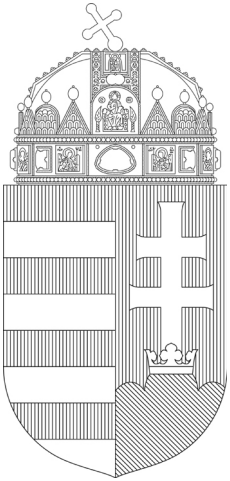
A Nemzeti Adatvédelmi és Információszabadság Hatóság

Beszámolója

a 2017. évi tevékenységéről

B/19656

Nemzeti Adatvédelmi és Információszabadság Hatóság
Budapest, 2018



Bevezető

Köszöntöm az Olvasót!

Az uniós adatvédelmi hatóságok életében a 2017-es esztendő egyértelműen a felkészülés jegyében telt. Négy év előkészítés után 2016-ban elfogadásra került az uniós adatvédelmi reform csomag két eleme, a GDPR és a Bűnügyi Irányelv, és mindkét uniós jogszabály 2018 májusában lép életbe azzal a különbséggel, hogy míg a rendelet közvetlenül alkalmazandó, addig az irányelv szabályait a nemzeti jogrendekbe át kell ültetni.

2018-tól izgalmas időszak következik tehát, az adatvédelmi szabályozás normavilága bizonyos értelemben megkettőződik: kötelező, egységes rendszerbe foglalva érvényesülnek a tág értelemben vett közösségi normák, ugyanakkor lesznek olyan adatvédelmi panaszok, ügyek, ahol a nemzeti jog primátusa – és a nemzeti különbségek – továbbra is fennmaradnak, akár azért, mert erre maguk az uniós jogszabályok nyújtanak lehetőséget, akár azért, mert olyan területekről van szó, melyek nem tartoznak az uniós jog hatálya alá. Gondoljunk csak a nemzetbiztonsági célú vagy akár a bíróságok *„igazságügyi feladatainak”* végrehajtásával járó adatkezelésekre.

Az uniós adatvédelmi reform célja a gyors technológiai fejlődés és a globalizáció kihívásaira adott megfelelő válasz, mely a gazdasági fejlődést előmozdítja, segíti és semmiképp sem gátolja. Az adatvédelmi szabályok egységes alkalmazása megakadályozza a visszaéléseket, *„ügyeskedéseket”*, az adatkezelők a jövőben már nem válogathatnak az uniós országok között költség, vagy egyéb könnyítések miatt, hiszen az elvárások és a szankciók – adatvédelmi szempontból – az Unión belül mindenhol ugyanazok vagy hasonlók lesznek.

Ugyanakkor érdekes és izgalmas kihívásokkal is szembesülhetünk a jövőben, hiszen a jogalkalmazásban vannak olyan kategóriák, tényezők, melyek erős függő viszonyban állnak az adott ország jogi és kulturális hátterével. Ilyen például a *„tisztességes eljárás”*, a gyermek legfőbb érdeke vagy *„a természetes személyek jogaira és szabadságaira”* hatással lévő adatkezelések körülményeinek megítélése.

Az új szabályozással szemben támasztott elvárások minden oldalról magasak, de a magyar adatvédelmi hatóság vezetőjeként meggyőződésem, hogy készen állunk feladataink elvégzésére.

Budapest, 2018. 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 2012. január 1-jei megalapítása óta már hat év telt el. Ebben az évben is az előző évekről megszokott adatokkal, grafikonokkal mutatjuk be, hogy a Hatóság feladatainak ellátása miként valósult meg, milyen változások, trendek figyelhetőek meg a hozzánk érkező bejelentések tartalmában, mennyiségében, az elmúlt évben jelentkezett kihívásokban. A feladataink sokszínűségét, számosságát és változatosságát jól lehet szemléltetni a számok, adatok tárgyilagos, ám szerteágazó, de nagyon is informatív áttekintésével, egy sajátos képet adva az elmúlt évről.

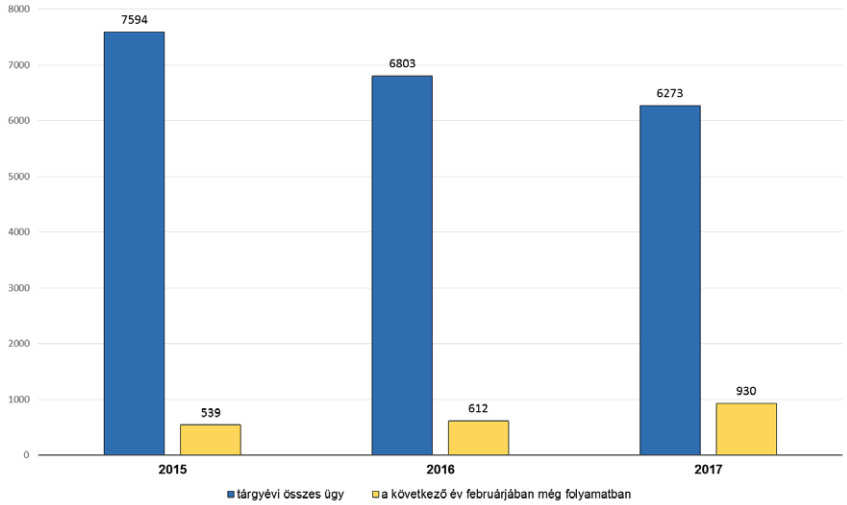
Ebben az évben az elektronikus iktatókönyvben összesen 6273 iktatott ügyiratot vett nyilvántartásba a NAIH, ez 530 üggyel kevesebb, mint az előző évben. A csökkenés egyértelmű oka az, hogy az adatvédelmi nyilvántartásba érkező bejelentések egyre nagyobb arányban érkeznek iktatást nem igénylő elektronikus úton. Az adatvédelmi nyilvántartásba 2017 során minden korábbinál több, összesen 26.728 ügyet dolgoztunk fel, ebből *„csupán”* 2522 irat igényelt iktatást. Az adatok részletes ismertetése és elemzése során is megfigyelhető lesz, hogy a NAIH egyéb érdemi feladatait érintő ügyeiben nem következett be számbeli csökkenés, sőt egyes területeken – éppen ellenkezőleg – markáns ügyszámnövekedés mutatkozik.

Az ügyeink közül 2017 során 68 ügyben folyt hatósági eljárás. A nyilvántartott 6273 ügyünkből 2792 bejelentést vizsgálati ügyként kezeltünk. A vizsgálati ügyeink száma az előző évekhez képest is tovább emelkedett, ez évben 130-al.

A további ügyfajták a NAIH Infotv.-ben szereplő feladatköreit érintik, melyek jellemzően az adatvédelmi nyilvántartás vezetésével összefüggő ügyek, a jogalkotással kapcsolatos tevékenységeink, jogszabály-véleményezés, a nemzetközi ügyek, a belső adatvédelmi felelősök konferenciája, az adatvédelmi audit és BCR ügyek, a titokfelügyelettel kapcsolatos ügyeinek, valamint a Hatóság üzemeltetésével, gazdálkodásával összefüggő belső ügyiratok, illetve ügyviteli iratok voltak. A hatósági eljárások részletes adatait, eredményeit az Adatvédelmi illetve a Titokfelügyeleti fejezetben ismertetjük.

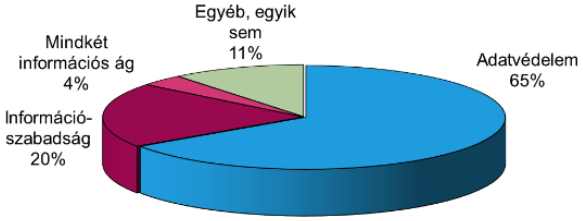
A 2017-ben folyamatban lévő ügyek közül 2018. február 1-jén 930 ügy vizsgálata még nem zárult le, ez az összes ügy 14%-a, az előző 2016-os évből összesen 688 ügy átiktatására került sor 2017-ben.

A NAIH iktatott és folyamatban lévő ügyei 2015-2017



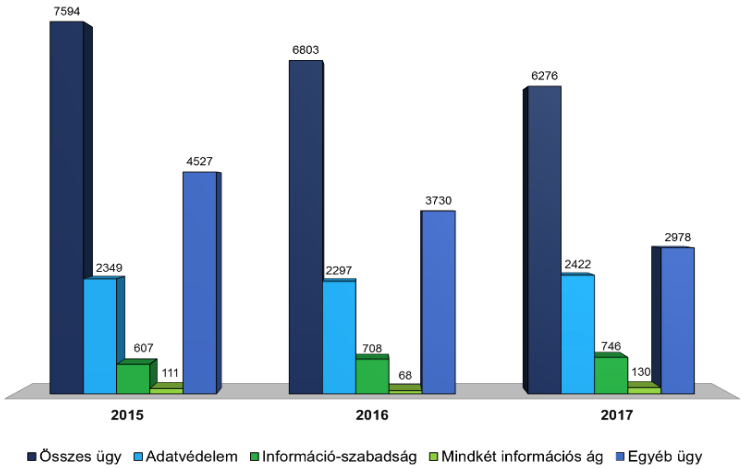
Az Infotv. alapján a NAIH elsődleges feladata a személyes adatok védelméhez, valamint a közérdekű és a közérdekből nyilvános adatok megismeréséhez való jog érvényesülésének ellenőrzése és elősegítése. A következő ábra az információs jogok szemszögéből mutatja be, hogy az egyes beérkező ügyiratok mennyiben érintették a személyes adatok védelmét, illetve a közérdekű adatok nyilvánosságát. A korábbi évek gyakorlatának megfelelően, ebben az ábrában nem szerepelnek az adatvédelmi nyilvántartás vezetésével összefüggő ügyeink (ez összesen 2575 az adatvédelmi nyilvántartást érintő ügy), mivel azok nem érintik közvetlenül egyik alapjogot sem, illetve jelentős számuk miatt a tényleges alapjogi összetétel aránytalanul módosulna.

A NAIH ügyeinek megoszlása információs ágak szerint 2017.
(az adatvédelmi nyilvántartást érintő ügyek nélkül)



Az ügyeink információs jogok szerinti megoszlása a következő: adatvédelmet érint 2422 (65%), (2016-ban: 2297). Információszabadságot érint: 746 (20%) (2016: 708), mindkét alapjogot érintette: 130 (4%) (2016: 68), egyéb, a Hatóság más feladatkörébe tartozó ügy: 400 (11%) (2016: 479) és az itt figyelembe nem vett, az adatvédelmi nyilvántartást érintő ügyek száma 2575 (2016-ban: 3251) volt. Mint arra már a bevezetőben utaltunk, az iktatott adatvédelmi nyilvántartási ügyek száma 676-tal kisebb volt, ellenben az információs jogokat érintő ügyek száma emelkedett. A közérdekű, illetve közérdekből nyilvános adatok megismeréséhez való alapjogot valamilyen formában a beérkezett ügyek összesen 24%-a, összesen mintegy 876 ügy érintette, amely pont 100-zal több, mint a korábbi évben. Ez összességében azt jelenti, hogy mind az adatvédelmet, mind az adatnyilvánosságot érintő ügyek száma emelkedett. Az arányokat tekintve az információszabadságot érintő ügyek 2%-ot kitevő mértékben nőttek az előző évhez képest.

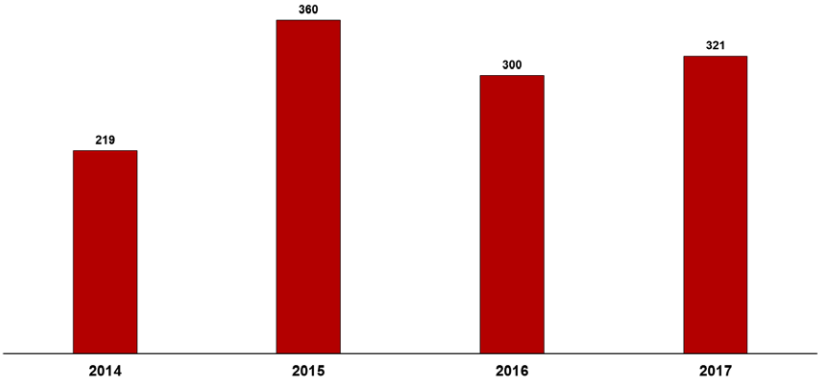
A beérkezett ügyiratok információs ágak szerinti száma 2015-2017
(az adatvédelmi nyilvántartási ügyek itt az egyéb kategóriában)



2017 során 321 jogszabály-véleményezést érintő ügyünk volt, amely 21-el több, mint az előző évi.

A Hatóság jogalkotási monitoring rendszert működtet, és rendszeresen figyelemmel kíséri az információs jogokat érintő kodifikációs tevékenységet, és amennyiben az szükséges, hivatalból véleményezi a hozzánk el nem küldött jogszabálytervezeteket, vagy az országgyűlési tárgysorozatba vételt követően benyújtott módosító javaslatokat.

Az iktatott jogszabály-véleményezések száma 2014-2017



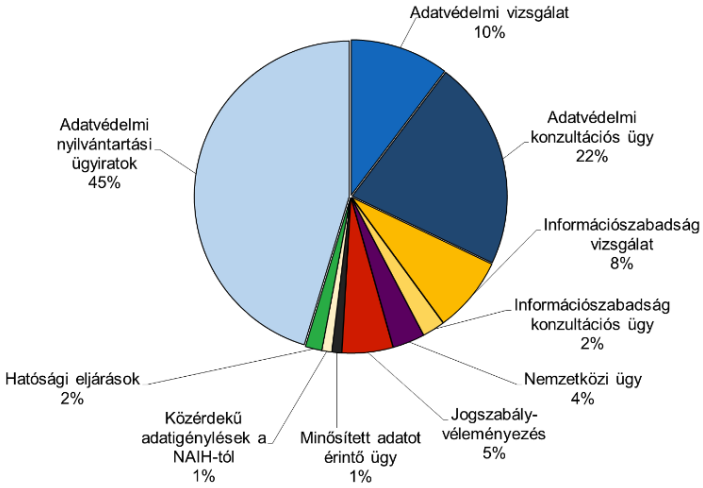
A 2017. év során vizsgált ügyeinkben összesen 33 jogszabály módosítást kezdeményeztünk, ezek közül 31 az adatvédelmet, 2 a közérdekű adatok nyilvánosságát érintette. A jogszabály véleményezéseink során összesen 581 észrevételt tettünk. A NAIH jogalkotást érintő tevékenységéről a beszámoló VIII. fejezetében számolunk be részletesen.

Előfordul, hogy a Hatósághoz tett bejelentés tárgya és tartalma alapján nem állapítható meg a hatáskörünk, ezen esetek egy részében a bejelentést a hatáskörrel rendelkező szervekhez áttesszük, melyre összesen 31 alkalommal került sor, melyből három ügyet az alapvető jogok biztosához tettünk át.

A vizsgálati eljárás megindítását kérelmező bejelentések közül 231 adatvédelmet érintő, és 90 a közadatok nyilvánosságát érintő bejelentés vizsgálatát utasítottuk el. Az elutasított ügyek száma összességében 37-tel nőtt az előző évhez képest.

Az alábbi ábra azt szemlélteti, hogy a NAIH-hoz beérkezett ügyiratok közül az érdemi intézkedést, eljárást, válaszadást igénylő ügyek aránya miként viszonyult egymáshoz.

Az érdemi ügyiratok megoszlása 2017.



Tényleges vizsgálati eljárás alá összesen 1033 ügyet vontunk, ami 43 üggyel több, mint 2016-ban. Ezek közül 585 (56%) adatvédelmi, és 448 (44%) információszabadság tárgyú volt. Ebben az évben is megfigyelhető tendencia, hogy mindkét információs ágat érintő vizsgálati eljárásaink száma nőtt, és kiemelendő, hogy az információszabadságot érintő vizsgálatot generáló bejelentések száma 40-nel több volt, mint az előző évben, és az arányuk is három százalékkal emelkedett az adatvédelmi ügyek arányához képest.

Az 1033 vizsgálat alá vont ügyben 2018 januárjáig összesen 564 vizsgálatban állapítottunk meg részben vagy egészben valamilyen jogellenes adatkezelési gyakorlatot. A megállapított jogsértések száma 82-vel növekedett 2016-hoz képest.

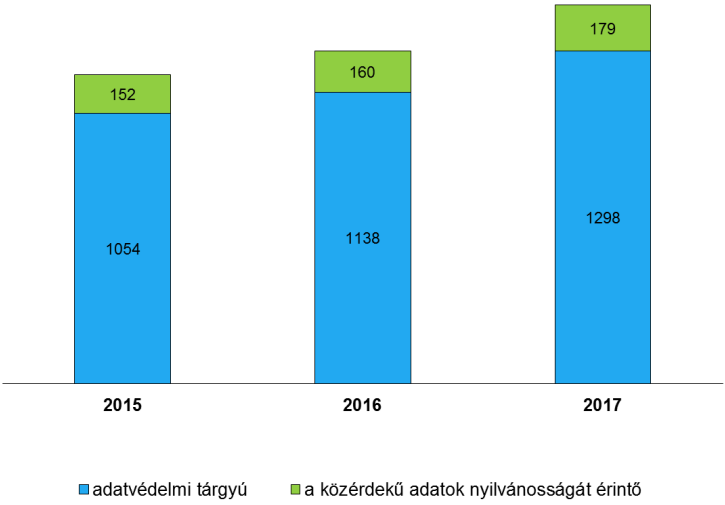
A jogsérelmet megállapító ügyek közül 279 a személyes adatok kezeléséhez és 285 a közadatok nyilvánosságához volt köthető. A megállapított jogsértések száma az adatvédelmi ügyek esetében nőtt (30 eset) és az információszabadságot érintően is növekedett (52 eset). Kijelenthető, hogy 2017 volt az első olyan év 1995, az adatvédelmi biztos intézményének létrejötte óta, amikor egy adott évben a magyar adatvédelmet és információszabadságot felügyelő szervezet több, a közadatok nyilvánosságát érintő jogsértést állapított meg, mint az információs önrendelkezési joggal összefüggő sérelmet.

A Hatóság vizsgálati eljárásai mellett fontos kiemelni az érdemi jogi állásfoglalást, tájékoztatást tartalmazó 1370 konzultációs ügyet is, melyek száma minden évben töretlenül nő, ebben az évben 72-vel emelkedett.

A konzultációs ügyek számának állandósuló növekedését az GDPR (általános adatvédelmi rendelet) alkalmazására történő felkészülésből hátralévő idő rövidsége, és a rendelet szabályainak helyes értelmezését igénylő kérdések megválaszolása is magyarázza. Emellett összefüggésben áll a Hatóság következetes jogalkalmazói, hatósági eljárási és bírságolási gyakorlatával is. A konzultációs, vagyis: tájékoztatást, illetve a jó adatkezelési gyakorlatokat ismertető állásfoglalások jelentősen hozzájárulnak ahhoz, hogy az Infotv. 38. § (2) bekezdésében meghatározott, az információs jogok érvényesülésének elősegítésére irányuló tevékenységünk és törekvéseink eredményei a mindennapi gyakorlatban is megvalósulhassanak.

A konzultációs tárgyú beadványok közül 1237 az adatvédelemre, 133 pedig a közérdekű vagy közérdekből nyilvános adatok megismerhetőségére vonatkozott. A konzultációs ügyeink esetében egyértelmű tendencia, hogy az adatvédelmet érintő megkeresések száma ismételten emelkedett, az adatnyilvánosságot érintő konzultációk száma csökkent. A konzultációs ügyek adatait és a tendenciákat az alábbi grafikon szemlélteti.

Az információs jogokat érintő konzultációs beadványok száma 2015-2017



A Hatósághoz érkeznek olyan bejelentések is, melyekben a vizsgálati eljárás megindításának feltételei nem állnak fenn, vagy a konzultációs ügyek vizsgálata során is megállapíthatóvá vált, hogy valamely adatkezelő gyakorlata nem felelt meg a törvényesség követelményének, illetve az állásfoglalás kibocsátásával egy jogsértő helyzet kialakulását, vagy annak közvetlen veszélyét előztük meg. 2017-ben 105 ügyben: 61 adatvédelmi, illetve 46 információszabadság ügyben állapítottunk, illetve előztünk meg jogsértést, ez 31 esettel több, mint az előző évben. Ebben az ügycsoportban az információszabadságot érintő ügyek száma emelkedett (33 eset).

Egyéb kiemelt ügycsoportok

A minősített személyes vagy közérdekű adatok kezelését összesen 58 vizsgálat érintette, a titokvédelmi ügyeink száma az előző évhez képest csökkent. A titokfelügyeleti vizsgálatokról a IX. fejezetben számolunk be.

2017-ben összesen 116 nemzetközi ügyünk volt, ezen kívül 74 egyéb ügynek külföldi vonatkozása is volt (például európai uniós, vagy harmadik országbeli adatkezelőt, adatfeldolgozót, nemzetközi adattovábbítást érintett a bejelentés) A nemzetközi ügyeket és tevékenységeinket a beszámoló X. fejezetében ismertetjük.

Az adatvédelmi audit ügyek száma 15 volt, melyek közül 7 audit valósult meg 2017-ben. A BCR-eket, a kötelező szervezeti szabályozások (Binding Corporate Rules) ügyiratainak száma 62 volt. A BCR Hatóság általi jóváhagyását érintő ügyeink száma összesen 14 volt. Az audit és BCR ügyeinkről a beszámoló VI. fejezetében esik szó.

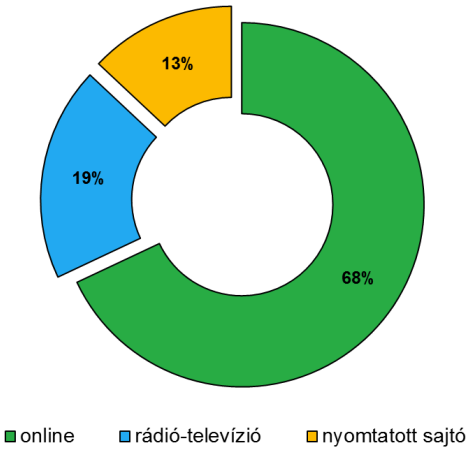
A NAIH-hoz 2017-ben 53 közérdekű adatigénylés érkezett, melyek mindegyikét megválaszoltuk. Az adatigénylések száma az előző évhez képest kismértékben emelkedett (+6).

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

A következőkben a Hatóság 2017. évi média megjelenéseit összegezzük. 2017. január 1. és december 31. között összesen 4284 hírt közöltek a médiaszereplők a Nemzeti Adatvédelmi és Információszabadság Hatóságról, ez több, mint 2000-rel kevesebb, mint a megelőző évben volt. A médiatípusok közül legtöbb-

ször továbbra is az online médiában találkozhattunk a Hatóság tevékenységéről szóló híradásokkal, szám szerint 2926 alkalommal (68%). A nyomtatott sajtóban, 537 esetben, (13%), az elektronikus médiában pedig 821-szer (19%) szerepelt a NAIH.

A NAIH megjelenéseinek aránya a különböző médiumokban 2017-ben



Forrás: Observer Budapest Médiafigyelő Kft.

II. A Magyar adatvédelem első 25 éve az Avtv.-től a GDPR-ig

A magyar adatvédelmi szabályozás 25 éves története

A történeti áttekintés kezdetén említést kell tenni arról, hogy az 1989-es rendszerváltoztatáshoz kapcsolódó jogállami alkotmány szakít az államcentrikus megközelítéssel, hiszen alapvetően nem az állam polgárait, hanem az államot kívánja korlátozni. Az alapvető alkotmányos jogok egyrészt az államhatalommal szemben biztosítják a polgár szabadságát, másrészt a jogok érvényesülésének elősegítésére aktív állami cselekvést írnak elő. 1990 tavaszán a módosított Alkotmányba (német mintára) olyan rendelkezést iktattak be, mely megtiltja az alapjogok lényeges tartalmának módosítását. Ez utóbbi meghatározás gyakorlati kialakításának terhe az Alkotmánybíróság értelmezésére hárul(t), mely közül is az adatvédelem területén legfontosabb és úttörő szerepű a személyi szám univerzális használatának alkotmányellenességéről szóló 15/1991. (IV. 13.) AB határozatban szereplő, az információs önrendelkezési jogot meghatározó kifejtés. Az információs jogok az Alkotmány alapvető jogok és kötelességek fejezetében kaptak helyet.

A magyar adatvédelmi szabályozás legfontosabb állomása emellett – 25 éve – az 1992-es adatvédelmi törvény megszületése volt. *„Az általános törvényt azért is vállalni kell, mert le kell szögezni valahol azt az értékrendet, amelyet a speciális jogszabályok konkretizálhatnak, de nem gyengíthetnek. Az informatikai törvény modellszerepére annál is inkább szükség van, mert semmilyen más témában nincs napirenden az állampolgári szabadságot illetően ilyen alapvetően érintő törvényalkotás. Számolni kell továbbá azzal, hogy a konkrét hozzáférhetési, helyesbítési stb. jogok tényleges érvényesítési területét a bírói gyakorlat fogja kiépíteni. Ez a személyiségi jogokra általában jellemző, sőt szükségszerű."* – írta Sólyom László 1988-ban az ún. *„informatikai törvény"* előkészítésénél.[1]

Az első magyar adatvédelmi törvénynek (Avtv., 1992. évi LXIII. törvény a személyes adatok védelméről és a közérdekű adatok nyilvánosságáról) is volt előzménye. A Központi Statisztikai Hivatal Számítástechnika-alkalmazási Főosztályán – a Minisztertanács elnökének jóváhagyásával – már az 1980-as évek elején

1 Sólyom László: Adatvédelem és személyiségi jog in.: Világosság 1988/9. szám. 1988. január

hozzáfogott egy szakértői csapat az adatvédelmi norma megszövegezéséhez. Ebben az időben az állami szervek állampolgárokra vonatkozó adatkezelését semmilyen jogszabály nem korlátozta, a szervezett és nyilvános adatgyűjtés pedig leginkább az állami népesség-nyilvántartás körére volt jellemző. Nem véletlen, hogy az Alkotmánybíróság a vonatkozó jogszabályt 1991-ben egyértelműen alkotmányellenesnek nyilvánította és megsemmisítette. A Minisztertanács 1989-ben határozatot hozott a személyes adatok kezeléséről és a közérdekű adatok nyilvánosságáról szóló jogszabály elkészítéséről, információs szempontból haladó, de még a *„szocialista demokrácia"* szellemében. 1990 elején elkészül a törvénytervezet és a közigazgatási egyeztetés során beérkezett vélemények hatására már feltűnik a független ellenőrző szerv, az adatvédelmi biztos intézménye is.

1992 tavaszán a kormány az Igazságügyi Minisztérium által előkészített 4544. számú törvényjavaslatot sürgős tárgyalást kérve nyújtja be az Országgyűlésnek, melyhez összesen 140 módosító indítvány érkezik (ezek többségét azonban a határozathozatal során elutasítják)[2]. A törvényt végül 1992. november 11-én kihirdették és hat hónappal később hatályba is lépett.

Az Avtv. unikális sajátossága az európai szabályozáshoz képest, hogy szokásosan használt címével ellentétben nem *„adatvédelmi"* norma volt, hanem az információs szabadságjogok törvénye, vagyis a személyes adatok védelmén túl az információszabadság garanciáit is tartalmazza és a két szabadságjog felügyeletével az adatvédelmi biztost bízza meg, aki speciális ombudsmanként 1995-től meg is kezdi működését. *„Az Adatvédelmi Biztos Irodája működésének kezdetétől, az első állampolgári panaszok feldolgozásától kezdve folyamatosan szembesül azzal az igen pozitív ténnyel, hogy a magyar társadalom tagjait – anyagi helyzettől vagy iskolázottságtól függetlenül! – „érzékenyek" és elkötelezettek személyes adataik védelme iránt és bizalommal fordulnak eme speciális jogvédő szervezethez segítségért, tájékoztatásért".*[3]

A nemzetközi elismerést 2000-ben az *„adekvát védelmi szintről"* hozott döntés, valamint az uniós csatlakozást megelőző, a magyarországi adatvédelem helyzetét előzetesen felmérő 2002-es uniós szakértői jelentés egyaránt megalapozta. Az uniós csatlakozással kezdődik az az átmeneti időszak, ami az ombudsmani *„puha"* eszköztárat kezdi törvénymódosítások útján erősíteni és a hatósági átalakulást célozza.

2 Könyves Tóth Pál: Az adatvédelmi törvény metamorfózisai in.: Fundamentum 2010/2. sz. 53-43.o.

3 Az ombudsmanok tíz éve, Országgyűlési Biztos Hivatala, 2005, 22.o.

„Az új Alaptörvény 2011-ben átszabta az alapjogvédelem rendszerét. A nemzetközi elvárásoknak megfelelő, független adatvédelmi hatóság az egységes alapjogi biztos szervezetétől teljesen elkülönülten folytathatta csak munkáját.[4] A Nemzeti Adatvédelmi és Információszabadság Hatóság 2012-2018 között az Infotv. (2011. évi CXII. törvény az információs önrendelkezési jogról és az információszabadságról) keretei között működik, fogadja és vizsgálja az adatvédelemmel és információszabadsággal összefüggő bejelentéseket, kérelmeket.

2018. májusa után azonban a magyarországi adatvédelem jogi és intézményi történetében egyaránt egy új jogtörténeti szakasz kezdődik, hiszen véget ér az elsődleges nemzeti szabályozás uralma és egy egységes, közvetlenül ható uniós jogi rendelkezés veszi át a legfőbb (bár tegyük hozzá, nem kizárólagos) szabályozó szerepét. Jelenleg még az összes uniós országban tart az erre a kihívásra való felkészülés.

4 NAIH 2012. évi Beszámolója, NAIH 2013, 4.o.

III. A GDPR, az európai általános adatvédelmi rendelet alkalmazására való felkészülés 2017-es állomásai

III.1. A honlapon közzétett munkacsoporti iránymutatások

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 (a továbbiakban: Rendelet) 2018. május 25-től alkalmazandó. Az adatvédelmi szabályozás ezáltal az Európai Unió területén egységessé válik, így annak értelmezésének is egységesnek kell lennie az összes tagállamban. Az egységes alkalmazást elősegítő, a személyes adatok feldolgozása vonatkozásában az egyének védelméről és az ilyen adatok szabad áramlásáról szóló 95/46/EK irányelv 29. cikke alapján létrehozott Adatvédelmi Munkacsoport (a továbbiakban: 29-es Munkacsoport) 2017 folyamán iránymutatásokat dolgozott ki, amellyel segíteni kívánta a Rendelet egységes értelmezését.

Ezen állásfoglalások egy részét nem hozzák nyilvánosságra, hiszen a hatóságok közötti együttműködésre nézve tartalmaznak iránymutatásokat. Azon állásfoglalások, amelyek az adatkezelők, adatfeldolgozók, illetve az érintettek számára nyújtanak tájékoztatást, természetesen bárki számára hozzáférhetők. Az iránymutatások mindegyikét lefordítják az Európai Unió valamennyi hivatalos nyelvére.

Az iránymutatások mindegyike a Munkacsoport tagjainak közös értelmezését mutatja be. A dokumentumok előkészítése a Munkacsoport kilenc alcsoportjának valamelyikében történik. Az alcsoportok tevékenységéről a beszámoló X. fejezetben szólunk, itt azokat a dokumentumokat mutatjuk be, amelyeket a Munkacsoport plenáris ülése, általában egy hathetes nyilvános konzultációt követően jóváhagyott.

III.2. Adathordozhatóság

A GDPR új jogosultságként vezeti be az adatok hordozhatóságához való jogot, ez is indokolta, hogy a Munkacsoport ebben a témában az értelmezési kérdéseket iránymutatásában tisztázza. A dokumentum értelmezést nyújt abban, hogy

milyen módon értelmezendő az adatok hordozhatóságához való jog a többi érintetti jogosultság kontextusában, továbbá abban is, hogy mely gyakorlati esetekre terjed ki az új jog. Az iránymutatás nem csupán az adatkezelők számára hasznos, hanem tájékozódási pontként szolgál az érintettek számára is, akiknek 2018. május 25-étől, tehát a GDPR alkalmazandóvá válásától nyílik meg a lehetőségük e jog gyakorlására.

III.3. Adatvédelmi tisztviselő

Az adatvédelmi tisztviselő több tagállamban már ismert szereplője volt az adatvédelmi intézményrendszernek, így Magyarországon is. A belső adatvédelmi felelősök bizonyos szektorokban már régóta működnek és nagyban hozzájárulnak a személyes adatok védelmét szolgáló szabályok érvényre juttatásához. A Munkacsoport adatvédelmi tisztviselőkkel kapcsolatos iránymutatása tisztázza, hogy miként értelmezendő a kinevezési kötelezettség egy-egy feltétele, mint például a tisztviselőt alkalmazandó adatkezelők meghatározása, vagy a nagymértékű, illetve nagy számban történő adatkezelés megállapításának kritériumai. A gyakorlati kérdések közé tartozik annak felmérése, hogy mikor köteles egy adatfeldolgozó – az adatkezelő oldalán fennálló kinevezési kötelezettségtől függetlenül – adatvédelmi tisztviselőt kinevezni. Az adatvédelmi tisztviselő szerepe sajátos, hiszen független szerepet tölt be az adott adatkezelő szervezeten belül, belső tanácsadóként és panaszok kivizsgálójaként, és emellett őt személyesen felelősség nem terheli az adatkezelés jogszerűségéért. A fő dokumentumot kiegészíti egy kérdések és válaszok formájában elkészített összefoglaló, amely vezetők számára is gyors tájékozódási lehetőséget nyújt a legfőbb döntési kérdéseket illetően.

III.4. A vezető hatóság azonosítása

A GDPR új fogalompárja a vezető és az érintett felügyeleti hatóság. Az egyablakos ügyintézés során a vezető adatvédelmi felügyeleti hatóság fog főszerepet betölteni, a döntés tervezetének előkészítése az ő feladata lesz, de a döntés csak konszenzussal, a többi érintett hatóság egyetértésével születhet. A vezető hatóság azonosításáról szóló dokumentum ebben az új jogi környezetben kíván eligazítást nyújtani. Határon átnyúló tevékenységekkel összefüggő adatkezeléseket eddig is vizsgáltak már a hatóságok, de az együttműködésre nézve nem voltak világos eljárási szabályok. A rendelet ezen is változtat, és a fő tevékenységi helyhez rendeli általában az eljáró hatóság illetékességét. A többi hatóság

érintett lehet az ügy megítélésében vagy azért, mert hozzá is panasz érkezett az adott ügyben, vagy az adott ország területén is megtalálható tevékenységi hely okán, vagy az országban tartózkodó adatalanyok jelentős mértékű érintettsége miatt. Minden eljárás kiindulópontja és első eljárásjogi kérdése a vezető hatóság azonosítása, amely a hatóság feladata ugyan, de ahhoz szükség esetén és kötelező jelleggel az adatkezelőnek is információkat kell szolgáltatnia.

III.5. Adatvédelmi hatásvizsgálat

Új jogintézmény a GDPR által bevezetett adatvédelmi hatásvizsgálat. A valószínűsíthető magas kockázat értelmezési kérdéseit a Munkacsoport szintén iránymutatásban foglalta össze. Bizonyos adatkezelések a rendelet erejénél fogva, mérlegelés nélkül esnek hatásvizsgálat alá. Ilyen adatkezelés a személyek módszeres és kiterjedt értékelése, különleges adatok nagy számban történő kezelése, illetve nyilvános helyek nagymértékű, módszeres megfigyelése. A Munkacsoport konkrét és gyakorlati szempontokat fogalmaz meg annak értékelésére nézve, hogy egy adatkezelés igényel-e előzetes adatvédelmi hatásvizsgálatot. Amennyiben az elemzés arra vezet, hogy a hatásvizsgálatot el kell végezni, úgy a munkacsoporti dokumentum ennek végrehajtására is iránymutatással szolgál. Az adatvédelmi hatásvizsgálatról készült dokumentumot lentebb bővebben is bemutatjuk.

III.6. Közigazgatási bírság

A GDPR egyik legtöbbet idézett szabálya a szankciókra vonatkozik, különösen is a magas összegű bírságokra. Az adatvédelmi felügyeleti hatóságok 2018 májusától a teljes éves világpiaci forgalom 2, vagy 4%-áig terjedő, illetve 10 millió, vagy 20 millió eurós bírságot szabhatnak ki. A kettő közül a magasabb összeget kell figyelembe venni. A dokumentum tulajdonképpen a hatóságok számára szóló egyfajta belső iránymutatás, azonban annak jelentősége nyilvánvalóan túlmutat az egyes eljárásokon, ezért azt a Munkacsoport nyilvánosságra hozta. Több országban a GDPR teremti meg a pénzügyi szankció alkalmazásának lehetőségét, ez is a közös álláspont kialakítását támasztotta alá. A Munkacsoport elfogadja, hogy a hatóságok továbbra is független módon határozzák meg, hogy egy-egy ügyben milyen szankciót alkalmaznak, mindazonáltal nagyon fontos, hogy azok alkalmazására összehangolt módon kerüljön sor, a rendelet egységes alkalmazásának igényével összhangban. A bírság kiszabásának szempontjai szerteágazóak, ezek közül számosat elemez a Munkacsoport dokumentuma,

így például hangsúlyt kell fektetni az érintettek számának meghatározására, figyelemmel kell lenni arra, hogy az adatkezelő kísérletet tett-e a sérelem orvoslására, részletesen taglalja a *„visszaesés”* eseteit, illetve ennek értékelését.

III.7. Munkahelyi adatkezelések

A 2017-ben elfogadott dokumentumok sorából valamennyire kilóg a munkahelyi adatkezeléseket elemző vélemény. Ezt az anyagot a Munkacsoport korábbi, 2001-ben és 2002-ben elfogadott véleményének kiegészítéseként kell kezelni. A dokumentum értéke, hogy figyelembe veszi a munkahelyi adatkezelések utóbbi időszakban bekövetkezett változásait, és ennek megfelelő időszerű ajánlásokat fogalmaz meg. Gyakorlati példák révén világít meg eseteket és így kívánja segíteni a jogalkalmazókat a napi feladataik ellátásában. A vélemény értelemszerűen már a GDPR rendelkezéseit veszi alapul, tehát időszerű dokumentum az iránymutatások sorában.

III.8. Adatvédelmi incidensek bejelentése

Az egyik dokumentum, amellyel a fent említetteken belül részletesen is foglalkozunk, a 2018-ban társadalmi egyeztetésre bocsátott, majd elfogadott, az adatvédelmi incidens bejelentésről szóló WP 250. számú iránymutatás (a továbbiakban: WP 250. számú iránymutatás).

Az adatkezelőnek az adatvédelmi incidensekkel kapcsolatosan több kötelezettséget is előír a rendelet. Egyrészről a Rendelet 33. cikk (5) bekezdése alapján az adatkezelő minden adatvédelmi incidensről nyilvántartást vezet. Másrészről azokat az adatvédelmi incidenseket, amelyek valószínűsíthetően kockázattal járnak a természetes személyek jogaira és szabadságaira nézve, bejelenti a felügyeleti hatóságnak [Rendelet 33. cikk (1) bekezdés]. Harmadrészről, ha az adatvédelmi incidens valószínűsíthetően magas kockázattal jár a természetes személyek jogaira és szabadságaira nézve, az adatkezelő indokolatlan késedelem nélkül tájékoztatja az érintettet az adatvédelmi incidensről [Rendelet 33. cikk (1) bekezdés].

Az adatkezelőnek természetesen először arról kell tudomást szereznie, azt kell megállapítania, hogy adatvédelmi incidens történt. A Rendelet 4. cikk 12. pontja értelmében adatvédelmi incidens *„a biztonság olyan sérülése, amely a továbbított, tárolt vagy más módon kezelt személyes adatok véletlen vagy jogellenes*

megsemmisítését, elvesztését, megváltoztatását, jogosulatlan közlését vagy az azokhoz való jogosulatlan hozzáférést eredményezi".

