 € összköltségvetésű (ebből 283.439,46 € uniós támogatás) STAR *(Support Training Activities on the data protection Reform)* project során az uniós adatvédelmi hatóságok és adatvédelmi tisztviselők részére szóló, a GDPR-hoz kapcsolódó képzési anyagok (diasorok, kézikönyv) kerülnek összeállításra és tesztelésre.

A 2018 augusztus 1. – 2020 július 31. közötti REC-RDAT-TRAI-AG-2017 programba tartozó, 814775 azonosítószámú, 560.580 € összköltségvetésű (ebből 448.544 € uniós támogatás) STAR II *(Support small And medium enterprises on the data protection Reform II)* projekt célja, hogy EU-szerte támogassa a kis- és középvállalkozásokat (KKV-k) az általános adatvédelmi rendelet megfelelő alkalmazásában. A projekt a KKV-k struktúráját és igényeit figyelembe véve nyújt támogatást a szóban forgó vállalkozásoknak a megfelelő gyakorlat kialakításában, továbbá elősegíti a GDPR egységes alkalmazását, a határokon átnyúló együttműködést, a legjobb gyakorlat terjesztését a tagállamok között. A NAIH a projekt keretében egy kimondottan erre a célra létrehozott, 2019. március közepétől egy évig élő e-mail címen (kkvhotline@naih.hu) fogadja az EU-ban működő KKV-k kérdéseit. Az ide érkező kérdések megválaszolásán túl, a KKV-k által felvetett problémakörök és gyakori kérdések alapján kidolgozásra kerül egy kézikönyv, amely széles körben elérhető és felhasználható lesz EU-szerte.

VIII.2. IJR Projekt a NAIH általános adatvédelmi rendelet alkalmazására történő felkészülését és szakfeladatainak végrehajtását támogató projektje

Az 1004/2016. (I.18.) Korm. határozat alapján a KÖFOP 1.0.0. – VEKOP-15 kiemelt kormányzati projekt keretében a költségvetési szervek adminisztratív ter-

heinek csökkentését célzó projektek között jött létre az Integrált Jogalkotási Rendszer (a továbbiakban: IJR).

A projekt keretében valósul meg a NAIH európai uniós kötelezettségeiből adódó jogszabály-változáshoz igazodó eljárásrendi, ügyviteli, információtechnológiai és információbiztonsági fejlesztése.

2017 áprilisában aláírásra került a 1585/2016. (X. 25.) Korm. határozat alapján az IJR projekt Támogatási Szerződés 1. számú módosítása, amely a konzorciumi partnerek között nevesíti a Hatóságot, illetve a projekt által támogatott és a GDPR-ból is fakadó feladatokat. A NAIH konzorciumi partnerként csatlakozott az IJR projekthez, figyelembe véve annak alapvető céljait és eszközrendszerét.

A GDPR-ban foglalt követelmények teljesítése a NAIH IT-szakmai területeinek teljes optimalizálását, áttervezését és ezek megvalósítását igényli. A NAIH szervezeti kereteinek is sokkal inkább a hatósági működési követelmények irányába szükséges elmozdulniuk, amely hangsúlyozottan egy feszesebb és kontrollálhatóbb működési megközelítést igényel. Ehhez az IT-fejlesztésnek, támogatásnak és az üzemeltetésnek is igazodnia kell.

Az IJR projekt keretében 2018-ban létrejött az adatvédelmi incidensek adatkezelők általi bejelentésére szolgáló rendszer (DBN), hiszen a GDPR 2018. május 25-től kötelezővé teszi a kezelt adatok tekintetében a bizalmasság, sértetlenség és a rendelkezésre állás sérülésével járó adatvédelmi incidensek bejelentését. Az illetékes tagállami adatvédelmi hatóság, azaz a NAIH nem csupán fogadja, hanem értékeli is a bejelentéseket. A fentiekben részletesen kifejtetteknek megfelelően a Hatóság a bejelentés tartalma, valamint a beszerezett információk alapján kötelezheti az adatkezelőt további intézkedések megtételére, illetve az érintettek tájékoztatására. Az incidens értékelésekor a NAIH dönthet úgy, hogy hatósági eljárást indít az ügyben. Ennek a feladatnak a végrehajtását hivatott támogatni az adatvédelmi incidens feldolgozó rendszer (DBP).

2018-ban az IJR projekt keretében folytatódott a NAIH számára egy integrált, intelligens ügyintéző és határozat-előkészítő modul fejlesztése, valamint sor került, továbbá a rendszerek informatikai, IT biztonsági és szervezeti implementációjára is.

A projekt keretében kialakításra kerül egy olyan, mind az uniós, mind a hazai elvárásoknak megfelelő rendszer, amely képes az eddigiekhez képest összetettebb és nagyságrendileg nagyobb ügyintézési terhelés professzionális kezelésére.

IX. Mellékletek

IX.1. Elutasított közérdekű adat igénylések és tájékoztatási kérelmek

IX.1.1. Az elutasított közérdekű adatigénylésekről és azok indokairól szóló 2018. évi tájékoztatási kötelezettség teljesítésének statisztikai adatai

A közérdekű és a közérdekből nyilvános adat megismerése iránti elutasított kérelmekről, valamint az elutasítások indokairól az Infotv. 30. § (3) bekezdés második fordulata alapján kell az adatkezelőnek a tárgyévet követő év január 31-éig tájékoztatnia a Hatóságot. Emellett az adott közfeladatot ellátó szervre vonatkozóan a közérdekű adatokkal kapcsolatos kötelező statisztikai adatszolgáltatást (ami megegyezik a Hatóságnak megküldöttel) közzé kell tenni az Infotv. 1. számú mellékletében meghatározott általános közzétételi lista II. 15. közzétételi egységében is.

Az Infotv. továbbra sem rendelkezik arról, hogy a közérdekű adattal rendelkező adatkezelők az elkészített adatszolgáltatásukat milyen módon és formában teljesítsék a Hatóság felé. A jelentéstételi kötelezettség teljesítését segítendő a Hatóság a honlapján (www.naih.hu) közzétette az általa elkészített adatlapot, melyet kitöltve az adatszolgáltatásra kötelezett szervek tájékoztathatják a Hatóságot.