A WP 250. számú iránymutatás az adatvédelmi incidenseket a következő három klasszikus adatbiztonsági kritériumon keresztül kategorizálja:

- *„Bizalmas jelleg sérülése"*, ami a személyes adatok jogosulatlan vagy véletlen közzétételének vagy az ezekhez való hozzáférésnek felel meg;
- *„Integritás sérülése"* alatt a személyes adatok felhatalmazás nélküli vagy véletlenül bekövetkező módosítását értjük;
- „*Rendelkezésre állás sérülése"*, mely a személyes adatok véletlen vagy jogosulatlan megsemmisítésének vagy a személyes adatok elvesztésének felel meg.

Az adatvédelmi incidensek ezen felosztásával kapcsolatban megjegyzendő, hogy – a körülményektől függően – elképzelhető olyan adatvédelmi incidens bekövetkezése is, amely két- vagy akár mindhárom kategória alá is besorolható, és míg a *„bizalmas jelleg sérülése"* és az *„integritás sérülése"* viszonylag könnyen megfoghatóak, addig a *„rendelkezésre állás sérülésének"* azonosítása nem minden esetben olyan nyilvánvaló. Ilyen eset fordulhat elő például akkor, ha a biztonságos módon titkosított személyes adatok esetében elvész a titkosítás feloldására szolgáló kulcs, és a személyes adatok a biztonsági mentésből sem állíthatóak vissza.

A Rendelet azt a követelményt támasztja az adatkezelővel szemben, hogy az adatvédelmi incidenst indokolatlan késedelem nélkül, és ha lehetséges, legkésőbb 72 órával azután, hogy az adatvédelmi incidens a tudomására jutott, bejelenti az illetékes felügyeleti hatóságnak. Ez a megfogalmazás felveti annak kérdését, hogy az adatkezelő mely időpontban szerez tudomást az adatvédelmi incidensről.

A tudomásszerzés időpontjával kapcsolatban az Adatvédelmi Munkacsoport WP 250. számú iránymutatásában úgy foglalt állást, hogy a tudomásszerzés időpontja az az időpont, amikor az adatkezelő ésszerű mértékben bizonyossággal bír afelől, hogy olyan biztonsági sérülés következett be, mely személyes adatok megsértéséhez vezetett. Ez függ a konkrét incidens körülményeitől, egyes esetekben már kezdettől fogva egyértelmű, hogy adatvédelmi incidens következett be, míg más esetekben hosszabb időt vehet igénybe ennek megállapítása.

Az Adatvédelmi Munkacsoport WP 250. számú iránymutatása néhány példával is szolgál az adatkezelő tudomásszerzésének időpontjával kapcsolatban, így többek között:

- ha harmadik személy jelzi az adatkezelőnek, hogy az ügyfeléről véletlenül személyes adatokat kapott meg és az ennek alátámasztására alkalmas bizonyítékokat juttat el az adatkezelő részére – ekkor nincs kétség afelől, hogy az adatkezelő tudomást szerzett az adatvédelmi incidens bekövetkezéséről;
- ha az adatkezelő észleli, hogy behatolás történt a hálózatába és megállapítja, hogy a hálózaton tároltak személyes adatokat, illetve, hogy azokat érintően következett be az incidens;
- ha kibertámadás elkövetője a rendszer feltörését követően felveszi a kapcsolatot az adatkezelővel, pénzt követelve, majd ezt követően az adatkezelő a rendszer átvizsgálását követően megerősíti, hogy azt valóban támadás érte, ilyen esetben az adatkezelőnek nyilvánvaló bizonyíték áll rendelkezésre az incidens bekövetkezéséről és a tudomásszerzéséhez sem férhet kétség.

Amennyiben egy valószínűsíthető adatvédelmi incidens bekövetkezéséről valamely magánszemélytől, a médiából, vagy egyéb forrásból értesül első ízben az adatkezelő, – valamint abban az esetben is, amennyiben saját maga észleli a biztonság sérülését –, úgy lefolytathat egy rövid ideig tartó vizsgálatot annak megállapítása érdekében, hogy bekövetkezett-e adatvédelmi incidens. Ezen rövid vizsgálat időszakában az adatkezelő úgy tekinthető, mint aki még nem szerzett megfelelő mértékű bizonyosságot arról, hogy adatvédelmi incidens következett be, ezért nem tekinthető úgy, hogy tudomást szerzett az incidensről. Ugyanakkor lényeges kiemelni, hogy ezen kezdeti vizsgálódással töltött idő nem lehet aránytalanul hosszú, illetve az adatkezelőtől elvárható, hogy a lehető legkorábbi időpontban megindítsa a vizsgálatot annak ésszerű mértékű bizonyossággal történő megállapítása érdekében, hogy bekövetkezett-e adatvédelmi incidens. Ezt a szakaszt követheti egy részletesebb vizsgálat lefolytatása.

Amint az adatkezelő tudomást szerez adatvédelmi incidens megtörténtéről, a bejelentési kötelezettség alá tartozó incidenst indokolatlan késedelem nélkül – és ha lehetséges, legkésőbb 72 órával azután, hogy az adatvédelmi incidens a tudomására jutott – be kell jelentenie a felügyeleti hatóságnak, amely időszak alatt az adatkezelő felméri a valószínűsíthető kockázat mértékét az incidens kezelését szolgáló intézkedések meghatározása végett.

Annak érdekében, hogy az adatkezelő képes legyen adatvédelmi incidensekkel felmerülő feladatainak teljesítésére, belső eljárásrendet kell kidolgoznia az adatvédelmi incidensek feltárása és kezelése céljából. Példaként említve, az adatkezelésben felfedezhető szabálytalanságok kiküszöbölésére az adatkezelőnek

meghatározott technikai intézkedéseket kell hoznia, adatfolyam- illetve naplófájlok elemzését végző szakértők bevonásával. A belső eljárás szempontjából hangsúlyos továbbá, hogy adatvédelmi incidens észlelésekor a menedzsment megfelelő szintjére érkezzen be a jelzés annak érdekében, hogy amennyiben szükséges, megtörténhessen az adatvédelmi incidensnek a Rendelet 33. cikke alapján a felügyeleti hatóság részére történő bejelentése, illetve – amennyiben a feltételek fennállnak – a Rendelet 34. cikke szerint az érintettek tájékoztatása.

Közös adatkezelőkre vonatkozóan a Rendelet 26. cikke megköveteli, hogy a közöttük létrejövő megállapodásban állapítsák meg az egyes adatkezelőknek a Rendelet előírásainak teljesítéséhez szükséges felelősségi körét, melynek keretében meg kell szabniuk többek között, hogy mely fél felel a Rendelet 33. és 34. cikkei rendelkezéseiben meghatározott kötelezettségek teljesítéséért. Az adatkezelők mellett az adatvédelmi incidens bejelentése kapcsán a Rendelet az adatfeldolgozókra is hárít kötelezettséget, amikor annak 33. cikk (2) bekezdése úgy rendelkezik, hogy az adatfeldolgozó az adatvédelmi incidenst, az arról való tudomásszerzést követően indokolatlan késedelem nélkül bejelenti az adatkezelőnek. Tekintettel arra, hogy a Rendelet explicite nem fogalmaz meg időkorlátot arra vonatkozóan, hogy az adatfeldolgozónak mennyi időn belül kell értesítenie az adatkezelőt az incidensről történt tudomásszerzését követően, az Adatvédelmi Munkacsoport az adatkezelő haladéktalan értesítését kívánja meg, oly módon, hogy amint további információk jutnak tudomására, szakaszosan jelentse az adatkezelő felé, ez amiatt lényeges, hogy az adatkezelő teljesíteni tudja 72 órán belül a felügyeleti hatóság irányában fennálló bejelentési kötelezettségét. A WP 250. számú iránymutatás kitér arra is, hogy abban az esetben, amennyiben az adatkezelő az adatfeldolgozóval kötött megállapodásban felhatalmazta erre, a nevében az adatfeldolgozó is bejelentést tehet a felügyeleti hatóság részére. Azt azonban lényeges megjegyezni, hogy a bejelentési kötelezettségért fennálló jogi felelősség a megállapodásban rögzítettektől függetlenül mindenkor az adatkezelőt terheli.

Az adatvédelmi incidens bejelentés tartalmi elemei tekintetében a Rendelet 33. cikk (3) bekezdése értelmében adatvédelmi incidens bekövetkezése esetén az adatkezelőnek az incidens bejelentése során ismertetnie kell a Hatósággal minimálisan az adatvédelmi incidens jellegét, az érintettek kategóriáit és hozzávetőleges számát, valamint az incidenssel érintett adatok kategóriáit és hozzávetőleges számát. A fentieken túlmenően közölnie kell az adatvédelmi tisztviselő vagy a további tájékoztatást nyújtó egyéb kapcsolattartó nevét és elérhetőségeit, az adatvédelmi incidensből eredő, valószínűsíthető következményeket, valamint az adatkezelő által az adatvédelmi incidens orvoslására tett vagy tervezett intéz-

kedéseket, beleértve adott esetben az adatvédelmi incidensből eredő esetleges hátrányos következmények enyhítését célzó intézkedéseket.

Az a körülmény, hogy a Rendelet 33. cikk (3) bekezdésében meghatározott információk nem állnak pontosan rendelkezésre – erre példaként szolgálhat az az eset, amikor az adatkezelő nem tudja meghatározni az incidenssel érintett természetes személyek pontos számát –, nem képezheti akadályát a kellő időben történő bejelentés megtételének. Arra az esetre, amennyiben nem lehetséges az információkat egyidejűleg közölni, a Rendelet 33. cikk (4) bekezdése tartalmazza annak lehetőségét, hogy az adatvédelmi incidens bejelentésére szakaszosan, több részletben kerüljön sor. Lényeges körülmény, hogy a kezdeti bejelentés megtételét követően az adatkezelőnek lehetősége van aktualizálni a bejelentést, ha az adatkezelő a kezdeti bejelentést követően lefolytatott vizsgálat nyomán olyan bizonyítékokra bukkan, amelyek azt támasztják alá, hogy a bekövetkezett esemény ténylegesen nem adatvédelmi incidens.

Az incidens kezeléssel kapcsolatban a Rendelet 34. cikkének (1) bekezdése további kötelezettséget ró az adatkezelőre abban az esetben, ha az adatvédelmi incidens valószínűsíthetően magas kockázattal jár a természetes személyek jogaira és szabadságaira nézve. Amennyiben az incidens által jelentett magas kockázat állapítható meg – a kockázatok értékelését illetően annak szempontrendszerét a Hatóság a fejezet későbbi részében fejti ki –, az érintettnek nyújtandó tájékoztatásban világosan és közérthetően ismertetni kell az adatvédelmi incidens jellegét, és közölni kell az adatvédelmi tisztviselő vagy a további tájékoztatást nyújtó egyéb kapcsolattartó nevét és elérhetőségét. Továbbá közölni kell az adatvédelmi incidensből eredő valószínűsíthető következményeket, valamint az adatkezelő által az adatvédelmi incidens orvoslására tett vagy tervezett intézkedéseket, beleértve adott esetben az adatvédelmi incidensből eredő esetleges hátrányos következmények enyhítését célzó intézkedéseket. A tájékoztatási kötelezettség alól a Rendelet 34. cikk (3) bekezdése[5] határoz meg szűk körben kivételeket.

5 A Rendelet 34. cikk (4) bekezdése alapján az érintettet nem kell az (1) bekezdésben említettek szerint tájékoztatni, ha a következő feltételek bármelyike teljesül: az adatkezelő megfelelő technikai és szervezési védelmi intézkedéseket hajtott végre, és ezeket az intézkedéseket az adatvédelmi incidens által érintett adatok tekintetében alkalmazták, különösen azokat az intézkedéseket – mint például a titkosítás alkalmazása –, amelyek a személyes adatokhoz való hozzáférésre fel nem jogosított személyek számára értelmezhetetlenné teszik az adatokat; az adatkezelő az adatvédelmi incidenst követően olyan további intézkedéseket tett, amelyek biztosítják, hogy az érintett jogaira és szabadságaira jelentett, az (1) bekezdésben említett magas kockázat a továbbiakban valószínűsíthetően nem valósul meg;

Az érintettekkel történő kapcsolatfelvétel módjával összefüggésben az Adatvédelmi Munkacsoport WP 250. számú iránymutatásában kifejtette, hogy azt tartja elfogadhatónak, amennyiben az adatkezelő külön, a célra rendelt üzenetek formájában tájékoztatja az érintetteket. Semmiképpen sem kapcsolható ez össze standard üzenetekkel, hírlevelekkel, általános frissítésekkel. Az érintettekkel történő kapcsolatfelvétel átlátható módja lehet közvetlen üzenetküldés (például: SMS, e-mail), kiemelt tájékoztató nagy látogatottságú internetes oldalakon, postai kommunikáció útján, kiemelt hirdetések nyomtatott sajtóban. Az adatkezelőknek kell a legmegfelelőbb kapcsolat-felvételi csatornát megtalálnia, különösen abban az esetben, ha a felek gyakran kommunikálnak. Az egyértelműen megállapítható, hogy az adatkezelőnek körültekintően kell megválasztania a kapcsolat-felvételi csatornát, különösen a veszélyeztetett csatorna használata esetére, amelyet a támadók esetleg veszélyeztethetnek.

Ez azt is jelenti, hogy a tudomásszerzését követően az adatkezelőnek nem csupán meg kell fékeznie az adatvédelmi incidenst, hanem emellett fel is kell mérnie annak a kockázatnak a súlyosságát, ami az incidensből következhet. Ennek két oka van: az egyik, hogy a kockázat valószínűségének és lehetséges súlyának tükrében az adatkezelő meg tudja választani a hatékony intézkedéseket, amelyek szükségesek az adatvédelmi incidens kezeléséhez; a másik indok pedig, hogy ez segítséget jelent az adatkezelőnek is annak meghatározásában, hogy szükséges-e bejelentést tennie a felügyeleti hatóság irányába, illetve abban is, hogy kell-e tájékoztatást nyújtania az érintetteknek. Ez utóbbi szempontból az érintettek tájékoztatási kötelezettségének sarokkövét az képezi, hogy az adatvédelmi incidens valószínűsíthetően magas kockázattal jár-e a természetes személyek jogaira és szabadságaira nézve. Ilyen magas kockázat pedig abban az esetben áll fenn, amikor a személyes adatok kezelésével kapcsolatban bekövetkező incidens fizikai, vagyoni vagy nem vagyoni károkat okozhat természetes személyeknek. Többek között az adatkezelésből hátrányos megkülönböztetést, személyazonosság-lopást, személyazonossággal való visszaélést, pénzügyi veszteséget, jó hírnév sérelmét, vagy bármilyen egyéb jelentős gazdasági vagy szociális hátrányt eredményezhet. Továbbá, ha olyan személyes adatok kezelése történik, amelyek faji vagy etnikai származásra, vagy politikai véleményre, vallási vagy világnézeti meggyőződésre utalnak, valamint ha a kezelt adatok genetikai adatok, egészségügyi adatok, a szexuális életre vagy büntetőjogi fele-

a tájékoztatás aránytalan tájékoztatás aránytalan erőfeszítést tenne szükségessé. Ilyen esetekben az érintetteket nyilvánosan közzétett információk útján kell tájékoztatni, vagy olyan hasonló intézkedést kell hozni, amely biztosítja az érintettek hasonlóan hatékony tájékoztatását.

lősség megállapítására, illetve bűncselekményekre, vagy ezekhez kapcsolódó biztonsági intézkedésekre vonatkoznak.

A kockázat felbecsülésekor a kockázat bekövetkezésének valószínűségét és annak a természetes személyek jogaira és szabadságaira jelentett kockázat súlyosságát szükséges tekintetbe venni. A kockázat értékelésének objektív módon kell történnie.

Érdemes e tekintetben kiemelni, hogy a természetes személyek jogaira és szabadságaira jelentett kockázat az adatvédelmi hatásvizsgálathoz képest más nézőpontot képvisel. Az adatvédelmi hatásvizsgálat tekintetbe veszi mind a tervezett adatkezelési műveletek során bekövetkező kockázatokat, mind pedig egy esetleges adatvédelmi incidenssel együtt járó kockázatot. Míg egy potenciális adatvédelmi incidens értékelése a bekövetkezés valószínűségére, valamint a lehetséges személyes károk azonosítására helyezi a hangsúlyt, addig a valós, bekövetkezett adatvédelmi incidens esetén a vizsgálat teljes egészében az annak eredményeként bekövetkezett kockázat érintettekre gyakorolt hatására fókuszál.

Az Adatvédelmi Munkacsoport WP 250. számú iránymutatása a következő kritériumokat javasolja tekintetbe venni az adatvédelmi incidens súlyosságának és lehetséges hatásainak felméréséhez:

- *az adatvédelmi incidens típusa:* befolyásolhatja az érintettekre jelentett kockázat súlyát. Példaként hozva a bizalmas jelleg sérülését, ami által egészségügyi adatok kerülnek nyilvánosságra, vagy harmadik személyek számára hozzáférhetővé. Ez az eset jól érzékelhetően más következményekkel jár, mintha az egészségügyi adatok elvesznének, illetve a továbbiakban nem lennének elérhetőek.
- *a személyes adat természete, érzékenysége, és mennyisége*: minél érzékenyebb egy személyes adat, annál magasabb a sérelem bekövetkezésének valószínűsége. Továbbá általánosságban elmondható, hogy egyes személyes adatok kombinációja tipikusan sokkal érzékenyebb, mint egyetlen személyes adat.
- *az érintettek azonosításának egyszerűsége:* a körülményektől függően, az adatvédelmi incidenssel érintett természetes személyek azonosítása megvalósulhat kizárólag az incidenssel érintett adatokból, illetve előállhat olyan helyzet is, amelyben még az adatvédelmi incidens bekövetkezte ellenére is kiemelkedően nehéz a személyes adatoknak érintettekhez kapcsolása. Megfelelő szinten titkosított személyes adatok a megismerésükre jogosultsággal nem rendelkező személyek számára a titkosítást feloldó kulcs hiányában értelmezhetetlenek. A megfelelően végrehajtott

pszeudonomizálás szintén alkalmas technika arra, hogy csökkentse az érintett azonosításának valószínűségét egy esetleges adatvédelmi incidens bekövetkezése esetén.

- *az érintettekre ható következmények súlyossága*: az adatvédelmi incidenssel együtt járó személyes adatok, így például különleges adatok, az érintettekre ható potenciális kár különösen súlyos következményekkel járhat, főként, ha az személyazonosság-lopáshoz, személyazonossággal való visszaéléshez, fizikai sérelemhez, lelki gyötrelmekhez, megalázáshoz vagy a jó hírnév sérelméhez vezetne.
- *az érintett személyek speciális jellemzői*: ebben a tekintetben a kiszolgáltatott helyzetben lévő személyek – ideértve a gyermekeket is – érdemelnek említést;
- *az érintettek száma*: általánosságban véve, minél nagyobb számú érintettre van hatással az adatvédelmi incidens, az adatvédelmi incidens annál nagyobb hatással járhat. Ez azonban nem zárja ki, hogy egyetlen érintettre kiható adatvédelmi incidens ne járhatna súlyos hatásokkal;
- *az adatkezelő különleges ismérvei:* az adatkezelő jellege, szerepe, valamint az általa ellátott tevékenységek hatással lehetnek egy adatvédelmi incidenssel összefüggésben bekövetkező kockázat nagyságára. E tekintetben lényeges különbség figyelhető meg egy egészségügyi szolgáltató kezelésében lévő személyes adatok, valamint egy folyóirat címzettjeinek adatait kezelő kiadó cég adatállománya ellen elkövetett adatvédelmi incidens lehetséges kockázatai között.

Annak megítélésekor, hogy az adatvédelmi incidens milyen mértékű kockázattal jár, figyelembe kell továbbá venni az úgynevezett „*másodlagos kihatásokat"*[6] is, amely alá sorolható lenne például egy zenei szórakoztató társaság honlapjának feltörése, a felhasználói adatbázis ellopása és közzététele az interneten.

Ezen adatsértés esetében a magánszemélyekre gyakorolt közvetlen kihatás esetenként meglehetősen korlátozottnak tűnhet (például: a zenei preferenciákra vonatkozó információ kiszivárogtatása). Ugyanakkor mivel ilyen esetben rendszerint jelszavakat is feltörnek, ezeket az adatkezelőnek meg kell újítania, és ekkor szükségessé válik a felhasználók tájékoztatása arról, hogy milyen eljárásban kerítenek sort a jelszavaik megújítására. Ezen túlmenően – mivel a felhasználók jelentős hányada ugyanazt a jelszót használja különböző fiókjaihoz – valószínű, hogy az adatsértés másodlagos hátrányos kihatásaként egy másik fiók tekinte-

6 Az Adatvédelmi Munkacsoport 03/2014 sz. véleménye a személyes adatok megsértése bejelentéséről (WP 213)

tében is felveti a bizalmas jelleg megsértésének lehetőségét, az érintett ezeket a másodlagos kihatásokat minimalizálhatja, ha valamennyi fiókja jelszavát megváltoztatja. Ezért az értesítésnek tájékoztatást kell tartalmaznia a más fiókokkal kapcsolatos valószínű hátrányos kihatásokról, és javasolnia kell a felhasználónak, hogy a különböző fiókjaiban változtassa meg minden olyan fiókja jelszavát, amelyhez a feltört jelszót használta korábban.

Az adatvédelmi incidenshez kapcsolódó adatkezelői kötelezettségek elmulasztása esetén alkalmazható szankciók tekintetében a Rendelet (87) preambulumbekezdése úgy fogalmaz, hogy *„meg kell bizonyosodni arról, hogy az összes megfelelő technológiai védelmi és szervezési intézkedés végrehajtásra került-e, egyrészt az adatvédelmi incidens haladéktalan megállapítása, másrészt a felügyeleti hatóságnak történő bejelentés és az érintett sürgős értesítése érdekében. Azt, hogy az értesítésre indokolatlan késedelem nélkül került-e sor, különösen az adatvédelmi incidens jellegére és súlyosságára, valamint annak az érintettre gyakorolt következményeire, illetve hátrányos hatásaira figyelemmel kell megállapítani. A felügyeleti hatóságnak történt bejelentést az e rendeletben meghatározott feladataival és hatásköreivel összhangban történő beavatkozását eredményezheti”*. Abban az esetben, ha az adatkezelő elmulasztja teljesíteni bejelentési, vagy tájékoztatási kötelezettségét, a felügyeleti hatóságot megilleti a választás lehetősége a rendelkezésére álló korrekciós hatáskörei gyakorlása közül, amibe beletartozik a körülményeknek megfelelő közigazgatási bírság kivetése, továbbá a Rendelet 58. cikk (2) bekezdése szerinti korrekciós hatáskörében megtehető egyéb intézkedés alkalmazása vagy annak mellőzése. Közigazgatási bírság alkalmazása esetén a kiszabható legmagasabb bírság 10 000 000 EUR, illetve a vállalkozások esetében az előző pénzügyi év teljes éves világpiaci forgalmának legfeljebb 2%-át kitevő összeg. A szankciók alkalmazása szempontjából kiemelést érdemel az a tény, hogy amennyiben az adatkezelő elmulasztja bejelenteni az adatvédelmi incidenst, az felszínre hozhatja biztonsági intézkedések hiányosságait, vagy esetlegesen azok teljes hiányát is. Ebben az esetben a felügyeleti hatóságnak lehetősége van jogkövetkezményeket alkalmazni mind a bejelentés, illetve a tájékoztatás elmulasztásáért (Rendelet 33. cikk, 34. cikk.), mind pedig a megfelelő biztonsági intézkedések elmaradásáért (Rendelet 32. cikk), mint teljesen különálló jogsértésekért.

Az adatkezelőnek a Rendeletben meghatározott körülmények esetén fennálló bejelentési, valamint az érintettek tájékoztatási kötelezettségén túlmenően, a Rendelet 33. cikk (5) bekezdése előírja az adatvédelmi incidensek dokumentálását, amely dokumentációt arra tekintet nélkül meg kell őriznie, hogy az in-

cidenssel összefüggésben terhelte-e bejelentési kötelezettség a felügyeleti hatóság irányában. Az Adatvédelmi Munkacsoport WP 250. számú iránymutatása alapján a nyilvántartásnak tartalmaznia kell az az adatvédelmi incidens okait, az esemény leírását, az incidenssel érintett személyes adatokat, az adatvédelmi incidens hatásait és következményeit, továbbá az orvoslására tett intézkedéseket.

Az Adatvédelmi Munkacsoport javasolja továbbá az adatkezelőnek azon okfejtés dokumentálását, ami a megtett intézkedésekhez vezetett. Különös jelentősége van azon döntés alátámasztásául szolgáló dokumentációnak, amely alapján az adatkezelő úgy döntött, hogy nem jelenti az adatvédelmi incidenst a felügyeleti hatóság irányában, ebben a tekintetben úgyszintén tartalmaznia kell annak indokait, amelyek alapján az adatkezelő úgy ítéli meg, hogy valószínűsíthetően nem jár kockázattal a természetes személyek jogaira és szabadságaira nézve. Az adatkezelőnek a nyilvántartásban van lehetősége azt annak bizonyítékait rögzíteni, amennyiben a Rendelet 34. cikk (3) bekezdése szerinti értesítési kivétel áll fenn.

Az adatvédelmi incidensek részletes dokumentálása arra is alkalmas lehet, hogy a felügyeleti hatósághoz történő bejelentés késedelme esetén az adatkezelő igazolni tudja a késedelem alapjául szolgáló indokokat. Mindezeken túlmenően, abban az esetben, amikor az adatkezelő tájékoztatja az érintetteket az adatvédelmi incidensről, ennek a tájékoztatásnak hatékonyan és megfelelő időben kell megtörténnie. Ennek megfelelően, a kommunikáció bizonyítékául szolgáló dokumentáció megőrzése elősegíti az elszámoltathatóság elve megtartásának bizonyítását.

Az adatvédelmi incidensek bejelentésére a Rendelet alkalmazandóságától kezdődően a Hatóság a www.naih.hu cím alatt található hivatalos honlapján egységes online felületet, illetve a bejelentésre szolgáló formanyomtatványt fog biztosítani. A kitöltendő formanyomtatvány tartalmi elemeiről a következőkben ad tájékoztatást a Hatóság, amelyek iránymutatásul szolgálhatnak arra nézve, hogy az adatkezelőknek már a belső eljárásrendjük kialakításuk során mely körülmények minél hatékonyabb feltárására érdemes kiemelt figyelmet fordítaniuk:

- Bejelentő adatai;
- Időpontok – az adatvédelmi incidens időpontja, az incidensről való tudomásszerzés időpontja; az incidens észlelésének módja; esetleges késedelmes tájékoztatás indokai;
- Az adatvédelmi incidens jellege, például: eszköz elvesztése vagy ellopása; informatikai rendszer feltörése; rosszindulatú számítógépes progra-

mok például: zsarolóprogram; személyes adatok téves címzett részére történő elküldése, stb.;
- Az adatvédelmi incidenssel érintett személyes adatok (személyes adatok, különleges adatok);
- Az adatvédelmi incidenssel érintett személyes adatok becsült száma;
- Érintettek kategóriái (például: alkalmazottak, ügyfelek, kiskorúak stb.);
- Az incidens előtt alkalmazott intézkedések;
- Következmények megjelölése, amely lehet:
    - Bizalmas jelleg sérülése (például: szélesebb körű hozzáférés, mint ami szükséges, vagy amihez az érintett hozzájárult; az adat összekapcsolhatóvá vált az érintett egyéb adatával; az adat más célokból, vagy tisztességtelen módon történő kezelése lehetséges; egyéb);
    - Integritás sérülése (az adat módosíthatóvá vált annak ellenére, hogy archivált elavult adat volt; az adatot valószínűsíthetően módosították egyébként pontos adatokra, és azokat eltérő célokra használhatták; egyéb);
    - Rendelkezésre állás sérülése (az érintettek számára történő kritikus szolgáltatásnyújtás képességének elvesztése vagy módosulása; az egyéb rendelkezésre állást érintő következmény leírása);
- Az érintetteket ért fizikai, anyagi vagy nem vagyoni károk, vagy egyéb jelentős következmények – ami az incidens valószínűsíthető hatásainak feleltethető meg az érintettekre vonatkozóan) –, valamint a valószínűsíthető következmények súlyossága;
- Megtett intézkedések, ideértve az érintettek tájékoztatását – annak időpontját, formáját, tartalmát, a tájékoztatott érintettek számát, esetlegesen a tájékoztatás hiányának indokait –; az adatvédelmi incidens orvoslására tett intézkedések; egyéb bejelentések (többek között: a vezető hatóságnak bejelentett határokon átnyúló adatvédelmi incidens; az EU felügyeleti hatóságok listája, amelyeket az adatvédelmi incidens érinthet).

III.9. Adatvédelmi Hatásvizsgálat

A 29-es Munkacsoport 2017 folyamán társadalmi konzultációt követően kiadta az „*Iránymutatás az adatvédelmi hatásvizsgálat elvégzéséhez és annak megállapításához, hogy az adatkezelés az (EU) 2016/679 rendelet alkalmazásában „valószínűsíthetően magas kockázattal jár-e”* című iránymutatását (a továbbiakban: 248-as számú Iránymutatás).

Az adatvédelmi hatásvizsgálat egy adatkezelés esetleges kockázatainak felmérését és a feltárt kockázatok mértékéhez igazodó intézkedések megtételét hivatott vizsgálni.

Adatvédelmi hatásvizsgálatot 2018. május 25. után megkezdett adatkezelések tekintetében, valamint abban az esetben kell lefolytatni, amennyiben az adatkezelés körülményeiben a Rendelet alkalmazandóságának időpontját követően jelentős változás áll be. Ilyen eset lehet például, amennyiben az adatkezelés folyamatába új technológia bevezetését vonják be, vagy ha személyes adatok kezelésére a korábbiaktól eltérő célokra is sor kerül. Jóllehet tehát, hogy 2018. május 25-ig nincs szükség adatvédelmi hatásvizsgálatra, az adatkezelőnek azonban az általános elszámoltathatósági kötelezettségei részeként gondoskodnia kell a Rendeletnek történő megfeleltetésről, az adatkezelő szolgáltatásait úgy kell megtervezni, hogy már az első lépéstől kezdve felmérje az esetleges kockázatokat és megfelelő időben a szükséges kockázatkezelő intézkedéseket megtervezze és végrehajtsa.

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.

Az adatvédelmi hatásvizsgálat a rendelet betartásának elérésére és bizonyítására szolgáló eljárás és szoros kapcsolatban áll az elszámoltathatóság alapelvével, amely, mint adatkezelőkre rótt kötelezettség a Rendelet 24. cikkében is megfogalmazódik.

Az adatvédelmi hatásvizsgálatot akkor kell elvégezni a Rendelet 35. cikk (1) bekezdése alapján, amikor az adatkezelés *„valószínűsíthetően magas kockázattal jár a természetes személyek jogaira és szabadságaira nézve”*. A kockázati szint a súlyosság és valószínűség szempontjából jellemez valamilyen eseményt és annak következményeit. A súlyosság a kockázat szintjét határozza meg, és alapvetően a potenciális hatás sérelmes következményétől függ. A valószínűség a kockázat bekövetkezésének lehetőségét mutatja. A kettő együtt határozza meg a kockázat szintjét.

Az adatvédelmi hatásvizsgálat ugyan más körülmények között is kötelező lehet, mindazonáltal a Rendelet 35. cikk (3) bekezdése néhány példával szolgál azokra

az esetekre, amikor az adatkezelési művelet valószínűsíthetően magas kockázattal jár. Ezek a következők:

- a természetes személyekre vonatkozó egyes személyes jellemzők olyan módszeres és kiterjedt értékelése, amely automatizált adatkezelésen – ideértve a profilalkotást is – alapul, és amelyre a természetes személy tekintetében joghatással bíró vagy a természetes személyt hasonlóképpen jelentős mértékben érintő döntések épülnek;
- a személyes adatok különleges kategóriái (9. cikk (1) bekezdés), vagy a büntetőjogi felelősség megállapítására vonatkozó határozatokra és bűncselekményekre vonatkozó személyes adatok (10. cikk) nagy számban történő kezelése; vagy
- nyilvános helyek nagymértékű, módszeres megfigyelése.

A Munkacsoport a 248-as számú iránymutatásban az adatkezelők számára az eredendően magas kockázatuk miatt kötelező adatvédelmi hatásvizsgálat hatálya alá tartozó adatkezelési műveletek körének meghatározása érdekében – a Rendelet 35. cikkében írtakra, valamint a kapcsolódó preambulum bekezdés értelmében tagállami szinten elfogadandó jegyzékre, továbbá a Rendeletben a *„valószínűsíthetően magas kockázattal járó”* adatkezelési műveletekre tett egyéb utalásokra figyelemmel – a következő szempontok mérlegelését, vizsgálatát javasolja:

- Értékelés vagy pontozás, ideértve a profilozást és az előrejelzést is, különösen az érintett munkahelyi teljesítményére, gazdasági helyzetére, egészségi állapotára, személyes preferenciáira vagy érdeklődési körére, megbízhatóságra vagy viselkedésre, tartózkodási helyére vagy mozgására vonatkozó jellemzők alapján. Erre példaként említhető a pénzügyi vállalkozás, amely hitelreferencia-, pénzmosás és a terrorizmus finanszírozása elleni vagy csalásellenes adatbázist használ ügyfelei szűrésére, vagy a biotechnológiai vállalat, amely közvetlenül a fogyasztóknak kínál genetikai vizsgálatokat, hogy értékelje, és előre jelezze a betegségek kockázatát és az egészségügyi kockázatokat.
- Joghatással vagy hasonló jelentős hatással járó automatizált döntéshozatal: adatkezelés, amelynek célja a természetes személy tekintetében joghatással bíró vagy a természetes személyt hasonlóképpen jelentős mértékben érintő döntések meghozatala. Az adatkezelés adott esetben egyének kirekesztését vagy hátrányos megkülönböztetését eredményezheti. A körben további felvilágosítást nyújt majd az Adatvédelmi Munkacsoport soron következő, profilalkotásról szóló iránymutatása.
- Módszeres megfigyelés: érintettek megfigyelése, nyomon követése vagy ellenőrzése céljából végzett adatkezelés (jellemzően közterületeken

vagy nyilvános helyeken történő megfigyelés például: bevásárlóközpont, nyilvános könyvtár).

- Különleges adatok vagy fokozottan személyes jellegű adatok: ide sorolhatóak a Rendelet 9. cikke szerinti különleges adatok, a 10. cikkben meghatározott, büntetőjogi felelősség megállapítására vonatkozó határozatokra és bűncselekményekre vonatkozó személyes adatok. A Rendelet e rendelkezésein túlmenően bizonyos adatkategóriák tekinthetőek úgy, hogy fokozzák az egyének jogait és szabadságait érintő lehetséges kockázatokat. Ezek a személyes adatok kihatnak valamely alapvető jog gyakorlására, vagy az őket érintő jogsértések egyértelműen súlyos hatást gyakorolnak az érintett mindennapi életére. E tekintetben lényeges lehet, hogy az érintett vagy valamely harmadik személy már nyilvánosan hozzáférhetővé tette-e az adatokat. A személyes adatok nyilvános hozzáférhetősége az értékelés során egyik tényezőként figyelembe vehető, ha az adatok bizonyos célú további felhasználására lehet számítani.
- Nagy számban kezelt adatok: az Adatvédelmi Munkacsoport ajánlása szerint ennek megállapításakor az alábbi tényezőket kell figyelembe venni: az érintettek száma konkrét számadatként vagy a lakosság arányában; a kezelt adatok mennyisége vagy adatfajták köre; az adatkezelési tevékenység időtartama vagy állandó jellege; az adatkezelési tevékenység földrajzi kiterjedése.
- Adatkészletek egymással való megfeleltetés vagy összevonása: például két vagy több, különböző célokból, illetve eltérő adatkezelők által végzett adatkezelési műveletből származó adatokkal, az érintett ésszerű elvárásait meghaladó módon.
- Kiszolgáltatott helyzetben lévő érintettekkel kapcsolatos adatok, például: gyermekek, munkavállalók, idősek, mentális betegségben szenvedők.
- Új technológiai vagy szervezési megoldások innovatív használata vagy alkalmazása: az ujjlenyomat- és az arcfelismerés együttes használata a hatékonyabb beléptetés érdekében; továbbá bizonyos, a *„dolgok internetét”* használó alkalmazások jelentős hatást gyakorolhatnak az egyének mindennapi életére és magánéletére, ezért szükségessé teszik az adatvédelmi hatásvizsgálat elvégzését. Az ilyen technológiák használatához újfajta adatgyűjtési és -felhasználási formák kapcsolódhatnak, amelyek magas kockázattal járhatnak az egyének jogaira és szabadságaira nézve. Az új technológiák bevezetésének személyes és társadalmi következményei tehát beláthatatlanok lehetnek.
- Azok az esetek, amikor az adatkezelés önmagában véve megakadályozza, hogy az érintettek a jogaikat gyakorolják vagy szolgáltatásokat ve-

gyenek igénybe vagy szerződést érvényesítsenek (Rendelet 22. cikk és (91) preambulumbekezdés): erre példa amennyiben egy bank hitelreferencia-adatbázis alapján szűri ügyfeleit annak érdekében, hogy eldöntse, kínál-e nekik hitelt.

Az esetek többségében az adatkezelő kiindulhat abból, hogy két szempontnak megfelelő adatkezelés esetében szükség van adatvédelmi hatásvizsgálatra. A Munkacsoport véleménye szerint, minél több kritériumnak felel meg az adatkezelés, annál nagyobb a valószínűsége annak, hogy az adatkezelés magas kockázattal jár az érintettek jogaira és szabadságaira nézve, ezért pedig szükségessé teszi az adatvédelmi hatásvizsgálat elvégzését.

Az adatkezelőknek további segítséget nyújt a Rendelet 35. cikkének (4) bekezdése szerinti adatkezelési műveletek típusainak a jegyzéke, amelyekre vonatkozóan adatvédelmi hatásvizsgálatot kell végezni, és amelyet a felügyeleti hatóságoknak kell összeállítania és nyilvánosságra hoznia. A NAIH 2018 májusában állítja össze és hozza nyilvánosságra az előbb említett adatkezelések listáját.

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 adatkezelőknek folyamatosan értékelniük kell az adatkezelési tevékenységeiből eredő kockázatokat, hogy felismerjék, ha az adatkezelés valamely fajtája *„valószínűsíthetően magas kockázattal jár a természetes személyek jogaira és szabadságaira nézve”*. Az adatvédelmi hatásvizsgálat egy folyamat, különösen akkor, ha az adatkezelési művelet dinamikus, és állandóan változik. Az adatvédelmi hatásvizsgálatot nem egyetlen alkalommal, hanem folyamatosan kell végezni.

Az adatvédelmi hatásvizsgálatot több fajta, különböző módszertan segítségével el lehet végezni, de a hatásvizsgálatnál figyelembe veendő szempontok azonosak, hiszen a Rendelet meghatározza az adatvédelmi hatásvizsgálat alapvető jellemzőit. Az adatvédelmi hatásvizsgálat elvégzésének általános, ismétlődő folyamata a következő:

- a tervezett adatkezelési műveletek leírása és az adatkezelés céljának ismertetése;

- szükségesség és arányosság vizsgálata;
- a természetes személyek jogait és szabadságát érintő kockázatok vizsgálata;
- a kockázatok kezelését, valamint a Rendelettel való összhang igazolását célzó intézkedések.