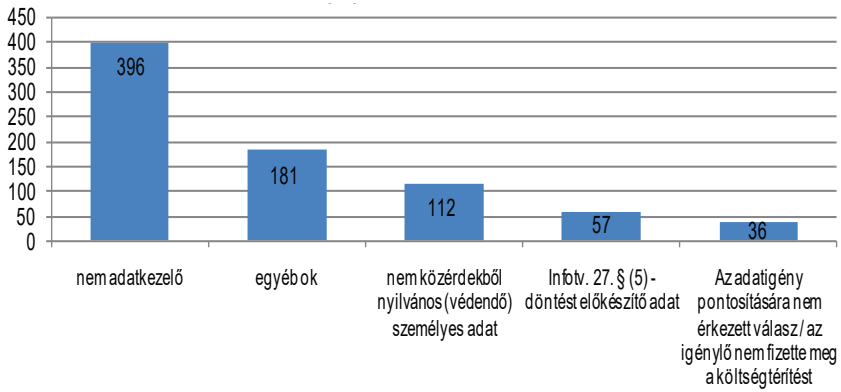
A Hatósághoz 2019 februárjáig 256 adatkezelő tett eleget az Infotv. szerinti tájékoztatási kötelezettségének. A beérkezett jelentések összesített adatai azonban nem tekinthetőek pontos adatoknak, mivel az adatkezelők eltérő módon és részletezettséggel teljesítik adatszolgáltatásukat a Hatóság felé. Van szervezet, amely kizárólag az elutasított adatigénylésekkel kapcsolatos információkról nyújt tájékoztatást, és van, amely a Hatóság honlapján elérhető adatlapot kitöltve, részletekbe menően teljesíti az Infotv. szerinti kötelezettségét és információt szolgáltat az adott évben hozzá benyújtott közérdekű adatok megismerésére irányuló kérelmek és a teljesített adatigények számáról is. Ezen eltérő adatközlésekből adódik az, hogy e tekintetben a Hatóság nem rendelkezik pontos információval.

A közérdekű és a közérdekből nyilvános adatigénylések teljesítése/elutasítása tekintetében nyújtott 2018. évi összesített adatok			
adatkezelők száma	összes adatigénylés (db)	ebből	
		teljesített (db)	elutasított/részben elutasított (db)
256	**3717**	**2882**	**940**

IX.1.2. Az adatmegismerés megtagadási okai

A közérdekű és közérdekből nyilvános adatokra vonatkozó adatigénylések megtagadása, azok elutasítási okait tekintve széles skálán mozognak. Az áttekinthetőség érdekében az első öt leggyakrabban alkalmazott elutasítási okot jelenítettük meg a jelmagyarázatban.

Az öt leggyakrabban alkalmazott megtagadási ok



A közérdekű és a közérdekből nyilvános adatok iránti igények teljesítésére/elutasítására vonatkozó 2018. évi statisztika

A Hatóságnak megküldött jelentésekben a közfeladatot ellátó, közpénzzel gazdálkodó, illetve közszolgáltató szervek legtöbbször arra hivatkozással tagadták meg a hozzájuk benyújtott adatigénylés teljesítését, hogy az igényelt adat vonatkozásában nem minősülnek adatkezelőnek. Ezen okból történő elutasítás a Hatóság számára ismert 3717 jelentés közül 396 esetben (10,6 %) történt. Ez az elutasítási ok a 42 %-át teszi ki az összes elutasításnak.

Lényegesen kevesebbszer történt hivatkozás a többi, a grafikonon megjelenített okokra:

- egyéb ok – 181 db (19 %)
- az igényelt adat nem közérdekből nyilvános (védendő) személyes adat – 112 db (11,9 %)
- az igényelt adat döntést előkészítő adat – 57 db (6 %)
- az adatigény pontosítására nem érkezett válasz/az igénylő nem fizette meg a költségtérítést – 36 db (3,8 %)

IX.1.3. Az „egyéb ok" – mint elutasítási ok részletezése

Az összes elutasítási esetből 18 alkalommal ún. „egyéb ok" eredményezte az adatigénylés sikertelenségét. A Hatóság felé adatszolgáltatást teljesítő közfeladatot ellátó szervek közül 49 szerv tagadta meg ezzel az indokkal az adatigénylés teljesítését, ez a szám a jelentést megküldő szervek 19 %-át teszi ki.

Jellemző „egyéb" megtagadási okok:

- nem áll a közfeladatot ellátó szerv rendelkezésére a kért adat,
- nem lelhető fel az adatkezelőnél az adat,
- a kérelemben megjelölt adatokat az ügyek nyilvántartási adatai nem tartalmazzák és a kért adatszolgáltatás köre – az ügyek számán felül – meghaladta a szerv által statisztikai és iratkezelési célból kezelt adatok körét,
- a kért adatokat az adatkezelő nem állította elő,
- a kért adatok nem minősülnek sem közérdekű, sem közérdekből nyilvános adatnak,
- nem áll az adatkezelő rendelkezésére az adat,
- nem köteles előállítani az adatkezelő a kért adatot,
- új, minőségileg más adat előállítására lett volna szükség,
- a kért adatokat a közfeladatot ellátó szerv nem gyűjti, azok az eljárások irataiban szerepelnek, melyek nyilvánosságára, megismerhetőségére külön jogszabályok vonatkoznak.

IX.1.4. A Hatósághoz 2018. évben benyújtott közérdekű adatigénylések adatai

A Hatósághoz 2018. év folyamán 74 db közérdekű adatigénylést nyújtottak be az adatigénylők. Az igények többségükben a GDPR-ra való felkészüléssel kapcsolatos információkra, illetve 2018. május 25-ét követően pedig az adatkezelések GDPR szerinti nyilvántartására, az adatkezelések tájékoztatóira, valamint a Hatósághoz bejelentett adatvédelmi incidensekre vonatkozó adatok megismerésére irányultak.

2018-ban a Hatósághoz benyújtott adatigénylésekből 59-et a Hatóság teljesített, míg 3 esetben azokat részben, 12 esetben pedig teljes egészében elutasította. Két adatigénylés megtagadási oka sorolható az „egyéb" elutasítási okok közé, nevezetesen: nem áll a Hatóság rendelkezésére a kért adat, illetve az igénylő visszavonta közérdekű adatigénylését.

IX.2. Az adatvédelmi tisztviselők nyilvántartása

A GDPR 37. cikk (7) bekezdése szerint az adatkezelőnek vagy adatfeldolgozónak az általa kijelölt adatvédelmi tisztviselő elérhetőségét közzé kell tennie és erről tájékoztatnia kell az illetékes felügyeleti hatóságot.

Az Infotv. 25/L. § (4) bekezdése alapján pedig az adatkezelő, illetve az adatfeldolgozó tájékoztatja a Hatóságot az adatvédelmi tisztviselő nevéről, postai és elektronikus levélcíméről, ezen adatok változásáról, valamint ezen adatokat nyilvánosságra hozza.

A Hatóság az adatkezelők, illetve adatfeldolgozók számára külön erre a célra létrehozott elektronikus felületen 2018. szeptember 17-től tette lehetővé az adatvédelmi tisztviselő, illetve tisztviselők bejelentését.

A Hatóság az Infotv. 70/B. § (1) és (2) bekezdése alapján az érintettek és az adatkezelők tájékozódásának elősegítése érdekében közzéteszi a Hatóság részére bejelentett adatvédelmi tisztviselő

- nevét,
- postai és elektronikus levélcímét,
- által képviselt adatkezelő vagy adatfeldolgozó megnevezését.

A felsorolt adatok közérdekből nyilvános adatok.

A Hatóság az adatvédelmi tisztviselő bejelentő rendszerbe az adatvédelmi tisztviselőre vonatkozó bejelentést akkor tekinti megtettnek, ha az adatvédelmi tisztviselő a bejelentő rendszerbe rögzített e-mail címére küldött értesítés alapján az adatokat 15 napon belül jóváhagyja.

Amennyiben az adatvédelmi tisztviselő a bejelentő rendszerbe rögzített e-mail címére küldött értesítés alapján a bejelentést nem hagyja jóvá vagy 15 napon belül nem erősíti meg, a Hatóság a bejelentést meg nem tettnek tekinti és az adatvédelmi tisztviselőre vonatkozó adatokat nem teszi közzé.

A Hatóság weboldalán a nyilvános adatvédelmi tisztviselő nyilvántartásban adatkezelő megnevezése alapján bárki számára elérhetőek az adatvédelmi tisztviselő adatai (https://dpo-online.naih.hu/DPO/Search).

Az adatvédelmi tisztviselő bejelentő rendszerbe 2018-ban 1786 bejelentés érkezett.

IX.3. A Hatóság 2018. évi gazdálkodása

2018. december 31-én zárult a Hatóság működésének és gazdálkodásának 7. éve. Ezen gazdálkodással összefüggő adatokról az alábbiakban adunk rövid tájékoztatást.

IX.3.1. A bevételi előirányzat és teljesítési adatai 2018. évben

A NAIH 2018. évi költségvetése, eredeti előirányzata 1 084 100 eFt volt, melyből a kiemelt személyi előirányzat 631 300 eFt, a munkáltatói járulék és szociális hozzájárulás előirányzat 121 400 eFt, a dologi kiadások kiemelt előirányzata 200 400 eFt, a felhalmozási célú előirányzat 131 000 eFt.

A 2018. év módosított előirányzata 1 182 356 eFt volt, mely tartalmazza az eredeti előirányzatot, a 67 558 eFt kötelezettségvállalással terhelt 2017. évi maradványt, valamint a STAR I és II EU-pályázatokból származó, 11 145 eFt egyéb bevételt. Ezen kívül, az egyéb működési célú 16 391 eFt bevételt, az egyéb szolgáltatások+áfa bevételét, mely 1 840 eFt. Idén 43 eFt tárgyi eszköz értékesítéséből, valamint BCR-bevételünk 266 eFt értékben keletkezett. A bérkompenzáció és garantált bérminimum összege 1 056 eFt-ot tett ki a központi, irányítószervi támogatásból. Az erre vonatkozó számokat a következő táblázat mutatja:

Megnevezés	Eredeti előirányzat	Módosított előirányzat	Teljesítés	Alap-tevékenység 2018. évi maradványa
Eredeti előirányzat	1 084 100			
Közhatalmi bevételek		266	266	
Szolgáltatások bevételei		1 440	1 440	
Kiszámlázott forgalmi adó bevétel		400	400	
Árfolyamnyereség		1 669	1 669	
Biztosító általi fizetett kártérítés		36	36	
Egyéb működési bevételek		14 643	14 643	
Tárgyi eszköz értékesítés		43	43	
Egyéb működési c. átvett pénzeszköz (STAR I&II)		11 145	11 145	
2017. évi költségvetési maradvány		67 558	67 558	
Központi, irányító szervi támogatás	1 084 100	1 085 156	1 085 156	
ebből: bérkompenzáció, garantált bérminimum		1 056	1 056	
Bevételi előirányzatok mindösszesen:	1 084 100	1 182 356	1 182 356	-
Személyi juttatások előirányzata	631 300	632 461	620 693	11 768
Munkáltatói járulék és szociális hozzájárulási adó	121 400	139 833	137 578	2 255
Dologi kiadások előirányzata	200 400	218 925	120 865	98 060

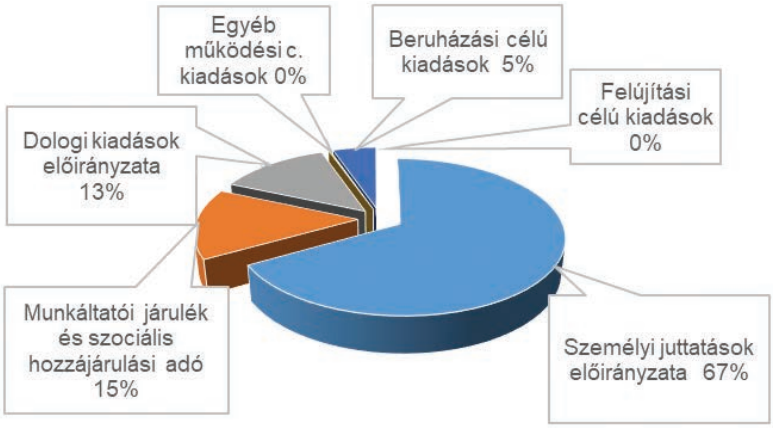
Egyéb működési c. kiadások	-	1 651	1 651	-
Beruházási célú kiadások	115 100	151 851	47 253	104 598
Felújítási célú kiadások	15 900	2 635	1 517	1 118
Egyéb felhalmozási célú kiadások	-	35 000		35 000
Kiadási előirányzatok mindösszesen:	**1 084 100**	**1 182 356**	**929 557**	**252 799**