A hatásvizsgálat folyamatosan ismétlődő jellegét a Munkacsoport kihangsúlyozta, az adatkezelőknek a gyakorlatban valószínűleg a vizsgálat mindegyik szakaszát többször el kell végeznie a hatásvizsgálat lezárulta előtt. Azt követően is javasolt minden évben az ismétlése – az adatkezelések meghatározása, az intézkedések és kockázatok meghatározása körében például – és minden egyes jelentősebb változás bekövetkezésekor is indokolt a hatásvizsgálat felülvizsgálata.

A Hatóság fontosnak tartja külön felhívni az adatkezelők figyelmét a 248-as számú Iránymutatás 2. számú mellékletére, 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 Rendelet rendelkezéseit. Az Adatvédelmi Munkacsoport álláspontja szerint az adatkezelő választja ki a módszertant, a kiválasztott módszereknek azonban meg kell felelnie az Iránymutatás 2. mellékletében megadott szempontoknak. Az adatvédelmi Munkacsoport ágazat specifikus adatvédelmi hatásvizsgálati keretek kidolgozását szorgalmazza, a keretek ezáltal az egyedi ágazati ismeretekre épülhetnek, így az adatvédelmi hatásvizsgálatok az adott jellegű adatkezelési művelet sajátosságaira összpontosíthatnak. Ennek keretében az adatvédelmi hatásvizsgálatok az adott gazdasági ágazatban, illetve bizonyos technológiák használatakor vagy meghatározott jellegű adatkezelési műveletek végrehajtásakor felmerülő kérdésekkel foglalkozhatnak.

Az Adatvédelmi Munkacsoport a következő szempontok figyelembevételét javasolja az adatkezelők számára annak értékeléséhez, hogy az adatvédelmi hatásvizsgálat vagy az adatvédelmi hatásvizsgálathoz használt módszer kellően átfogó-e ahhoz, hogy összhangban legyen az általános adatvédelmi rendelettel:

- módszeres leírás készült az adatkezelésről (a 35. cikk (7) bekezdésének a) pontja);
    - figyelembe vették az adatkezelés jellegét, hatókörét, körülményeit és céljait ((90) preambulumbekezdés);
    - a személyes adatokat, a címzetteket, valamint a személyes adatok tárolásának időtartamát rögzítették;

- funkcionális leírás készült az adatkezelési műveletről;
- a személyes adatokhoz használt eszközöket (hardverek, szoftverek, hálózatok, személyek, papírok vagy papíralapú továbbítási csatornák) azonosították;
- figyelembe vették a jóváhagyott magatartási kódexek előírásainak teljesítését (a 35. cikk (8) bekezdése);

- értékelték a szükségességet és az arányosságot (a 35. cikk (7) bekezdésének b) pontja):
  - a rendelet betartására irányuló intézkedéseket meghatározták (a 35. cikk (7) bekezdésének d) pontja és a (90) preambulumbekezdés), figyelembe véve az alábbiakat:
    - az adatkezelés arányosságát és szükségességét előmozdító intézkedések a következők alapján:
      - meghatározott, kifejezett és jogos cél(ok) (az 5. cikk (1) bekezdésének b) pontja);
      - az adatkezelés jogszerűsége (6. cikk);
      - megfelelőek, relevánsak, és a szükséges adatokra korlátozódnak (az 5. cikk (1) bekezdésének c) pontja);
      - korlátozott tárolási időtartam (az 5. cikk (1) bekezdésének e) pontja);
    - az érintettek jogait támogató intézkedések:
      - az érintetteknek nyújtott tájékoztatás (12., 13. és 14. cikk);
      - betekintési jog és az adathordozhatósághoz való jog (15. és 20. cikk);
      - a helyesbítéshez és a törléshez való jog (16., 17. és 19. cikk);
      - kifogásolási jog és az adatkezelés korlátozásához való jog (18., 19. és 21. cikk);
      - a feldolgozókkal fennálló kapcsolatok (28. cikk);
      - a nemzetközi adattovábbításhoz kapcsolódó garanciák (V. fejezet);
      - előzetes konzultáció (36. cikk);
- az érintett jogait és szabadságait érintő kockázatokat kezelik (a 35. cikk (7) bekezdésének c) pontja):
  - a kockázatok forrását, jellegét, egyediségét és súlyosságát felmérték (vö. (84) preambulumbekezdés) vagy konkrétabban mindegyik kockázat (jogosulatlan hozzáférés, nemkívánatos módosítás és az adatok eltűnése) esetében az érintettek szemszögéből:
    - figyelembe vették a kockázatforrásokat ((90) preambulumbekezdés);

        - az érintettek jogaira és szabadságaira esetlegesen gyakorolt hatásokat beazonosították olyan eseményekre vonatkozóan, mint a jogosulatlan hozzáférés, a nemkívánatos módosítás és az adatok eltűnése;
        - az esetleg jogosulatlan hozzáféréshez, nemkívánatos módosításhoz vagy adatok eltűnéséhez vezető veszélyeket beazonosították;
        - felmérték a valószínűséget és a súlyosságot ((90) preambulumbekezdés);
    - az említett kockázatok orvoslására irányuló intézkedéseket meghatározták (a 35. cikk (7) bekezdésének d) pontja és a (90) preambulumbekezdés);
- az érdekelteket bevonták:
    - kikérték az adatvédelmi tisztviselő tanácsát (a 35. cikk (2) bekezdése);
    - adott esetben kikérték az érintettek véleményét (a 35. cikk (9) bekezdése).

A fentiekből adódóan a Hatóság a magasabb szintű megfelelés érdekében olyan módszertan kiválasztását javasolja, amelyet az adott adatvédelmi hatóság már összhangba hozott a Rendelet rendelkezéseivel. Ilyen például a francia adatvédelmi hatóság (CNIL) módszertana, amely alkalmazását tovább erősíti az a tény, hogy a CNIL közzétett egy nyílt forráskódú szoftvert, amellyel az adatkezelők könnyen elkészíthetik a módszertannak megfelelő adatvédelmi hatásvizsgálatot.

Az adatkezelőnek sem bejelentési, sem nyilvántartásba vételi kötelezettsége nincs. Saját döntése alapján nyilvánosságra hozhatja a hatásvizsgálat eredményét, akár egy összefoglaló formájában is, üzleti titkainak, adatbiztonságának feltárása nélkül.

Az adatkezelő kötelezettsége és felelőssége az adatvédelmi hatásvizsgálat elvégzése, ugyanakkor ahol van kijelölt adatvédelmi tisztviselő, ott fontos szerepe van a hatásvizsgálat elvégzésében, a tanácsát is ki kell kérni.

Az adatvédelmi hatásvizsgálat eredményéről 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 (tehát a fennmaradó kockázatok továbbra is jelentősek). 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).

III.10. A NAIH engedélyezési hatáskörei a GDPR alapján

A GDPR alapján a NAIH feladatköre bővülni fog az 58. cikk (3) bekezdése szerinti engedélyezési hatáskörökkel. Ezen hatáskörök gyakorlásának eljárási szabályait nemzeti jogszabályban kell rendezni, ezekkel kapcsolatban tehát irányadó az Infotv. módosítás tervezete (a továbbiakban: tervezet). A tervezet alapján a NAIH ezen hatásköreinek gyakorlására létrejönne az adatkezelési engedélyezési eljárás, amelyek során a NAIH-nak az Ákr. rendelkezéseit az Infotv.-ben szereplő kiegészítésekkel kellene alkalmaznia. A tervezet ilyen kiegészítést tartalmaz például a kérelem tartalmi elemeire, illetve az eljárás határidejére vonatkozóan.

III.11. Magatartási kódex

A tervezet alapján a Hatóság a GDPR szerinti magatartási kódexek tervezetének, kiegészítésének vagy módosításának jóváhagyása iránti kérelmek benyújtása esetén adatkezelési engedélyezési eljárást folytat le.

A magatartási kódex a GDPR által megnevezett egy olyan eszköz, amelynek önkéntes alkalmazása segít az adatkezelőknek abban, hogy a GDPR-nak való megfelelést biztosítsák. Az adatkezelők vagy adatfeldolgozók kategóriáit képviselő egyesületek és egyéb szervezetek magatartási kódexeket dolgozhatnak ki, hogy pontosítsák a GDPR alkalmazását. A GDPR tartalmaz egy példálózó felsorolást arra vonatkozóan, hogy melyek azok a kérdések, amelyekre vonatkozóan egy magatartási kódex pontosíthatja a GDPR alkalmazását.

Amennyiben egy egyesület vagy egyéb szervezet magatartási kódexet kíván kidolgozni vagy meglévő kódexet akarnak módosítani vagy kibővíteni, a tervezetet benyújtja az illetékes felügyeleti hatóságnak. A NAIH ebben az esetben 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 kódex több tagállamot is érintő adatkezelési tevékenységekre is vonatkozik, ebben az esetben az illetékes hatóság a jóváhagyást meg-

előzően a GDPR szerinti egységességi mechanizmus keretében benyújtja azt az Európai Adatvédelmi Testületnek (a továbbiakban: Testület) 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 tevékenységekre. Amennyiben egy kódex a Bizottság döntése alapján általános érvényű, akkor a nyilvánosságáról is a Bizottságnak kell gondoskodnia. Emellett a Testület valamennyi jóváhagyott magatartási kódexet egy nyilvántartásban állítja össze, és megfelelő módon nyilvánosan elérhetővé teszi őket.

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 (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; és
– 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 tenni honlapján az ellenőrző szervezet akkreditációjával kapcsolatos szempontokat, amelynek tervezetét az egységességi mechanizmus keretében meg kell küldeni a Testület részére is.

Az ilyen szervezet akkreditációjával kapcsolatban a tervezet alapján szintén engedélyezési eljárást kell alkalmazni. Ennek keretében a NAIH engedélyezi a magatartási kódexnek való megfelelés ellenőrzését végző szervezet tevékenységét. 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.

III.12. Harmadik országba való adattovábbítással kapcsolatos engedélyezési hatáskörök

A GDPR, illetve a tervezet alapján a NAIH engedélyezési hatásköreinek egy része a harmadik országba történő adattovábbítás során megfelelő garanciákat nyújtó eszközök jóváhagyására, engedélyezésére vonatkozik.

Ennek keretében a NAIH a tervezet alapján adatkezelési engedélyezési eljárást folytat le az adatkezelő vagy adatfeldolgozó és a harmadik országbeli adatkezelő, adatfeldolgozó vagy a személyes adatok címzettje között létrejött szerződéses rendelkezések, illetve a közhatalmi vagy egyéb, közfeladatot ellátó szervek között létrejött, közigazgatási megállapodásba beillesztendő rendelkezések engedélyezésére. Mind a két eszköz arra szolgál, hogy az adatkezelő vagy adatfeldolgozó, amely személyes adatokat kíván továbbítani harmadik országban letelepedett adatkezelő vagy adatfeldolgozó részére, megfelelő garanciákat, illetve érvényesíthető jogokat és hatékony jogorvoslati lehetőségeket biztosítson az érintettek számára. Az ilyen engedélyezési eljárások során tehát a NAIH-nak azt kell megvizsgálnia, hogy a kérelemben foglalt szerződéses, illetve közigazgatási megállapodásba illesztendő rendelkezések alkalmasak-e arra, hogy megfelelő garanciákat nyújtsanak az érintettek számára.

A fentiek mellett szintén adatkezelési engedélyezési eljárást folytat le a NAIH a kötelező erejű vállalati szabályok (a továbbiakban: BCR) jóváhagyása iránti kérelem benyújtása esetén. A BCR szintén egy olyan eszköz, amely megfelelő garanciákat nyújt az érintetteknek, és amely alapján így sor kerülhet a harmadik országba történő adattovábbításra. A BCR azonban speciális eszköz, amely arra szolgál, hogy egy vállalatcsoport EGT-térségen belüli, illetve harmadik ország-

ban letelepedett társaságai közötti adattovábbításra vonatkozóan az adatkezelő a harmadik országba történő adattovábbítások során megfelelő garanciákat teremtsen az egyének magánéletének, alapvető jogainak és szabadságainak védelme, továbbá a kapcsolódó jogok gyakorlása tekintetében.

A GDPR-t megelőzően is alkalmazott eszköz jogi hátterét korábban az adatvédelmi irányelv[7] 26. cikk (2) bekezdése jelentette. Annak érdekében, hogy az Európai Unión belül a BCR jóváhagyására irányuló eljárást a tagállami adatvédelmi hatóságok egységes követelmények alapján bírálják el, a 29-es Munkacsoport több dokumentumot is kidolgozott, amelyeknek figyelembe vételével jártak el az adatvédelmi hatóságok.

A GDPR ezeket a BCR-ra vonatkozó munkacsoporti iránymutatásokat jogszabályi szintre emelte, a megfelelő garanciákat nyújtó eszközök közül kiemelten, részletesen tartalmaz rendelkezéseket. Nemcsak a pontos definícióját határozta meg, hanem a szabályzat tartalmára vonatkozó követelményeket is megfogalmaz, illetve a jóváhagyásra irányuló eljárásra vonatkozóan is tartalmaz iránymutatást.

A 29-es Munkacsoport kijelölt alcsoportja a 2017-es év során a GDPR-ra való felkészülés jegyében elkezdte felülvizsgálni korábbi iránymutatást tartalmazó dokumentumainak felülvizsgálatát, így az adatkezelői és az adatfeldolgozói BCR-ra vonatkozókat is. A felülvizsgált, és a Munkacsoport által közzétett dokumentumok táblázatos formában foglalják össze, hogy milyen elemeket kell tartalmaznia egy BCR-nak, és így segítséget nyújt az adatkezelők és adatfeldolgozók számára a BCR összeállításához. Ezek a dokumentumok szintén segítséget nyújtanak azoknak a vállalatcsoportoknak, amelyeknek a szabályzatát már korábban jóváhagyták, de a GDPR alkalmazandóvá válásával felül kell azt vizsgálniuk. Az útmutató segítségével tehát beazonosíthatóak azok az elemek, amelyekkel ki kell egészíteni a korábban jóváhagyott BCR-okat.

A GDPR 46. cikk (5) bekezdése alapján a valamely felügyeleti hatóság által az adatvédelmi irányelv alapján kiadott engedélyek hatályban maradnak mindaddig, amíg azokat szükség esetén a felügyeleti hatóság nem módosítja, nem váltja fel vagy nem helyezi hatályon kívül. A 29-es Munkacsoport álláspontja szerint ettől függetlenül a korábban már jóváhagyott BCR-okat a vállalatcsoportoknak módosítaniuk kell annak érdekében, hogy azok megfeleljenek a GDPR BCR-ra

7 A személyes adatok feldolgozása vonatkozásában az egyének védelméről és az ilyen adatok szabad áramlásáról szóló 95/46/EK európai parlamenti és tanácsi irányelv.

vonatkozó rendelkezéseinek. Ezeket a módosított szabályzatokat azonban a 46. cikk (5) bekezdése alapján nem szükséges ismételten benyújtani jóváhagyásra az illetékes felügyeleti hatóságoknak, hanem elegendő, ha a szabályzatok módosításairól tájékoztatják az érintett hatóságokat.

A BCR jóváhagyására irányuló eljárással kapcsolatban a GDPR 47. cikk (1) bekezdése az irányadó, mely alapján az illetékes felügyeleti hatóság a BCR-t az egységes mechanizmus alkalmazásával hagyja jóvá. A GDPR azonban az ilyen jóváhagyási eljárások vonatkozásában nem határozza meg azt, hogy mi alapozza meg egy felügyeleti hatóság illetékességét, ezért a 29-es Munkacsoport ki fog dolgozni egy iránymutatást ezzel kapcsolatban, amely emellett rendezni fogja a felügyeleti hatóságok közötti, a BCR-ral kapcsolatos együttműködés kereteit.

III.13. Tanúsítás

A GDPR alapján a NAIH feladatai közé tartozik a tanúsítási szempontok jóváhagyása, amelyre a tervezet szintén az adatkezelési engedélyezési eljárást rendeli alkalmazni.

A tanúsítás egy olyan eszköz, amelyet a GDPR abból a célból vezet be, hogy segítséget nyújtson az adatkezelőknek abban, hogy a GDPR-nak való megfelelést biztosítsák és igazolják. A GDPR a tanúsítást nem jogként vagy kötelezettségként szabályozza az adatkezelők számára, a 42. cikk (3) bekezdése alapján ez egy önkéntes eszköz, amelynek segítségével az adatkezelő igazolhatja az érintettek és a felügyeleti hatóságok felé az adatvédelmi szabályoknak való megfelelést. Ezen eszköz alkalmazása az adatvédelem területén újdonságot jelent a magyar adatkezelők számára.

A GDPR alapján az átláthatóság és a GDPR-nak való megfelelés elősegítése érdekében a felügyeleti hatóságoknak ösztönözniük kell olyan tanúsítási mechanizmusok, és adatvédelmi bélyegzők illetve jelölések létrehozását, amelyek lehetővé teszik az érintettek számára, hogy gyorsan értékelni tudják az adott termékek és szolgáltatások adatvédelmi szintjét. A tanúsítási mechanizmus tehát elősegíti az érintettek számára az átláthatóságot, illetve az adatkezelők számára a GDPR-nak való megfelelés igazolását.

A GDPR 57. cikk (1) bekezdése alapján a felügyeleti hatóságok egyik feladata az adatvédelmi tanúsítási mechanizmusok ösztönzése. A GDPR tehát nem teszi

kötelezővé a felügyeleti hatóságok számára azt, hogy tanúsítási szervezetként járjanak el, azonban általánosságban feltételezi az ehhez szükséges szakértelem meglétét. Tanúsítványt a GDPR alapján a felügyeleti hatóság, vagy az erre akkreditált tanúsító szervezet bocsáthat ki. Ez alapján tehát többféle megoldás elképzelhető a felügyeleti hatóság tanúsítással összefüggő feladataival kapcsolatban:

- a hatóság a saját tanúsítási rendszere alapján állít ki tanúsítványt;
- a hatóság saját tanúsítási rendszere alapján állít ki tanúsítványt, de a megfelelőség-értékelés egy részét vagy egészét más szervezetekre delegálja;
- a hatóság megalkotja saját tanúsítási rendszerét, amely alapján aztán más tanúsító szervezetek állítják ki a tanúsítványt;
- ösztönzi a piaci szereplőket arra, hogy tanúsítási rendszereket dolgozzanak ki, amelyekre vonatkozóan a tanúsítási szempontokat a hatóság jóváhagyja.

A GDPR alapján tanúsítványt tehát nem csak a felügyeleti hatóságok, hanem az erre akkreditált tanúsító szervezetek is kiállíthatnak, amelyek megfelelő szakértelemmel rendelkeznek az adatvédelem területén. A GDPR ezért a 43. cikkében rendelkezik arról, hogy milyen módon kerülhet sor az ilyen szervezetek akkreditációjára. Ez a cikk több lehetőséget is felvázol, amelyek közül a tagállamoknak meg kell határozniuk, hogy pontosan melyiket alkalmazzák, és milyen módon.

A 43. cikk (1) bekezdése alapján három megoldás lehetséges az akkreditáció elvégzésére:

- az akkreditációt a felügyeleti hatóság végzi az általa kidolgozott követelményrendszer alapján;
- az akkreditációt a 765/2008/EK parlamenti és tanácsi rendelettel összhangban megnevezett nemzeti akkreditáló testület végzi az EN-ISO/IEC 17065/2012 szabvánnyal, illetve a felügyeleti hatóságok által megállapított kiegészítő követelményekkel összhangban;
- az akkreditációt mind a felügyeleti hatóság, mind az akkreditáló testület végzi.

Azon tagállamoknak, amelyek az első megoldást választják, biztosítaniuk kell, hogy az akkreditáló testület rendelkezzen ehhez az új feladathoz megfelelő erőforrásokkal és szakmai tudással. Emellett ezen megoldás esetén a felügyeleti hatóságoknak ki kell dolgozniuk az adatvédelemre vonatkozó további követelményeket, amelyek kiegészítik a 765/2008/EK rendelet alapján megállapított

akkreditációs szabályokat, illetve azon technikai szabályokat, amelyek meghatározzák az akkreditációs testületek módszereit és eljárásait. A felügyeleti hatóságok által kidolgozott kiegészítő követelményeket úgy kell megalkotni, hogy azok megkönnyítsék a tanúsító szervezetek függetlenségére, illetve adatvédelmi szakértelmére vonatkozó megfelelőség-értékelést.

A tervezet alapján, Magyarországon, a fent felsorolt három opció közül az első lesz alkalmazandó, vagyis a tanúsító szervezetek akkreditációját a Nemzeti Akkreditációs Hatóság (a továbbiakban: NAH) fogja végezni. Az akkreditáció során a NAH, ahogy azt a GDPR is előírja, az EN-ISO/IEC17065/2012 szabványt fogja alkalmazni. A NAIH által a GDPR alapján megalkotott kiegészítő követelmények tehát e szabványban megfogalmazott általános követelményeket fogják kiegészíteni adatvédelem specifikus követelményekkel. A tervezet alapján a NAH az akkreditációs eljárás során szakhatóságként be fogja vonni a NAIH-ot. Ezáltal a NAIH fogja szakhatósági eljárás keretében megvizsgálni, hogy az EN-ISO/IEC17065/2012 szabvány általános követelményeit kiegészítő, adatvédelem specifikus követelményeknek megfelel-e az adott tanúsító szervezet. A NAIH véleménye kötelező lesz a NAH-ra nézve.

A tanúsítási szempontok jóváhagyását a GDPR a felügyeleti hatóságok feladatai között említi, azonban a szempontok kidolgozását nem. Elvileg azonban lehetséges az, hogy az illetékes felügyeleti hatóság „*jóváhagyja*" a saját maga által kidolgozott szempontokat, de erre nincs kötelezettsége a hatóságoknak. Mindenesetre a tanúsításnak minden esetben jóváhagyott szempontokon kell alapulnia.

A szempontok jóváhagyása érdekében a hatóságnak egyértelmű álláspontot kell kialakítani azzal kapcsolatban, hogy mit vár el, különös tekintettel az alkalmazási területre, illetve a GDPR-nak való megfelelés igazolására vonatkozóan. Figyelembe kell vennie emellett a GDPR alkalmazásának nyomon követésére és kikényszerítésére vonatkozó alapfeladatát is.

A tanúsító szervezet feladata az, hogy tanúsítványokat állítson ki, vizsgáljon felül és újítson meg a tanúsítási mechanizmusok és a jóváhagyott tanúsítási szempontok alapján. Ehhez az szükséges, hogy a tanúsítási szervezet vagy egyéb tanúsítási rendszer tulajdonos eljárásokat dolgozzon ki, így különösen az ellenőrzésre, felülvizsgálatra, panaszkezelésre és a visszavonásra vonatkozóan, illetve megállapítson tanúsítási szempontokat, amelyek alapján a tanúsítvány kiállítható. A tanúsítási szervezet akkreditációjának feltétele a tanúsítási mechanizmus, illetve a tanúsítási szempontrendszer megléte.

Ahogy korábban is kifejtettük, tanúsítványt csak az akkreditált tanúsítási szervezet állíthat ki jóváhagyott szempontok alapján. A szempontokat tehát a tanúsítást megelőzően jóvá kell hagynia vagy az illetékes felügyeleti hatóságnak, vagy a Testületnek. A tervezet alapján a hozzá benyújtott tanúsítási szempontokat a NAIH adatvédelmi engedélyezési eljárás keretében fogja elbírálni, és amennyiben megfelelőnek találja, jóváhagyni.

Azt, hogy melyik tagállam felügyeleti hatósága illetékes, a GDPR 55. és 56. cikke határozza meg. A saját területén minden felügyeleti hatóság illetékes a tanúsítási szempontok jóváhagyására. Amennyiben egy tanúsítási szervezet több tagállam területén rendelkezik szervezeti egységgel, vagy amennyiben több tagállamban kívánja folytatni tevékenységét, akkor minden tagállami felügyeleti hatóságnál külön kell kérelmeznie az általa kidolgozott tanúsítási szempontok jóváhagyását. Azon tanúsítási szervezet vonatkozásában, amely az Unió egész területén szeretné folytatni tevékenységét, vagy európai adatvédelmi bélyegzőt kíván kiállítani, a Testület rendelkezik hatáskörrel.

A GDPR 43. cikk (1) bekezdése alapján a tanúsító szervezetek kötelesek tájékoztatni az illetékes felügyeleti hatóságot arról, ha egy tanúsítványt kívánnak kiállítani, illetve megújítani, amely lehetővé teszi, hogy a hatóság gyakorolja korrekciós hatásköreit. Emellett a GDPR 43. cikk (5) bekezdése azt is megköveteli, hogy a tanúsító szervezet közölje az illetékes felügyeleti hatósággal a kért tanúsítvány megadásának vagy visszavonásának okait.

Bár a GDPR lehetővé teszi, hogy a felügyeleti hatóságok meghatározzák, hogy milyen módon fogadják, illetve dolgozzák fel az így kapott információt, lehetséges, hogy ezzel kapcsolatban egy egységes eljárás és kritériumrendszer születik meg, amely alapján az egyes tanúsítványokkal kapcsolatban kapott információt a hatóság feldolgozza. Tekintettel arra, hogy a kapott információk alapján az illetékes felügyeleti hatóságok gyakorolhatják azon hatáskörüket, hogy elvégezzék a kiadott tanúsítványok felülvizsgálatát, illetve hogy utasítsák a tanúsító szervezetet, hogy a tanúsítványt ne adja ki, vagy vonja vissza, ezért egy egységes eljárás biztosíthatná az egységes alkalmazást. Elősegítené továbbá azt is, hogy a felügyeleti hatóságok számára könnyen elérhetőek legyenek egy adott szerv tanúsításával kapcsolatos információk. A tanúsítási szervezeteknek e kötelezettség teljesítése érdekében javasolt, hogy nyilvántartást vezessenek a sikeres tanúsításokról, amely tartalmazza legalább a tanúsítás tárgyát és érvényességét.

III.14. A GDPR gyakorlati megvalósításának egyes kérdései

A GDPR gyakorlatilag valamennyi szereplő számára hoz változásokat, ezen túl új jogokat, új jogintézményeket vezet be, létrehozza az Európai Adatvédelmi Testületet – hogy csak néhány újítást emeljünk ki. Ebben az időszakban a felkészülés zajlik, amely 2018-ra is átnyúlik.

Eldőlt, hogy az Európai Unió adatvédelmi hatóságai egy közös informatikai platformon fognak egymással kommunikálni a GDPR keretében folytatandó közös eljárások lefolytatása érdekében. Ez a közös platform hivatott az egyablakos ügyintézés, a kölcsönös segítségnyújtás, a közös műveletek támogatására, továbbá az Európai Adatvédelmi Testület véleményének megfogalmazását megelőző eljárás, továbbá az úgynevezett vitarendezési eljárás egyes feladatai is ebben a virtuális térben valósulnak majd meg.

Az adatvédelmi hatóságok, amelyeket a GDPR adatvédelmi felügyeleti hatóságként említ, Unió-szerte többlet forrásokat kapnak annak érdekében, hogy a rendeletből fakadó többletfeladataikat megfelelően el tudják látni.

IV. A bűnügyi adatvédelmi irányelv

Az új uniós adatvédelmi csomag másik eleme a bűnüldözési célból kezelt személyes adatok védelmére vonatkozó irányelv (2016/680/EU irányelv – Bűnügyi Irányelv), melyet – a GDPR-tól eltérően – a tagállamoknak 2018. május 6-ig kell átültetniük nemzeti jogszabályaikba. Magyarországon a nemzeti jogba történő implementálás folyamata – az Infotörvény módosítása, kiegészítése útján – jelen beszámoló megírásakor még nem zárult le.

A Bűnügyi Irányelv esetében a reform célja a büntetőügyekben folytatott rendőrségi és igazságügyi együttműködés keretében feldolgozott személyes adatok védelméről szóló 2008/977/IB tanácsi kerethatározatban lefektetett szabályok korszerűsítése, valamint a bűnüldözési célból kezelt személyes adatok belföldi kezelésére és határokon átnyúló továbbítására vonatkozó szabályok egységesítése, melynek hatására az elvárások szerint megerősödik a tagállamok és harmadik országok bűnüldöző szervei közötti együttműködés is.

A bűnüldözés során a tagállamok hatóságainak – a nemzetközi bűnözés és terrorizmus elleni küzdelem részeként – egyre gyakrabban kell személyes adatokat feldolgozniuk és továbbítaniuk. Ebben az összefüggésben az érintett hatóságok közötti együttműködés javításához elengedhetetlenül fontos, hogy az adatvédelemre uniós szinten világos és koherens szabályozás vonatkozzon.

Az Irányelv hatálya a kerethatározathoz képest szélesebb, ugyanis a bűnüldözési, bűnmegelőzési célú (beleértve a terrorizmus, a szervezett bűnözés és a számítástechnikai bűnözés elleni küzdelmet is) adatkezelés mellett a közbiztonságot fenyegető cselekmények elleni védelemre és azok megelőzésére, a büntetés-végrehajtás során keletkezett adatokra, valamint a nem állami, de bűnüldözési célból adatokat kezelő gazdasági társaságokra, szervezetekre (például: magánüzemeltetésű börtönök) is kiterjed. Ugyanakkor az úgynevezett *„kivett”* ügyek közé tartoznak a nemzetbiztonsági (uniós jog hatályán kívül), a bírósági (*„45. cikk (2): igazságügyi feladat”*) ügyek és az uniós intézmények (Regulation 45/2001) eljárásai.

Az Irányelv a GDPR-hoz hasonlóan új jogintézményekkel bővíti az adatvédelem keretrendszerét, amelyeket a bűnüldözési célból adatkezelést folytató szervezeteknek is alkalmazniuk kell. Itt is megjelenik a beépített adatvédelem és alapértelmezett adatvédelem elve – melyet a bűnüldöző hatóságoknak és szerveknek a személyes adatokkal kapcsolatos valamennyi eljárás kezdetén (például: új

adatbázisok kialakításakor) alkalmazniuk kell. Az adatvédelmi hatásvizsgálat elvégzéséből és az adatvédelmi hatósággal folytatott előzetes konzultációból eredő, valamint az adatkezelési tevékenység nyilvántartására és azok naplózására vonatkozó részletes és széles körű kötelezettségek szintén rendkívül fontosak. Ezen túlmenően, az adatkezelésért felelős személyek elszámoltathatóak lesznek munkájukért, a hatóságoknak pedig adatvédelmi tisztviselőt kell kinevezniük, aki a szervezeten belül felelős a személyes adatok védelméért, valamint adatvédelmi incidens esetén előírja a nemzeti felügyeleti hatóság mielőbbi értesítését.

Az új rendelkezések összességében tehát az adatvédelmi hatóságokkal való szorosabb együttműködésre és az általuk javasolt szempontrendszer még szélesebb körű érvényre juttatására kötelezik az adatkezelőket. Figyelemmel arra, hogy a külföldre történő adattovábbítások száma várhatóan nő majd, és előzetes jóváhagyásukra, ellenőrzésükre vonatkozóan új feltételrendszer alkalmazandó, az adatvédelmi hatóságok előzetes kontrollja az eddiginél nagyobb szerepet kaphat.

A NAIH-hoz a 2017-es év során számos bűnüldözési célú adatkezeléssel kapcsolatos beadvány és panasz érkezett. Az utóbbiak legtöbb esetben a különböző nyomozóhatóságok (rendőrség, NAV, ügyészség), közterületi kamerás megfigyelést végző szervek (rendőrség, közterület felügyelet) és büntetés-végrehajtási intézmények adatkezelését érintették.

Az Irányelv jövőbeli alkalmazása szempontjából említendő ügyben az egyik magyarországi büntetés-végrehajtási intézetben fogva tartott panaszos fordult az adatvédelmi hatósághoz. A fogvatartottak a zárkájukban legálisan, az intézet beleegyezésével olyan elektronikus adathordozókat tárolhatnak (például: pendrive-okat, DVD lemezeket), amelyeken a hivatalos szervektől és ügyvédjüktől érkezett dokumentumokat és levelezést tárolhatják elektronikus formában. Az ilyen adathordozókat az intézet informatikusa rendszeresen ellenőrzi, azon tiltott tartalmakat keresve. Egy ilyen ellenőrzés után, amikor a panaszos visszakapta az általa használt pendrive-ot, azon olyan új adatokat talált, amelyek más fogvatartottakhoz tartoztak (bírósági, ügyvédi levelezések). A pendrive-ra továbbá az intézet kamerás megfigyelő rendszere által rögzített néhány olyan felvétel is megjelent, melyen más fogvatartottak is szerepelnek. A NAIH megkereste az intézetet, amely kivizsgálta és elismerte az incidens megtörténtét. Ezen eset kapcsán kiemelendő, hogy a fenti eset adatvédelmi incidensnek minősül az Infotv. jelenleg hatályos előírásai alapján is, és a Bűnügyi Irányelv rendelkezéseinek hatálybalépésével az ilyen esetet be is kell jelenteni majd a NAIH-hoz.

V. Adatvédelem

V.1. Statisztikai adatok

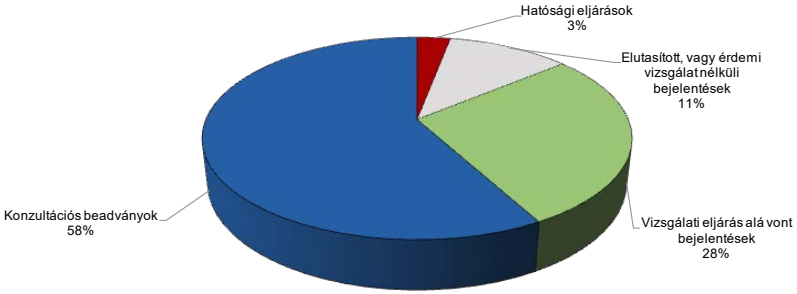
A 2017-es évben az adatvédelmi ügyek intézése az eddig kialakított eljárási rend szerint, de már az új általános közigazgatási rendtartásról szóló törvény és az új általános adatvédelmi rendeletre való felkészülés szellemében folyt.

Az adatvédelmi ügyek 58 %-a volt ebben az évben konzultációs típusú ügy. A konzultációs beadványokra általában az jellemző, hogy – akár valamely állampolgár, akár egy adatkezelő – tanácsot, tájékoztatást kér egy általa leírt adatkezelést érintő esetről, illetve annak jogszerűségéről szeretne állásfoglalást kapni a Hatóságtól.

Az ezekben az ügyekben megfogalmazott tájékoztatásoknak, állásfoglalásoknak fontos szerepük van abban, hogy az adatkezelők jogkövető magatartását erősítsék, és ezáltal hatékonyan hozzájáruljanak a jogsértések megelőzéséhez, megszüntetéséhez vagy a lehető legjobb adatkezelési gyakorlat kialakításához, továbbá az érintettek figyelmét is ráirányítják az egyéni jogérvényesítés, a tájékoztatás, módosítás, vagy adattörlés kérésének lehetőségére, az adatvédelmi jogtudatosság fontosságára.

A 2017-ben folyt vizsgálati eljárások aránya az összes ügyszámhoz képest 28%, ez növekedést jelent az előző évi 22%-hoz képest. A Hatóság a vizsgálati eljárás alá vont adatvédelmi bejelentések 47 %-ában jogsértést állapított meg.

Adatvédelmi ügyek 2017



A 2017-es évről is elmondható, hogy az előző évről áthúzódott folyamatban lévő és a 2017-ben indult új vizsgálati eljárások száma magasabb volt, mint a hatósági eljárások száma. A hatósági eljárások megindítását megelőzően figyelembe vettük az esetleges vizsgálati előzmények tapasztalatait és az Infotv. által megjelölt kötelezően vizsgálandó eseteket is. A hatósági eljárás sok esetben egy-egy egyedi panaszügy vizsgálatán túl az adatkezelőnek a panasz tárgyához kapcsolódó teljes adatkezelési folyamatát átfogta, így az adott adatkezelő általános adatkezelési gyakorlatát is vizsgálta a Hatóság. A hatósági eljárás során a vizsgált adatkezelés pontos megismerése, a tényállás részletes feltárása a *„jogsértés hatósági bizonyítása”* formalizáltabb eljárási szabályok között zajlik, ezért ezek az eljárások hosszabb ideig tartanak.

2017-ben 17 hatósági eljárás indult, az előző évekről áthúzódott ügyekkel együtt pedig összesen 68 hatósági eljárás volt folyamatban. A Hatóság a 2016-os évhez képest kevesebb új hatósági eljárást indított. Ennek egyik oka az általános adatvédelmi rendeletre való felkészülés volt, mely feladat nem csak a Hatóságra, hanem az adatkezelőkre is jelentős terheket rótt.

A Hatóság a folyamatban lévő hatósági eljárások közé sorolta azokat a 2017-es ügyiratszámmal rendelkező ügyeket is, melyekben az eljárás az előző években hozott határozatok teljesítésének, végrehajtásának ellenőrzésére irányult. Ugyanis ezeknek az ügyeknek a végleges lezárását a végrehajtás elmaradása vagy a nem megfelelő végrehajtás akadályozta.

A Hatóság 2017-ben az áthúzódott ügyeket is figyelembe véve összesen 27 hatósági eljárásban hozott határozatot, melyek közül összesen 20 született az előző években indult ügyekben. A Hatóság az adatkezelők kis- és középvállalkozási minőségére tekintettel a határozataiban csak 14 esetben szabhatott ki bírságot. A beszámoló elkészítéséig a Hatóság további 4 határozatot hozott, melyek közül 2 ügyben bírsággal is sújtotta a jogsértő adatkezelőt.

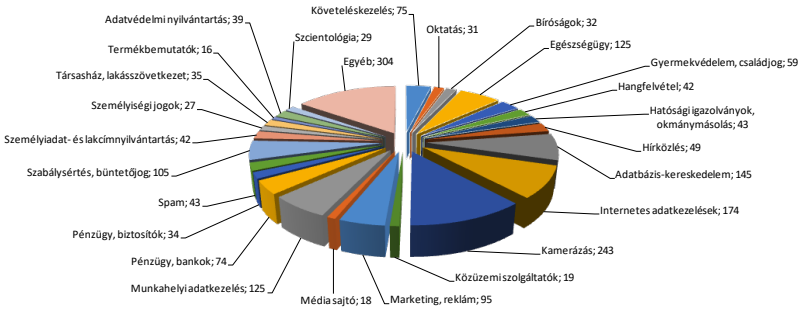
A Fővárosi Közigazgatási és Munkaügyi Bíróság 2017-ben a Hatóság 20 döntésének (érdemi határozatának és önálló jogorvoslattal megtámadható végzésének) felülvizsgálata során hozott ítéletet vagy végzést. A felülvizsgálati perek 15 esetben zárultak a Hatóság pernyertességével és 2 esetben részbeni pernyertességével, emellett 3 ügyben lett pervesztes a Hatóság. A bírósági döntések 3 kivétellel az előző években hozott döntések felülvizsgálatának tárgyában születtek.

2017-ben – függetlenül attól, hogy annak közigazgatási perben való felülvizsgálatát törvény nem teszi lehetővé – a Hatóság vizsgálati eljárásban hozott intéz-

kedéseinek bírósági felülvizsgálatát is kezdeményezte egy ügyfél. A bíróság 5 alkalommal utasította el a felperes keresetét.

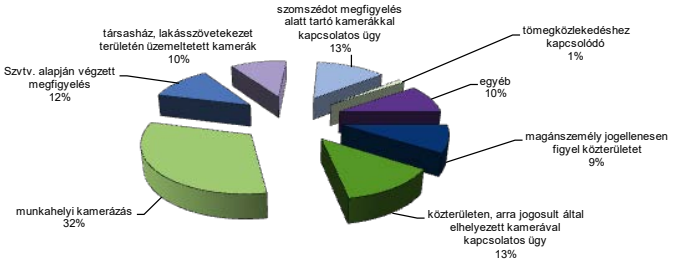
Az adatvédelmi tárgyú beadványok – panaszok, bejelentések és konzultációs kérések – a közigazgatás és a magánszféra számtalan szféráját érintik, vagyis a Hatósághoz igen sok területet érintő témakörben érkeznek különféle típusú levelek. Egy beadványban vizsgálni kért bejelentés vagy megválaszolni kért kérdés esetenként több területet is érintett. Az alábbi diagram azt szemlélteti, mely területet érintő témakörben milyen számban érkeztek a beadványok.

Adatvédelmi ügyek ügytípus szerinti gyakorisága 2017



A Hatósághoz 2017-ben is jelentős mennyiségű olyan bejelentés és konzultációs beadvány érkezett, amely az elektronikus megfigyelőrendszerekhez, kamerarendszerekhez kapcsolódó adatkezelésre vonatkozott. A „*kamerás ügyek*” jelentették ez évben is a leggyakoribb ügytípust, arányában a legtöbb beadvány e tárgyban érkezett.

Kamerás ügyek típusai 2017



Ahogy a fenti diagramból is látható, a kamerás megfigyeléssel kapcsolatban küldött beadványok sokszínűek, több kategóriába sorolhatóak. Az ügytípusok között számos esetben átfedés van, a korábbi évhez hasonlóan most is rendszeresen előfordult például az, hogy egy olyan ügyben indult vizsgálat, melyben a panasszal érintett adatkezelő egyszerre tartott megfigyelés alatt közterületet és szomszédos ingatlant is.

V.2. GDPR alkalmazására vonatkozó tájékoztatási kérelmek

2017-ben az új általános adatvédelmi rendelet (a továbbiakban: GDPR) alkalmazására történő felkészülés jegyében több adatkezelő is tájékoztatást kért a Hatóságtól a GDPR rendelkezéseinek értelmezésével kapcsolatban.

Az uniós rendelet olyan jogi eszköz, mely valamennyi tagállamban közvetlenül – a nemzeti jogba való átültetés nélkül – alkalmazandó. Tehát a GDPR is közvetlenül alkalmazandó, de több helyen is eltérést enged a rendelkezéseitől, vagy pontosító, kiegészítő szabályozás kialakítását írja elő a hazai jogalkotó részére. Tekintettel arra, hogy a GDPR magyarországi végrehajtásához szükséges jogszabály-módosítások az elmúlt évben és még jelenleg is előkészítés alatt állnak, ezért a Hatóság az adatkezelők kérdéseire adott tájékoztatóit a rendelet szövegére és a 29-es Munkacsoport által közzétett állásfoglalásokra alapozta.

Az adatkezelőket foglalkoztató főbb kérdések és az ezekre adott válaszok a következők voltak:

1) Hozzájáruláson alapuló adatkezelés esetében a meglévő adatbázis további kezeléséhez a GDPR rendelkezéseire figyelemmel kell-e új adatkezelési hozzájárulást beszerezni az érintettektől?

A GDPR (171) preambulumbekezdése értelmében a rendelet alkalmazásának időpontja előtt megkezdett adatkezeléseket összhangba kell hozni a rendelettel. Amennyiben hozzájáruláson alapuló adatkezelésről van szó, és a hozzájárulás megfelel a rendeletben előírt feltételeknek, úgy nem kell ismételten az érintett engedélyét kérni ahhoz, hogy az adatkezelő a rendelet alkalmazási időpontját követően is folytathassa az adatkezelést. Amennyiben a hozzájárulás nem felel meg a rendelet követelményeinek, különösen a 7. és 8. cikkben foglalt feltételeknek, úgy új hozzájárulást kell beszerezni az érintettektől.

2) A GDPR rendelkezéseinek megfelelő új tájékoztató közzétételével, új hozzájárulás beszerzése nélkül folytatható-e egy már évek óta fennálló adatkezelés?

Az átlátható tájékoztatás kapcsán a GDPR 12. cikkének (1) bekezdésére figyelemmel szükséges az adatkezelési tájékoztatók felülvizsgálata. A módosított tájékoztató kiadásával azonban nem váltható ki az új hozzájárulás beszerzése, ha az érintettek hozzájárulása nem felel meg a GDPR követelményeinek.

3) A kisvállalkozásokra nézve a rendelet tartalmaz-e valamilyen kivételszabályt?

A GDPR 30. cikk (1) bekezdése alapján az adatkezelő vagy az adatfeldolgozó a rendeletnek való megfelelés bizonyítása érdekében nyilvántartást köteles vezetni az általa végzett adatkezelési tevékenységekről. A GDPR 30. cikk (5) bekezdése mentesíti a 250 főnél kevesebb főt foglalkoztató vállalkozásokat a nyilvántartási kötelezettség alól, amennyiben az adatkezelés valószínűsíthetően nem jár magasabb kockázattal az érintettek jogaira és szabadságaira nézve, vagy ha az adatkezelés alkalmi jellegű, illetve, ha nem terjed ki a személyes adatok különleges kategóriáinak kezelésére.

4) Az adatvédelmi tisztviselőnek kell-e valamilyen adatvédelmi szakirányú képesítés?

Az adatvédelmi tisztviselőt szakmai rátermettség, és különösen az adatvédelmi jog és gyakorlat szakértői szintű ismerete, valamint a GDPR 39. cikkében említett feladatok ellátására való alkalmasság alapján kell kijelölni. A szakértői ismeretek szükséges szintjét különösen az adatkezelő vagy az adatfeldolgozó által végzett adatkezelés, valamint az általuk kezelt személyes adatok tekintetében megkövetelt védelem alapján kell meghatározni.

5) Az állami tulajdonú közfeladatot ellátó szerveknek kell-e majd adatvédelmi tisztviselőt alkalmazniuk?

GDPR nem határozza meg a *„közhatalmi szerv vagy egyéb, közfeladatot ellátó szerv”* fogalmát. A GDPR 37. cikkének (1) bekezdése rendelkezik arról, hogy az adatkezelő és az adatfeldolgozó adatvédelmi tisztviselőt milyen esetben jelöl ki.

Ehhez segítséget nyújt az Adatvédelmi Irányelv 29. cikke szerint létrehozott Adatvédelmi Munkacsoport az adatvédelmi tisztviselőkkel kapcsolatban kibocsátott 243. számú iránymutatása, (http://naih.hu/29-es-munkacsoport-iranymutatasai.html.) Ez alapján a közhatalmi szerv vagy közfeladatot ellátó szerv fogalmát

– a GDPR-ban írt definíció híján – a nemzeti jog szerint kell meghatározni. Az iránymutatás kitér arra is, hogy *„nem csupán közhatalmi szerv vagy egyéb, közfeladatot ellátó szerv láthat el közfeladatot, hanem a közjog vagy magánjog hatálya alá tartozó egyéb természetes és jogi személyek is – az egyes tagállamok nemzeti szabályozása szerint – olyan ágazatokban, mint például a tömegközlekedés, a víz- és energiaellátás, a közúti infrastruktúra, a közszolgálati műsorszolgáltatás, az állami (önkormányzati) lakáshoz jutás vagy a szabályozott szakmák fegyelmi testületei."* És bár ezekben az esetekben a GDPR alapján nem kötelező, a Munkacsoport jó gyakorlatként azt ajánlja, hogy az ilyen magánjogi szervezetek is jelöljenek ki adatvédelmi tisztviselőt.

Az adatvédelmi tisztviselővel összefüggésben a GDPR szűk keretek között enged csak teret a tagállami jogalkotásnak [ld. 37. cikk (4) bekezdése és 38. cikk (5) bekezdés], így annak eldöntéséhez, hogy állami tulajdonú közfeladatot ellátó szervnek kell-e majd tisztviselőt alkalmaznia, a GDPR fenti hivatkozott rendelkezését kell kiindulópontnak tekinteni.

6) Amennyiben eljárása során jogsértést állapít meg a Hatóság, mindenképpen bírságot szab majd ki, vagy helyette más intézkedések alkalmazására is lesz lehetősége?

A GDPR (148) preambulumbekezdése úgy rendelkezik a bírságról, hogy a GDPR szabályainak minél erősebb betartatása érdekében a GDPR megsértése esetén a GDPR által előírt megfelelő intézkedések mellett vagy helyett szankciókat, akár közigazgatási bírságot is ki kell szabni. A bírság helyett azonban figyelmeztetést is lehet alkalmazni, ha a bírság a természetes személy számára aránytalan terhet jelentene.

A GDPR (150) preambulumbekezdése rögzíti azt is, hogy a szabályozás célja a szankciók szigorítása és harmonizálása, melynek érdekében minden tagállam felügyeleti hatósága bírságolási hatáskörrel rendelkezik. A GDPR több körülményt is meghatároz, melyeket mérlegelni kell a bírság kiszabásakor. GDPR 83. cikk (4)-(6) bekezdésében több mérlegelendő tényező szerepel, mint a jelenlegi magyar szabályozásban.

7) Egy cég működését felfüggesztheti-e a Hatóság a GDPR valamely rendelkezésének megszegése esetén?

Az adatvédelmi szabályok megsértése esetén alkalmazandó jogkövetkezményeket a GDPR és az Infotv. tartalmazza. Ezek egyike sem biztosít ilyen hatáskört a felügyeleti hatóság számára.

V.3. A bűnüldözési célú adatkezelések az európai adatvédelmi reform kapcsán és a NAIH kapcsolódó gyakorlata

Az Európai Parlament és a Tanács 2016. április 27-én fogadta el az új uniós adatvédelmi csomagot, amelynek két eleme az adatvédelem általános keretét meghatározó rendelet (2016/679/EU rendelet – GDPR) és a bűnüldözési célból kezelt személyes adatok védelmére vonatkozó irányelv (2016/680/EU irányelv – Bűnügyi Irányelv).

Míg a GDPR 2018. május 25-től EU-szerte közvetlenül alkalmazandó, addig az irányelvet a tagállamoknak 2018. május 6-ig kell átültetniük nemzeti jogszabályaikba. Magyarországon a Bűnügyi Irányelv rendelkezéseinek a nemzeti jogba történő átültetése jelenleg folyamatban van.

A bűnüldözés során a tagállamok hatóságainak – a nemzetközi bűnözés és terrorizmus elleni küzdelem részeként – egyre gyakrabban kell személyes adatokat feldolgozniuk és továbbítaniuk. Ebben az összefüggésben az érintett hatóságok közötti együttműködés javításához elengedhetetlenül fontos, hogy az adatvédelemre uniós szinten világos és koherens szabályozás vonatkozzon.

Az Irányelv hatálya a kerethatározathoz képest szélesebb, ugyanis a bűnüldözési, bűnmegelőzési célú (beleértve a terrorizmus, a szervezett bűnözés és a számítástechnikai bűnözés elleni küzdelmet is) adatkezelés mellett a közbiztonságot fenyegető cselekmények elleni védelemre és azok megelőzésére, a büntetés-végrehajtás során keletkezett adatokra, valamint a nem állami, de bűnüldözési célból adatokat kezelő gazdasági társaságokra, szervezetekre (pl. magánüzemeltetésű börtönök) is kiterjed.

Az Irányelv a GDPR-hoz hasonlóan új jogintézményekkel bővíti az adatvédelem keretrendszerét, amelyeket a bűnüldözési célból adatkezelést folytató szervezeteknek is alkalmazniuk kell. A GDPR-hoz hasonlóan megjelenik a beépített adatvédelem és alapértelmezett adatvédelem elve – melyet a bűnüldöző hatóságoknak és szerveknek a személyes adatokkal kapcsolatos valamennyi eljárás kezdetén (például: új adatbázisok kialakításakor) alkalmazniuk kell. Az adatvédelmi hatásvizsgálat elvégzéséből és az adatvédelmi hatósággal folytatott előzetes konzultációból eredő, valamint az adatkezelési tevékenység nyilvántartására és azok naplózására vonatkozó részletes és széles körű kötelezettségek szintén rendkívül fontosak. Ezen túlmenően, az adatkezelésért felelős személyek elszámoltathatóak lesznek munkájukért, a hatóságoknak pedig adatvédelmi tisztviselőt kell kinevezniük, aki a szervezeten belül felelős a személyes adatok

védelméért, valamint adatvédelmi incidens esetén előírja a nemzeti felügyeleti hatóság mielőbbi értesítését.

Az Irányelv rendelkezései összességében tehát az adatvédelmi hatóságokkal való szorosabb együttműködésre és az általuk javasolt szempontrendszer még szélesebb körű érvényre juttatására kötelezik az adatkezelőket. Figyelemmel arra, hogy a külföldre történő adattovábbítások száma várhatóan nő majd, és előzetes jóváhagyásukra, ellenőrzésükre vonatkozóan az irányelv új feltételrendszert állít fel, az adatvédelmi hatóságok előzetes kontrollja az eddiginél nagyobb szerepet kaphat.

A NAIH-hoz a 2017-es év során számos bűnüldözési célú adatkezeléssel kapcsolatos beadvány és panasz érkezett. A panaszok legtöbb esetben a különböző nyomozóhatóságok (rendőrség, NAV, ügyészség), közterületi kamerás megfigyelést végző szervek (rendőrség, közterület felügyelet) és büntetés-végrehajtási intézmények adatkezelésével kapcsolatosak voltak.

Az Irányelv jövőbeli alkalmazása szempontjából kiemelendő egyik 2017-es vizsgálati ügyet a bűnügyi adatvédelmi irányelvről szóló fejezet végén, a 47. oldalon, már ismertettük.

V.4. Kamerás adatkezelések

Amint a statisztikai adatokról szóló pont bemutatta, a Hatósághoz a tavalyi év során is több konzultációs- és panaszbeadvány érkezett közterületi térfigyelő kamerarendszerek és vagyonvédelmi biztonsági kamerák kiépítésével és üzemeltetésével kapcsolatosan. Emellett továbbra is nagy számban érkeznek olyan panaszbeadványok, melyben a bejelentők társasházakban elhelyezett kamerákkal, kamerarendszerekkel kapcsolatosan fordulnak a Hatósághoz.

V.4.1 Társasházakban elhelyezett kamerák, kamerarendszerek

a) A panaszok egyik nagy csoportjába tartoznak azok az esetek, amikor a társasházak által elhelyezett és üzemeltetett kamerarendszerekkel kapcsolatosan merül fel – elsősorban illetéktelen hozzáférés, vagy jogtalanul megfigyelt terület miatt – a jogellenesség.

A társasházakról szóló 2003. évi CXXXIII. törvény (a továbbiakban: Thtv.) tartalmazza a társasházi kamerarendszer létesítésére és üzemeltetésére vonatkozó

szabályokat.[8] Fontos szabály, hogy a közös tulajdonban álló épületrészek, helyiségek és területek megfigyelését szolgáló, zárt rendszerű műszaki megoldással kiépített elektronikus megfigyelőrendszer létesítéséről és üzemeltetéséről a közgyűlés az összes tulajdoni hányad szerinti legalább kétharmados többségével rendelkező tulajdonostársak igenlő szavazatával dönthet. A közgyűlésen tehát az összes tulajdoni hányad szerinti kétharmaddal rendelkező tulajdonostárs igenlő szavazatára van szükség a kamerarendszer létesítéséhez és üzembe helyezéséhez előírt érvényes döntéshez, nem pedig a közgyűlésen jelen lévő tulajdonostársak többségének, vagy kétharmadának szavazatára.

A kamerarendszer nem irányulhat a külön tulajdonban álló lakás vagy nem lakás céljára szolgáló helyiség bejáratára vagy más nyílászárójára akkor sem, ha az a közös tulajdonban álló épületen, épületrészen vagy területen van elhelyezve, továbbá nem helyezhető el kamera a közös tulajdonban és a tulajdonostársak közös használatában álló olyan helyiségben sem, amelyben a megfigyelés – a helyiség rendeltetéséből fakadóan – az emberi méltóságot sértheti.

b) Háztartási adatkezelés társasházakban

A panaszok másik nagyobb csoportja esetében a bejelentők azt nehezményezik, hogy a társasház egy vagy több lakója szerel fel és üzemeltet a közös tulajdonban álló területeken kamerákat. Fontos kiemelni, hogy a fentiektől eltérő megítélés alá esik ez az adatkezelés, ugyanis – ebben az esetben – a fő szabály az, hogy egy lakó nem helyezhet el olyan módon kamerát, hogy azzal a társasház közös tulajdonban álló épületrészét, helyiségét és területét tartsa megfigyelés alatt. Amennyiben tehát a kamera nem helyezhető el olyan módon, hogy annak látószöge csak és kizárólag az azt felszerelő lakó vagy lakók tulajdonára irányul, úgy azt jogszerűen felszerelni és működtetni nem lehet.

Az adatkezelés jogalapját ebben az esetben nem a Thtv. rendelkezései jelentik. Az Infotv. 2. § (4) bekezdése szabályoz egy kivételt, mely szerint nem kell alkalmazni a rendelkezéseit abban az esetben, ha az adatkezelés természetes személynek kizárólag saját személyes céljait szolgálja. A rendelkezéssel tehát a jogalkotó megteremtette annak a lehetőségét, hogy bizonyos esetekben képfelvétel készítésre nem kell alkalmazni az Infotv. szabályait. Ilyen esetnek minősül például, ha egy természetes személy, saját ingatlanán vagyonvédelmi célból kamerákat helyez el.

8 Thtv. 25. §-a

Ebben az esetben sem lehet azonban eltekinteni attól, hogy a kamera által megfigyelt területre belépni szándékozó személyek figyelmét felhívja a kamera üzemeltetője a kamerás megfigyelés tényére, például oly módon, hogy az ingatlan bejáratánál szöveges felhívás vagy piktogram segítségével jelezze a kamerás megfigyelést. A Hatóság álláspontja szerint a fenti kivételt azonban szűken kell értelmezni, mert el kell kerülni azt, hogy pusztán valamely természetes személy egyoldalú kijelentése vagy önhatalmú döntése alapján valamely adatkezelés e kivétel alá tartozzon. Ennek megfelelően az Infotv. fenti rendelkezése – az Európai Unió Bíróságának ítéletével[9] összhangban – akkor jelenthet csak kivételt az Infotv. rendelkezései alól, ha a természetes személy adatkezelése, annak teljes időszakában a *„saját személyes cél”* fordulat alá tartozik.

Amennyiben tehát a kamerák látószöge a kamerás megfigyelőrendszerrel adatkezelést végző személy magánszféráján kívülre – például közterületre, a társasház közös tulajdonban álló területére, vagy más, harmadik személy tulajdonában álló területre – irányul, úgy nem tekinthető a fenti kivétel alá tartozó *„személyes, illetve otthoni”* tevékenységnek.

V.4.2 További, gyakran előforduló panaszok kamerákkal összefüggésben

V.4.2.1 Munkahelyen elhelyezett kamerás megfigyelőrendszer

A Hatósághoz sok beadvány érkezik olyan témában is, mikor az adatkezelő, mint munkáltató helyez el kamerát egy munkahely területén, mely a dolgozókat tartja megfigyelés alatt. A Hatóság – évek óta fennálló, következetes – álláspontja, hogy kamerákat a munkavállalók és az általuk végzett tevékenység elsődleges, kifejezett megfigyelése céljából működtetni nem lehet. Jogellenesnek tekinthető az olyan elektronikus megfigyelőrendszer alkalmazása, amelynek – akár nem deklarált – célja a munkavállalók munkahelyi viselkedésének a befolyásolása.

A tájékoztatási kötelezettséggel kapcsolatban szükséges kiemelni, hogy a munkáltatónak minden egyes kamera vonatkozásában pontosan meg kell jelölnie, hogy az adott kamerát milyen célból helyezte el az adott területen és milyen területre, berendezésre irányul a kamera látószöge. A munkáltató ezzel igazolni tudja a munkavállalók számára azt, hogy miért tekinthető szükségesnek az adott terület megfigyelése. Nem fogadható el az a gyakorlat, amikor a munkáltató általánosságban tájékoztatja a munkavállalókat arról, hogy elektronikus meg-

9 http://curia.europa.eu/juris/celex.jsf?celex=62013CJ0212&lang1=hu&type=TXT&ancre

figyelőrendszert alkalmaz a munkahely területén. Tilos továbbá a rejtett kamera használata.

A Hatóság egy ügyben megállapította, hogy az adatkezelő nem nyújtott megfelelő előzetes tájékoztatást az adatkezelésről és annak körülményeiről sem az általa foglalkoztatott munkavállalók, sem az adatkezelő által üzemeltetett áruházakban megforduló harmadik személyek részére, továbbá a vizsgált áruházban a célhoz kötött adatkezelés elvének megsértésével üzemeltetett kamerákat. Az ügyben a vagyonvédelmi kamerák működtetésével kapcsolatosan a Hatóság megállapította, hogy az adatkezelés céljára tekintettel az adatkezelő nem egyértelműen jelölte meg adatkezelésének jogalapját, így annak pontosítása szükséges.

A Hatóság az ügyben a munkavállalók ellenőrzéséhez kapcsolódó adatkezelés tekintetében kitért arra a körülményre is, hogy a kamerás megfigyelésnek abszolút korlátját jelenti az emberi méltóság tiszteletben tartása. Ezen alapelvből adódóan kamerákat a munkavállalók és az általuk végzett tevékenység állandó jellegű, kifejezett cél nélküli megfigyelésére működtetni nem lehet. A fentiek miatt jogellenesnek tekinthető az olyan elektronikus megfigyelőrendszer alkalmazása is, amelynek célja a munkavállalók munkahelyi viselkedésének a befolyásolása. A Hatóság eljárása során megállapította, hogy az adatkezelő megsértette az Infotv. 4. § (1)-(2) bekezdése szerinti célhoz kötött adatkezelés és szükségesség elvét. A Hatóság megállapította azt is, hogy az adatkezelő a vizsgált időszakban az adatkezelés jogalapját nem megfelelően határozta meg, amikor az Mt. 11. § (1) bekezdését, a személy- és vagyonvédelmi, valamint a magánnyomozói tevékenység szabályairól szóló 2005. évi CXXXIII. törvény (a továbbiakban: Szvtv.) szabályait, valamint a munkavállalók által aláírt nyilatkozatokat jelölte meg, vagyis a vizsgált adatkezelés megfelelő jogalap nélkül történt. A Hatóság bírságot szabott ki, valamint határozatában elrendelte, hogy az adatkezelő a megjelölt kamerák esetében a jogellenes adatkezelést vagy a kamerák leszerelésével, vagy azok áthelyezésével, illetve látószögük módosításával szüntesse meg. [*Ügyszám: NAIH/2017/984/H*]

V.4.2.2 Üzletekben elhelyezett kamerák

Mind a fenti ügyben, mind pedig a Hatósághoz beérkező panaszokban visszatérő probléma, hogy adatkezelők az általuk üzemeltetett üzletek területén nem megfelelően végeznek kamerás megfigyelést.

Az ilyen adatkezelésekre irányadó szabályokat az Szvtv. tartalmazza. Fontos kiemelni azonban, hogy a törvényben foglalt rendelkezések az Infotv. rendelkezéseivel összhangban alkalmazandók. Az Szvtv. alapján végzett adatkezelés

akkor tekinthető tehát jogszerűnek, ha az adatkezelő az adatkezeléssel kapcsolatban mindenkor betartja az Infotv. alapvető rendelkezéseit: a célhoz kötött és a tisztességes adatkezelés elvét.

Az elektronikus megfigyelőrendszerek alkalmazhatóságának szintén fontos korlátja, hogy semmiképp sem lehet kamerát elhelyezni olyan helyiségben, területen, ahol a megfigyelés az emberi méltóságot sértheti.[10] Az Alkotmánybíróság az Szvtv. alkotmányossági kontrollja során is hangsúlyozta az emberi méltóság tiszteletben tartásának fontosságát.[11] A tulajdont érintő jogsértések kiküszöbölésére, kriminális magatartások megelőzésére számos más olyan eszköz áll rendelkezésre, amely az emberi méltóságot nem sérti, ugyanakkor a tulajdon technikai értelemben vett védelmét hatékonyan megoldja. A fentiekre tekintettel a Hatóság álláspontja szerint nem üzemeltethető kamera olyan helyen, ahol fennáll annak a lehetősége, hogy az érintettekről az emberi méltóságukat sértő módon, intim helyzetben rögzítenek képfelvételeket.

A Hatóságot egy bejelentésben arról értesítették, hogy egy áruház területén rejtett kamerarendszert helyeztek el. A rejtett kamerák olyan berendezések voltak, melyek füstérzékelő-készüléknek tűntek, azonban azokban egy-egy – felvételek rögzítésére is alkalmas – kamera üzemelt. A Hatóság megállapította, hogy ezek az eszközök egyértelműen olyan *„álcázott”* kamerának számítanak, melyek első látásra, illetve az érintettek többsége számára nem tűnnek megfigyelő berendezésnek. Az adatkezelő a rejtett kamerák felszerelését elismerte, mindemellett előadta, hogy az eszközök, bár csatlakoztatva voltak a kamerarendszerre, ám gyenge minőségük miatt az azokkal készített felvételeket nem használták fel, illetve a Hatóság eljárásának megindítása után le is szerelték őket. A Hatóság a fentiek miatt felszólította az adatkezelőt, hogy távolítsa el a rejtett kamerákat. [*NAIH/2017/5072/V*]

V.5. Adatvédelmi aggályok a követeléskezeléssel összefüggésben

V.5.1. Környezettanulmány és ingatlanról készített fotók tilalma

A Hatóság az egyes ügyekben felhívta a figyelmet, hogy a követelés érvényesítéséhez szükségtelen környezettanulmány készítése az adós fizetőképességének felmérésére. A Hatóság több ügyben is felszólítást intézett adatkezelőkhöz,

10 Szvtv. 30. § (3) bekezdés
11 36/2005. (X. 5.) AB határozat III. 2. pont

amelyben kötelezte őket, hogy a sérelmezett adatkezelést szüntessék meg, és a zálogtárgyat képező ingatlanról jogalap nélkül készített fotókat töröljék.

V.5.2. Hitelképesség vizsgálatának szükségtelensége

A követeléskezeléssel foglalkozó pénzintézeteknek nem jogszabályi kötelezettsége az adósok hitelképességének, illetve a hitelezhetőségének vizsgálata, a természetes személy vagy a természetes személy háztartása jövedelmi helyzetének felmérése. Ebből kifolyólag a vagyoni és jövedelmi helyzetre vonatkozó adatok kezelésének jogalapja csak az érintett hozzájárulása lehet. Mivel az érintett vagyoni és jövedelmi helyzetére vonatkozó adatok kezelését törvény nem írja elő a követeléskezelő cégek részére, valamint azok kezelése nem szükséges a behajtási célhoz, így ezen adatok kezelése jogellenesnek tekinthető.

V.5.3. Előzetes tájékoztatás hiánya

Több ügyben kellett a Hatóságnak állást foglalnia állomány-átruházáshoz köthető jogügyletek adatvédelmi összefüggéseiről, amelyek számos hasonlóságot mutatnak a követelésvásárlással, ugyanakkor annyiban más a helyzet, hogy élő szerződések átruházásáról van szó és nem hátralékos követelésről, ezért ezekben az esetekben a késedelembe esett és szerződésszerűen teljesített követelésekre eltérő megközelítés szükséges.

Az érintettet az adatkezelés minden fázisában megilleti az a jog, hogy az adatai kezeléséről tájékoztatást kérjen, így az előzetes tájékoztatásnak teljes körűnek, átláthatónak kell lennie valamennyi, az alapjogviszonnyal összefüggő tervezett adatkezelési művelettel összefüggésben. Így a követelés átruházása során is előre látnia kell az érintettnek, hogy a jogosult kinek fogja átadni a követelést, milyen feltételekkel, milyen díjszabás alapján.

A Hatóság több ízben is felhívta a beadványozók figyelmét arra, hogy az adatkezelővel szemben élhet a tájékoztatáshoz való jogával és célszerű információt kérni a követelés elemeiről (díj, költség, stb.) és azok jogalapjáról is.

V.5.4. Harmadik személyek – szomszédolási gyakorlat tilalma

A Hatóság ebben az évben is súlyos adatvédelmi visszaélésként értékelte harmadik személyek bevonását, az úgynevezett „*szomszédolási*” gyakorlatot az egyes ügyek kapcsán. Elfogadhatatlan, ha kívülálló, a követeléskezelés alapjául

szolgáló jogviszonyhoz semmilyen formában nem kapcsolódó harmadik személyek, jellemzően szomszédok adatait kezelik, sőt adatbázisokba, nyilvántartásokba rendszerezik. A tapasztalatok szerint ez a gyakorlat visszaszorult.

V.5.5. Adattörlés megtagadása

A Hatóság általános tapasztalata a követeléskezeléssel foglalkozó cégek gyakorlatában, hogy az érintett személyes adataira vonatkozó törlési kérelmeknek az adatkezelők nem mindig tesznek eleget, például a telefonszámot kérés ellenére nem törlik, jogos érdekre hivatkozással tovább kívánják használni. (Erről részletesebben e fejezet V.15. pontja szól.)

V.6. Előzetes tájékoztatás követelménye

A Hatóság tapasztalatai alapján az idei évben is jellemző volt az, hogy az adatkezelők nem fordítottak kellő figyelmet az előzetes tájékoztatás követelményére.

Az adatkezelőknek olyan előzetes tájékoztatást kell nyújtaniuk az érintettek számára, amelyen keresztül az adatalanyok felismerhetik azt, hogy az adatkezelés milyen hatással járhat a magánszférájukra. Bár az adatkezelők sok esetben elkészítik adatkezelési tájékoztatóikat, azonban ezek gyakran nem felelnek meg az Infotv.-ben meghatározott követelményeknek.

Ahogy a Hatóság honlapján közzétett[12] az előzetes tájékoztatás adatvédelmi követelményeiről szóló ajánlásában is kifejtette, nem elfogadható az a gyakorlat, ha az adatkezelő pusztán szó szerint megismétli a jogszabályok szövegét, mivel az adatkezelési tájékoztató lényege, hogy az adatkezelő milyen módon tartja meg a jogszabályban foglalt követelményeket, valamint, hogy milyen gyakorlatot alakít ki ezekre vonatkozóan. A jogszabályi rendelkezések szó szerinti átvétele egyes érintettek számára nehezen érthető, ezek a rendelkezések az adatkezelési tájékoztató szövegét számos esetben bonyolulttá és nehézkessé teszik.

A Hatóság a NAIH/2017/4318/V számú ügyében megállapította, hogy bár az adatkezelő rendelkezett adatkezelési szabályzattal, és az az érintettek számára is elérhető volt, nehézkes jogi nyelvezeten alapult, emellett sokszor az Infotv. rendelkezéseit ismételte.

12 www.naih.hu/files/tajekoztato-ajanlas-v-2015-10-09.pdf

Gyakran előforduló probléma az adatkezelési tájékoztatók esetében, hogy azok hiányosak, például nem tüntetik fel benne az adatkezelő személyére és elérhetőségére vonatkozó tájékoztatást, sokszor nem derül ki egyértelműen, hogy az adatkezelés milyen célból történik, vagy e célokat elnagyoltan, nem közérthetően fogalmazzák meg. Az érintett hozzájárulása csupán abban az esetben tekinthető az adatkezelés jogszerű jogalapjának, ha az kellően részletes és egyértelmű előzetes tájékoztatáson alapul.

V.7. Hatósági igazolványok fénymásolatának, szkennelt változatának kezelésével kapcsolatos ügyek

A Hatósághoz 2017-ben is több olyan bejelentés érkezett, melyekben leírták, hogy valamely adatkezelő – több esetben biztosítótársaság vagy biztosításközvetítést végző társaság, online kereskedelmi teret működtető szolgáltató, ügyvédi tevékenysége körében eljáró ügyvéd – a bejelentőt személyazonosító igazolványa, lakcímet igazoló hatósági igazolványa, egyes esetekben akár adókártyája, társadalombiztosítási igazolványa, bankkártyája (a továbbiakban együttesen: okmányok) fénymásolatának, szkennelt változatának benyújtására szólította fel, az adott szolgáltatás teljesítéséhez kapcsolódó indokokra hivatkozással.

Az okmányok adattartalmának, fénymásolatának, szkennelt változatának jogszerű kezeléséhez szükséges egyik alapvető feltétel, hogy az adatkezelő megfelelő jogalappal rendelkezzen az adatkezeléshez. Az adatkezelés jogalapja lehet például valamely törvény adatkezelésre vonatkozó kötelezést előíró, illetőleg felhatalmazást biztosító rendelkezése, az érintett hozzájáruló nyilatkozata (feltéve természetesen, hogy az érvényes hozzájárulás feltételei[13] maradéktalanul teljesülnek)[14], valamint az, ha az adatkezelés az adatkezelő, vagy az adatokat átvevő harmadik fél, vagy felek jogszerű érdekének érvényesítéséhez szükséges, feltéve, hogy a jogos érdek arányosan korlátozza az érintettek személyes adatok védelméhez való jogát, magánszféráját[15].

Az érvényes adatkezelési jogalap megléte esetén is csak abban az esetben jogszerű azonban az adatkezelés, ha megfelel a célhoz kötöttség elvének[16], te-

13 Infotv. 3. § 7. pont.
14 Infotv. 5. § (1) bekezdés.
15 Az Európai Parlament és a Tanács 95/46/EK irányelve a személyes adatok feldolgozása vonatkozásában az egyének védelméről és az ilyen adatok szabad áramlásáról (Adatvédelmi Irányelv) 7. cikk f) pont.
16 Infotv. 4. § (1) bekezdés.

hát az adott okmánymásolat, szkennelt változat adattartalmának kezelése jog gyakorlása, kötelezettség teljesítése érdekében szükséges, ilyen cél hiányában az okmánymásolat adattartalmának kezelése ugyanis készletezőnek minősül. További lényeges követelmény a szükségesség elvének[17] való megfelelés, melynek értelmében csak az adott adatkezelési célhoz elengedhetetlenül szükséges személyes adatok köre kezelhető, és csak az elengedhetetlenül szükséges ideig. Így például a regisztrációs adatok egyeztetése körében indokolatlan és jogsértő az érintett fényképnek, aláírásnak, illetve az ezeket tartalmazó okmánymásolatok, szkennelt változatok kezelése, amennyiben ezen adatok magához a regisztrációhoz sem voltak szükségesek.

Az okmánymásolatok, okmányfénymásolatok kezelése körében lényeges, hogy a 2017. június 26. napjáig hatályos, a pénzmosás és a terrorizmus finanszírozása megelőzéséről és megakadályozásáról szóló 2007. évi CXXXVI. törvény (a továbbiakban: régi Pmt.) főszabály szerint még nem tette lehetővé a hatálya alá tartozó szolgáltatók[18] részére, hogy az ügyfél-átvilágítás keretében kezeljék ügyfeleik személyazonosság igazolására alkalmas hatósági igazolványának, valamint lakcímet igazoló hatósági igazolványának másolatát, csak ezen okmányoknak a régi Pmt-ben meghatározott egyes adatait (például: családi és utónevét (születési nevét), lakcímét, állampolgárságát)[19]. Ebből következően az ügyfél-azonosítás céljából bemutatott okmányok egészének fénymásolására, szkennelésére irányuló általános adatkezelői gyakorlat jogellenes volt. Ezen általános szabály alól kivételt jelentettek a fokozott ügyfél-átvilágítás körébe tartozó esetek[20], amikor az ügyfél a szolgáltatóval történő szerződéskötéskor nem jelent meg személyesen azonosítás és a személyazonosság igazolása céljából, erre napjainkban leggyakrabban az online szerződéskötések alkalmával kerül sor. A fokozott ügyfél-átvilágítási kötelezettség körében ugyanis a személyazonosság igazoló ellenőrzése érdekében az ügyfél köteles volt a szolgáltató részére benyújtani a régi Pmt. vonatkozó rendelkezései által meghatározott okirat hiteles másolatát[21]: e célból az ügyfél személyazonosság igazolására alkalmas hatósági igazolványának és lakcímkártyájának hiteles másolata volt elfogadható, egyszerű fénymásolat készítése ezen okmányokról tehát ebben az esetben sem volt alkalmas az azonosítási kötelezettség teljesítésére.

17 Infotv. 4. § (2) bekezdés.
18 Régi Pmt. 1. § (1) bekezdés.
19 Régi Pmt. 7. § (2) bekezdés.
20 Régi Pmt. 14. § (1) bekezdés.
21 Régi Pmt. 14. § (2) bekezdés.

Változást jelent az okmánymásolás jogi megítélésében a pénzmosás és a terrorizmus finanszírozása megelőzéséről és megakadályozásáról szóló 2017. évi LIII. törvény (a továbbiakban: új Pmt.), mely 2017. június 26. napjától váltotta fel a régi Pmt-t. Az új Pmt. a régi Pmt-vel lényegében azonos módon szabályozza a szolgáltató által kezelhető és kezelendő adatok körét[22], lényeges különbség azonban, hogy – az egyszerűsített ügyfél-átvilágítás ugyancsak kivételszabálynak tekinthető esetét ide nem értve – a szolgáltató az új Pmt. alapján már az ügyfél-átvilágítás általános, fokozott átvilágításnak nem minősülő esetében is köteles másolatot készíteni a személyazonosság igazoló ellenőrzése érdekében bemutatott okiratról[23]. Főszabály szerint változatlanul hiteles másolatot kell benyújtani abban az esetben, ha az ügyfél nem jelent meg személyesen az azonosítás és a személyazonosság igazolása céljából, mely kötelezettség teljesítése csak a szolgáltató belső szabályzatában rögzített, fokozott ügyfél-átvilágítási intézkedésekkel helyettesíthető[24]. A Hatóság álláspontja szerint ugyanakkor az új Pmt. „*okmánymásolást*" előíró rendelkezései sem adnak jogalapot a törvényben nem nevesített személyes adatok – az érintett fényképe, aláírása, valamint személyi azonosítója – kezelésére.

Egy, a Hatóság által az Infotv. 52. §-a alapján lefolytatott – még a régi Pmt. rendelkezései alapján megítélendő – vizsgálati eljárás alapját képező panaszban a bejelentő azt kifogásolta, hogy az általa az adatkezelő biztosítótársasággal kötött utazási garancia biztosítási szerződésre tekintettel benyújtott kárbejelentés során a biztosítótársaság munkatársai fénymásolatot készítettek a személyazonosító igazolványáról, lakcímet igazoló hatósági igazolványáról és bankkártyájáról.

A Hatóság álláspontja szerint a bejelentő bankkártyájának egyes személyes adatai kezelésére jogalapot nyújthatnak a biztosítási tevékenységről szóló törvény vonatkozó rendelkezései[25], de csak abban az adatkörben, amely a biztosítási szerződés alapján követelhető igények teljesítéséhez, illetve követelések megítéléséhez szükségesek. Sem e törvény rendelkezései, sem más jogszabály nem ad azonban jogalapot a bankkártyáról történő fénymásolat készítésére. Az adatkezelésre jogalapot biztosító törvényi felhatalmazás hiányában a törvényben nem nevesített személyes adatok kezelését sem a régi, sem az új Pmt. vagy más jogszabály rendelkezéseinek tükrében nem tekinti jogszerűnek a Hatóság, emellett a bejelentő által kifogásolt adatkezelés nemcsak a megfelelő

22 Új Pmt. 7. § (2)-(3) bekezdés.
23 Új Pmt. 7. § (8) bekezdés.
24 Új Pmt. 17. § (1)-(3) bekezdés.
25 A biztosítási tevékenységről szóló 2014. évi LXXXVIII. törvény 135. § (1) bekezdése.

jogalapot nélkülözte, hanem a célhoz kötöttség és a szükségesség (adatminimalizálás) Infotv.-ben rögzített elveibe is ütközött (készletező jellegű volt), ezért mind a régi Pmt., mind az új Pmt., illetve az Infotv. rendelkezéseinek tükrében jogellenes volt.

2017-ben több olyan beadvány is érkezett a Hatósághoz, melyben a bejelentő ügyvédi tevékenységet folytató személyek által végzett okmánymásolat-kezelési gyakorlatot kifogásolt.