IX.3.2. Kiadási előirányzatok és teljesítési adatai

A 2018. évi költségvetés eredeti előirányzata 1 084 100 eFt volt. A módosított kiadási előirányzat 1 182 356 eFt, melyből a teljesített személyi előirányzat kiadása 620 693 eFt. A munkáltatói járulék és szociális hozzájárulási adó kiadások teljesítése 137 578 eFt. A dologi kiadások összesen 120 865 eFt. A felhalmozási kiadások 48 770 eFt, az egyéb működési célú kiadások összege pedig 1 651 eFt volt.

A következő grafikon a módosított előirányzatok teljesült kiadásait mutatja %-os megoszlásban:

Teljesített kiadási előirányzatok megoszlása



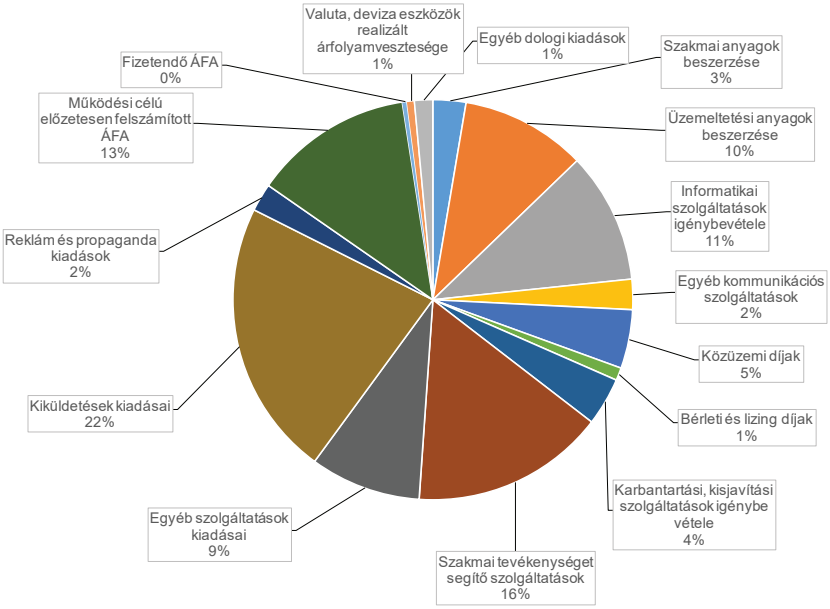
A 2018. évi módosított előirányzatok 67%-a személyi juttatások kiadásaként teljesültek. A munkáltatói járulék és szociális hozzájárulási adó 15% volt a teljes kiadáshoz mérten. A kiemelt dologi előirányzatok az összes módosított költségvetés 13%-át tették ki. A beruházási és felújítási célú kiadások a teljes költségvetés 5 %-aként teljesültek. Az egyéb működési célú kiadások értéke 1% alatt volt.

A Hatóság alaptevékenységének 2018. évi maradványa 252 mFt lett, ebből kötelezettségvállalással terhelt 102 mFt maradvány és 150 mFt maradványt utalunk vissza a központi költségvetési maradványszámlára. Erre azért kerül sor, mert a Hatóság feladat- és létszámbővítése következtében a tervezett elhelyezési feladat nem valósult meg 2018-ban, ezen feladatok végrehajtása 2019. gazdálkodási évre tolódik el.

IX.3.3. A dologi kiadások megoszlása

A következő diagram a teljesült kiadási előirányzatok rovatrend szerinti %-os megoszlását mutatja.

Teljesült dologi kiadások megoszlása 2018.



A dologi kiadások legnagyobb részét, a kiküldetési kiadások teszik ki, mely 27 006 eFt, azaz 22%. A 2018. évi GDPR bevezetése miatt jelentős mértékben megnövekedett az uniós együttműködésben történő részvétellel szükségszerűen együtt járó utazások mennyisége.

A működési célú előzetesen felszámított ÁFA, – mivel Hatóságunk nincs visszaigénylő pozícióban – 13 %-a a teljes dologi kiadásnak, mely 15 575 eFt. A szakmai tevékenységet segítő szolgáltatás kiadásainak értéke 18 913 eFt. Az üzemeltetési anyagok értéke 12 246 eFt, valamint az informatikai szolgáltatások igénybe vételéért 12 750 eFt-ot fizetett ki a Hatóság. A közüzemi díjakért Hatóságunk mindösszesen 5 742 eFt-ot fizetett ki.

IX.3.4. A bírságbevételek alakulása

A Hatóság által kiszabott és befolyt bírság 40 236 eFt volt, mely teljes egészében a központi költségvetés bevétele.

IX.3.5. A Hatóság létszámának alakulása

2018. évre tervezett létszám 114 fő volt. A jelentős létszámbővülés több szakaszban, lépcsőzetesen valósul meg, mivel a 2018. évi költségvetésünk személyi előirányzata erre adott fedezetet. A személyi erőforrás felvétele napjainkban is folyik, melynek sajnos, határt szab a jelenlegi, mielőbb megoldandó elhelyezési problémánk.

IX.4. Fényképek a Hatóság eseményeiről

A Berlini munkacsoport ülése Budapesten 2018. április 9-én

A STAR II. Projekt alakuló ülése Budapesten 2018. szeptember 10-én

Az első információszabadság Case Handling Workshop ülése Budapesten 2018. november 26-án

IX.5. A Hatóság elnökének részvétele szakmai konferenciákon, rendezvényeken 2018-ban

IX.5.1. Nemzetközi események

2018. január 31. – Budapest – International Scientific Conference on Cyber Security in Public Service – *The General Data Protection Regulation and its Effects on Public Services*

2018. március 5-6. – Bécs – DATAPROTECTION 2018, Data & Democracy – Digital challenges for the cities - *Főbb adatvédelmi kihívások az önkormányzatok adatkezelésében*

2018. március 19-20. – Genf - Magyarországnak a Polgári és politikai Jogok Nemzetközi Egyezségokmánya végrehajtásáról egyszerűsített jelentéstételi eljárás keretében benyújtott hatodik jelentésének tárgyalása az Emberi Jogi Bizottság előtt

2018. március 27-28. – Washington – International Association of Privacy Professionals' (IAPP) Global Privacy Summit – *kerekasztal beszélgetések*

2018. május 3-4. – Tirana – Conference of European Data Protection Authorities – *kerekasztal beszélgetések*

2018. június 19-21. – Strasbourg - 36th plenary meeting of the Committee of Convention 108 – *kerekasztal beszélgetések*

2018. szeptember 17. – Berlin – Networked Oversight – New Approaches for Cooperation of Security and Intelligence Review Bodies in Germany and Europe – *kerekasztal beszélgetések*

2018. szeptember 25-26. – Brüsszel – European University Association Expert Group Meeting – Open Access / *kerekasztal beszélgetések*

2018. október 4-5. – Párizs - Centre for Information Policy Leadership (CIPL) - GDPR workshop on „Accountability under the GDPR – how to implement, demonstrate and incentivize it" – *kerekasztal beszélgetések*

2018. november 12-13. - Párizs – IMODEV Conference - ACADEMIC DAYS ON OPEN GOVERNMENT AND DIGITAL ISSUES - *Protection of fundamental rights in the light of freedom of information*

Az IMODEV és a Panthéon-Sorbonne Egyetem által támogatott, a nyílt kormányzati és digitális kérdésekről szóló nemzetközi „tudományos napok" elsődleges célja az, hogy összegyűjtse a különböző érdekelt feleket, hogy tudományos megközelítéssel elemezzék és megvitassák a nyílt kormányzati kérdéseket globális szinten. A multidiszciplináris esemény társítja a jogot, a politikatudományt, a közgazdaságtant, a menedzsmentet, a matematikát, a számítástechnikát, a társadalomtudományt, a történelmet, a szociológiát, a környezeti tudományt, a művészetet és minden más témát vagy területet, amely ezekhez a kérdésekhez kapcsolódik. A tudományos napok létrehozása az OGP (Open Government Partnership – Nyílt Kormányzati Együttműködés) tagországok azon tapasztalataira épült, hogy kiemelkedően fontos a kormányok és a civil szervezetek közötti hatékony együttműködés és kommunikáció kialakítása az átlátható és nyílt kormányzás megvalósításához.

IX.5.2. Hazai események

2018. január 16. – Budapest, Novotel Budapest City – Magyar Szállodák és Éttermek Szövetségének konferenciája az új adatvédelmi rendeletről – ***Az új európai adatvédelmi szabályozás és a magyar vonatkozásai***

2018. január 24. – Budapest, Bankcentrum – Magyar Kereskedelmi és Iparkamara központi tájékoztató rendezvénye a GDPR kapcsán – ***Az új európai adatvédelmi szabályozás és a magyar vonatkozásai***

2018. január 25. – Budapest, ÁSZ Üvegterem – Fókuszban: az etikus közpénzügyi vezetőképzés, Az Állami Számvevőszék és a Miskolci Egyetem Gazdaságtudományi Kar közös konferenciája és könyvbemutató kerekasztal beszélgetés – ***kerekasztal megbeszélés***

2018. február 1. – Budapest, Hotel Hungaria City Center – Infoszféra Konferencia – ***Az új európai adatvédelmi szabályozás és a magyar vonatkozásai***

2018. február 5. – Debrecen, Nonprofit Gazdaságfejlesztő Szervezetek Háza – Hajdú-Bihar Megyei Kereskedelmi és Iparkamara által szervezett „GDPR – az EU Általános Adatvédelmi Rendelete – minden vállalkozás életét érintő jog-

szabály" című konferencia – ***Az új európai adatvédelmi szabályozás és a magyar vonatkozásai***

2018. február 14. – Budapest, Petőfi Sándor Művelődési Ház – Magyar Gyógyszergyártók Országos Egyesületének tagvállalati szakemberei számára tartott képzés az EU Általános Adatvédelmi Rendeletéről – ***Az új európai adatvédelmi szabályozás és a magyar vonatkozásai***

2018. február 15. – Budapest, MÜPA – Medical Tribune GDPR – „Betegek, orvosok, ipar. Adatok és adatvédelem" Konferencia– ***Az új európai adatvédelmi szabályozás és a magyar vonatkozásai***

2018. február 27. – Budapest, Marriott Hotel – Portfolio Konferencia, „GDPR Summit 2018, Adatkezelés újragondolva" – ***GDPR itthon – a legfontosabb változások a háttérszabályozásban***

2018. március 2. – Budapest, Danubius Hotel Arena – „2018. GDPR átfogóan – Adatvédelem kezdőknek és haladóknak" szakmai rendezvény – ***Az adatvédelem szabályozásának megújítása***

2018. március 12. – Szeged – A Csongrád Megyei Kereskedelmi és Iparkamara és a Szegedi Tudományegyetem Munkaügyi Kapcsolatok és Társadalombiztosítási Képzések Intézete által szervezett „GDPR - az EU Általános Adatvédelmi Rendelete - minden vállalkozás életét érintő jogszabály" című rendezvény - ***A GDPR az üzleti szektor szemszögéből***

2018. március 13. – Budapest – Wolters Kluwer szakmai konferenica: „GDPR a gyakorlat oldaláról" - ***Az új európai adatvédelmi szabályozás és a magyar vonatkozásai***

2018. március 13. – Budapest, Fortuna Szálloda- és Étteremhajó, – Magyar Detektív Szövetség, Detektív Klubnap ***– Az új európai adatvédelmi szabályozás és a magyar vonatkozásai***

2018. március 21. – Budapest, Budapest Music Center – Danubian GDPR Summit Konferencia – ***A nyilvánosság és a privacy határa***