Egy beadványozó a Hatóság tájékoztatását kérte azzal kapcsolatban, hogy jogszerűen készíthet-e fénymásolatot egy ingatlan tulajdonjogának átruházásánál közreműködő ügyvéd az ingatlan tulajdonosainak személyazonosító igazolványáról, lakcímet igazoló hatósági igazolványáról (a továbbiakban: lakcímkártya), valamint adóigazolványáról – a Magyar Ügyvédi Kamara (a továbbiakban: MÜK) 1/2017. (VII.10.) MÜK szabályzatára hivatkozással – továbbá kérhető-e ehhez hozzájáruló nyilatkozat a tulajdonosoktól.

Hivatkozással az új Pmt. vonatkozó rendelkezéseire[26], – melyek értelmében az ügyvédet az ügyfél átvilágítási és bejelentési kötelezettsége akkor terheli, ha ingatlan tulajdonjogának átruházásával kapcsolatos ügyvédi tevékenységet végez – a Hatóság megállapította, hogy az új Pmt. alapján az ügyvéd az ügyfél-átvilágítási intézkedések körében az ügyfél személyazonosságának ellenőrzése érdekében köteles megkövetelni a magyar állampolgár magánszemély ügyfél személyazonossága igazolására alkalmas hatósági igazolványának, továbbá lakcímkártyájának bemutatását, valamint ezen okiratokról köteles másolatot készíteni.

V.8. Egészségügy

1) Az egészségügyi adatkezelés terén 2017-ben a legfontosabb esemény az Elektronikus Egészségügyi Szolgáltatási Tér (EESZT) gyakorlati indulása volt. Az EESZT az egészségügyi szolgáltatók összekapcsolásával és a számukra létrehozott egységes kommunikációs tér biztosításával lehetővé teszi a szolgáltatók és ellátottak közötti hatékonyabb együttműködést, leegyszerűsödik az ellátás folyamán keletkezett adatok és dokumentumok elérhetősége, biztosítottá válik az egészségügyi ágazat számára a rendelkezésre álló adatok egységes

26 Új Pmt. 73. § (1) bekezdés b) pont.

és hatékony elemzése[27], az érintettek önrendelkezési jogának egyidejű biztosításával.

Az EESZT-hez kapcsolódó adatkezelések sajátossága, hogy az elsődlegesen törvényi felhatalmazás alapján végzett adatkezelésnek tekinthető (Infotv. 5. § (2) c) pontja), amelyben az érintett döntése alapján érvényesülhet az érintett információs önrendelkezési joga. Az adatkezelés során az adatalany több, jelentős döntési jogkörrel rendelkezik, így például az ő belátásán múlik, ki milyen személyes és különleges adatait ismerheti meg, ezért e vonatkozásban alapvetően hozzájáruláson alapuló adatkezelésről beszélhetünk. Azonban ez utóbbi esetben is jogszabály tartalmazza az adatkezelés főbb körülményeit, így az adatkezelés jogalapja sajátosan kettős karakterű. Az alapbeállítás szerint egy kezelőorvos csak a szakterülete szerint rá tartozó adatokhoz férhet hozzá, de a beteg a portálon keresztül szűkítheti vagy bővítheti a hozzáférhető adatokat. Emellett a felhasználó értesítést kérhet az őt érintő dokumentum feltöltésekor, és azt is nyomon követheti, hogy az adataihoz ki és mikor fért hozzá[28].

Két beadványban is arról érdeklődtek egészségügyi dolgozók, hogy ők jogszerűen kötelezhetőek-e az új típusú személyazonosító igazolvány kiváltására az EESZT használatához kapcsolódóan.

Az elektronikus egészségügyi szolgáltatási térhez 2017. november 1-től informatikai rendszere útján csatlakozni köteles minden közfinanszírozott egészségügyi szolgáltató. Az EESZT-be történő bejelentkezés természetes személyeknek (háziorvosok, egészségügyi intézmények dolgozói, stb.) úgynevezett két faktoros azonosítást követően lehetséges. Ennek lényege, hogy a rendszerbe történő bejelentkezéshez szükséges név/jelszó megadása után következik egy második biztonsági elem használata, ami lehet birtoklás alapú, vagy biometrikus azonosító. A rendszer működtetője a Belügyminisztériummal történt megállapodása alapján az egységes egészségügyi informatikai rendszer biztonságos működését garantáló egységes azonosítást az e-személyazonosító igazolvány használatával tudja biztosítani.

Az EESZT szolgáltatásainak használata komoly biztonsági előírások mentén valósulhat meg, amit a rendszer legmagasabb szintű biztonsági fokozata előír minden felhasználó esetében. A belépéshez használható e-személyi igazolvány

27 https://e-egeszsegugy.gov.hu/fooldal

28 http://www.kormany.hu/hu/emberi-eroforrasok-miniszteriuma/egeszsegugyert-felelos-allamtitkarsag/hirek/megkezdodott-az-elektronikus-egeszsegugyi-szolgaltatasi-ter-probauzeme

mind a beteg azonosítására, mind a rendszert használó orvosok, egészségügyi dolgozók és gyógyszerészek számára biztonságos azonosítási lehetőséget biztosít.

Az EESZT használatához olyan azonosítási megoldás szükséges, amely már alkalmazott és a megfelelő biztonsági szintet is biztosítja, valamint sem a fejlesztésben, sem a felhasználók számára nem jelent költséget. Ez az azonosítási megoldás az e-személyi igazolvány, azaz a tároló elemet tartalmazó személyazonosító okmány.

Az új típusú igazolvány alkalmas arra, hogy az egyes alkalmazásokhoz különböző jogosultsági feltételek kapcsolódjanak[29]. Lényegét tekintve tehát azt jelenti, hogy az EESZT használata érdekében történő azonosítás nem jár együtt azzal, hogy az azonosítás érdekében szükséges elemeken kívül az igazolvány más elemeit – mint pl. az ujjlenyomat, vagy adóazonosító jel – arra jogosulatlan személy ismerje meg.

Tekintve, hogy az állandó személyazonosító igazolvány kiváltása illetékmentes, anyagi terhet nem ró a használókra, ugyanakkor a differenciált hozzáférési jogosultságok és az adatbiztonsági követelmények – különös tekintettel a nagyszámú különleges adat kezelésére – megkívánják a felhasználó kétséget kizáró azonosítását, és ennek mind jogszabályi, mind gyakorlati feltételei biztosítottak, ezért a Hatóság nem látja aggályosnak azt, hogy a rendszer használóit az igazolvány kiváltásra kötelezzék. [*NAIH/2017/4198/V, NAIH/2017/4895/V*]

A Hatóság és az Állami Egészségügyi Ellátó Központ (a továbbiakban: ÁEEK) közötti megállapodás szerint negyedéves rendszerességgel történnek egyeztetések, ahol az ÁEEK munkatársai bemutatják az aktuális fejlesztéseket, melyekről hatékony információcsere zajlik a felek között, továbbá megegyezés született arról is, hogy a gyakorlati megvalósítás során felmerült, és a Hatósághoz érkezett problémákat a Hatóság jelzi az ÁEEK adatvédelmi felelősének.

2) Egészségügyi dokumentáció másolásának – a hozzáféréshez való jog biztosításának ügyében még mindig érkeznek beadványok a Hatósághoz. Ugyanakkor ezekben az ügyekben rendszerint már nem az a kifogásolt gyakorlat, hogy a

29 A tároló elemmel rendelkező személyazonosító igazolványról a Belügyminisztérium Nyilvántartások Vezetéséért Felelős Helyettes Államtitkársága a kekkh.gov.hu honlapon közérthetően tájékoztatja az állampolgárokat http://www.kekkh.gov.hu/Eszemelyi/mit_tartalmaz_a_tarolo_elem

szolgáltató nem kívánja a dokumentációt az érintett rendelkezésére bocsátani, hanem a kiadás részleteinek kérdései a problémásak.

Míg egy érintett azt kifogásolta, hogy az intézmény a dokumentációt nem küldi meg elektronikusan, így neki személyesen kell elmennie érte, ez viszont nem helyben lakó betegként számára megterhelést jelent, addig más azzal kapcsolatban fejezte ki aggályát, hogy mennyiben biztonságos a különleges adatok elektronikus továbbítása, ha a kérelmező személyazonossága nem beazonosítható.

A Hatóság nem tiltja azt, hogy elektronikus úton juttassák el a kért egészségügyi dokumentáció másolatát a beteg részére, különös tekintettel arra az esetre, ha az adatigénylő számára nagy költséget vagy áldozatot jelentene az, hogy személyesen megjelenjen az intézmény épületében az egészségügyi dokumentáció másolatának átvétele céljából. Ennek feltétele azonban az adatbiztonságot megfelelően garantáló eljárásrend kidolgozása (például: úgy, hogy az elektronikus úton teljesített adatigénylés során ellenőrző kérdéseket intéznek az érintetthez), mely során az intézményeknek kell gondoskodnia az adatbiztonsági követelmények[30] érvényesüléséről. [*NAIH/2017/2169/V*]

A Hatóság egyébiránt szorgalmazza az elektronikus adatátadást, amennyiben az érintett tudja azt ily módon fogadni, személyes átvétel esetén az adathordozó egyszeri költsége elmarad a nagyobb terjedelmű irat másolási költségétől, másrészt környezetvédelmi szempontból sem elhanyagolható a nagyobb mennyiségű nyomtatott változat helyett elektronikus formában az érintett rendelkezésére bocsátani az egyébként elektronikus formában meglévő iratokat.

Lezárult az a régebb óta húzódó ügy, amelyben az érintett személy halálának körülményeire vonatkozó, az intézmény munkatársai által készített szakértői vélemények megismerését kívánták az örökösök, az egészségügyi szolgáltató azonban a polgári perben való védekezési jogosultságára hivatkozva tagadta meg azok kiadását.

Noha az Infotv. hatálya élő személyekre terjed ki, ugyanakkor az Infotv. szempontjai és elvei az érintett halála után a kegyeleti jogban is érvényesülnek, az örökösök által gyakorolható módon. Elhunytak esetében a haláleseménnyel összefüggésben keletkezett iratok megismerése a Hatóság álláspontja szerint az érintett önrendelkezési jogának kvázi kiterjesztése, az Eütv. 13. §-ában foglalt

30 Infotv. 7. §-a

tájékoztatáshoz való jog része, melyet a körülmények miatt az érintett már nem, hanem az örökösök érvényesíthetnek. Ennek módja a betekintési jog gyakorlása[31] illetve a tájékoztatás megadása. A vizsgálat megállapította, hogy a szakvéleményekben szerepeltek olyan, az intézmény dolgozói által tett személyes megjegyzések, amelyek nem minősülnek az érintett személyes adatának, így a Hatóság ezen megjegyzések kitakarásával rendelte el a szakvélemények másolatainak kiadását, melynek az adatkezelő eleget tett. [*NAIH/2016/456/V*]

Egy esetben a Hatóság egészségügyi dokumentáció kiadása megtagadásának tárgyában is folytatott hatósági eljárást. A panaszos a kötelezett által korábban végzett műtétek dokumentációját kérte, mert a műtétek óta az állapota nem kielégítő, és egészségi problémáinak végleges megoldása érdekében meg kívánta ismerni a beavatkozások teljes anyagát. A kötelezett a panaszos megkereséseire nem reagált. A Hatóság megállapította a jogsértést, és a határozathozatalkor úgy találta, hogy a kis– és középvállalkozásokról, fejlődésük támogatásáról szóló 2004. évi XXXIV. törvény (Kkv. tv.) értelmében nem figyelmeztetést kell, hogy alkalmazzon szankcióként, mert a Kkv. tv. 12/A. § (2) bekezdés a) pontjában foglaltaknak megfelelően – „*nincs lehetőség a bírságtól való eltekintésre, ha a jogsértés emberi életet, testi épséget, vagy egészséget sért vagy veszélyeztet*" – bírság kiszabásának van helye. A Hatóság szerint – bár orvosszakmai kérdésben nem jogosult állást foglalni – a korábbi kezelés dokumentációjában foglaltak ismerete alapja lehet és kihatással lehet a további kezelések megválasztására, szükséges a jelen egészségi állapothoz vezető okok feltárásában. Mivel a dokumentációval a kötelezett rendelkezik, az más forrásból nem elérhető, így az egészséget veszélyeztető magatartás megállapítható.

A bíróság a jogsértés tekintetében helyben hagyta a Hatóság döntését, azonban a szankciót nem találta megfelelőnek, mert indokolása szerint a Hatóság nem folytatott le bizonyítást arra vonatkozóan, hogy a jogsértés valóban veszélyezteti-e a panaszos egészségét. Így e tekintetben a Hatóság új eljárást fog folytatni. [*NAIH/2017/472/H*]

Egy háziorvos beadványában előadta, hogy hallásszűréssel foglalkozó cég egyegy körzet betegeinek szűrésre invitáló névre szóló nyomtatványt küld. A vizs-

31 Eütv. 24. § (11) bekezdése: A beteg halála esetén törvényes képviselője, közeli hozzátartozója, valamint örököse – írásos kérelme alapján – jogosult a halál okával összefüggő vagy összefüggésbe hozható, továbbá a halál bekövetkezését megelőző gyógykezeléssel kapcsolatos egészségügyi adatokat megismerni, az egészségügyi dokumentációba betekinteni, valamint azokról kivonatot, másolatot készíteni vagy saját költségére másolatot kapni.

gálat során megállapítottuk, hogy a háziorvosok nem adták át a körzetükhöz tartozó érintettek adatait, hanem a kft. az orvosok által kiállított és megcímzett levelek postázását végezte, ezután az érintettek maguk kereshetik fel a céget a meghívó birtokában.

A Hatóság álláspontja szerint a háziorvosok az általuk az alapszolgáltatás keretében ellátott betegeik adatai tekintetében nincsenek jogszabály által felhatalmazva arra, hogy az adatokat egy profit-orientált gazdasági vállalkozás tevékenységének népszerűsítésére használják fel. Ez az adatkezelési tevékenység az ellátás érdekében történő célú adatkezeléstől eltérő – direkt marketing – célú adatkezelést valósít meg, amelyhez követelmény az érintettek előzetes hozzájárulása[32].

Ezen adatkezelési jogalap hiányán felül az érintettek által kézhez vett levél nem adott semmilyen tájékoztatást arról, hogy az orvos a betege adatát nem adta át harmadik személynek – a kft-nek –, az érintettek nincsenek tisztában az adatkezelés folyamatával és céljával. A beadványban foglaltak szerint is félrevezető az, hogy a betegek a saját háziorvosuk nevében és aláírásával kapnak egy szűrésre behívó levelet, miközben az érintettek számára nem egyértelmű, a cég honnan tudja, hogy a címzett személy hallássérült. Továbbá a levél megfogalmazása félrevezető, mert nem lehetőségként, hanem kötelező vizsgálatként értelmezhető, mivel az orvos a részvételre felhív. A levél a betegek számára félreérthető, azt hiszik, kötelező szűrőprogramról van szó, amin nekik kötelező megjelenni, mindezt a háziorvos pecsétje hitelesíti. Ezek a körülmények a tisztességes adatkezelés követelményét is sértik.

A Hatóság álláspontja szerint a hallásszűrés népszerűsítését a névre szólóan kiküldött meghívó helyett úgy is el lehet végezni, hogy a háziorvos a rendelésén megjelent beteg részére a rendelés során átadja a szűrést bemutató általános tájékoztatót, illetve a váróteremben elhelyezett tájékoztató plakát is informálhatja az érintetti kört a vizsgálat lehetőségéről. A Hatóság felszólította a céget a kifogásolt gyakorlat megszüntetésére, amely felszólításnak az adatkezelő eleget tett. [*NAIH/2016/3246/V*]

4) Az egészségügyet érintő konzultációs beadványok változatos képet mutattak. Volt online időpontfoglalással kapcsolatos kérdés, törzskarton átadásáról szóló felvetés, illetve egészségügyi szolgáltató területén történő kamerázás módja,

32 Eüak. 4. § (3) bekezdése.

ami az egészségügyi intézményekben szükségképpen előforduló különleges adatok miatt eltér az általános kamerázási gyakorlattól.

Az egészségügyi ellátások esetében csak kivételesen lehetséges a kamerás megfigyelés alkalmazása. Így például az ápolási ellátás esetén a célhoz kötött adatkezelés elve akkor teljesül, ha a beteg olyan súlyos betegségben szenved, amely miatt elengedhetetlen az állapotának folyamatos megfigyelése, azonban ennek megállapítása orvos-szakmai kérdés.

Kamerás megfigyelésre továbbá akkor kerülhet sor, ha az egészségügyi dolgozók az Eütv-ből fakadó kötelezettségeiket más, az érintettek magánszféráját kevésbé korlátozó módszerrel nem tudnák teljesíteni. A kamerák alkalmazását továbbá a legszükségesebb mértékre kell korlátozni. Ebből következik, hogy kizárólag a kamerák által közvetített élőképek megtekintésére van lehetőség, a felvételek rögzítése és tárolása már nem elfogadható. [*NAIH/2017/2440/V*]

Megkeresés érkezett azzal kapcsolatban, hogy háziorvosok ellenőrzése érdekében az ellátottakra vonatkozó nem anonim adatszolgáltatást kért a területi szakigazgatási szerv.

A háziorvos hatósági ellenőrzését végző szerv által igényelt adatkör megítéléséhez vizsgálandó, hogy az ellenőrzés céljának eléréséhez feltétlen szükséges-e a személyazonosító adatok kezelése, vagy a vizsgálat célja elérhető-e a dokumentációk anonim módon történő továbbításával, amellyel az orvos által alkalmazott szakmai eljárások ellenőrizhetőek, ugyanakkor a beteg személye nem azonosítható. Az ellenőrzést végző szervnek kell alátámasztania, hogy az ellenőrzés céljához a betegek azonosítása miért szükséges. [*NAIH/2017/2876/V*]

Egy másik konzultációs megkeresésben pszichiátriai klinika vezetője kérte a Hatóság állásfoglalását azzal kapcsolatban, hogy a beteg mely adatai és hogyan továbbíthatóak a gyámhivatal felé – hatósági megkeresés nélkül, illetve a beteg beleegyezése nélkül erre vonatkozó kifejezett törvényi felhatalmazás hiányában –, ha a beteg mentális zavara alapján felmerül a cselekvőképességet korlátozó gondnokság alá helyezési eljárás megindításának szükségessége. A klinika megkeresésében arról tájékoztatta a Hatóságot, hogy gyakori eset, hogy a mentőszolgálat súlyos mentális hanyatlásban (mentális zavarban) szenvedő pácienst szállít be a pszichiátriai osztályra. Hozzátartozót, gondoskodó segítőt a szociális munkásnak sok esetben nem sikerül felkutatnia, a betegről nem érdeklődik senki, és otthonában egyedül él.

Az Eüak. és az Eütv. vonatkozó rendelkezései szerint az orvosi titoktartási kötelezettség alól alapvetően csak a beteg vagy a helyette nyilatkozni jogosult személy írásbeli felhatalmazása alapján mentesül az adatkezelő. Bizonyos esetekben a beteg beleegyezése nélkül is megszegehető a titoktartás, ha törvény rendeli el az adatkezelést, adattovábbítást, adatközlést, vagy sürgős szükség, vagy a beteg vagy mások veszélyeztető állapota miatt ez szükséges.

A Hatóság álláspontja szerint az Infotv. 6. § (2) bekezdésében foglalt létfontosságú érdek védelme, valamint az életet veszélyeztető állapot, betegség olyan elháríthatatlan oknak minősül, amely alapján a személyes adatok védelméhez fűződő jog érvényesítése nem lehet akadálya az emberi élet, a testi épség és az egészség védelmének, illetve az ezeket fenyegető veszély megelőzésének.

A fentiek alapján a megkeresésben hivatkozott Eütv. 189. § (2) bekezdése[33] nem ad megfelelő felhatalmazást az adattovábbításhoz. A Hatóság álláspontja szerint csak abban az esetben továbbíthatják a gyámhatóságnak a pszichiátriai beteg személyes és egészségügyi adatait, ha valóban nincs a pszichiátriai betegnek hozzátartozója, vagy megállapítható a létfontosságú érdek védelme, illetve az adattovábbítás célja a beteg testi épségének, egészségének védelme, továbbá a betegre fennálló közvetlen veszély más módon nem hárítható el, mint gondnoksággal. Ennek a kérdésnek az eldöntése olyan szakmai kérdés, ami túlmutat a Hatóság kompetenciáján.

A fentieken kívül figyelembe veendő a Polgári Törvénykönyvről szóló 2013. évi V. törvény kommentárja, mely a 2:28. §-a szerinti gondnokság alá helyezéssel kapcsolatban az alábbiakat ismerteti: *„Ha a gondnokság alá helyezés szükségességéről – akár hivatali eljárása során, akár bejelentésre – a gyámhatóság tudomást szerez, erről előbb tájékoztatja a perindításra jogosult közeli hozzátartozókat, és ha azok valamelyike az ezt követő hatvan napon belül nem indítja meg a keresetet, akkor a gyámhatóságnak kell a gondnokság alá helyezési eljárást megindítani."* Erre tekintettel a klinika jogosult bejelentést tenni a gyámhatóságnál, ha fent ismertetettek fényében a gondnokság alá helyezés szükségessége feltétlenül indokolt. [*NAIH/2016/5693/V*]

33 Eütv. 189. § (2) bekezdése: A pszichiátriai betegnek a 6-25. § szerinti jogai – egészségügyi ellátása során – csak az e törvényben foglaltak szerint, a feltétlenül szükséges mértékben és ideig, továbbá – a 193. §-ban foglalt kivétellel – abban az esetben korlátozhatók, ha a beteg veszélyeztető vagy közvetlen veszélyeztető magatartást tanúsít. Az emberi méltósághoz való jog azonban ebben az esetben sem korlátozható.

V.9. Gyermekek adatainak kezelése

V.9.1. Szülői felügyelettel kapcsolatos adatkezelés

A NAIH-hoz számos olyan beadvány érkezett, amelyekben a különélő vagy elvált szülő azt sérelmezi, hogy sem a házastárstól, volt házastárstól, sem különböző intézményektől nem kap tájékoztatást a kiskorú gyermekekkel kapcsolatos adatokról. Sok esetben azért nem, mert vitatott, hogy a szülői felügyeleti jogot közösen vagy kizárólagosan gyakorolják. Ha valamely intézmény tájékoztatást ad, akkor pedig a másik szülő kifogásolja az adatkezelés teljesítését.

Az alapvető probléma tehát a szülők gyermekre vonatkozó adatmegismerésének kérdése, valamint a szülőt megillető, a gyermek személyes és különleges adataival[34] kapcsolatos tájékoztatáshoz való joga.

A Hatóság egy vizsgálati eljárása során megállapította, hogy ha az intézménynél a gyermek adatairól érdeklődik a különélő szülő, akkor az intézmény köteles őt tájékoztatni.

„A jogszabályok gyakorlati alkalmazása során az egészségügyi szolgáltatók vélelmezik a közös felügyeleti jog fennállását, csak akkor tagadhatják meg a tájékoztatást, ha kétséget kizáróan megbizonyosodtak arról, hogy az érdeklődő szülő nem rendelkezik törvényes képviselői és/ vagy szülői felügyeleti joggal." [*NAIH/2017/48/V*]

A NAIH az oktatásért felelős államtitkárhoz fordult, figyelemmel arra, hogy az egyik vizsgálati ügyben egy pedagógiai szakszolgálat a gyermekétől különélő édesapát nem értesítette arról, hogy szakértői bizottsági vizsgálatra kerül sor, mindezt arra hivatkozással mellőzte, hogy elegendőnek[35] találta az édesanya által tett szülői nyilatkozatot, hogy jogosult a távollevő szülő képviseletére.

---

34 Az Infotv. 3. § 2. pontja értelmében: *"személyes adat: az érintettel kapcsolatba hozható adat – különösen az érintett neve, azonosító jele, valamint egy vagy több fizikai, fiziológia, mentális, gazdasági, kulturális vagy szociális azonosságára jellemző ismeret-, valamint az adatból levonható, az érintettre vonatkozó következtetés."*
Az Infotv. 3. § 3. pontja szerint: *„különleges adat:*
a faji eredetre, a nemzetiséghez tartozásra, a politikai véleményre vagy pártállásra, a vallásos vagy más világnézeti meggyőződésre, az érdek-képviseleti szervezeti tagságra, a szexuális életre vonatkozó személyes adat"

35 A pedagógiai szakszolgálati intézmények működéséről szóló 15/2013. (II.26.) EMMI rendelet 14. § (2) bekezdése szerint: *„A szakértői vizsgálat megkezdéséhez a szü-*

A Hatóság álláspontja szerint ez a szabályozás és gyakorlat a távollévő szülő jogainak ellehetetlenülésére ad lehetőséget. Aggályos, hogy a gyermek személyes adatainak kezeléséhez, illetve a szakértői vizsgálatához való hozzájárulást megadhatja-e úgy az egyik szülő, hogy olyan tartalmú nyilatkozatot tesz, hogy a másik szülő nevében ő nyilatkozattételi jogosultsággal rendelkezik.

A fentiekre tekintettel a Hatóság azzal a javaslattal fordult az oktatásért felelős államtitkárhoz, hogy szükséges az EMMI rendelet olyan kiegészítése, amely kizárja a jogszabályi vélelmet a gyermek személyes adatainak kezeléséhez való hozzájárulás esetében, vagyis mindkét szülőre tekintettel kell lenni.

Egy bejelentő azért fordult a Hatósághoz, mert az egyik család-és gyermekjóléti központtól kért tájékoztatást a gyermekeivel kapcsolatos adatokról, azonban az adatkérését megtagadták, figyelemmel arra, hogy az adatkezelés célját és jogalapját nem jelölte meg.

A kiskorú gyermekekkel kapcsolatos iratok kezelését érintő jogalapot a gyermekek védelméről és a gyámügyi igazgatásról szóló 1997. évi XXXI. törvény (a továbbiakban: Gyvt.) 136/A. § (*1)* bekezdése alapozza meg. A Hatóság megállapította, hogy a gyermekvédelmi nyilvántartás gyermekre vonatkozó adatlapjaiba, továbbá gyermekkel kapcsolatos iratokba a bejelentő betekinthet, azokról kivonatot, másolatot kérhet – tehát a bejelentő által a gyerekekkel kapcsolatban feltett azon kérdések, amelyek a fenti adatlapokból, iratokból megválaszolhatóak, azokra a kérdésekre választ kell adni – kivéve, ha a szülői felügyeleti joga korlátozott, és a korlátozás miatt ezt egyébként nem teheti meg.

Erre tekintettel a bejelentő által a gyerekekkel kapcsolatban feltett azon kérdések, amelyek a fenti adatlapokból, iratokból megválaszolhatóak, azokra a kérdésekre választ kell adni. Amennyiben a szülő az iratokról másolatot kér, azt rendelkezésére kell bocsátani. A másolatkérés joga kifejezetten nevesítve van a jogi szabályozásban, az nem szűkíthető vagy korlátozható a betekintés jogára.

---

lői felügyeletet gyakorló mindkét szülő együttes jelenléte szükséges. Kétség esetén vélelmezni kell, hogy a vizsgálaton megjelent szülő a távollevő szülő képviseletére jogosult. Erről a jelenlévő szülőt tájékoztatni kell, az ezzel kapcsolatos nyilatkozatát be kell szerezni. A szakértői vizsgálat során a szülő köteles közreműködni a vizsgálaton – annak zavarása nélkül – jogosult mindvégig jelen lenni."

V.9.2. A gyermekek személyes adatainak politikai szerepvállalás keretében történő kezelése

A Hatósághoz több újságírói megkeresés érkezett, melyben azzal kapcsolatban érdeklődtek, hogy az oktatási intézményeket látogató politikusok milyen feltételek megléte esetén szerepelhetnek a tanulókkal, hallgatókkal fényképfelvételeken, és ezek közölhetők-e a médiában.

Politikusok rendszeresen vesznek részt olyan eseményeken, amelyeken gyermekek is jelen vannak. Az eseményekről szóló beszámolókban, a nyomtatott vagy az online sajtóban közzétett hírekben számos esetben hoznak nyilvánosságra olyan fényképeket, amelyeken a résztvevő politikusok mellett például az adott intézmény tanulói is láthatók. A Hatóság ezért egyik eseti állásfoglalásában [*NAIH/2017/5206/V*] meghatározta azokat az adatvédelmi követelményeket, amelyek betartása elengedhetetlen a gyermekek magánélet tiszteletben tartásához, valamint a személyes adatok védelméhez fűződő alkotmányos joga érvényesüléséhez.

Az említett adatkezelések során a gyermekek és kiskorúak mindenekfelett álló érdekét kell figyelembe venni akár az online, akár az offline térben közzétett személyes adataik, így a fényképfelvételek tekintetében. A gyermekek személyes adatai különös védelmet érdemelnek, mivel ők kevésbé lehetnek tisztában az adatkezeléssel összefüggő kockázatokkal, annak következményeivel és az ahhoz kapcsolódó garanciákkal és jogosultságokkal.

A Hatóság garanciális követelményeket állapított meg a hozzájárulás, mint az adatkezelés jogalapja szempontjából is. Az adatkezelőknek minden egyes, 16 év alatti gyermekről közzétett fényképfelvétel esetében rendelkezniük kell a törvényes képviselő adatkezeléshez adott írásbeli hozzájárulásával. A szülők sok esetben év elején nyilatkozatot tehetnek arról, hogy hozzájárulnak-e gyermekük fényképének iskolai honlapon való közzétételéhez. Hangsúlyozandó azonban, hogy ezen általános hozzájárulás nem lehet megfelelő jogalap a sajtótermékekben nyilvánosságra hozott fényképfelvételek esetében. Minden egyedi esetben – azaz adatkezelésenként – be kell szerezni az érintettek megfelelő tájékoztatáson alapuló hozzájárulását az adott adatkezeléshez.

A hozzájárulás beszerzése előtt nyújtott tájékoztatás során külön figyelmet kell fordítani arra, hogy annak tartalma mind a szülő, mind pedig a gyermek számára világos, könnyen megérthető legyen. Ügyelni kell arra, hogy a tájékoztatás egyértelműen kiterjedjen az adatkezelés céljára, az érintetti jogok gyakorlásának lehetőségeire és módjaira, a jogorvoslati lehetőségekre, valamint a különleges

adatok kezelésének lehetséges – a gyermek magánéletére gyakorolt – jövőbeli hatásaira is. Továbbá lehetőséget kell biztosítani a gyermekek számára, hogy kifejtsék véleményüket az adatkezeléssel összefüggésben, és amennyiben nem kívánnak az adott közszereplés részeként a felvételeken szerepelni, biztosítani kell a számukra azt, hogy e véleményüknek további hátrányos következmények nélkül hangot adhassanak.

A rögzített felvételek nyilvánosságra hozatala előtt – abban az esetben is, amennyiben az adatkezelő rendelkezik az ahhoz szükséges írásbeli hozzájárulással – lehetőséget kell biztosítani a szülők számára, hogy adott esetben visszavonhassák a korábban adott hozzájárulásukat.

A Hatóság végezetül hangsúlyozta, hogy különös figyelmet kell fordítani az érintett azon jogára, hogy személyes adatait töröljék, amennyiben arra az adatkezelés eredeti céljaival összefüggésben már nincs szükség, a hozzájárulást visszavonták, vagy ha személyes adatok kezelése egyéb szempontból jogsértő. „*Ez a jog különösen akkor lényeges, ha az érintett gyermekként adta meg hozzájárulását, amikor még nem volt teljes mértékben tisztában az adatkezelés kockázataival, később pedig el akarja távolítani a szóban forgó személyes adatokat, különösen az internetről”*.[36]

V.10. A Facebook közösségi portált érintő esetek és a Hatóság álláspontja

V.10.1.) Az elmúlt időszakban több állampolgári panasz érkezett a Hatósághoz a Facebook közösségi oldal adat- és profilkezelési gyakorlatával, valamint biztonsági intézkedéseivel összefüggésben. A bejelentők leggyakrabban a névhasználattal és névmódosítással, illetve a felhasználói profil előzetes tájékoztatás nélküli zárolásával/törlésével, illetve az ezekkel kapcsolatos eljárásokkal összefüggésben tesznek panaszbejelentést, vagy kérnek tájékoztatást a Hatóságtól.

Az egyik leggyakoribb kérdés az okmánymásolatok kérésének jogszerűsége volt. Kétféle okból fordulhat elő, hogy a Facebook személyazonosító okmány beolvasott képét vagy fényképét kéri:

- A fiók tulajdonjogának igazolására: Azért, hogy a felhasználón kívül senki más ne lépjen be a fiókba.

36 Általános Adatvédelmi Rendelet (65) preambulumbekezdés.

- A felhasználó nevének megerősítése céljából: A Facebook felhasználási feltételeinek értelmében a felhasználók a regisztráció során valódi nevüket és adataikat adják meg.

A névellenőrzés során a felhasználók által rendelkezésre bocsátott dokumentumok esetében a személyazonosításhoz szükséges részeket kivéve valamennyi adat (okmány száma, lakcím, stb.) kitakarható. A felhasználó által digitális formában rendelkezésre bocsátott okiratot nem őrzik meg, nem tárolják, az csak a beazonosítást szolgálja.

A letiltott Facebook profillal összefüggésben a közösségi oldal felhasználási feltételeinek a 14. „*Megszűnés*" címet viselő fejezete tartalmaz feltételeket.[37]

Számos megkeresés érkezett a Hatósághoz, melyben a panaszosok profiljuk feltörésével, álprofil létrehozásával, sértő bejegyzésekkel kapcsolatban fogalmazták meg beadványukat. Az internetes profilok feltörésének elkerülése érdekében a NAIH javasolja, hogy az érintett változtassa meg jelszavát egy legalább 10 karakterből álló, kis- és nagybetűt, valamint számokat is tartalmazó jelszóra, valamint minden egyes használat után lépjen ki profiljából, különösen abban az esetben, ha a számítógépét más is használja, illetőleg nyilvános számítógépről lép be profiljába.

V.10.2.) A Facebook európai felhasználóinak adatait a Facebook Ireland Ltd. kezeli. Az adatkezelővel szemben a Facebook európai felügyeletét ellátó ír adatvédelmi hatósághoz lehet fordulni. A Hatóság a Facebook névhasználattal és névmódosítással, valamint az okmánymásolatok bekérésével kapcsolatos gyakorlatával és eljárásaival összefüggésben konzultációt folytatott az ír adatvédelmi hatósággal, amely arról tájékoztatta a Hatóságot, hogy a 2011-2012-ben elvégzett auditja során megvizsgálta a közösségi oldal névellenőrzésre irányuló eljárását, azonban azt megfelelőnek találta. Az ír társszerv megerősítette, hogy a felhasználók által a Facebook rendelkezésre bocsátott okmányok a felhasználó beazonosítását követően törlésre kerülnek. A konzultáció folyamatban van, ugyanis a Hatóság kifogásolta a Facebook tájékoztatási gyakorlatát is.

37 *„Ha megsérti jelen Nyilatkozat tartalmát vagy szellemiségét, vagy egyéb módon számunkra kockázatot teremt, illetve lehetséges jogvitának tesz ki bennünket, akkor az Ön számára részben vagy egészben megszüntethetjük a Facebook használatának lehetőségét. Önt e-mailben vagy a fiókjához történő következő hozzáférési kísérlete során fogjuk értesíteni."*

V.11. A blokklánc („blockchain”) technológia

A Hatósághoz eljuttatott konzultációs beadványában egy magyar állampolgár állásfoglalást kért a Bitcoin virtuális fizetőeszköz és az alapját képező blokklánc technológia *(„blockchain”*) adatvédelmi kérdéseiről.
A blokklánc technológia első képviselője a digitális piacon a Bitcoin elnevezésű virtuális fizetőeszköz volt. A blokkláncban az adatokat a blokkok tárolják, amelyek gyakorlatilag kis adatbázisokként viselkednek. Amennyiben a felhasználók a blokklánc decentralizált adatbázisához újabb adatokat adnak hozzá, akkor az új adatok egy új blokkban fognak letárolódni. A blokkok létrehozása során azokból egy láncolat jön létre, ezt nevezzük tulajdonképpen blokkláncnak. A blokklánc akkor számít érvényesnek, ha az úgynevezett „ősblokkal” (az első létrejött blokk) kezdődik, és ha a benne foglalt összes, az adatokkal végzett tranzakció is érvényes. A lánc bármely blokkjától csak egyetlen, egyenes út vezet vissza az ősblokkig.

Az egyes blokkokban a rendszer nem csak az adatokat, hanem az adatokkal végzett valamennyi rendszeren belüli műveletet is letárolja. Az adatokon végzett tranzakciók lebonyolítása nem úgy történik, hogy tényleges adatmozgás valósul meg az egyes blokkok között, hanem a rendszer csak hozzárendeli az egyes adatokhoz az azokat tároló blokkban, hogy afelett épp melyik felhasználó jogosult rendelkezni. A rendszer az egyes felhasználók digitális aláírásaival látja el a blokkokban tárolt adatokat, és ez alapján ítéli meg, hogy adott blokkban tárolt adathalmaz felett melyik felhasználó jogosult rendelkezni.

A blokklánc technológia tárolásának alapja egy olyan decentralizált hálózat, melyben nincs központi entitás vagy bármilyen egyéb külső szerv, ami az abban tárolt adatokkal végzett tranzakciók külső ellenőrzését végezné. A blokkláncot nem egy központi adatkezelő tárolja, hanem azt gyakorlatilag valamennyi felhasználó tárolja saját számítógépein.

A Bitcoin-rendszerben a blokklánc technológiát egy olyan virtuális fizetőrendszer kifejlesztésére használták fel, amely anonim módon használható, mivel az egyes érmékkel végzett műveletek kivitelezéséhez nincs szükség személyes adatok megadására. Ettől függetlenül elképzelhető olyan blokklánc technológiát használó rendszer is, amelyben a blokkokat személyes adatok tárolására is felhasználják, így például a blokkban tárolt, alapvetően fizetésre használt adatokhoz személyes adatokat is kapcsolnak.

Amennyiben a blokkláncban lévő egyes blokkokat személyes adatok tárolására is felhasználják, úgy felmerülhet a kérdés, hogy ki minősül ebben az esetben adatkezelőnek. Az Infotv. fogalmai szerint adatkezelőnek elsősorban az a személy minősül, aki a személyes adatok kezelésének célját meghatározza, az erre vonatkozó döntéseket meghozza és végrehajtja. Mivel a blokklánc kapcsán egy olyan decentralizált hálózatról beszélünk, ahol nincs olyan központi entitás, amely felügyeleti jogot gyakorol a rendszer működése és az adatokkal végzett tranzakciók felett, ezért az adatok kezelését gyakorlatilag az egyes felhasználók végzik.

A blokklánc kapcsán tehát minden egyes olyan felhasználó, amely blokkokat és abban tárolt adatokat ad hozzá a rendszerhez, egyben adatkezelőnek minősül. Később a rendszerhez adatokat hozzáadó felhasználó kizárólagos rendelkezési jogosultságot kap a blokkokban tárolt adatai felett, így ő határozhatja meg, hogy az adatokat mely tranzakciók kivitelezéséhez fogja felhasználni. Amennyiben a tranzakciók révén a blokkban tárolt személyes adatok feletti rendelkezési jogosultság átadásra (*„átutalásra”*) került egy másik felhasználónak, onnantól kezdve ez a felhasználó (az adatok címzettje) szerez az adatok felett kizárólagos rendelkezést, így ő fog adatkezelőnek minősülni.