2018. március 21. – Budapest, Groupama Aréna – Microsoft Future Decoded Konferencia – ***Mit kell tenni a megfelelőség érdekében a hatóság szemszögéből? Mit és hogyan fog ellenőrzizni a hatóság?***

2018. március 22. - Balatonakarattya – Magyar Honvédség Adatvédelmi Konferencia - ***A NAIH feladatai és hatáskörei 2018. május 25-től, és az Európai Adatvédelmi Testület jogállása, tevékenysége***

2018 április 4. – Budapest, Lurdy Ház – „Hogyan feleljünk meg a GDPR elvárásainak?" – a Menedzser Praxis Szakkiadó által szervezett szakmai nap – ***Állásfoglalások, ajánlások, szankciók - Tanácsok a NAIH elvárásainak való megfeleléshez***

2018. április 11. – Budapest, Hotel Hungaria City Center – Infoszféra Konferencia – ***Az új európai adatvédelmi szabályozás és a magyar vonatkozásai***

2018. április 14. - Hollókő, Hotel Castellum – Egyenlő Bánásmód Hatóság által szervezett szakmai konferencia – ***Az EBH szempontjából releváns rendelkezések a GDPR-ban és az Infotv. tervezett módosításában***

2018. április 17. – Szombathely, Agora Savaria Filmszínház nagyterme - „GDPR – ADATVÉDELMI KONFERENCIA - alapvető tudnivalók az új adatvédelmi rendelet alkalmazásáról" című tájékoztató rendezvény a Vas Megyei Kereskedelmi és Iparkamara szervezésében - ***Az új európai adatvédelmi szabályozás és a magyar vonatkozásai***

2018. május 7. – Budapest, Hotel Hungaria City Center – Infoszféra Konferencia – ***Az új adatvédelmi rendelet hazai alkalmazása, a felkészülés és az ellenőrzés sarokpontjai, várható szankciók***

2018. május 9. - Budapest, Aquaworld Resort Budapest – Cyber Kockázatok Konferencia – ***Öveket bekapcsolni… - GDPR és adatvédelmi „checklist"***

2018. május 10. - Budapest - Országos Bírói Hivatal, Magyar Igazságügyi Akadémia – Adatvédelmi Szakmai Nap – ***Mérföldkő az adatvédelemben, hatályba lép az új adatvédelmi rendelet***

2018. május 14. - Kecskemét, Neumann János Egyetem, Kancellári Hivatal – Adatvédelmi Szakmai Nap - ***Az új európai adatvédelmi szabályozás és a magyar vonatkozásai***

2018. május 15. - Budapest, Villa Bagatell – Az AmCham szervezésében: zártkörű GDPR reggeli – ***Kerekasztal megbeszélés***

2018. május 15. - Budapest, Aquincum Hotel Budapest – a Magyar Márkaszövetség és az Országos Kereskedelmi Szövetség közös hatósági konzultációja ***- Az új európai adatvédelmi szabályozás és a magyar vonatkozásai***

2018. május 17. - Budapest, Zsigmond Király Egyetem – Versenyképesség 2018 Konferencia – ***Adatvédelmi kihívások a digitalis világban***

2018. május 22. - Siófok, Prémium Hotel Panoráma – I. Országos Magánbiztonsági Konferencia – ***Az új európai adatvédelmi szabályozás és a magyar vonatkozásai***

2018. május 31. - Balatonkenese – Gazdasági Versenyhivatal - Szakmai Napok – ***A GDPR következményei a belső adatkezelésre***

2018. június 7. - Budapest, Hotel Griff – Nemzeti Akkreditáló Hatóság szervezésében: Akkreditálási Világnap – Egy biztonságosabb világ megteremtése – ***GDPR, személyes adataink biztonsága***

2018. június 7. - Budapest, Magyar Telekom Székház – ISACA Konferencia – ***Az új európai adatvédelmi szabályozás és a magyar vonatkozásai***

2018. június 14. - Budapest, Francia Intézet – A személyes adatok védelme – Big data – Francia-magyar-európai konferencia – „Connected health": az összekapcsolt személyes egészségügyi adatok védelmének etikai és jogi kérdései – ***Az egészségügyi adatok védelme***

2018. június 18. - Budapest, Dunacorso Étterem – 10th Annual Sedona Conference International Programme on Cross-Border Data Transfers and Data Protection Laws – ***Kerekasztal beszélgetések***

2018. június 22. - Budapest, Testnevelési Egyetem – SPORTJUS Magyar Sportjogász Társaság által szervezett szakmai tájékoztató konferencia – ***A GDPR és a sport***

2018. szeptember 7. - Debrecen – Magyar Közgazdasági Társaság éves Vándorgyűlése – ***Az új EU-s adatvédelmi rendelet alkalmazásának tapasztalatai***

2018. szeptember 11. - Deloitte Legal Ügyvédi Iroda – szakmai reggeli „Modern technológiák és a munkaviszony" címmel - ***kerekasztal beszélgetések a munkahelyi adatkezelésekről és a felügyeleti szempontokról***

2018. szeptember 19. - Budapest, Hotel Hilton – Portfolio – GDPR 2.0 Konferencia – ***Változások a háttérszabályozásban – Menetrend és egyeztetések a szektorokkal***

2018. szeptember 27***. –*** Budapest, Groupama Aréna – ITBN Conf-Expo – ***kerekasztal beszélgetések a GDPR alkalmazásának első tapasztalatai***

2018. október 1. **–** Balatonföldvár, Jogar Továbbképző Központ és Hotel – Belügyminisztérium Országos Katasztrófavédelmi Főigazgatóság III. Rendvédelmi Adatvédelmi Konferenciája – ***A módosított Infotv. és a GDPR kapcsolata***

2018. október 1. **–** Siófok – XV. Biztosításszakmai Konferencia és Kiállítása – ***A módosított Infotv. és a GDPR kapcsolata***

2018. október 2. **–** Budapest – A Nemzetközi Gyermekmentő Szolgálat és az Európai Unió „Safer Internet Program" támogatásával megrendezett „Az internet hatása a gyermekekre és a fiatalokra" című konferenciája – ***Oktatás – gyermekvédelem – közösségi háló***