A blokkláncban tárolt személyes adatok kezelésének jogalapját a jelenleg hatályos jogszabályok alapján az érintett hozzájárulása, vagy a felhasználó jogos érdeke képezheti. Amennyiben az érintett nem járul hozzá ahhoz, hogy a személyes adatait a blokkban tárolt adatok felett rendelkező felhasználó tárolja, illetve azokkal műveleteket végezzen, továbbá a felhasználó az adatkezeléssel kapcsolatban jogos érdeket sem tud bizonyítani, úgy az adatkezelés nem lehet jogszerű. A blokkláncban kezelt személyes adatokról az érintett kérésére az adatkezelő köteles 25 napon belül teljes körű tájékoztatást adni.

V.12. Adatvédelmi incidensek

Adatvédelmi incidensnek tekintjük a személyes adatok jogellenes kezelését vagy feldolgozását, így különösen a jogosulatlan hozzáférést, megváltoztatást, továbbítást, nyilvánosságra hozatalt, törlést vagy megsemmisítést, valamint a véletlen megsemmisülést és sérülést, amely az adatbiztonsági szabályok megsértésével hozható összefüggésbe.

A Hatóság több, kisebb és nagyobb súlyú incidenst is vizsgált. A következő jelentősebb esetek fordultak elő:

- A biztosításközvetítő ténylegesen nem rendelkezett a bejelentő hozzájárulásával az adattovábbításhoz, valamint nem volt olyan jogszabályi rendelkezés, amely alapján az incidenst elkövető biztosítást közvetítő mentesülne a biztosítási titok megőrzésének kötelezettsége alól. A biztosításközvetítő nem győződött meg arról, hogy a bejelentő meghatalmazottjaként bemutatkozó személy vonatkozásában a bejelentő valóban hozzájárult-e személyes adatai továbbításához, illetve, hogy e személy ténylegesen jogosult-e hozzáférni a bejelentő személyes adataihoz, továbbá hogy a bejelentő meghatalmazottjaként bemutatkozó személy jogosult-e módosítani a biztosításközvetítő weboldalán a bejelentő személyes adatait. [*NAIH/2017/477/V*]
- A cég egy olyan lakásbiztosítási szerződéssel kapcsolatos dokumentumokat küldött meg az ügyfélnek elektronikus levél útján, mely szerződést nem az ügyfél írta alá, illetve a továbbított dokumentumokban található személyes adatok sem az ügyfél adatai. A cég munkatársai tévedésből küldték meg az ügyfélnek a kérdéses dokumentumokat, egy azonos nevű ügyfelük helyett. [*NAIH/2017/4691/V*]
- A Hatósághoz számos bejelentés érkezett egy közlekedési társaság által üzemeltetett online jegyértékesítési rendszerrel összefüggő adatkezeléssel kapcsolatban. A bejelentők azt kifogásolták, hogy a társaság online jegyértékesítési rendszere nem felel meg az adatbiztonsági követelményeknek, emellett több panaszban kifogásolták, hogy a sajtóban megjelent hírek alapján valószínűsíthető, hogy a regisztráció során megadott személyes adataikhoz harmadik személyek jogosulatlanul hozzáférhettek.

A társaság által üzemeltetett online jegyértékesítési rendszer adatbázisából kigyűjtött, a regisztrált felhasználók személyes adatait tartalmazó adatbázishoz arra jogosulatlan személyek is hozzáférhettek. A Hatóság megállapította, hogy az adatbiztonság olyan mértékben sérült, ami az adatokhoz való jogosulatlan hozzáférést eredményezte, vagyis adatvédelmi incidens történt. [*NAIH/2017/3979/H, NAIH/2018/356/H*]

A NAIH ezzel kapcsolatban az alábbiakat állapította meg:
Az adatkezelés megtervezése során az adatkezelő nem tette meg azokat a technikai és szervezési intézkedéseket, és nem alakította ki azokat az eljárási szabályokat, amelyek az adatok biztonságát szolgálják. Az ilyen intézkedések hiányát bizonyítja az is, hogy nem tudta megállapítani azt, hogy az általa végzett adatkezelés vonatkozásában adatvédelmi incidens következett be.

Az adatfeldolgozóval kötött szerződésben nem tért ki az adatkezeléssel kapcsolatos kérdésekre a cég, így abban nem rögzítettek adatbiztonsági előírásokat, követelményeket sem. A szerződés megkötését követően sem adott utasításokat az általa igénybe vett adatfeldolgozónak az adatbiztonsági intézkedések vonatkozásában.

Emellett 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.

A fentiek alapján a Hatóság adatvédelmi bírság megfizetésére kötelezte az adatkezelőt, 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 regisztrált felhasználókat tájékoztassa. Kötelezte továbbá arra, hogy megfelelően gondoskodjon az adatbiztonsági követelmények teljesítéséről.

V.13. Az Adatvédelmi Nyilvántartás

Ahogyan az elmúlt években, így 2017-ben is sok konzultációs beadvány érkezett a Hatósághoz, amelyben az állampolgárok/szervezetek aziránt érdeklődtek, hogy adatkezelésüket be kell-e jelenteniük a Hatóság felé az adatvédelmi nyilvántartásba vétel céljából, illetőleg számos alkalommal az adatvédelmi nyilvántartáshoz kapcsolódó egyéb kérdéseket tettek fel.

A jelenleg hatályos szabályozás szerint a Hatóság az adatkezelők személyes adatokra vonatkozó adatkezeléseiről az érintettek tájékozódásának elősegítése érdekében hatósági nyilvántartást vezet, amely nyilvántartásban fel kell tüntetni az adatkezelésre vonatkozó minden lényeges körülményt, így például az adatkezelés célját, jogalapját, időtartamát.

A Hatóság minden olyan adatkezelői tevékenységről nyilvántartást vezet, ami nem tartozik az Infotv. által meghatározott kivételek közé, ilyen kivétel – egyebek mellett – az, ha az adatkezelő a vele munkaviszonyban álló személyekre vonatkozó adatokat kezel.

Jelenleg az adatkezelők kötelezettsége, hogy az adatkezelés megkezdése előtt bejelentsék tevékenységüket a Hatóság felé, azonban ez a szabály megváltozik. Az általános adatvédelmi rendelet nem tartalmaz az Irányelv, illetve az Infotv. jelenlegi szabályozásához hasonló, a tagállami hatóságok által vezetendő országos adatvédelmi nyilvántartásra vonatkozó szabályozást. Az általános adatvédelmi rendelet 30. cikke az adatkezelők, illetve adatfeldolgozók kötelezettségévé teszi, hogy a felelősségükbe tartozóan végzett adatkezelési tevékenységekről vezessenek nyilvántartást. Ez azt fogja jelenteni, hogy az adatkezelőknek, adatfeldolgozóknak saját maguknak kell nyilvántartást vezetniük adatkezeléseikről, azokat azonban nem kell bejelenteniük a Hatóságnak. Tehát a jelenlegi nyilvántartásba történő bejelentési kötelezettség 2018. május 25. napjától megszűnik.

A Hatóság telefonos ügyfélszolgálatára is sok hívás érkezik e kérdéskör vonatkozásában. Számos esetben elmondható, hogy a telefonálók bejelentési kötelezettségeik teljesítését – a jogszabályi környezet változása ellenére – fontosabbnak vélik, minthogy az egyéb jogszabályokban rögzített követelményeknek megfeleljenek.

Az általános adatvédelmi rendelet két esetben ír elő bejelentési kötelezettséget: az adatvédelmi tisztviselő nevét és elérhetőségét, továbbá az adatvédelmi incidenseket kell az illetékes hatóságnak bejelenteni. A Hatóság a honlapján ezekre külön felületet fog biztosítani.

V.14. A közérdekű bejelentő védelme

A Hatósághoz több olyan panaszbeadvány érkezett, amelyben a bejelentők azt kifogásolták, hogy közérdekű bejelentést vagy panaszt tettek egy adatkezelőnél, amely eljárása során felfedte a bejelentő kilétét annak hozzájárulása nélkül a bepanaszolt szerv vagy személy előtt.

A hozzájárulás fogalmát a Hatóság álláspontja szerint nem lehet kiterjesztően, valamennyi adatkezelési művelet vonatkozásában értelmezni, így például az adattovábbítás, tehát az adat meghatározott harmadik személy – az adatkezelő által eljárás alá vont szerv vagy személy – számára történő hozzáférhetővé tétele kapcsán.

Az Infotv. rendelkezéseivel nincs összhangban az a gyakorlat, mely alapján a panaszt tevő személyes adatainak részben vagy egészben zártan történő keze-

lésére vonatkozó kérelme hiányában az adatkezelő a személyes adatok továbbításhoz való hozzájárulást önmagában a kérelem benyújtásának ténye alapján megadottnak tekinti az Infotv. 6. § (6) bekezdése alapján, különös tekintettel arra is, hogy a panaszosok előtt nem feltétlenül ismert a személyes adatok zártan történő kezelésének lehetősége. E körben különösen lényeges az Infotv. 6. § (8) bekezdésben foglalt azon rendelkezése, mely szerint kétség esetén azt kell vélelmezni, hogy az érintett a hozzájárulását nem adta meg.

Ha az adatkezelő számára nem áll rendelkezésre egyértelmű információ arra nézve, hogy a panaszbeadvány a panaszos személyes adatainak megismerésére alkalmas módon továbbítható-e az eljárás alá vont szerv vagy személy részére, a panaszbeadvány továbbítását megelőzően ahhoz az érintett hozzájárulását kell kérnie.

Amennyiben az adatkezelő álláspontja szerint a panaszos személyazonosságának felfedése nélkül az eljárás nem folytatható le, erről a panaszost tájékoztatnia kell annak érdekében, hogy a panaszos információs önrendelkezési jogával élve maga mérlegelhesse az eljárás lefolytatásához, illetve a személyes adatai védelméhez fűződő érdekét, és ennek alapján határozhasson személyes adatainak sorsáról.

A fentieken túl, a panaszbejelentések kezelése során az adatkezelőknek a szükségesség elvének figyelembe vételével kell eljárniuk, amennyiben tehát a panasz, illetve bejelentés kivizsgálásához a bejelentő nevének kezelése, illetve továbbítása szükségtelen, akkor a panaszos adatai akkor sem továbbíthatóak az eljárás alá vont szerv vagy személy részére, ha ahhoz egyébként előzetesen hozzájárult.

A panaszos beadványában előadta, hogy fegyelmi eljárást kezdeményezett az egyik ügyvédi kamaránál (a továbbiakban: Kamara) az ügyvédjével szemben. A Kamara a fegyelmi ügyben elrendelhető előzetes vizsgálatot megelőzően, a panaszos hozzájárulása nélkül, oly módon adta át a panaszbeadványt az ügyvédnek, hogy abból megismerhetőek voltak a panaszos személyes adatai, melyet az ügyvéd utóbb polgári peres eljárás megindítására használt fel a panaszossal szemben. A bepanaszolt ügyvéd tevékenysége a panaszos személyén túlmenően több személyt is érintett, a kifogásolt tevékenység általánosan vizsgálható lett volna a konkrét panaszos nevének ismerete nélkül, ezért a Hatóság a vizsgálat során megállapította, hogy a Kamara kötelező adatkezelés hiányában megsértette az Infotv. 5. § (1) bekezdését, valamint az Infotv. 7. § (2) bekezdésében foglalt adatbiztonság követelményét.

V.15. Jogos érdek, mint jogalap

A két legalapvetőbb jogalap az érintetti hozzájárulás, valamint a kötelező adatkezelés. Az Infotv. 6. §-a ezt a két jogalapot egészíti ki azzal, amikor bizonyos esetekben, speciális, jogos érdekekből az érintett hozzájárulása hiányában, és kifejezett jogalkotói rendelkezés nélkül is lehetőséget biztosít az adatok kezelésére. Ilyen jogalapként született meg az Infotv. 6. § (1) bekezdésének b) pontja, mely szerint személyes adat kezelhető akkor is, ha az érintett hozzájárulásának beszerzése lehetetlen vagy aránytalan költséggel járna, és a személyes adat kezelése az adatkezelő vagy harmadik személy jogos érdekének érvényesítése céljából szükséges, és ezen érdek érvényesítése a személyes adatok védelméhez fűződő jog korlátozásával arányban áll.

Az Infotv. 6. § (5) bekezdésének b) pontja alapján is kezelhetőek az érintett személyes adatai, ugyanis ha a személyes adat felvétele az érintett hozzájárulásával történt meg, az adatkezelő a felvett adatokat törvény eltérő rendelkezésének hiányában az adatkezelő vagy harmadik személy jogos érdekének érvényesítése céljából további külön hozzájárulás nélkül is kezelheti, ha ezen érdek érvényesítése a személyes adatok védelméhez fűződő jog korlátozásával arányban áll.

Emellett az adatkezelők a személyes adatok feldolgozása vonatkozásában az egyének védelméről és az ilyen adatok szabad áramlásáról szóló 1995. október 24-i 95/46/EK európai parlamenti és tanácsi irányelv (a továbbiakban: Adatvédelmi Irányelv) 7. cikk f) pontját is alkalmazhatják jogalapként. Az Adatvédelmi Irányelv 7. cikk f) pontja értelmében személyes adat kezelhető abban az esetben is, ha az adatkezelés az adatkezelő, vagy az adatokat megkapó harmadik fél, vagy felek jogszerű érdekének érvényesítéséhez szükséges, kivéve, ha ezeknél az érdekeknél magasabb rendűek az érintettek személyes adatok kezelése vonatkozásában a magánélet tiszteletben tartásához való joguk. Az Európai Bíróság a C-468/10. és C-469/10. sz. egyesített ügyekben hozott ítéletében ugyanis kimondta, hogy az Adatvédelmi Irányelv 7. cikk f) pontjának közvetlen hatálya van, így a tagállami bíróság előtt adatkezelők e jogalapra hivatkozhatnak. Az általános adatvédelmi rendelet 6. cikk (1) bekezdésének f) pontja alapján szintén alkalmazható lesz ez a jogalap.

A Hatóság ellenőrzési tapasztalatai azt mutatják, hogy sok esetben az adatkezelők nincsenek tisztában azzal, hogy mikor lehet a jogos érdekre, mint jogalapra hivatkozni, illetve amennyiben alkalmazzák is, gyakran helytelenül teszik.

Példaként hozhatóak fel általános gyakorlatként a munkahelyi ellenőrzésekkel összefüggő adatkezelések – különösen az elektronikus megfigyelőrendszerekkel összefüggő adatkezelések –, amelyeknél a munkáltatók gyakran a munkavállalók „*hozzájárulása*" alapján üzemeltetnek kamerarendszert. A Hatóság többször kifejtette, miért nem alkalmazható a hozzájárulás jogalapként. Ennek ellenére továbbra sem ismert széles körben a munkáltatók előtt a jogos érdeken alapuló adatkezelés, mint jogalap, illetve ha ismert is, anélkül hivatkoznak e jogalapra, hogy az adatkezeléshez fűződő szükséges és jogos érdeküket az adatkezelés megkezdése előtt elvégzett érdekmérlegelési teszt eredményével alátámasztanák.

Másik általános példaként említhetőek a követeléskezeléssel foglalkozó pénzügyi intézmények, amelyek adatkezelési tájékoztatóikban az érdekmérlegelésen alapuló adatkezelésük jogalapját általában csak az Infotv. 6. § (1) és (5) bekezdésének szó szerinti idézetével támasztják alá. Tájékoztatóikban nem szerepel, hogy a felsorolt jogalapokat mely adatok kezelésére, milyen esetekben, mely jogos érdekük érvényesítése érdekében alkalmazzák, illetve szintén anélkül hivatkoznak az érdekmérlegelési jogalap alkalmazására, hogy azt az adatkezelés megkezdése előtt elvégzett érdekmérlegelési teszt eredményével alátámasztanák. Gyakori, hogy tudatosan mellőzik az érdekmérlegelés elvégzését az adattörlések elkerülése érdekében.

Függetlenül attól, hogy az adatkezelő az Infotv., az Adatvédelmi Irányelv, illetve 2018. május 25. napjától az általános adatvédelmi rendelet rendelkezésére hivatkozik, minden esetben el kell végeznie az érdekmérlegelés tesztjét. Az érdekmérlegelési teszt egy három lépcsős folyamat, melynek során azonosítani kell az adatkezelő jogos érdekét, valamint a súlyozás ellenpontját képező adatalanyi érdeket, az érintett alapjogot, végül a súlyozás elvégzése alapján meg kell állapítani, hogy kezelhető-e a személyes adat. A teszt elvégzése során az adatkezelőnek számos szempontra figyelemmel kell lennie, az adatkezeléstől függően, azonban minden esetben követelmény, hogy a teszt eredményéről – miért tartja úgy az adatkezelő, hogy az adatkezeléshez fűződő érdeke arányosan korlátozza az érintett érdekeit és jogait – közérthető és világos módon megfogalmazott tájékoztatást kell nyújtania az érintettek számára.

Az érdekmérlegelési teszt dokumentálása azért is fontos, mert az általános adatvédelmi rendelet alapelvi szintre emelte az elszámoltathatóság elvét, melynek értelmében az adatkezelő felelős minden további adatkezelési elv, adatvédelmi követelmény betartásáért, az azoknak való megfelelésért, és képesnek kell lennie e megfelelés igazolására.

A Hatóság például az alábbi konkrét ügyek kapcsán vizsgálta a jogos érdek, mint jogalap kérdését.

A NAIH/2017/280/H számú adatvédelmi hatósági eljárásban a bejelentő a munkahelyén, egy idősek otthonában üzemelő elektronikus megfigyelőrendszert, illetve azt kifogásolta, hogy a munkáltató nem tett eleget a rendszer üzemeltetésére vonatkozó tájékoztatási kötelezettségének.

A Kötelezett által kiadott, kamerarendszer üzemeltetéséről szóló főigazgatói utasítás a munkavállalók megfigyelésének jogalapjaként hivatkozott az adatkezelő jogos érdekén alapuló adatkezelésre. A Kötelezett azt nyilatkozta, hogy az intézményeknél a kamerával megfigyelt területeken jellemzően idős lakók tartózkodnak, így ők tekinthetőek adatalanyoknak, illetve ugyanezen személyek az adatok címzettjei – akiknek érdekében történik a kamerarendszer üzemeltetése – is, erre tekintettel *„az érdekmérlegelés Intézményünkben formál logikai, paradigmatikai értelemben nem volt elvégezhető, hiszen az adatalany és az adatok címzettje egybeesik, egy matematikai halmazt alkot, monopólusú rendszert képez."* A Hatóság a határozatában felszólította a kötelezettet – többek között – arra, hogy az általa hivatkozott jogalap igazolására készítse el a kötelezően elvégzendő érdekmérlegelési tesztet, melyet végül az eljárás végén elkészített.

A NAIH/2017/435/V számú vizsgálati eljárásban a bejelentő által kifogásolt alapprobléma az volt, hogy az egyik áramszolgáltató munkatársai fényképet készítettek a bejelentő személyes adatnak minősített ingatlanáról abból a célból, hogy igazolják a mérőóra-csere céljából történő bejutási kísérlet sikertelenségét, mivel ennek fogyasztó részéről történő akadályozása szerződésszegésnek minősül. Az adatkezelés jogalapjaként az adatkezelő az Infotv. 6. § (1) bekezdésének a) pontját jelölte meg, azonban a vizsgálat során nyújtott első válasza alapján nem volt megállapítható, hogy az adatkezelői jogos érdekre alapozott adatkezelést megelőzően kidolgozta, és elvégezte volna az érdekmérlegelési tesztet, illetve hogy általában véve ismeri-e és alkalmaz-e a szóban forgó érdekek mérlegelésére alkalmas tesztet, avagy sem.

A fenti hiányosságokra tekintettel a Hatóság felszólította az adatkezelőt egy megfelelő érdekmérlegelési teszt kidolgozására, továbbá az érintett ügyfelek számára történő hozzáférhetővé tételre. Az adatkezelő végül egy elfogadható érdekmérlegelési tesztet nyújtott be, így a Hatóság lezárta az ügyet.

V.16. Az elfeledtetéshez való jog

Információs társadalmunkban a világhálóra szabadon feltölthető és szerkeszthető tartalmak általánossá válásával egyre inkább előtérbe kerül e tartalmak kontrollálásának az igénye is, vagyis az érintettek azon joga, hogy a rájuk nézve releváns, online fellelhető információk törlését kérjék. Az elfeledtetéshez való joggal kapcsolatban Hatóságunkhoz is több kérelem érkezett 2017-ben.

A témában a legfontosabb döntés a *„Google ítélet"*[38], melyben kifejtett szempontokat a Hatóság egy tájékoztatóban[39] is rögzítette, és azóta is ennek megfelelően értékeli a hasonló ügyeket.

Alapvetően kétféle helyzet különböztethető meg. Egyrészt, amikor az érintett az információkat megjelentető weboldal működtetőjétől, mint adatkezelőtől kéri személyes adatainak törlését, avagy a teljes bejegyzés eltávolítását. A másik eset pedig az, amikor egy internetes keresőszolgáltatás működtetőjéhez (leggyakrabban a Google) fordul az érintett, és a szóban forgó link eltávolítását kéri a keresési találatok közül. A Google keresőmotorjának találati listájából való törlés nem azonos az adatkezelő általi törléssel. Míg az előbbi csupán az elérési utat törli technikailag, az utóbbinál lehetőség van az adatnak a teljes törlésére.

Az EUB egyértelműen rámutatott arra ítéletében, hogy a keresőmotor működtetője köteles arra, hogy az egy személy nevére való keresés nyomán megjelenő találati listáról törölje a harmadik fél által közétett és e személlyel kapcsolatos információkat tartalmazó weboldalakra mutató linkeket, és a tagállamok adatvédelmi hatóságai – ahogyan a NAIH is – mind ezen ítéletből vezetik le gyakorlatukat. Mindazonáltal a Google, mint adatkezelő nem egy esetben hivatkozik egyszerűen a nyilvánosság hozzáférési jogára, mint erősebb érdekre, és nem teljesíti a törlés iránti kérelmeket.

A *„Google ítélet"* nyomán egyre inkább a szabályozás homlokterébe került az elfeledtetéshez való jog, és ez szükségszerűen magával hozta az ítélet által megfogalmazott elvek jogszabályban való rögzítésének igényét is. Ez meg is történt

38 Az Európai Unió Bíróságának C-131/12. számú, a Google Spain SL és Google Inc. kontra Agencia Española de Protección de Datos (AEPD) és Mario Costeja González ügyben 2014. május 13-án hozott ítélete. http://eur-lex.europa.eu/legal-content/HU/TXT/?uri=CELEXCELEXCELEX%3A62012CJ0131

39 A NAIH tájékoztatója a személyes adatoknak a Google keresőmotorjának találati listájából való eltávolításával kapcsolatos ügyek megítélése során figyelembe vett szempontokról. https://www.naih.hu/files/2015-07-29-Tajekoztato_Google_talalati_list_eltavol.pdf

a 2018. május 25-től alkalmazandó általános adatvédelmi rendelettel, mely a személyes adatok törlése iránti kérelem mellett kifejezetten nevesíti az elfeledtetéshez való jogot.[40]

Az általános adatvédelmi rendeletben az elfeledtetés jogára vonatkozik az a rendelkezés, miszerint a személyes adatot nyilvánosságra hozó adatkezelőnek nem csupán törlési kötelezettsége áll fenn a meghatározott esetekben, hanem tájékoztatnia kell a többi adatkezelőt is arról, hogy az érintett kérte a személyes adataira mutató link eltávolítását. Az általános adatvédelmi rendelet kijelöli az elfeledtetés jogának a korlátait is. Az adatkezelő a jövőben sem köteles az érintett kérelmét teljesíteni például akkor, ha az adatkezelés a véleménynyilvánítás szabadságához és a tájékozódáshoz való jog gyakorlása céljából szükséges, vagy ha azt az érintett közszereplő volta, közéletben betöltött szerepe indokolja. Minden egyéb esetben az adatkezelő köteles biztosítani az érintett elfeledtetéshez való jogát, és haladéktalanul törölni a személyes adatot tartalmazó linket.

V.17. A Sziget fesztiválon történő adatkezelés

I.) Vizsgált adatkezelés: A Hatósághoz több panasz érkezett a VOLT Fesztivállal és a Sziget Fesztivállal kapcsolatban, melyekben a bejelentők a szervezők beléptetésnél alkalmazott azon gyakorlatát sérelmezték, melynek során beszkennelik a vendégek személyazonosító igazolványát, továbbá azt, hogy nem tájékoztatják megfelelően az érintetteket az adatkezelés körülményeiről, így arról, hogy milyen célból és mennyi ideig kezelik az igazolványokról készített másolatot.

II.) A Hatóság vizsgálata: Az adatkezelő az általa szervezett fesztiválokra történő beléptetés során a belépésre jogosító karszalagot hozzárendeli annak birtokosához azáltal, hogy rögzíti a látogató személyes adatait személyazonosító igazolványának szkennelése során. A személyazonosság fényképes személyazonosító okmánnyal történő igazolása tehát előfeltétele a rendezvényen való részvételnek. Az adatrögzítés során leolvassák a belépőjegyen lévő vonalkódot, majd beszkennelik az igazolványt és hozzárendelik a karszalaghoz. Ahol olyan chip található az igazolványban, amiből ki tudja olvasni a szkenner a szükséges adatokat úgynevezett MRZ kód alapján, azt rögzítik, azonban a régebbi típusú személyazonosító igazolványokból csak a személyes adatokat olvassa ki a szkenner (név, születési dátum, okmánytípus, száma, lejárata, ország/nemzeti-

40 Általános adatvédelmi rendelet 17. cikke.

ség, nem), a profilképet nem, ezért szükséges a fényképes oldalának rögzítése, beszkennelése is.

A vállalkozó nyilatkozata szerint az új beléptető rendszer bevezetésének oka az Európában egyre gyakoribbá váló terrorcselekmények voltak. Véleményük szerint azáltal, hogy a karszalag átvételekor a karszalag birtokosa azonosításra kerül, komoly mértékben képes csökkenteni a terrorveszélyt.
Az adatkezelés jogalapjaként az érintetti hozzájárulást jelölték meg, továbbá előadták, hogy a látogatók személyes adatainak beléptetéssel összefüggésben végzett kezelése nem jelent olyan mértékű korlátozást, amely ne állna arányban az elérni kívánt célokkal, vagyis a látogatók élethez való jogának védelmével és az egyéb visszaélések megakadályozásával. Emellett kiemelték, hogy az általuk kidolgozott rendszer alkalmazása – a generális és speciális prevenció útján – alkalmas arra, hogy megelőzze, illetve megakadályozza terrorcselekmények elkövetését.

III.) Megállapítások: A Hatóság döntésében áttekintette a vizsgált adatkezelés kapcsán felmerülő valamennyi alkalmazható jogalapot, valamint értékelte az adatkezelő előzetes tájékoztatási gyakorlatát is.

a. A Hatóság álláspontja szerint a hozzájárulás nem tekinthető megfelelő jogalapnak olyan esetben, amikor a hozzájárulás meg nem adása nélkül nem érvényesülhet egy másik adatkezelés, illetve az ellenszolgáltatás megfizetésével igénybe vett szolgáltatás. A Hatóság meglátása szerint tehát nincs valódi választási lehetősége az érintetteknek a beléptetéssel összefüggő adatkezelés során.
b. Az adatkezelő ugyan szabályzataiban nem alkalmazta, de a vizsgálati eljárás során érvelt egy másik jogalap, a jogos érdeken alapuló jogalap alkalmazása mellett is. A Hatóság ennek értékelése során megvizsgálta annak alkalmazásának feltételeit, vagyis az érdekmérlegelési teszt egyes elemeinek (az adatkezelő, illetve harmadik személy jogos érdekének azonosítása, az adatalanyi érdekek meghatározása, annak vizsgálata, hogy a cél elérése érdekében feltétlenül szükséges-e személyes adat kezelése végül a súlyozás elvégzése) a fennállását.

A fesztiválátogatók biztonságának garantálását fontos és elfogadható célnak tekintette a Hatóság, melyben egyszerre jelentkezik mind a rendezvényt szervező vállalkozás gazdasági érdeke, mind az állampolgárok, látogatók biztonsága, mind a közérdek.

Az alkalmazott gyakorlat elengedhetetlenségének, illetve megfelelőségének vizsgálata körében több, hasonló méretű európai fesztivál beléptetési gyakorlatát állította példaként a Hatóság annak bemutatására, hogy milyen egyéb módszerekkel lehet magas szintű védelmet biztosítani olyan eszközök alkalmazásával, melyekkel kevésbé sérül az érintettek információs önrendelkezési joga.

A Hatóság a látogatók biztonságának megteremtésére választott eszközt, illetve módszert továbbra sem tartja alkalmasnak az elérni kívánt cél megvalósulásához, valamint a Hatóság álláspontja szerint arányosnak sem tekinthető a személyazonosító igazolvány szkennelése és az ezzel együtt járó adatkezelés az általa megvalósított jogkorlátozással.

c. A Hatóság döntésében utalt arra, hogy annak megállapítása és kimondása, hogy a fesztiválllátogatók biztonságának garantálása közérdek lenne, továbbá ebben az esetben a védelem megfelelő szintjét biztosító intézkedések, lépések megtétele jellemzően állami feladat. Ebből adódóan a Hatóság véleménye szerint megoldást jelentene, ha a kérdést a jogalkotó megfelelően szabályozná, és törvényes jogalapot teremtene a megfelelő védelmi szint eléréséhez feltétlenül szükséges adatok kezeléséhez.

A Hatóság fentiekre tekintettel felszólította a Kft.-t, hogy vizsgálja felül beléptetési rendszerét és az annak során megvalósuló adatkezelési gyakorlatát és alakítsa át, valamint készítsen olyan adatkezelési tájékoztatót, illetve szabályzatot, amely megfelelő tájékoztatást nyújt az érintettek számára. A Hatóság külön felhívta az adatkezelő figyelmét arra is, hogy adatkezelési gyakorlatának áttekintésekor legyen tekintettel az általános adatvédelmi rendeletnek való megfelelési kötelezettségére is.

V.18. A Magyarországi Szcientológia Egyház és a Szcientológia Egyház Központi Szervezet adatkezelése

V.18.1. Az eljárás bemutatása

A Magyarországi Szcientológia Egyház adatkezelését mind az adatvédelmi biztos, mind a Hatóság is több alkalommal vizsgálta. A hatósági eljárást megelőzően is érkeztek panaszok a Hatósághoz, melyekben a panaszosok a Magyarországi Szcientológia Egyházat (továbbiakban: MSZE), a Szcientológia

Egyház Központi Szervezetét (továbbiakban: MSZE Központi Szervezet) (mindkét szervezetre vonatkozó megállapítás esetében a továbbiakban: Egyház) és az MSZE vidéki Misszióinak adatkezelési gyakorlatát sérelmezték.

A panaszbeadványokban foglaltak személyes adatok jogellenes kezelését valószínűsítették. Emellett az is valószínűsíthető volt, hogy a jogellenes adatkezelés személyek széles körét és különleges adatokat is érint, ezért a Hatóság hivatalból adatvédelmi hatósági eljárást indított.

A Hatóság a tényállás tisztázása érdekében – előzetes értesítés mellőzésével – helyszíni szemléket tartott és iratokat, valamint elektronikus adathordozókat foglalt le.

A Hatóság szükségesnek tartotta számítástechnikai és informatikai igazságügyi szakértő, valamint klinikai pszichológiai igazságügyi szakértő közreműködését is.

V.18.2. A Dossziék típusai

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

Ilyen dosszié az úgynevezett PC dosszié, mely az Egyház legfőbb szolgáltatásai – az auditálás és a méregtelenítés – során keletkező feljegyzéseket, jegyzőkönyveket, jelentéseket tartalmazza. 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, továbbá a Munkatársi dosszié, melyben a munkatársi megállapodások, kvalifikációhoz szükséges nyomtatványok, interjúk, tesztek vannak összegyűjtve.

V.18.3. Az adatkezelések azonosítása

A Hatóság álláspontja szerint az áttekintett adatkezelési folyamat négy 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 dos sziékban jelenik meg;
III. Direkt marketing cél → Levelező dosszié;
IV. Személy és vagyonvédelmi cél → vagyonvédelmi kamera.

V.18.4. 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. Az auditálás során végzett tevékenységek eszközeinek és módszereinek vizsgálata alapján a pszichológus szakértő megállapította, hogy az auditálás során alkalmazott módszerek zömében tudatmódosulást indukálnak (gyakorlatilag hipnoterápiának tekinthetőek), de az ettől eltérő módszereik is a tudat beszűkítését és az alany szociális behódolását eredményezik. Mind a szuggesztív, tudatmódosító módszerek (hipnoterápia), mind pedig a biofeedback eljárás gyógyászati eljárás és álláspontja szerint egészségügyi tevékenységnek minősülnek, melynek során nagy mennyiségben kezeli az Egyház a hívők személyes és egészségügyi különleges adatait és harmadik személyek személyes adatait.

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, ez egy olyan program, amely kontrollált étkezésből, meghatározott típusú és mennyiségű vitaminok fogyasztásából, szaunázásból és fizikai gyakorlatból áll, és célja – a Szcientológia Egyház szerint – hogy az ember szervezetéből kitisztítsa és kitakarítsa a drog- vagy kémiai maradványokat, amelyek megakadályozhatják a Dianetika vagy Szcientológia auditálásokból/processzingből származó eredmények elérését.

A kirendelt igazságügyi pszichológus szakértő szakvéleménye szerint a szcientológiai „*méregtelenítés*" nevében teljesen megegyezik az orvostudományban is létező „*méregtelenítéssel*", noha attól teljességgel eltérő eljárás. Az tulajdonképpen hashajtás, izzasztás (futással és szaunázással) és extrém nagydózisú vitamin adása, amelynek semmi köze a tudományos orvosláshoz – izzadással és fokozott salakürítéssel ugyanis nem lehet az emberi szervezetet méregteleníteni.

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 (például: vérnyomás érték; van-e valamilyen tünete vérszegénységnek, szívbetegségnek, májbetegségnek, cukorbetegségnek, kábítószer fogyasztási szokások, szedett gyógyszerek, korábbi műtétek, stb.)

A Hatóság a PC dossziék esetében 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. 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 pontosan, 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.

A Méregtelenítő program esetében megállapította továbbá a Hatóság, hogy a felvett egészségügyi adatokat, állapotfelmérést és leleteket csak a vizsgáló or-

vos, egészségügyi szolgáltató kezelheti hozzájárulás alapján, pusztán az arra vonatkozó információ továbbításával, hogy az érintett megfelel-e vagy nem a programban való részvétel feltételeinek, de a nyilatkozat teljes tartalma az érintett részletes egészségügyi állapotfelmérésével és leleteivel a Hatóság álláspontja szerint vallási szervezetnek nem adható át.

Mindezekből következően az Egyház megsértette az Infotv. 20. § (2) bekezdését és az elégtelen előzetes tájékoztatás miatt megsértette az Infotv. 3. § 7. pontja szerinti hozzájárulásra vonatkozó követelményeket is.

A Hatóság megállapította azt is, hogy az Egyház az auditálás és méregtelenítés során különleges adatokat kezel, melyek kezelése vonatkozásában nem volt megállapítható, hogy azok kezelésére megfelelő jogalappal rendelkezne, figyelemmel arra is, hogy az adatkezelés célját vallási szolgáltatásként jelölte meg, és ez a cél nem illeszthető bele sem az egészségügyi és a hozzájuk kapcsolódó személyes adatok kezeléséről és védelméről szóló 1997. évi XLVII. törvény (a továbbiakban: Eüak.) 4. § (1) bekezdésébe – amely az egészségügyi ellátóhálózaton 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 részletezettek miatt nem támasztható alá.

A határozatban megállapított kiemelkedő súlyú jogsértés volt a harmadik személyek adatainak kezelése. Az Infotv. fogalomrendszere alapján 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 az egyes dokumentumokban harmadik személyek különleges adatát kezelte az Egyház, annak ellenére, hogy azok kezelésére nem rendelkezett felhatalmazással az érintettektől.

A tisztességes adatkezelés elve alapján a személyes adatok felvételének és kezelésének tisztességesnek és törvényesnek kell lennie. A személyes adatok védelméhez fűződő jogot sérti az adatkezelés, amennyiben az adatkezelő, bár eljárása formálisan megfelel a vonatkozó törvényi előírásoknak, tisztességtelen módon kezeli a személyes adatokat.

A célhoz kötött adatkezelés elve az adatkezelésre vonatkozó egyik legfontosabb, nemzetközileg kimunkált alapelv, amely értelmében személyes adat kizárólag meghatározott célból kezelhető. A cél csak társadalmilag indokolt, jog gyakor-

lása vagy kötelezettség teljesítése lehet. Az adatkezelésnek minden szakaszában, így például az adattovábbítás esetén is meg kell felelnie az adatkezelés céljának. Az adatkezelés célját előre meg kell határozni és közölni az érintettel, aki ily módon – az adatkezelés céljának ismeretében – megfelelően gyakorolhatja információs önrendelkezési jogát.

Az adatminimalizálás elve szerint az adatfelvételbe bevont érintettek körét és a cél eléréséhez szükséges adatfajtákat az adatkezelés célja határozza meg, ennél fogva csak olyan személyes adat kezelhető, amely az adatkezelés céljának megvalósulásához elengedhetetlen és a cél elérésére alkalmas. Ezen alapelv figyelembe vétele szavatolja, hogy az adatkezelés céljára tekintettel csupán a legszűkebb, indokolt adatkör kezelésére kerül sor. Az adatminimalizálás elve továbbá kizárja a készletezésre történő adatkezelést is, vagyis azt, hogy kizárólag olyan adatok felvételére kerüljön sor, amelyeket egy később meghatározott célra gyűjtenek.

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 MSZE 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 e harmadik személyeknek az Egyház nemcsak, hogy nem nyújt tájékoztatást az adatkezelési körülményekről, hanem úgy tartja nyilván e 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 az érintett 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 kívülálló 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 az érintettek magánszférájába.

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

Tehát az MSZE 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 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.

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, valamint a harmadik személyek személyes adatainak törlését és egyúttal megtiltotta a harmadik személyekre vonatkozó adatgyűjtési gyakorlatukat.

A PC dossziékhoz kapcsolódó jogsértésként állapította meg a Hatóság azt is, 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. Azonban követhetővé és ellenőrizhetővé

kell tenni az adatalany számára az adatkezelés útját, vagyis joga van tudni, hogy ki, mikor, milyen adatát és mire használja fel az adatkezelő.

V.18.5. A Munkatársi dossziék és az Életút kérdőív

Az eljárás másik fajsúlyos kérdése a Munkatársi dossziékban nyilvántartott adatok köre volt. Az Egyház Központi Szervezetében dolgozók alkalmazását megelőzően egy hosszadalmas felvételi procedúrán kell átesniük, melynek során többféle jelentkezési lapot, alkalmassági tesztet és kérdőívet kell kitölteniük, melyek rendkívül nagy mennyiségű személyes és különleges adatot szolgáltatnak az Egyház számára.

Az igazságügyi pszichológiai szakértő ezen tesztek kapcsán kiemelte, hogy azok alkalmazása szakmaiatlan, a kérdések sok esetben nem köthetőek semmilyen pszichológiai jellegzetességhez, túl általános témájúak, vagy egyértelműen nem megválaszolható elemeket tartalmaznak, a személy akkor válaszol helyesen, ha világképe megegyezik a szcientológia tanaival, azok vizsgáló módszerként való beállítása az alany azon előzetes tájékoztatása nélkül, hogy abból semmiféle megalapozott következtetés nem vonható le – szándékos félrevezetés.

A kitöltendő jelentkezési lapok közül kiemelkedik a 130 kérdést tartalmazó *„Életút kérdőív”* nevű dokumentum, melynek az Egyház által megjelölt célja a posztra való alkalmasság szűrése, a kitűzött magas etikai standardoknak való megfelelés, valamint az Egyházzal szembeni rosszhiszeműség és ártó szándék kiszűrése.