2018. október 9. **–** Budapest – előadás és konzultáció az Európai Parlament és a Tanács 2016/679 Rendelete fontosságáról, értelmezéséről és áttekintéséről – ***Az új európai adatvédelmi szabályozás és a magyar vonatkozásai***

2018. október 30. **–** Budapest, Láng Művelődési Központ – ITOSZ, „GDPR READY"

2018 – Szakkonferencia – ***Az új európai adatvédelmi szabályozás és a magyar vonatkozásai***

2018. november 5. **–** Budapest– Katolikus Szeretetszolgálat szakmai napja – ***Az új európai adatvédelmi szabályozás és a magyar vonatkozásai***

2018. november 7. **–** Budapest– Zukunft Personal Hungary Konferencia – ***Pódiumbeszélgetés a GDPR-ról***

2018. november 7. **–** Budapest – Belügyi Tudományos Tanács, *A biztonság sokszínű arca* című nemzetközi tudományos-szakmai konferencia – ***Adatvédelem, adatbiztonság a közszolgálatban***

2018. november 8. **–** Budapest – Magyar Biztonságvédelmi Egyesület egyesületi ülése - ***Az új európai adatvédelmi szabályozás és a magyar vonatkozásai***

2018. november 15. **–** Budapest, Hotel President – Joint Venture Szövetség, „Adatvédelem, mint versenyképességi tényező" konferencia - ***A NAIH 2018. évi tevékenysége és a GDPR első alkalmazási tapasztalatai***

2018. november 15. **–** Budapest, Budapest Congress Center – Önkormányzati Fejlesztések Figyelemmel Kísérése (ÖFFK) II. Nemzetközi Konferencia – ***Az önkormányzatok információgazdálkodása***

2018. november 21. **–** Budapest – Wolters Kluver Hungary Kft. szakmai konferenciája „GDPR a gyakorlatban: Mindenki másképp csinálja?!" címmel - ***A módosított Infotv. és a GDPR alkalmazásának első tapasztalatai***

2018. november 21. **–** Budapest, Nemzeti Közszolgálati Egyetem Ludovika Campus Díszterem – „Biztonság, szolgáltatás, fejlesztés – avagy új irányok a bevételi hatóságok működésében" nemzetközi szakmai és tudományos konferencia a NAV és az NKE szervezésében – ***A módosított Infotv. és a GDPR alkalmazásának első tapasztalatai***

2018. november 28. **–** Budapest, Dunamelléki Református Egyházkerület Székházának I. emeleti díszterme – Magyarországi Református Egyház Zsinati Hivatala által szervezett intézményvezetői értekezlet – ***A módosított Infotv. és a GDPR alkalmazásának első tapasztalatai***

IX.6. A beszámolóban említett jogszabályok és rövidítések jegyzéke

- 108-as egyezmény, az Európa Tanács Adatvédelmi Egyezménye: az egyének védelméről a személyes adatok gépi feldolgozása során Strasbourgban, 1981. január 28-án kelt Egyezmény, Magyarországon kihirdette az 1998. évi VI. törvény
- Adatvédelmi Irányelv, a személyes adatok feldolgozása vonatkozásában az egyének védelméről és az ilyen adatok szabad áramlásáról szóló 95/46/EK európai parlamenti és tanácsi irányelv
- A felsőoktatási intézmények alaptevékenységének finanszírozásáról szóló 389/2016. (XII.2.) Korm. rendelet
- A jogalkotásról szóló 2010. évi CXXX. törvény (Jat.)

- A jogszabályok előkészítésében való társadalmi részvételről szóló 2010. évi CXXXI. törvény
- A környezet védelmének általános szabályairól szóló 1995. évi LIII. törvény
- A környezeti ügyekben az információhoz való hozzáférésről, a nyilvánosságnak a döntéshozatalban történő részvételéről és az igazságszolgáltatáshoz való jog biztosításáról szóló, Aarhusban, 1998. június 25-én elfogadott Egyezmény kihirdetéséről szóló 2001. évi LXXXI. törvény
- A közadatok újrahasznosításáról szóló 2012. évi LXIII. törvény
- A közérdekű adatok elektronikus közzétételére, az egységes közadatkereső rendszerre, valamint a központi jegyzék adattartalmára, az adatintegrációra vonatkozó részletes szabályokról szóló 305/2005. (XII.25.) Korm. rendelet
- A közérdekű adat iránti igény teljesítéséért megállapítható költségtérítés mértékéről szóló 301/2016. (IX. 30.) Korm. rendeletet
- A köztulajdonban álló gazdasági társaságok takarékosabb működéséről szóló 2009. évi CXXII. törvény
- A közzétételi listákon szereplő adatok közzétételéhez szükséges közzétételi mintákról szóló 18/2005. (XII.27.) IHM rendelet
- Alaptörvény, alkotmány: Magyarország Alaptörvénye (2011. április 25.)
- A magánélet védelméről szóló 2018. évi LIII. törvény
- A nyilvánosság környezeti információkhoz való hozzáférésének rendjéről szóló 311/2005. (XII.25.) Korm. rendelet
- A sportról szóló 2004. évi I. törvény
- A Vízuminformációs rendszer létrehozásáról szóló 2004/512/EK határozat módosításáról és a 2008/633/IB tanácsi határozat hatályon kívül helyezéséről
- a közpénzekből nyújtott támogatások átláthatóságáról szóló 2007. évi CLXXXI. törvény
- Az egyének védelméről a személyes adatok gépi feldolgozása során, Strasbourgban, 1981. január 28. napján kelt Egyezmény kihirdetéséről szóló 1998. évi VI. törvény
- Az Európai Parlament és a Tanács 536/2014/EU rendelete (2014. április 16.) az emberi felhasználásra szánt gyógyszerek klinikai vizsgálatairól és a 2001/20/EK irányelv hatályon kívül helyezéséről
- Az Európai Parlament és a Tanács 810/2009/EK rendelete (2009. július 13.) a Közösségi Vízumkódex létrehozásáról
- Az Európai Parlament és a Tanács 2017/2226 rendelete (2017. november 30.) a tagállamok külső határait átlépő harmadik országbeli állampolgárok belépésére és kilépésére, valamint beléptetésének megtagadására vonatkozó adatok rögzítésére szolgáló határregisztrációs rendszer (EES)

létrehozásáról és az EES-hez való bűnüldözési célú hozzáférés feltételeinek meghatározásáról, valamint a Schengeni Megállapodás végrehajtásáról szóló egyezmény, a 767/2008/EK rendelet és az 1077/2011/EU rendelet módosításáról

- Az Európai Parlament és a Tanács 2016/399 rendelete (2016. március 9.) a személyek határátlépésére irányadó szabályok uniós kódexéről
- Az Európai Parlament és a Tanács 603/2013/EU rendelete (2013. június 26.) a harmadik országbeli állampolgár vagy hontalan személy által a tagállamok egyikében benyújtott nemzetközi védelem iránti kérelem megvizsgálásáért felelős tagállam meghatározására vonatkozó feltételek és eljárási szabályok megállapításáról szóló 604/2013/EU rendelet hatékony alkalmazása érdekében az ujjlenyomatok összehasonlítását szolgáló Eurodac létrehozásáról, továbbá a tagállamok bűnüldöző hatóságai és az Europol által az Eurodac-adatokkal való, bűnüldözési célú összehasonlítások kérelmezéséről, valamint a szabadságon, a biztonságon és a jog érvényesülésén alapuló térség nagyméretű IT-rendszereinek üzemeltetési igazgatását végző ügynökség létrehozásáról szóló 1077/2011/EU rendelet módosításáról
- Az Európai Parlament és a Tanács 2002/58/EK irányelve (2002. július 12.) az elektronikus hírközlési ágazatban a személyes adatok kezeléséről, feldolgozásáról és a magánélet védelméről
- Az Európa Tanácsnak a személyes adatok gépi feldolgozása során az egyének védelméről szóló egyezményét (108. sz. egyezmény) módosító jegyzőkönyvnek az Európai Unió érdekében történő megerősítésére a tagállamoknak adott felhatalmazásról szóló Tanácsi határozata
- Itv. az illetékekről szóló 1990. évi XCIII. törvény
- Ákr. az általános közigazgatási rendtartásról szóló 2016. évi CL. törvény
- Általános adatvédelmi rendelet lásd: GDPR
- Bit., a biztosítási tevékenységről szóló 2014. évi LXXXVIII. törvény
- Bűnügyi adatvédelmi irányelv, a bűnüldözési célból kezelt személyes adatok védelmére vonatkozó irányelv, az Európai Parlament és a Tanács (EU) 2016/680 irányelve (2016. április 27.) a személyes adatoknak az illetékes hatóságok által a bűncselekmények megelőzése, nyomozása, felderítése, a vádeljárás lefolytatása vagy büntetőjogi szankciók végrehajtása céljából végzett kezelése tekintetében a természetes személyek védelméről és az ilyen adatok szabad áramlásáról, valamint a 2008/977/IB tanácsi kerethatározat hatályon kívül helyezéséről
- Eüak., az egészségügyi és a hozzájuk kapcsolódó személyes adatok kezeléséről és védelméről szóló 1997. évi XLVII. törvény.
- Eütv., az egészségügyről szóló 1997. évi CLIV. törvény.

- GDPR, általános adatvédelmi rendelet: az Európai Parlament és a Tanács (EU) által elfogadott, a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK irányelv hatályon kívül helyezéséről szóló 2016/679 Rendelet. 2018. május 25-től alkalmazandó
- Grt., a gazdasági reklámtevékenység alapvető feltételeiről és egyes korlátairól szóló 2008. évi XLVIII. törvény
- Gyvt., a gyermekek védelméről és a gyámügyi igazgatásról szóló 1997. évi XXXI. törvény
- Infotv. Infotörvény, az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény
- Kjt., a közalkalmazottak jogállásáról szóló 1992. évi XXXIII. törvény
- Knt., a nemzeti köznevelésről szóló 2011. évi CXC. törvény
- Kttv., a közszolgálati tisztviselőkről szóló 2011. évi CXCIX. törvény
- Mavtv., a minősített adat védelméről szóló 2009. évi CLV. törvény
- Módtv., az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvénynek az Európai Unió adatvédelmi reformjával összefüggő módosításáról, valamint más kapcsolódó törvények módosításáról szóló 2018. évi XXXVIII. törvény
- Mötv. a Magyarország helyi önkormányzatairól szóló 2011. évi CLXXXIX. törvény
- Mt., a munka törvénykönyvéről szóló 2012. évi I. törvény
- Mttv., a médiaszolgáltatásokról és a tömegkommunikációról szóló 2010. évi CLXXXV. törvény
- Nbtv., a nemzetbiztonsági szolgálatokról szóló 1995. évi CXXV. törvény
- Ptk. új, a Polgári Törvénykönyvről szóló 2013. évi V. törvény
- PSI irányelv, a közszféra információinak további felhasználásáról szóló 2003/98/EK európai parlamenti és tanácsi irányelv
- SIS II, a Schengeni Információs Rendszer második generációjának létrehozásáról, működtetéséről és használatáról szóló 1987/2006/EK számú európai parlamenti és tanácsi rendelet
- Szaktv., az igazságügyi szakértőkről szóló 2016. évi XXIX. törvény
- Sztv., a számvitelről szóló 2000. évi C. törvény
- VIS rendelet, az Európai Parlament és a Tanács 767/2008/EK rendelete (2008. július 9.) a vízuminformációs rendszerről (VIS) és a rövid távú tartózkodásra jogosító vízumokra vonatkozó adatok tagállamok közötti cseréjéről

Tartalomjegyzék

Nemzeti Adatvédelmi és
Információszabadság Hatóság

1125 Budapest, Szilágyi Erzsébet fasor 22/c
Levelezési cím: 1530 Budapest, Pf.: 5

Telefon: +36 (1) 391-1400
Fax: +36 (1) 391-1410

Internet: http://www.naih.hu
e-mail: ugyfelszolgalat@naih.hu

Kiadja: a Nemzeti Adatvédelmi és Információszabadság Hatóság
Felelős kiadó: Dr. Péterfalvi Attila elnök
ISSN 2063-403X (Nyomtatott)
ISSN 2063-4900 (Online)