Az Életút kérdőívben rendkívül nagyszámú személyes adatot kér az Egyház. Például: az érintett adósságairól, esetleges hírszerző tevékenységéről, médiában, katonai szervezetekben, kormányban való részvételéről, kábítószer fogyasztási szokásairól, korábbi betegségeiről, műtéteiről, stb.. De nem csak az adott posztra jelentkező hívő személyes és különleges adatait kezeli, hanem harmadik személyek személyes és különleges adatait is, hiszen a jelentkezőnek teljes részletességgel be kell számolnia jelenlegi és korábbi párkapcsolatairól, szexuális szokásairól, továbbá meg kell adnia családtagjai és barátai ismert adatait is.

A Hatóság álláspontja szerint ezen adatkezelés jogszerűsége kérdésében is fontos szerepe van a *„célhoz kötött adatkezelés elve”* vizsgálatának. A cél meghatározásán túl a cél jogszerűsége is követelmény, vagyis az adatkezelésnek társadalmilag indokolt célra kell irányulnia, azaz személyes adat kizárólag jog gyakorlása és kötelezettség teljesítése érdekében kezelhető. A célhoz kötött adatke-

zelés elvéből következik, hogy a meghatározott cél nélküli, *„készletre”*, előre nem meghatározott jövőbeni felhasználásra való adatgyűjtés és -tárolás jogellenes.

A munkavégzésre irányuló jogviszonyokkal összefüggő adatkezelések általánosságban több csoportba sorolhatóak: egyes adatok kezelése jogszabályon alapul, ilyenek például a társadalombiztosítással, adózással, valamint a jogszabályban meghatározott egészségügyi alkalmassággal kapcsolatos adatok. Az adatok másik fontos, és adatvédelmi szempontból érzékeny köre az alkalmasságra vonatkozó adatkör. A munkáltató meghatározhatja az alkalmasság feltételeit, ezt jogosult ellenőrizni, és az ezzel kapcsolatos adatokat is ellenőrizni. Ebben a körben rendkívül változatos lehet az adatkezelés: végzettség, nyelvtudás, pszichikai alkalmasság, egyes készségek mérése. Egy további adatkör a munkavégzéssel összefüggésben keletkezik: minősítés, fegyelmi vétségek és büntetések. Megemlítendő még a munkavállalók ellenőrzésével összefüggő adatkezelés, melynek jogalapja a munkáltató jogos érdeke lehet.

Mindebből adódóan jogszerűnek minősülhet az olyan adatkezelési cél, amely a munkakörre, jelen esetben az egyházi posztra való alkalmasság megállapítására irányul. A Hatóság álláspontja szerint jogszerű adatkezelési cél lehet az alkalmasság vizsgálata, azonban figyelembe kell venni azt is, hogy milyen posztról is van szó, hiszen ahhoz igazodó alkalmassági feltételek írhatók elő.

Egyértelmű, hogy valamennyi foglalkoztatási jogviszonyban kezelni kell az érintett személyazonosításához szükséges adatokat, valamint azon adatokat, amelyek kezelését törvények előírnak (például: társadalombiztosítás, adózás). Egyebekben a célhoz kötött adatkezelés és a szükségesség elvének kell érvényesülnie.

Az Életút kérdőív esetében a munkakörre, posztra való alkalmasság megállapításához ugyanis csak olyan adatok kezelése valósulhat meg, amelyek a foglalkoztatási jogviszony – jelen esetben megbízási jogviszony – létesítése, teljesítése vagy megszűnése szempontjából lényegesek. Lényeges adat lehet az érintett iskolai végzettsége, nyelvtudása, szakmai tapasztalata – meghatározott esetben vallási meggyőződése. Ugyanakkor a Hatóság álláspontja szerint az MSZE Központi Szervezeténél betöltendő úgynevezett magasabb szintű szervezetvezetői – például ügyvezetői – posztok esetében az alkalmasság megállapításához – mint ahogyan az úgynevezett *„hétköznapi foglalkoztatási jogviszonyok”* esetében is elmondható – nem lényeges és nem lehetnek szükségesek, így nem kezelhetőek a kérdőívben szereplő különleges adatok. Ezen adatkörök: az egészségügyi adatok, kóros szenvedélyre vonatkozó adatok, bűnügyi személyes adatok, szexuális életre vonatkozó adatok, pénzügyi tartozásra vonatkozó

adatok, politikai véleményre, pártállásra vonatkozó adatok, érdek-képviseleti szervezeti tagságra, harmadik személyekre vonatkozó, illetve a harmadik személyekkel való kapcsolatra vonatkozó adatok.

A Hatóság álláspontja szerint egyházak számára nem jogszerű az olyan kérdések feltétele, mint amelyek az Életút kérdőívekben szerepelnek.

V.18.6. Etikai dossziék

A dossziéban lehetnek 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, az MSZE-ben 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.

Rendszeresen szerepelnek feljegyzések a dossziékban a hívők tartozásairól (adóhatóság, vagy magánszemélyek felé, illetve egyéb számlatartozások is fellelhetőek), hiteleiről.

Ebben az aktatípusban szerepelnek a saját belső igazságszolgáltatásukkal 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 belső igazságszolgáltatási eljárásról készült dokumentumok jellemzően angol nyelven íródtak, illetve a magyar nyelven született bizonyítékok angol nyelvre is le voltak fordítva. Ezek az akták nagyon részletes, *„világi”* bírósági bizonyítási eljáráshoz hasonló eljárásokat felvonultató eljárások. Megtalálható bennük az ügy tárgyához kapcsolódó összes *„Tudomásjelentés”* és más jelentések, egészségügyi adatokat, TAJ számot tartalmazó (például: bántalmazással kapcsolatban született) ambuláns lap, járóbeteg vizsgálati lap, orvosszakértői vélemények, vagy például egy adott ügyben a peres fél szexuális életről, prostitúcióról szóló

kihallgatások jegyzőkönyvei, valamint a Munkatársi dossziékban megismert, kitöltött Életút kérdőív is megtalálható néhány dossziéban.

A Hatóság e dossziétípus 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.

V.18.7. Levelező dossziék és direkt marketing

A Hatóság ebben a körben a Central File elnevezésű levelező dossziékban és az elektronikus tagnyilvántartásnak tekinthető, úgynevezett Addresso adatbázisban található személyes adatok kezelésének jogszerűségét tekintette át. A Hatóság megvizsgálva az Egyház által a direkt marketing célú adatkezelésekhez használt különböző papír alapú nyomtatványaikat, honlapon történő könyvértékesítés és online tesztek kitöltésére szolgáló oldalakon alkalmazott tájékoztatókat, valamint az Addresso elnevezésű elektronikus adatbázist, két vonatkozásban találta jogsértőnek az Egyház marketing célú adatkezelését:

- nem szerzett be megfelelő hozzájárulást az érintettektől, valamint
- nem állapítható meg az érintettek hozzájárulásának forrása.

V.18.8. Rendelkező rész és a bírságkiszabás

A Hatóság a fentiek miatt megtiltotta a Kötelezettek további jogellenes adatkezelését és felszólította őket arra, hogy 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 sem minősülő harmadik személyek személyes adatainak gyűjtésére vonatkozó gyakorlatukat és elrendelte az így kezelt személyes adatok törlését is. Felszólította továbbá a Kötelezetteket arra, hogy gondoskodjanak a külföldre történő adattovábbítás megszüntetéséről.

A Hatóság mindezeken felül 20-20 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.

V.19. Kulcsocska, a NAIH gyermekjogi projektjének folytatása

A magyar adatvédelmi hatóság kiemelt figyelmet fordít a gyermekek személyes adatainak védelmére, ezért született meg 2013-ban a 10-16 éves gyerekek internetezési szokásairól szóló, *Kulcs a net világához!* című tanulmánykötetünk (mely 2016-ban második kiadást is megért, felfrissítve és kiegészítve az aktuális témákat). 2014-ben Vastag Tamás dalával indítottuk útjára figyelemfelhívó médiakampányunkat és csatlakoztunk 2015-ben az ARCADES elnevezésű uniós projekthez, melynek eredményeképp (magyar nyelven is) pedagógusoknak szóló adatvédelmi kézikönyvek születtek.[41]

A cél minden esetben ugyanaz: a gyermekeket, fiatalokat közvetlenül, és az értük felelős, őket nevelő felnőttek segítségével hozzásegíteni ahhoz, hogy a modern digitális világban tudatosan éljenek, az eszközökkel nem csak ügyesen, de hozzáértően bánjanak és magukért, valamint másokért is felelősséget vállaljanak a virtuális valóságban is.

A 2000 után született úgynevezett *„szuper-most”* generáció esetében az internethasználatnál már olyan jellegzetességek láthatók, amik a korábban születettekre nem jellemző. Az óvodának a szocializációban óriási a szerepe, hiszen itt kezdődik el a csoportban, közösségben létezés, amin az iskolai teljesítménykényszer még egyet *„csavar”*. Minden kornak meg van a maga sajátos tanulási folyamata, ezek, ha rosszul rögződnek, később komoly gondokat tudnak okozni egyéni, családi, de akár társadalmi szinten is.

Az ez irányú nevelést nem lehet elég korán elkezdeni, mert a személyes adatok védelme egyfelől minden élő személyt kortól függetlenül megillet – ahogy a veszélyek is elérik –, másfelől a digitális eszközhasználat korhatára egyre jobban csúszik lefelé. Ezen nem is lehet csodálkozni, hiszen egy kisbaba napjainkban már egy olyan környezetbe születik bele, ahol a mobiltelefon, a számítógép és egyéb eszközök a mindennapi használati tárgyak sorába illeszkednek, sőt, néhol és némelyek számára ezek talán fontosabbak bárminél. Amíg azonban egy kamasz gyermeknél az önálló döntéshozatalra való felkészítésen van a hangsúly, egy 10 év alatti kisgyermeknél még a védelem az elsőrangú szempont.

2017-ben a NAIH a 10 év alatti kisgyermekekre koncentrált. *Kulcsocska a net világához!* című tanulmánykötetünk arra tesz kísérletet, hogy feltérképezze azokat a veszélyforrásokat, amik az óvodás- és kisiskolás korosztály magánéletét,

41 https://www.naih.hu/adatvedelemr-l-fiataloknak--kulcs-a-net-vilagahoz--projekt.html

személyes adatainak védelmét és ezáltal egészséges fejlődését leginkább károsíthatja. Egy saját kezdeményezésű, összesen 131 szülő és 66 pedagógus válaszain alapuló felmérés adatait is felhasználva megállapítható, hogy a világháló felől érkező veszélyek már elérik, elérhetik a legfiatalabb korosztályokat is, és erre az őket nevelő felnőtteket fel kell készíteni. Így többek között a játékfüggőség, a szülői szorongásokkal visszaélő *„kuruzslók”*, a *„modellkedés”* és szépségversenyek buktatói, a digitális gyerekrablás vagy a szülői felügyeleti jog gyakorlásával összefüggő konfliktusok mind egy-egy külön fejezetet kaptak a kötetben.

Célunk semmiképp sem az elrettentés, sokkal inkább a figyelemfelhívás azokra a jelenségekre, melyek a legfiatalabb korosztályokat a digitális térből érinthetik napjainkban és a jövőben. Tesszük ezt egyrészt társadalmi felelősségvállalásként, de az adatvédelmi felügyelő hatóságokat terhelő kötelezettségünk végrehajtásaként is, hiszen a 2018. májusban életbe lépő új uniós általános adatvédelmi rendelet (GDPR) a gyermekek adatainak védelmét és az erről szóló felvilágosító munkát kiemelt feladatként kezeli.

VI. Adatvédelmi Audit és BCR-ek

VI.1. Kötelező szervezeti szabályozás

A NAIH 2017-ben 14 kötelező szervezeti szabályozást (a továbbiakban: BCR) hagyott jóvá. A jóváhagyott BCR-ek mindegyikének esetében sor került a NAIH általi jóváhagyást megelőzően a 29-es Munkacsoport WP 107-es munkadokumentuma szerinti együttműködési eljárás lefolytatására, illetve a vezető hatóság jóváhagyására.

A NAIH az alábbi adatkezelők (vagy adatkezelők csoportja) által alkalmazott BCR-okat hagyta jóvá 2017-ben, amelyeknek megnevezését az érintettek tájékoztatása érdekében a honlapunkon is közzé tettük:

Jóváhagyás dátuma	**Vállalatcsoport megnevezése**	**A BCR-t Magyarországon alkalmazó adatkezelők megnevezése**
2017.11.29	IBM	IBM Magyarországi Kft.
2017.11.29	IBM	IBM Data Storage Systems Információtechnológiai Kft.
2017.11.29	IBM	IBM Hungary International Shared Service Centre Kft.
2017.11.29	IBM	IBM Capital Hungary Kft.
2017.11.29	Schneider Electric	Schneider Electric Hungária Villamossági Zrt.
2017.11.29	Schneider Electric	SE-CEE Kft.
2017.11.29	Schneider Electric	M&C Energia Kft.
2017.11.29	Schneider Electric	Schneider-Electric Energy Magyarország Villamos Kapcsolóberendezések Gyártó Kft.
2017.10.30	Cardinal Health	Cardinal Health Poland spółka z organiczoną odpowiendzialnością
2017.10.04	Atos	ATOS Magyarország Kft.
2017.10.04	Atos	Atos International Kft.
2017.10.04	Atos	Unify Communications Szolgáltató Kft.
2017.07.11	Merck Sharp & Dohme (MSD)	Intervet Hungária Kft.

2017.07.11	Merck Sharp & Dohme (MSD)	MSD Pharma Hungary Kft.
2017.05.23	Michelin	Michelin Hungária Abroncsgyártó Kft.
2017.05.23	Accenture	Accenture Tanácsadó Kft.
2017.05.23	Accenture	Accenture Industrial Software Solutions Kft.
2017.05.12	Sanofi Aventis	CHINOIN Zrt.
2017.05.12	Sanofi Aventis	SANOFI-AVENTIS Zrt.
2017.04.25	Mastercard	Mastercard Europe SA Magyarországi Kereskedelmi Képviselete
2017.03.31	ENGIE	GDF SUEZ Energia Holding Hungary Zrt.
2017.03.31	ENGIE	Égáz-Dégáz Földgázelosztó Zrt.
2017.03.31	ENGIE	COTHEC Energetikai Üzemeltető Kft.
2017.03.31	ENGIE	COFELY Épületgépészeti Kft.
2017.03.31	ENGIE	FABRICOM ELECTRICAL-PVV Villanyszerelő Ipari Kft.
2017.03.13	DSM	DSM Nutritional Products Hungary Kft.
2017.03.08	Legrand	Legrand Magyarország Villamossági Rendszerek Zrt.
2017.03.08	Legrand	Legrand Közép- és Kelet-európai Disztribúciós Kft.
2017.01.25	JACOBS DOUWE EGBERTS	JACOBS DOUWE EGBERTS HU Zrt.
2017.01.17	Siemens	Siemens Zrt.

VI.2. Adatvédelmi audit

Az Infotv. módosítás tervezete (a továbbiakban: tervezet) megszünteti az adatvédelmi audit intézményét, szerepét a GDPR-ban az adatvédelmi tanúsítás tölti be. Ezzel lezárul egy rövid, 2013-tól tartó időszak, amikor a magasabb szintű adatvédelmi megfelelést kívánó adatkezelők önkéntes alapon, az adatvédelmi hatósággal ellenőriztethették adatkezeléseiket. Az elmúlt évek auditált adatkezelőitől kapott visszajelzések alapján egy sikeres és hasznos eszköz szűnik meg, amely a Hatóság számára is nyújtott visszajelzést az adatkezelők számára fontos témakörökről, amely által az auditok tapasztalatai a Hatóság ajánlásaiban is megjelenhettek.

VII. Információszabadság

A 2017. év alapvetően az általános adatvédelmi rendeletre történő felkészülés jegyében telt mind közfeladatot ellátó szervek, mind pedig a Hatóság szempontjából. Az új adatvédelmi szabályoknak való megfelelés azonban nem jelentette azt, hogy a másik információs jog, az információszabadság háttérbe szorult volna. Éppen ellenkezőleg, a Hatóság a korábbinál is nagyobb figyelmet fordított a közérdekű és közérdekből nyilvános adatok megismeréséhez és terjesztéséhez fűződő jog érvényesítésére, az azzal kapcsolatos teendők ellátására, valamint az információszabadsággal kapcsolatos kötelezettségek tudatosítására.

A Hatóság az elmúlt évekhez hasonlóan kiemelten foglalkozott a közpénzek és a nemzeti vagyon kezelésére, felhasználására vonatkozó adatok nyilvánosságával. Az említett közjavakkal való gazdálkodást mindenkor az átláthatóság és a közélet tisztasága elvének betartásával, annak megfelelően kell végezni. Ezen alaptörvényben is nevesített értékek, célok megvalósulásához elengedhetetlenül fontos az információszabadság megléte és érvényesülése.

Ebben az évben a Hatóság tovább szélesítette, fejlesztette gyakorlatát a közérdekű adatigénylések teljesítéséért megállapítható költségtérítés szabályainak alkalmazási területén. 2017 volt ugyanis az első olyan év, amelyben a vonatkozó előírások már az év egészében hatályban voltak. A közfeladatot ellátó szervek esetenként oly módon alkalmazták a költségtérítés szabályait, amelyek több alkalommal is jogsértéshez vezettek. A Hatóság ezért minden ügyben igyekezett nem csak az adott ügy szempontjából lényeges tényeket, körülményeket mérlegelni, hanem általános útmutatást is nyújtani az érintett szervek, személyek részére.

Végezetül kiemelendő, hogy a Hatóság továbbra is aktív szerepet vállalt a korrupció megelőzésével összefüggő állami feladatok ellátásában. Emellett a Hatóság aktívan részt vett az információszabadsággal foglalkozó nemzetközi és európai fórumokon is. E konferenciák célja mindenekelőtt a szorosabb nemzetközi együttműködés elősegítése, valamint a különböző nemzeti gyakorlatok közelítése volt.

VII.1. A nemzeti vagyon és a közpénzek felhasználásának átláthatósága

Alapvető társadalmi elvárás, hogy a polgárok közössége ellenőrizze a közpénzek és a nemzeti vagyon felhasználását. Az említett vagyonelemek kezelésének felügyeletét ezért az alkotmányos kontrollmechanizmusok – az Állami Számve-

vőszék, a Kormányzati Ellenőrzési Hivatal és a nyomozó hatóságok eljárásai – mellett az információszabadság érvényre juttatása is szolgálja. A közérdekű és közérdekből nyilvános adatoknak a sajtó, a civil szervezetek, illetve a társadalom tagjai számára biztosított megismerhetősége és terjesztésének lehetősége így mindenkor a demokratikus jogállam egyik legfontosabb értéke és egyben célja is.

A hatályos jogszabályi környezet – az Alaptörvény és annak Nemzeti hitvallása szellemében – a tisztességes közélet, a nemzeti vagyonnal való felelős gazdálkodás és annak előfeltételeként a nyilvánosság általi ellenőrizhetőséget is megteremti. Ennek megfelelően az Alaptörvény, a nemzeti vagyonról szóló 2011. évi CXCVI. törvény (Nvtv.) és az állami vagyonról szóló 2007. évi CVI. törvény (Ávtv.) rendelkezései, valamint az Infotv. irányadó szabályai mind az átláthatóság, az elszámoltathatóság és a közélet tisztaságának elveit hivatottak érvényre juttatni. A közpénzek és a nemzeti vagyon felhasználására vonatkozó adatok nyilvánosságát pedig mindenekelőtt a NAIH felügyeli.

A Hatóság 2017. folyamán is számos esetben vizsgálta a közpénzek és a nemzeti vagyon felhasználásának átláthatóságát. Ezek során a NAIH abból indult ki, hogy – az Alaptörvény sokszor idézett rendelkezése értelmében – *„[a] közpénzekkel gazdálkodó minden szervezet köteles a nyilvánosság előtt elszámolni a közpénzekre vonatkozó gazdálkodásával. A közpénzeket és a nemzeti vagyont az átláthatóság és a közélet tisztaságának elve szerint kell kezelni. A közpénzekre és a nemzeti vagyonra vonatkozó adatok közérdekű adatok”*.[42]

Ezen alkotmányos követelmény kiterjed a közpénzekkel való gazdálkodás követhetőségére, átláthatóságára, a nemzeti vagyon átengedésének nyilvánosság előtti elszámoltathatóságára is. Az Alaptörvény 39. cikk (2) bekezdése így tulajdonképpen a közhatalom gyakorlásának, a közpénzek felhasználásának egyik legfontosabb korlátját fogalmazza meg. A nyilvánosság általi ellenőrizhetőséget egyrészt az egyének alapjogának deklarálásával biztosítja, másrészt – azt egyértelműsítve, kiegészítve – a közpénzek felhasználásával kapcsolatos adatokat közérdekű adattá nyilvánítja, harmadrészt az átláthatóságot a közfeladatot ellátó szervek, a közpénzekkel gazdálkodó szervek alkotmányos kötelezettségévé teszi.

A nemzeti vagyon alapvető rendeltetése a közfeladatok ellátásának biztosítása.[43] A nemzeti vagyonnal felelős módon, rendeltetésszerűen kell gazdálkodni. A nemzeti vagyongazdálkodás feladata a nemzeti vagyon rendeltetésének meg-

42 Alaptörvény 39. cikk.
43 Nvtv. 7. §-a.

felelő, az állam, az önkormányzat mindenkori teherbíró képességéhez igazodó, elsődlegesen a közfeladatok ellátásához és a mindenkori társadalmi szükségletek kielégítéséhez szükséges, egységes elveken alapuló, átlátható, hatékony és költségtakarékos működtetése, értékének megőrzése, állagának védelme, értéknövelő használata, hasznosítása, gyarapítása, továbbá az állam vagy a helyi önkormányzat feladatának ellátása szempontjából feleslegessé váló vagyontárgyak elidegenítése. A nemzeti vagyont, annak értékét és változásait a tulajdonosi joggyakorló nyilvántartja. Az érték nyilvántartásától el lehet tekinteni, ha az adott vagyontárgy értéke természeténél, jellegénél fogva nem állapítható meg.[44] A nyilvántartásnak tartalmaznia kell a vagyon elsődleges rendeltetése szerinti közfeladat megjelölését is. A nyilvántartási adatok – a minősített adatok kivételével – nyilvánosak.

Emellett a NAIH azt is figyelembe vette, hogy az Alkotmánybíróság a 25/2014. (VII. 22.) AB határozatban mindenkire nézve kötelező erővel megerősítette, hogy az állami vagyonnal gazdálkodó vagy azzal rendelkező szervek és személyek az Infotv. szerinti közfeladatot ellátó szerveknek minősülnek.[45] Az állami vagyonnal való gazdálkodásra és az azzal való rendelkezésre vonatkozó, közérdekű adatnak nem minősülő adatok pedig közérdekből nyilvánosak.[46] Az Alkotmánybíróság tehát egyértelműen megerősítette, hogy az átláthatóság követelménye általánosságban kiterjed az állami vagyonnal gazdálkodó szervekre és személyekre, tovább erősítve a közpénzek, az állami vagyon működtetésének átláthatóságát és ellenőrizhetőségét.

Összefoglalóan megállapítható, hogy a jelenlegi jogszabályi környezet nem csak arra helyezi a hangsúlyt, hogy valamely szerv, személy jogszabályban meghatározott tényleges közfeladatot lát-e el, hanem a nemzeti vagyonnal való rendelkezés és gazdálkodás tényére is. Az Alaptörvény, illetőleg az annak cikkeit részletekkel megtöltő törvényi rendelkezések tehát kétszeresen biztosítják a közpénzekkel való gazdálkodás átláthatóságát. Egyrészt az adatokra vonatkozóan már maga az Alaptörvény kimondja azok közérdekű és közérdekből nyilvános adat minőségét. Mivel ez Magyarország jogrendszerének alapja, megállapítható, hogy közpénzekkel való gazdálkodás átláthatósága a legmagasabb, alkotmányos szinten biztosított. Másrészt, az Ávtv., valamint az Nvtv. szabályaira tekintettel alkalmazni kell ebben a vonatkozásban az Infotv. közérdekű és közérdekből nyilvános adatok megismerhetőségére vonatkozó rendelkezéseit is.

44 Nvtv. 10. § (1) bekezdés.
45 Ávtv. 5. § (2) bekezdés.
46 Ávtv. 5. § (1) bekezdés.

1.) Az egyik ügyben a NAIH-hoz konzultációs beadvány érkezett, melyben a beadványozó azzal kapcsolatban kért állásfoglalást, hogy a Pallas Athéné Alapítványoknál, valamint egy általuk alapított gazdasági társaságnál munkavállalók munkabére és az őket megillető egyéb juttatások nyilvános adatok-e[47].

A NAIH az állásfoglalásában mindenekelőtt azt mérlegelte, hogy a Pallas Athéné Alapítványok, valamint az általuk alapított gazdasági társaság közfeladatot ellátó szerveknek minősülnek-e. Ebben a tekintetben a Hatóság figyelembe vette, hogy a Magyar Nemzeti Bankról szóló 2013. évi CXXXIX. törvény (MNBtv.) 162. § (2) bekezdése értelmében a Magyar Nemzeti Bank (MNB) feladataival és elsődleges céljával összhangban, többségi tulajdonában álló gazdasági társaságot alapíthat vagy alapítványt hozhat létre. Az Alkotmánybíróság a 8/2016. (IV. 6.) AB határozatban ezzel összefüggésben kifejtette, hogy *„[a]mennyiben az állami tulajdonban álló MNB gazdasági társaságot vagy alapítványt hoz létre, akkor az alapítás során nyújtott vagyoni hozzájárulás, illetve az alapítványnak juttatott, a működéshez szükséges vagyon (induló vagyon és később nyújtott támogatás) forrása szükségképpen közpénz”*.[48]

Az Alkotmánybíróság az említett döntés indokolásában megállapította, hogy *„az MNB által alapított, és többségi vagy kizárólagos tulajdonában – tehát az irányítása alatt – álló gazdasági társaságok, valamint az MNB által létrehozott alapítványok közpénzt kezelnek, ebből következően pedig – tekintettel az Alaptörvény 39. cikk (2) bekezdésére – az Alaptörvény VI. cikk (2) bekezdése és a vonatkozó törvények megfelelő előírásai szerint az általuk kezelt közérdekű és közérdekből nyilvános adatok vonatkozásában az adatnyilvánosság biztosítására kötelesek”*.[49] Következésképpen, mind a Pallas Athéné Alapítványok, mind pedig az általuk alapított gazdasági társaság közfeladatot ellátó szervnek minősül az Infotv. rendelkezései értelmében.

Ezt követően a NAIH azt vizsgálta meg, hogy az e szerveknél a Munka Törvénykönyvéről szóló 2012. évi I. törvény alapján foglalkoztatott munkavállalók munkabére és egyéb juttatásai az Infotv. és más jogszabályok értelmében közérdekből nyilvános adatok-e. A Hatóság ezzel kapcsolatban hangsúlyozta, hogy az alapítványok, valamint a gazdasági társaság munkavállalói, mint a közfeladatot ellátó szerv a közfeladatot ellátó szerv feladat- és hatáskörében eljáró személyek vonatkozásában is megállapítható egy bizonyos adatkör, amely tekintetében a nyilvánosságnak kell érvényt szerezni. Az érintett munkavállalók

47 NAIH/2017/871/V számú ügy.
48 8/2016. (IV. 6.) AB határozat, Indokolás [19].
49 8/2016. (IV. 6.) AB határozat, Indokolás [29].

azok, akiknek tevékenysége az adott közfeladatot ellátó szerv jogszabályban nevesített feladatkörébe tartozik. Esetükben elsősorban az Infotv. 26. § (2) bekezdésében felsorolt információk lesznek bárki számára megismerhetőek: a munkavállaló neve, feladatköre, munkaköre, vezetői megbízása.

A fenti adatkörön túl azonban a munkavállalók más, a közfeladat ellátásával összefüggő egyéb személyes adata is közérdekből nyilvánosnak minősülhet az Infotv. 26. § (2) bekezdése alapján. Mivel közpénzek felhasználásáról van szó, az átláthatóság és ellenőrizhetőség – mint közérdek – kiemelt fontosságú. Emiatt pedig az érintett munkavállalók részére kifizetett munkabér, valamint a rendszeres, eseti, pénzbeli és természetbeni juttatások, így a szabadságmegváltás, jutalom, helyettesítési díj, kereset-kiegészítés, céljuttatás összege a közfeladat ellátásával összefüggésben keletkezett személyes adatnak minősülnek, azokat bárki megismerheti.

Ugyanakkor az információszabadságnak és az információs önrendelkezési jognak egymásra tekintettel kell érvényesülnie, így a közfeladat ellátásával összefüggő egyéb személyes adatok körének meghatározásánál figyelembe kell venni, hogy azok nyilvánossága nem sérti-e aránytalanul a magánszférához való jogot.

A NAIH vonatkozó gyakorlata értelmében ezért azokra az alkalmazottakra vonatkozó – Infotv. 26. § (2) bekezdése szerinti – információk, akiknek a tevékenysége nem kapcsolódik közvetlenül az adott szerv közhatalmi feladatainak ellátásához, nem ismerhető meg. Ebbe a körbe tartoznak – többek között – azon munkavállalók, akik nem vesznek részt a döntések meghozatalában, sem mint a döntések előkészítői, sem mint döntéshozók. Példaként említhetők a gépkocsivezetők, takarító személyzet stb.

2.) Egy másik ügyben egy adatigénylő a NAIH vizsgálatát kérte egy, az MVM Magyar Villamos Művek Zrt. (MVM) által nem teljesített közérdekű adatigényléssel kapcsolatban[50]. Az adatigénylés tárgya a Civil Összefogás Közhasznú Alapítvány (CÖKA) részére nyújtott támogatással kapcsolatos dokumentumok másolataira irányult. Az MVM megtagadta az adatigénylés teljesítését, mivel szerinte a *„támogatásait nem közpénzből, hanem saját forrásból fedezi”*, így az azokkal kapcsolatos információk nem estek az Infotv. 26. § (1) bekezdésének hatálya alá.

50 NAIH/2017/4100/V számú ügy.

A NAIH a vizsgálat során megállapította, hogy – a nyilvánosan elérhető cégadatok értelmében – az MVM egyedüli részvényese a Magyar Állam, amely a tulajdonosi jogait a Magyar Nemzeti Vagyonkezelő Zrt.-n keresztül gyakorolja a társaságban. Az MVM tehát – tekintettel az Nvtv. és az Ávtv. vonatkozó rendelkezéseire – a nemzeti, illetőleg az állami vagyon körébe tartozik. Ebből következően az MVM közfeladatot ellátó szervnek minősül, amely köteles a közérdekű és közérdekből nyilvános adatok megismeréséhez fűződő jog érvényre juttatására.

A NAIH az ügyben hozott állásfoglalásában kimondta továbbá, hogy az MVM központi költségvetési szervnek minősülnek. Az MVM ezért megsértette az adatigénylő közérdekű adatok megismeréséhez fűződő alkotmányos alapjogát azáltal, hogy megtagadta az általa igényelt adatok rendelkezésre bocsátását.

3.) A NAIH hasonló álláspontot fogalmazott meg egy, az Antenna Hungária Zrt. által jogellenesen megtagadott közérdekű adatigényléssel kapcsolatosan folytatott vizsgálat kapcsán is[51]. Ebben az ügyben a társaság arra hivatkozott a NAIH első felszólítására küldött válaszlevelében, hogy a saját piaci tevékenységéből származó bevételek nem tartoznak a központi költségvetés fogalmi körébe, amellett, hogy tagadta közfeladatot ellátó szervi minőségét.

A Hatóság állásfoglalásában ezért ismételten felhívta a társaság figyelmét arra, hogy a köztulajdonban álló gazdasági társaságok közfeladatot ellátó szervi minőségét több tényező is megalapozza. Egyrészt ezek az entitások állami és önkormányzati tevékenységek, feladatok széles körét ellátják. Maguk a jogszabályok nevesítik azokat a konkrét gazdasági társaságokat, amelyek kiemelt közfeladatokat látnak el. Másrészt az állami vagy önkormányzati tulajdonban álló gazdasági társaságok rendelkezésére álló – anyagi és egyéb – eszközök az állami vagy a nemzeti vagyon körébe tartoznak.[52] E vállalkozások így annak kezelésével, felhasználásával összefüggésben hoznak döntéseket. Márpedig a nemzeti vagyon alapvető rendeltetése – az Nvtv. 7. § (1) bekezdésére tekintettel – kizárólag közfeladatok ellátásának biztosítása lehet. Az állami vagyonnal gazdálkodó szervek pedig az Ávtv. 5. § (2) bekezdése értelmében közfeladatot ellátó szerveknek minősülnek. Utóbbi jogszabályi rendelkezés vonatkozásában az

51 NAIH/2017/5250/V számú ügy.
52 8/2016. (IV. 6.) AB határozat, Indokolás [22].

annak hatálya alá tartozó szervezeteknek kizárólag az Ávtv. korábban hatályos mellékletében meghatározott körre szűkítése egyet jelentene az említett előírás kiüresítésével, következésképpen pedig az információszabadság alapjogának alaptörvény-ellenes korlátozásához vezetne.

A fentiekből következően egy állami vagy önkormányzati tulajdonban álló gazdasági társaság *„jogszabályban meghatározott egyéb közfeladatot ellátó szervként az általa kezelt közérdekű [és közérdekből nyilvános] adatok megismerhetővé tételére köteles”*.[53] Márpedig az Infotv. 3. § 5. pontja alapján a közérdekű adatok körébe minden olyan információ beletartozik, amely az adott közfeladatot ellátó szerv tevékenységére vonatkozik vagy közfeladatának ellátásával összefüggésben keletkezett, *„különösen a hatáskörre, illetékességre, szervezeti felépítésre, szakmai tevékenységre, annak eredményességére is kiterjedő értékelésére, a birtokolt adatfajtákra és a működést szabályozó jogszabályokra, valamint a gazdálkodásra, a megkötött szerződésekre vonatkozó adat”*. A vonatkozó jogszabályok ugyanakkor nem tartalmaznak kivételt közfeladatot ellátó szerv *„gazdálkodása”* tekintetében, így ebbe a körbe mind az állami vagy önkormányzati, mind pedig a piaci forrásból szerzett pénzeszközök beletartoznak. Az Antenna Hungária Zrt. eljárása így továbbra sem volt tekintettel a közérdekű adatok megismeréséhez fűződő alkotmányos alapjogra.

4.) Egy másik ügyben a NAIH a Bp2017 Nonprofit Kft. által nem teljesített közérdekű adatigényléssel kapcsolatban folytatott le vizsgálatot[54]. Ennek során a hatóság hangsúlyozta, hogy a társaság, mint nemzeti vagyonnal rendelkező szerv nem utasíthatta volna el az általa megkötött egyes szerződések rendelkezésére bocsátására irányuló adatigénylést az Infotv. 27. § (3) és (3a) bekezdései alapján arra hivatkozással sem, hogy az abban foglalt egyes adatok egy része nem megismerhető. Az úgynevezett adat-elv értelmében ugyanis az adott dokumentumban nyilvánosság-korlátozás hatálya alá eső adatokat felismerhetetlenné kell tenni, míg a megismerhető adatokat az igénylő által kívánt formában, illetve módon rendelkezésre kell bocsátani.[55] A NAIH ezért megállapította, hogy a Bp2017 Nonprofit Kft. megsértette az Infotv. vonatkozó rendelkezéseit.

5.) A NAIH vizsgálta egy, a www.gyal.hu honlapon közzétett közvilágítás korszerűsítésével kapcsolatos vállalkozási szerződés mellékletének nyilvánossága kérdését is. Gyál város polgármesteri hivatala ugyanis csak részben teljesítette a vonatkozó adatigénylést, mivel az – álláspontja szerint – üzleti információkat is

53 25/2014. (VII. 22.) AB határozat, Indokolás [46].
54 NAIH/2017/2725/V számú ügy.
55 Infotv. 30. § (1)-(2) bekezdései.

érintett volna. A NAIH az eljárása során a megismerni kívánt dokumentumokat (több, mint 350 oldal) és az abban feltüntetett adatokat részletesen áttekintette. Ezt követően megállapította, hogy a dokumentumok egyes részeiben szereplő adatok nyilvánossága – a törvény erejénél fogva közérdekből nyilvános (személyes) adatok (kamarai nyilvántartás, cégnyilvántartás) kivételével – jogszerűen korlátozhatóak *méltányolható üzleti érdekből, azaz a Polgári Törvénykönyvről szóló 2013. évi V. törvény 2:47. §*-ra, valamint az Infotv. 27. § (3) bekezdésére tekintettel. Az állásfoglalásban meg nem jelölt adatok megismerése ugyanakkor nem okozhat az üzleti tevékenység végzése szempontjából aránytalan sérelmet, így azokat az adatigénylő rendelkezésére kellett volna bocsátani, mely a vizsgálat nyomán meg is történt.

6.) A NAIH vizsgálta a Heves Megyei Vállalkozás- és Területfejlesztési Alapítvány (Alapítvány) eljárását is azzal kapcsolatban, hogy megtagadta egy olyan közérdekű adatigénylés teljesítését, amely – álláspontja szerint – sértette volna ügyfeleinek személyes – titoktartás körében felmerült – érdekeit.[56] A Hatóság az eljárás során megállapította, hogy az Alapítvány alapítói között megtalálható többek között Heves Megye Önkormányzata, Eger Megyei Jogú Város Önkormányzata, Hatvan Város Önkormányzata, valamint a Magyar Vállalkozásfejlesztési Alapítvány is. A NAIH ezért – nemzeti vagyonnal való gazdálkodás átláthatóságára vonatkozó szabályokra tekintettel – nem tartotta elfogadhatónak, hogy a közfeladatot ellátó szerv titoktartási megállapodást kössön ügyfeleivel a kezelésében lévő közérdekű és közérdekből nyilvános adatok nyilvánosságának korlátozása céljából. Az Alapítvány átlátható és elszámoltatható működéséhez így szorosan kapcsolódik, hogy az egyébként közpénzekkel gazdálkodó szervezet részleteiben is bemutassa az adatigénylő részére az általa kért adatokat.

7.) A NAIH vizsgálatot indított azzal kapcsolatban is, hogy közérdekből nyilvános adatnak minősül-e az, hogy a Magyar Edzők Társasága (MET) milyen havi juttatásban részesíti Shane Tusupot, Hosszú Katinka edzőjét, a Kiemelt Edzői Program (KEP) keretében.

A Hatóság az eljárás során egyrészt megállapította, hogy a KEP működtetésének és finanszírozásának pénzügyi forrását a Magyarország központi költségvetéséről szóló törvény kiemelt sportágak fejlesztésének sportszakmai támogatását szolgáló fejezeti kezelésű előirányzata biztosítja. Ebből következően a KEP keretében kezelt pénzek közpénznek minősülnek, így az azokra vo-

56 NAIH/2017/1368/V számú ügy.

natkozó információk az Alaptörvény értelmében közérdekű adatok.[57] A hatályos törvényi rendelkezések másrészt előírják, hogy az a természetes személy, aki az államháztartás alrendszerébe tartozó valamely személlyel pénzügyi vagy üzleti kapcsolatot létesít, köteles e jogviszonnyal összefüggő közérdekből nyilvános adatokra vonatkozóan bárki számára tájékoztatást adni.[58] Ebbe a körbe tartozik – többek között – az Emberi Erőforrások Minisztériuma és a MET között kötött támogatási szerződés összegének Shane Tusupra eső részösszege is.

Végezetül a NAIH figyelembe vette, hogy Shane Tusup részére a MET-tel fennálló munkaviszonya keretében juttatott munkabér az Infotv. szerint közérdekből nyilvános adatnak minősül.[59] Amennyiben ugyanis nem biztosított annak megismerése, hogy a KEP-ben résztvevő szakemberek milyen juttatásra jogosultak, nem biztosított a közpénzek felhasználásának Alaptörvény által lehetővé tett ellenőrzése sem.

VII.2. Az adatigénylés teljesítéséért megállapítható költségtérítés szabályai

A közfeladatot ellátó szerveknek az Infotv. módosítás hatályba lépésétől (2015. október 1-től) lehetősége van arra, hogy – meghatározott esetekben – költségtérítést állapítsanak meg a közérdekű adatigénylések teljesítéséért. A Kormány 2016-ban fogadta el a közérdekű adat iránti igény teljesítéséért megállapítható költségtérítés mértékéről szóló 301/2016. (IX. 30.) Korm. rendeletet (Rendelet), amely 2016. október 15-én lépett hatályba. A Rendelet hatályba lépése óta eltelt több mint egy év jogalkalmazói gyakorlatban felmerült tapasztalatai, és a Hatóság által megfogalmazott iránymutatások a következőkben foglalhatók össze.

Az adatigénylések teljesítéséért felszámítható költségtérítés kapcsán mindenekelőtt hangsúlyozandó, hogy – az Infotv. rendelkezéseire tekintettel – annak megállapítása nem kötelező. Ezért minden esetben az adott közfeladatot ellátó szerv dönti el, hogy él-e e joggal vagy sem. Amennyiben a szerv költségtérítést kíván megállapítani, akkor arra a Rendelet hatályba lépése után benyújtott adatigénylések esetében az ott meghatározottak szerint van lehetősége. A NAIH 2017-ben több olyan adatigénylést is megvizsgált, melyet még a Rendelet hatályba lépését megelőzően nyújtottak be. Ezen adatigénylések teljesítésekor a közfeladatot ellátó szervek a NAIH gyakorlatában kialakított elveknek és szabá-

57 Alaptörvény 39. cikk (2) bekezdés.
58 Infotv. 27. § (3) és (3a) bekezdések.
59 Infotv. 26. § (2) bekezdés.

lyoknak megfelelő módon számíthattak fel költségeket. A NAIH számos esetben felhívta a közfeladatot ellátó szervek figyelmét: dönthetnek úgy is, hogy mellőzik a költségtérítést.

Az adatigénylés teljesítése bizonyos mértékű munkaerő-ráfordítást szükségképpen igényel, ez a közérdekű adatok megismeréséhez fűződő alapjog intézményi biztosításának velejárója. A Rendelet alapján megállapítható mérték sem jelenti azt, hogy azt az adatkezelő minden esetben érvényesítheti, a költségtérítésnek ugyanis a valós költségekhez kell igazodnia, így ha azok a rendeletben meghatározott összegeknél alacsonyabbak, az adatkezelőnek a tényleges költséget kell figyelembe vennie.

Másrészt kiemelendő, hogy a közérdekű adatok megismerése iránti igény teljesítése továbbra sem tartozik ÁFA körbe, mivel az általános forgalmi adóról szóló 2007. évi CXXVII. törvény (a továbbiakban: ÁFA tv.) 2. §-a alapján a törvény hatálya az adóalany által belföldön és ellenérték fejében teljesített termékértékesítésére, szolgáltatásnyújtására, a terméknek az Európai Közösségen belüli egyes, belföldön és ellenérték fejében teljesített beszerzésére és a termék importjára terjed ki. Az ÁFA tv. 5. § (1) bekezdése értelmében adóalany az a jogképes személy vagy szervezet, aki (amely) saját neve alatt gazdasági tevékenységet folytat, tekintet nélkül annak helyére, céljára és eredményére. Az ÁFA tv. 6. § (1) bekezdése szerint gazdasági tevékenység: valamely tevékenység üzletszerű, illetőleg tartós vagy rendszeres jelleggel történő folytatása, amennyiben az ellenérték elérésére irányul, vagy azt eredményezi, és annak végzése független formában történik.

A Rendelet az Infotv. vonatkozó rendelkezésének megfelelően háromfajta költségelem felszámolását teszi lehetővé. A teljesítés során kizárólag a felhasznált adathordozó, a kézbesítés, valamint a munkaerőforrás ráfordítás költségeit lehet jogszerűen igényelni. Ezen túlmenően más költségelem nem vehető figyelembe.

Az Infotv. alkalmazása során a legtöbb probléma az adatigénylések teljesítéséhez szükséges munkaerőforrás-ráfordítás költségének megtérítésével kapcsolatban merült fel, különösen annak tükrében, hogy az adatigénylőkkel kifizetendő költségtérítés legnagyobb hányadát – az esetek döntő többségében – ez a költségelem tette ki.

A Rendelet értelmében munkaerőforrás-ráfordításként vehető figyelembe 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 az időtartam 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 Rendelet értelmében – legfeljebb 4400 Forintot jelent. A járulékok, prémiumok, jutalmak és egyéb juttatások, például a béren kívüli juttatások, nem vehetőek figyelembe.

Az Infotv. 29. § (5) bekezdésének c) pontja alapján, ha az adatigénylés teljesítése a közfeladatot ellátó szerv alaptevékenységének ellátásához szükséges munkaerőforrás aránytalan mértékű igénybevételével jár, az adatigénylés teljesítésével összefüggő munkaerő-ráfordítás költsége figyelembe vehető a költségtérítés mértékének meghatározása során. Vagyis a munkaerő-ráfordításért abban az esetben lehet költségtérítést felszámolni, ha az a közfeladatot ellátó szerv:

I. az alaptevékenységének ellátásához szükséges munkaerőforrás,
II. aránytalan mértékű igénybevételével jár, továbbá
III. 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 3 feltételnek együttesen kell érvényesülnie.

A NAIH 2017-ben kidolgozta azokat a szempontokat, módszertani elveket, melyek annak vizsgálatát tették lehetővé, hogy mi minősül a munkaerő-ráfordítás aránytalan mértékű igénybevételének a költségtérítés mértékének meghatározása során. A NAIH olyan információk alapján mérlegelt, mint hány fő dolgozik a közfeladatot ellátó szervnél, az adatigénylés teljesítésében résztvevő alkalmazottak milyen munkakörben dolgoznak, illetve az adatigénylés teljesítésében résztvevő alkalmazottak munkaköre hogyan viszonyul a közfeladatot ellátó szerv alaptevékenységéhez, és mely alaptevékenységét nem tudná/vagy tudta ellátni a szerv az adatigénylés teljesítése miatt. A NAIH vizsgálatai során arra is rákérdezett, miért vélik úgy, hogy az alaptevékenység ellátásához szükséges munkaerőforrás igénybevétele aránytalan mértékű, illetve azt, hogy az adatigénylő által megismerni kívánt adatok jelentős terjedelműek. A NAIH a közfeladatot ellátó szerv rendelkezésére álló technikai feltételeket is figyelembe vette (például: hány nyomtató és szkenner működik az adott intézményben, és ezeket milyen időtartamban kellett az adatigénylés teljesítéséhez igénybe vennie). Természe-

tesen az is vizsgálandó, hogy az adatigénylő által igényelt adatok az általa kívánt formában rendelkezésre állnak-e. A NAIH vizsgálata arra is kiterjedt, 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.

Az Infotv 29. § (4) bekezdése kimondja, hogy ha az adatigénylés teljesítése a közfeladatot ellátó szerv alaptevékenységének ellátásához szükséges munkaerőforrás aránytalan mértékű igénybevételével jár, vagy az a dokumentum vagy dokumentumrész, amelyről az igénylő másolatot igényelt, jelentős terjedelmű, illetve a költségtérítés mértéke meghaladja a kormányrendeletben meghatározott összeget, az adatigénylést a költségtérítésnek az igénylő általi megfizetését követő 15 napon belül kell teljesíteni. Arról, hogy az adatigénylés teljesítése a közfeladatot ellátó szerv alaptevékenységének ellátásához szükséges munkaerőforrás aránytalan mértékű igénybevételével jár, illetve a másolatként igényelt dokumentum vagy dokumentumrész jelentős terjedelmű, továbbá a költségtérítés mértékéről, valamint az adatigénylés teljesítésének a másolatkészítést nem igénylő lehetőségeiről az igénylőt az igény beérkezését követő 15 napon belül tájékoztatni kell.

A Hatóság álláspontja szerint az adatigénylés költségeinek megelőlegezése két esetben lehetséges, ha

I. az adatigénylés teljesítése a közfeladatot ellátó szerv alaptevékenységének ellátásához szükséges munkaerőforrás aránytalan mértékű igénybevételével jár *és* a költségtérítés mértéke meghaladja a Rendeletben meghatározott összeget;
II. az a dokumentum vagy dokumentumrész, amelyről az igénylő másolatot igényelt, jelentős terjedelmű *és* a költségtérítés mértéke meghaladja a Rendeletben meghatározott összeget (5000 Ft).

A fentiek értelmében tehát az említett 2 feltételnek együttesen kell érvényesülnie. Az adatigénylés költségei megelőlegezésének további feltétele az is, hogy ennek tényéről, indokáról, valamint a költségtérítés mértékéről az adatigénylőt az igény beérkezésétől számított 15 napon belül az adatkezelő tájékoztassa. A NAIH-nak ezzel kapcsolatban az az álláspontja, hogy 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. Minden olyan esetben, ahol a szerv túllépte a fenti határidőt, a NAIH felszólította az adatkezelőt az adatigénylés költségtérítés megfizetése nélküli teljesítésére.

A joggyakorlat orientálása érdekében külön kiemelendő az is, hogy az Infotv. 29. § (2) bekezdése biztosítja az adatigénylés teljesítésére vonatkozó határidő meghosszabbításának lehetőségét. A jogalkotó oly módon szabályozta a teljesítésre nyitva álló határidő meghosszabbítását, illetve a költségtérítés megfizetését, hogy a közfeladatot ellátó szervek – választásuk szerint – élhetnek egyik vagy másik törvény adta lehetőséggel, valamint mindkettővel egyszerre. Az Infotv. 29. § (2) és (4) bekezdéseiben foglalt esetkörökben leírt feltételrendszer lényegében megfeleltethetők egymásnak. Ebből következően megállapítható, hogy az Infotv. 29. § (4) bekezdésében foglalt 15 napos tájékoztatási határidőt függetlenül attól, hogy az adott szerv meghosszabbította-e a teljesítésre nyitva álló határidőt vagy sem, be kell tartani. A tájékoztatási kötelezettség ugyanis ebben az esetben nem a meghosszabbított teljesítési határidőhöz kapcsolódik.

Ha az adatigénylés teljesítésére elektronikus úton kerül sor, a Rendelet szerint a másolat készítéséhez szükséges időtartam csak akkor vehető figyelembe, ha elektronikus formában rendelkezésre nem álló adatot igényeltek, vagy a másolat készítéséhez szükséges időtartam rövidebb az elektronikus formában rendelkezésre álló adat rendelkezésre bocsátásához szükséges időtartamnál. Vagyis elektronikus formában igényelt adat esetén a munkaerő-ráfordítás időtartama csak akkor vehető figyelembe, ha:

– az adat elektronikus formában nem áll rendelkezésre (scannelni kell) vagy
– scannelni/másolni gyorsabb lenne, mint az elektronikus fájlt előkeresni.

A NAIH továbbra is azt tartja szem előtt, hogy a közfeladatot ellátó szervek a közérdekű adatigénylések teljesítésekor nem szolgáltatást nyújtanak, hanem az Alaptörvényben meghatározott alapvető jogból eredő kötelezettségeiket teljesítik. E szervek továbbá nem gazdasági tevékenységük körében, üzletszerűen értékesítik a másolatokat, hanem lehetőségük van a felmerült anyagköltségek megtérítését kérni az adatigénylőtől.

Végezetül a NAIH hangsúlyozza, hogy az információszabadság megfelelő érvényesülése megköveteli a költségtérítés megállapításával kapcsolatos eljárás átláthatóságát. A transzparenciát leginkább a közérdekű adatigénylés teljesítéséért megállapított költségtérítéssel kapcsolatos tájékoztatás intézménye szolgálja. Az Infotv. értelmében a közfeladatot ellátó szervek tájékoztatni kötelesek az adatigénylőket a költségtérítés összegéről. Az Infotv. 29. § (3) bekezdése az *„összeg”* kifejezést használja, míg a 29. § (4) bekezdés a költségtérítés *„mértékéről”* rendelkezik. Pusztán az összegről szóló közlés azonban visszaélésekre adhat lehetőséget. Az ugyanis önmagában nem teszi lehetővé annak megítélését, hogy a költségtérítést jogszerűen állapították-e meg. A Hatóság ezért további

minimális tartalmi követelményeket is meghatározott a tájékoztatás tartalmával összefüggésben. Az információszabadság, mint alapjog érvényesüléséhez szükséges, hogy az adatigénylés teljesítéséért megállapított költségtérítésről szóló tájékoztatás kellően részletes legyen, abban a közfeladatot ellátó szervek kötelesek feltüntetni minden olyan indokot, illetőleg költségelemet, amelyek a megállapított összeg megalapozottságát támasztják alá. A megfelelő tájékoztatás nagyban hozzájárul ahhoz, hogy az igénylő valóban tisztában legyen, és megértse azt, hogy miért, milyen költségtérítést kell megfizetnie ahhoz, hogy a megismerni kívánt adatok birtokába jusson. A tájékoztatás alapján továbbá képes lesz a megfelelő döntést meghozni az igénybe vehető jogorvoslati lehetőséggel kapcsolatban. A NAIH álláspontja szerint a tájékoztatás kellően részletes, ha tartalmazza azt a ténybeli és jogi indokot, amely alapján költségtérítést állapítanak meg. Munkaerő ráfordítás esetében ki kell mutatni azt, 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 is, 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. Végezetül közölni kell az adatigénylővel az adatigénylés teljesítésének a másolatkészítést nem igénylő lehetőségeit is.

A költség megállapítása előzetes kalkulációt feltételez. Ez azt jelenti, hogy a közfeladatot ellátó szerv a teljesítést megelőzően elvégzett becslés alapján kialakított összeg megtérítését kérheti az adatigénylőtől, aki – amennyiben a tájékoztatás alapján fenntartja adatigénylését – azt köteles megfizetni. A költségtérítésnek azonban mindenkor az adatok rendelkezésre bocsátásával kapcsolatban közvetlenül és ténylegesen felmerült költségelemekre kell szorítkoznia. Így figyelembe kell venni, hogy eltérés mutatkozhat a teljesítés során valóban felmerült és az előzetesen kalkulált tételek között. A fentiek miatt a közfeladatot ellátó szervnek egy utólagos költségkalkulációt is el kell végeznie annak érdekében, hogy megállapítsa a ténylegesen felmerült költségek pontos összegét. E művelet eredményéről, valamint az azt alátámasztó számításokról, igazolásokról, munkaidő-kimutatásokról és egyéb dokumentumokról tájékoztatni kell az adatigénylőt. Sem az Infotv., sem pedig a Rendelet nem tartalmaz olyan rendelkezést, mely lehetővé tenné az előzetesen kalkulált költségekhez képest jelentkező többletköltségek utólagos felszámítását. Azaz a költségtérítés alulbecsléséből adódó különbözet utólagosan nem terhelhető az igénylőre. A Rendelet szerint azonban amennyiben az előzetesen kifizetett költségtérítés

összege több a ténylegesen felmerült költségek összegénél, a kettő különbözete az adatigénylőnek visszafizetendő. Az adatigényléssel összefüggésben keletkezett költségek dokumentumokkal történő alátámasztása amiatt is jelentőséggel bír, hogy egy esetleges jogvitában az adatkezelő felelőssége annak bizonyítása, hogy a pontos költségelemek miből tevődtek össze.

A NAIH bízik benne, hogy a Rendelet hatályba lépése óta eltelt idő elegendőnek bizonyult arra, hogy a jogalkalmazók a közérdekű adatigénylések teljesítése terén kellő tapasztalatokra tegyenek szert, és egy jól körülhatárolt eljárásrend kialakításával az Infotv.-t és a Rendelet szabályainak a jövőben maradéktalanul meg tudjanak felelni.

VII.3. A NAIH korrupció megelőzésével kapcsolatos tevékenységei

A NAIH számos – hazai és nemzetközi – szakmai vagy tudományos konferencián, előadáson, illetve workshopon képviseltette magát. Ezek keretében rendszeresen rávilágít az információszabadság és az átláthatóság fontosságára a korrupció megelőzésében, visszaszorításában és üldözésében. Ezen túlmenően a NAIH a témához kapcsolódó szakmai és tudományos publikációkban is felhívja a szakma és a közvélemény figyelmét e kérdéskör kiemelkedő szerepére és összefüggéseire.

Végezetül kiemelendő, hogy a NAIH a Nemzeti Védelmi Szolgálat munkatársának bevonásával 2017. február 26-án konferenciát szervezett a 15 000 főnél nagyobb városok önkormányzatai részére, amelynek alapvető témája az információszabadság volt. Ennek keretében az előadások elsősorban a közérdekű és közérdekből nyilvános adatok megismerésére, valamint az elektronikus közzététel gyakorlati kérdéseire összpontosítottak. A két szervezet a korábbi együttműködéseik során felhalmozott tapasztalatok alapján fogják kialakítani a konferencia programját és a bemutatandó témaköröket.

VII.3.1. Részvétel az információszabadság előmozdítására irányuló nemzetközi fórumokon

A NAIH 2017. folyamán két olyan nemzetközi fórumon is képviseltette magát, amelyek célja az információszabadság felügyeletére szakosodott nemzeti és nemzetközi intézmények közelítése, tevékenységének összehangolása volt.
A NAIH 2017. február 23-24. között részt vett az európai információszabadság biztosok Berlinben megrendezett konferenciáján. A német szövetségi adatvé-

delmi és információszabadság biztos által szervezett eseményen résztvevők ismertették az információszabadság alapjogának érvényesülésével kapcsolatos nemzeti tapasztalataikat, illetve betekintést nyertek más államok vonatkozó gyakorlatába is. A tapasztalatcsere mellett lehetőség nyílt egyes konkrét kérdések megvitatására is. Az európai adatvédelmi biztosok a konferencia zárásaként határozatot fogadtak el, amelyben az információszabadság érvényesülésének, illetve az azt felügyelő nemzeti intézmények szerepének megerősítésére hívták fel a nemzeti parlamenteket és a kormányokat.[60] Az információszabadság és az átláthatóság ugyanis a szabadon és demokratikusan működő jogrendszer alapvető eleme.

A NAIH továbbá aktívan részt vett a 2017. szeptember 20-21. között Manchesterben megrendezett, az információszabadság biztosok 10. nemzetközi konferenciáján is. Az eseményen, amelyen a világ különböző pontjairól több mint százan vettek részt, lehetőség nyílt az információszabadsággal kapcsolatos nemzeti és nemzetközi tapasztalatok megvitatására. A résztvevők a konferencia záró-nyilatkozatában hangsúlyozták és a jövőben kiemelt célkitűzésüknek tekintik a kiszervezett és a nem állami, önkormányzati szervezetek által nyújtott közszolgáltatások, illetve a közbeszerzések átláthatósága megerősítését.[61]

Az említett fórumok résztvevői több alkalommal is kifejezték az európai és nemzetközi szintű együttműködés elmélyítésének szükségességét, amelynek célja mindenekelőtt a megfelelő közös normák kialakítása. A NAIH reményét fejezi ki ezért azzal kapcsolatban, hogy a jövőben megrendezésre kerülő alkalmak a kooperáció lehetőségeinek további bővülését hozzák. Ez ugyanis végső soron akár – az adatvédelem szabályozásához hasonló – regionális vagy univerzális normák megalkotásához is elvezethet az információszabadság terén.

60 http://naih.hu/files/EU_Infoszab_bizt_nyil_2017-02-24.pdf.
61 http://naih.hu/files/2017-09-28-Infoszab_biztosok_hatarozata.pdf.

VIII. A Hatóság jogalkotással kapcsolatos tevékenysége

VIII.1. A jogi szabályozással kapcsolatos ügyek statisztikai adatai

2017-ben nem változott lényegesen a Hatóság által véleményezendő előterjesztések száma az előző évhez képest. Ugyanakkor jó ötödével nőtt az érdemi kifogást, javaslatot tartalmazó észrevételeink száma. Még inkább szignifikáns az eltérés, ha tartalmi szempontok szerint vizsgáljuk a javaslatok statisztikáját: 2016-hoz képest duplájára nőtt az adatvédelemmel kapcsolatos észrevételek mennyisége, míg az információszabadsággal kapcsolatosoké nagyjából a negyedére csökkent. Ez nem azt jelzi, hogy a Hatóság kevesebb figyelmet fordított volna az információszabadság érvényesülésének elősegítésére, hanem inkább abban látjuk a változás okát, hogy 2017 az adatvédelmi jogi keretrendszer megújulásának előkészítése jegyében telt és az információszabadságot érintő tervezetek száma is csökkent. Ezért 2017-ről szólva az adatvédelem van a beszámolónk fókuszában.

A jogi szabályozással kapcsolatos ügyek száma évenként és jogforrási szintenként			
Jogforrás/év	**2015**	**2016**	**2017**
Törvény	79	85	82
Kormányrendelet	133	98	89
Miniszteri rendelet	126	83	94
Kormányhatározat	61	29	33
Közjogi szervezetszabályozó eszközök	27	20	23
Összesen	**426**	**315**	**321**

A jogi szabályozással kapcsolatos tervezetekhez tett érdemi észrevételek száma			
Észrevételek jellege	**Észrevételek száma/év**		
	2015	**2016**	**2017**
Adatvédelemmel kapcsolatos	298	222	461
Információszabadsággal kapcsolatos	53	101	28
Egyéb	137	127	92
Összesen	**488**	**450**	**581**

VIII.2. Az adatvédelmi jogi szabályozási keretek változása

Mielőtt a személyes adatok kezelését és az információszabadságot érintő jogszabályokkal kapcsolatos főbb ügyeinket sorra vennénk, szót kell ejteni arról, hogy a GDPR (általános adatvédelmi rendelet) alkalmazandóvá válásával 2018-ban jelentősen meg fognak változni a személyes adatok védelmének jogi keretei. A Hatóság GDPR előkészítésével kapcsolatos tevékenységét a tavalyi beszámoló tárgyalta, így ennek megismétlésére, illetve a GDPR normaanyagának ismertetésére nincs szükség. Ehelyütt elég arra rámutatni, hogy a személyes adatok védelme az Alaptörvényben (korábban az Alkotmányban) megnevezett alapvető jog, melynek tartalmát, elveit az Alkotmánybíróság határozatai értelmezték és értelmezik, továbbá alapvető szabályait az Infotv. határozza meg. A GDPR révén annak hatálya alá tartozó adatkezelések esetében az adatvédelem szabályait nem törvény, hanem a GDPR fogja tartalmazni. A GDPR hatálya nem terjed ki valamennyi személyes adatkezelésre, ezért az Alaptörvényből levezethető az a szabályozási kötelezettség, hogy a GDPR hatálya alá nem tartozó tárgykörökben továbbra is törvény szabályozza az adatvédelem alapvető szabályait, vagyis az Infotv. hatályon kívül helyezése nem indokolt, hanem csak a hatályát szükséges megváltoztatni a GDPR-től való elhatárolás érdekében. Megemlítendő még, hogy a jogi keretrendszert összetettebbé teszik azok a további – jelenleg előkészítés alatt álló vagy már elfogadott – EU-s jogi normák, amelyek egy-egy szabályozási tárgykörben (például: bűnüldözés, on-line tér) speciális adatvédelmi követelményeket írnak elő. 2018-tól egy olyan jogi keretrendszer jön létre, amely mind a magyar jogalkotás, mind a Hatóság, mint jogalkalmazó szerv, mind az adatkezelők számára erős adaptációs igényt támaszt. Ami beszámolónk közelebbi tárgyát illeti, véleményünk szerint nem kell attól tartani, hogy a GDPR ellentétbe kerülne a személyes adatok védelmének az Alkotmánybíróság határozataiban kibontott tartalmával és így alkotmányos konfliktus alakulna ki, ugyanis a GDPR célja a magas szintű adatvédelem megteremtése, ezért várhatóan összességében előrelépést fog hozni, tehát a személyes adatok védelmének már elért szintje legalábbis fenntartható marad. Továbbá a GDPR kellően rugalmas, mert a hatálya alá tartozó adatkezelések esetében is hagy teret a tagállami jogalkotás számára, hogy az egyes országok alkotmányos felfogásában és hagyományaiban esetleg meglévő kisebb különbségek érvényre juthassanak a GDPR keretei között.

Ennek megfelelően a Hatóság 2017-es (és 2018-ban) folytatódó feladata az volt, hogy észrevételeivel és javaslataival támogassa a személyes adatok védelmének érvényesülését elősegítő jogszabályi környezet fenntartását az Infotv. GDPR miatt szükséges módosítása, valamint a szektorális adatkezelési jogszabályok GDPR-hez igazítása során. Ez a feladat a GDPR hatálya alá nem tartozó

adatkezelésekre vonatkozó jogszabályok esetében is adott volt, részben amiatt, mert az Infotv. módosításával kapcsolatban ágazati szinten is felmerülhetnek részben jogtechnikai jellegű korrekciós igények, részben a már említett további EU-s adatvédelmi jogi normák miatt.

VIII.3. Az Infotv. módosítása

A 2011-ben elfogadott Infotv. véleményünk szerint korszerű adatvédelmi törvény, amely eddig is nagymértékben megfelelt az európai jogfejlődés kívánalmainak, ezért a GDPR szabályaira való áttérés nem jelent szigorítást. A nemzeti szabályozási hatáskörben maradó adatvédelmi szabályozási területeken az Infotv. módosításával olyan adatvédelmi szabályozási környezetet célszerű kialakítani, amely fogalomrendszerét, az elveket és az egyes jogintézményeket tekintve minél inkább közelít a GDPR-hez, ugyanis mind az érintettek, mind az adatkezelők számára előnyös, ha az adatvédelem általános szabályai minél inkább egységes és áttekinthető jogi követelményrendszert írnak le. Ugyanis az új adatvédelmi szabályoknak való megfelelés nem csupán a NAIH számára kiemelt feladat, hanem az adatkezelőknek és adatfeldolgozóknak is időben meg kell kezdeniük az adatkezelési gyakorlatuk felülvizsgálatát.

Az Infotv. módosítására irányuló előkészítő munkában az igazságügyi tárca és a NAIH megegyezése alapján a NAIH-nak már a kezdetektől, 2017 januárjától lehetősége volt részt venni. A két szerv között rendszeres közvetlen munkakapcsolat alakulhatott ki ügyintézői szinten – hivatalos találkozók, észrevételezések közbeiktatásával – a szabályok konkrét tartalmának kidolgozására és a kérdések tisztázására.

A jogalkotási feladatok azonosítása során a NAIH azt az álláspontot képviselte, hogy feltehetőleg nem merül fel változtatási igény az információszabadságra vonatkozó rész tekintetében, miután az érintett uniós jogi aktusok csak a természetes személyek adatainak kezelését és a személyes adatok áramlását szabályozzák. Ezért az uniós kötelezettség teljesítése érdekében elegendőnek és megfelelőnek mutatkozott, ha az Infotv.-nek is csak az ugyanezen tárgyú rendelkezéseit érinti a módosítás.

A NAIH független jogállása az Alaptörvényen alapul, és a jogköreire, gazdálkodására, szervezetére vonatkozó hazai törvények vizsgálata alapján megállapítható, hogy azok összhangban vannak a tagállami felügyeleti hatóságok függetlenségét és ennek konkrét feltételeit előíró uniós szabályozással, ezért

úgy érveltünk, hogy a jelenlegi Infotv. e rendelkezései szintén alkalmasnak mutatkoznak az uniós szabályok végrehajtására.

Az anyagi jogi szabályok tekintetében azt az elvárást képviseltük, hogy az Infotv.-ben eddig is biztosított magas védelmi szintben ne történjen visszalépés.

Az Infotv. új eljárási szabályainak kialakításánál azt tartottuk szem előtt, hogy a NAIH képes legyen az uniós jogban előírt kötelezettségek teljesítésére és új hatásköreit az alkotmányos követelményeknek megfelelően tudja gyakorolni, az új eljárási rend továbbá zökkenőmentesen beilleszthető legyen a tagállamok felügyeleti hatóságai közti (korábbinál közvetlenebb formájú) nemzetközi együttműködésbe. További figyelembe veendő tényező volt, hogy 2018. január 1-jétől hatályos az általános közigazgatási rendtartásról szóló 2016. évi CL. törvény is, amelyet alkalmazni kell a NAIH hatáskörébe tartozó több eljárásra. Így az összhangot e szabályrendszerekkel együtt kellett elérni.

A NAIH és az Igazságügyi Minisztérium szoros együttműködésével kialakított törvénytervezet társadalmi és közigazgatási egyeztetése 2017 szeptemberében zárult le; a tervezettel kapcsolatban észrevétel nem maradt fenn a véleményezésre jogosult szervek részéről. A jelen beszámoló írásakor a törvényjavaslatot még nem vették tárgysorozatba.

A GDPR-hez és az Infotv. módosításához kapcsolódó szektorális törvények felülvizsgálata már 2018-ban indult el, ezért ezt a következő évi beszámoló fogja érinteni.

VIII.4. A titkos információgyűjtés külső engedélyezési rendszerének reformja

A nemzetbiztonsági szolgálatokról szóló 1995. évi CXXV. törvény (Nbtv.) módosítását a strasbourgi Emberi Jogok Európai Bíróságának (EJEB) 2016-os ítélete (a továbbiakban: Ítélet) teszi szükségessé. A múlt évi beszámoló számot adott a Hatóság Ítélettel kapcsolatos javaslatairól, valamint a törvénymódosítás érdekében történő fellépéséről. Az Nbtv. módosítás előkészítése áthúzódott 2017-re, ezért most a tárgyévi fejleményeket vesszük sorra.

Az Országgyűlés Nemzetbiztonsági bizottságának elnöke felkérte a NAIH elnökét a külső engedélyezési reformmal kapcsolatos álláspontjának kifejtésére. E felkérés lehetőséget ad a külső engedélyezési rendszer adatvédelmi szempontjainak felvázolására.

Az Alkotmánybíróság 2/2007. (I. 24.) AB határozatának indokolása az EJEB joggyakorlatát elemezve megállapította, hogy – [a titkos információgyűjtés esetében] „*az alkalmazást három szakaszból álló ellenőrzésnek kell alávetni: amikor a beavatkozást elrendelik, mialatt a beavatkozást végrehajtják, miután a beavatkozást befejezték*”. Ez az AB határozat elsősorban a bűnüldözési célú titkos információgyűjtéssel összefüggésben értelmezte az Alkotmányt, ám általános érvényű megállapításai véleményünk szerint a nemzetbiztonsági célú titkos információgyűjtésre is vonatkoztathatóak. Az Ítéletben foglaltak alapján most elsősorban az alkalmazás elrendelésének újraszabályozása került a figyelem fókuszába, ám a magyar alkotmányos követelmények alapján a titkos információgyűjtés garanciarendszerének összességében – azaz az elrendelés idején, az alkalmazás alatt és az utólagos ellenőrzést illetően – kell egyenszilárdnak lennie.

A magánszféra legmélyebb feltárására alkalmas speciális eszközök és módszerek esetében a titkos információgyűjtés előzetes engedélyhez kötése az ellenőrzési rendszer kulcseleme. Ám mivel az engedélyezési eljárás során rövid idő áll rendelkezésre a döntésre, amelyet szükségképp a nyilvánosság kontrolljától elzárva, alapvetően az engedélykérő szerv által összeállított adatokra és állításokra alapozva, az érintett személy érdekei intézményes képviseletének bevonását mellőzve kell meghozni, ezért az előzetes külső engedélyezési eljárás során nem érvényesülhetnek teljes körűen azok a *„jogalkalmazási minőségbiztosítási”* feltételek, amelyek egyébként a bíróság előtt folyó polgári-, vagy büntetőperekre főszabályként jellemzőek. A különleges eszközök külső engedélyezési eljárása során sem a bírói, sem a miniszteri hatáskörben hozandó döntés esetében nem adottak a következők: a kontradiktorius eljárás, a kötetlen bizonyítás, a tárgyalás nyilvánossága, az eljárás időkereteinek valamelyest rugalmassága az adott ügy bonyolultságának függvényében, valamint a jogorvoslati lehetőség. Ezért ahhoz, hogy a speciális eszközök alkalmazása az Ítéletben foglaltaknak megfelelően, valamint az Alkotmánybíróság intencióinak megfelelően kontrolláltan történjék, a Hatóság véleménye szerint az előzetes engedélyezés eljárási jogi reformjával együtt a titkos információgyűjtés végrehajtása közbeni és a beavatkozás utáni ellenőrzés szabályozása is további megfontolást igényel a törvény előkészítés folyamatában.

VIII.4.1. A titkos információgyűjtés végrehajtása közbeni ellenőrzéséről

Az eszközalkalmazásra kötött időkeretben, jellemzően olyan speciális körülmények között (szigorú konspiráció, leplezett feladatellátás stb.) kerül sor, amelyek rendszerint nem teszik lehetővé a beavatkozás egyidejű, külső ellenőrzését. Ezért a titkos információgyűjtés jogszerűségének biztosításában az eszközalkalmazással kapcsolatos feladatok ellátását végző szervezet a kulcsszereplő.

A Nemzetbiztonsági Szakszolgálat (NBSZ) speciális eszközalkalmazással kapcsolatos szolgáltató tevékenységének adatvédelmi auditálása során megállapítást nyert, hogy az Nbtv. által meghatározott munkamegosztási és feladat-ellátási rendben az NBSZ-nek a törvényből levezethető feladata, hogy az eszközalkalmazás végrehajtásának szakszerűségét és törvényességét biztosítsa. A Hatóság támogatja az NBSZ e törvényességi kontrollszerepének erősítését.

VIII.4.2. A speciális eszközök alkalmazásának utólagos ellenőrzéséről

A nemzetbiztonsági szolgálatok működésének legfontosabb független, általános ellenőrző szerve az Országgyűlés Nemzetbiztonsági bizottsága, amelyet a törvény megfelelő vizsgálati jogkörrel ruház fel a nemzetbiztonsági szolgálatok rendeltetésszerű működésének ellenőrzésével kapcsolatban. A nemzetbiztonsági szolgálatok titkos információgyűjtő tevékenysége elsősorban a személyes adatok védelme szempontjából ellenőrizendő. Az Alaptörvény VI. cikk (3) bekezdése értelmében a személyes adatok védelméhez való jog érvényesülését a Nemzeti Adatvédelmi és Információszabadság Hatóság ellenőrzi az Infotv.-ben meghatározottak szerint. A Hatóság a nemzetbiztonsági célú titkos információgyűjtés (utólagos) ellenőrzésére is jogosult. A nemzetbiztonsági szolgálatok információgyűjtő tevékenysége adatvédelmi szempontból különösen érzékeny adatkezelés, ezért kiemelt figyelmet érdemel a Hatóságunk részéről, ám jelenleg csak korlátozott eszközök állnak a rendelkezésünkre a titkos információgyűjtések törvényességének utólagos ellenőrzésére.

Jelenleg a következők a korlátozó tényezők:

- természetszerűleg csak kevés információ jut el a Hatósághoz a potenciálisan jogsértő titkos információgyűjtésekről;
- az Infotv.-ben meghatározott keretek között csak olyan feltételek fennállása esetén van módunk a titkos információgyűjtés törvényességének ellenőrzése céljából eljárást indítani, amely feltételek (például a célszemélytől származó beadvány, a titkos információgyűjtés tartalmára vonatkozó információ) titkos információgyűjtés esetén csak kivételesen fordulnak elő.

A korábban jelzett problémák nagy részére megoldást jelenthet a Belügyminisztérium által előkészített, az Nbtv. és az Infotv. módosítására irányuló törvénytervezet, amely a miniszter által engedélyezett titkos információgyűjtéssel kapcsolatban előzetes ellenőrzési jogkört, valamint törvénysértés észlelése esetén hatékony beavatkozási lehetőséget biztosítana a Hatóság számára a személyes adatok védelmének érvényesülése és az érintettek magánszférájá-

nak védelme érdekében. A törvénytervezet közigazgatási egyeztetése 2017-ben megtörtént. Ennek során az előterjesztő a Hatóság észrevételeit és javaslatait figyelembe vette. A vonatkozó törvényjavaslat Országgyűléshez történő benyújtása még nem történt meg.

VIII.4.3. A nemzetbiztonsági célú titkos információgyűjtés szabályozása az NBSZ adatvédelmi auditjának tükrében

Az NBSZ speciális eszközalkalmazással kapcsolatos szolgáltató tevékenységének adatvédelmi auditálása 2017-ben fejeződött be. Az audit során a Hatóság elsősorban a szolgáltató tevékenység jogi követelményeknek való megfelelését vizsgálta, ám arról is szereztünk tapasztalatokat, hogy mennyiben van összhangban a speciális eszközök alkalmazására vonatkozó joganyag az Alaptörvénnyel, az Infotv.-vel és az Alkotmánybíróság határozataiban megfogalmazott alkotmányossági követelményekkel. Az utóbbi kérdéskör vizsgálatát azért tartottuk fontosnak, mert amint arra a fentebb hivatkozott 2007-es AB határozat indoklása rámutat, a titkos eszközök alkalmazásának lehetővé tételéhez szigorú, az alapjogokba való beavatkozás minden részletkörülményére kiterjedő garanciákra van szükség. A titkos információgyűjtés kellően pontos és részletes szabályozása garanciális jelentőségű az érintettek jogainak védelme szempontjából és annak megítélésére, hogy ezek a garanciák kielégítik-e a törvényben meghatározottság, a jogbiztonság, az előreláthatóság, a kiszámíthatóság elvéből fakadó elvárásokat, s hogy megfelelnek-e a szükségesség és arányosság kívánalmainak, a nyílt eljárásokra vonatkozó szabályozás követelményeinél szigorúbb mérce érvényesül. Mind a személyes adatok védelme, mind a titkos információgyűjtést szükségessé tevő államérdekek érvényesülése, mind az NBSZ tevékenységének törvényessége és szakszerűsége szempontjából lényeges, hogy a jogi szabályozás esetleges hibái, illetve hiányosságai feltárásra kerüljenek. Az adatvédelmi audit a jogi szabályozás következő aspektusait és összefüggéseit járta körül.

VIII.4.3.1. A titkos információgyűjtés eszközeire és módszereire vonatkozó szabályozás rendszere az Nbtv.-ben – az egyes speciális eszközök és módszerek összefüggései és elhatárolásuk

Ez azért lényeges, mert az Nbtv. teljes körűen felsorolja a titkos információgyűjtés eszközeit és módszereit, azonban azok mibenlétét nem részletezi, ezért esetenként kérdés lehet, hogy azok mindegyike meghatározható és elhatárolható-e egymástól a törvényi szabályozás rendszerében, vagy jogalkalmazási bizonytalanságok, ellentmondások tapasztalhatók e tekintetben. Ehhez kap-

csolódóan több tesztet végeztünk el, melyek során például azt vizsgáltuk, hogy számítástechnikai eszközt tartalmazó postai küldemény átvizsgálásakor a gyakorlati munka során megfelelően elhatárolhatók-e egymástól a vonatkozó külső engedélyezési jogcímek (lásd: az Nbtv. 56. § c) és e) pontjait).

A törvényi szabályozásnak legalább olyan pontossággal el kell határolnia egymástól az egyes speciális eszközöket és módszereket, hogy a külső engedélyhez kötöttek és a külső engedélyt nem igénylők egyértelműen elhatárolhatók legyenek egymástól (hiszen egyébként esetenként meg lehetne kerülni a külső engedélyeztetési kötelezettséget). Az audit tapasztalatai szerint a törvényi szabályozás és a jogalkalmazási gyakorlat megfelel e szempontnak.

VIII.4.3.2. Az egyes speciális eszközök és módszerek törvényi meghatározása

Az Nbtv. az egyes speciális eszközök és módszerek megnevezésén túl nem ad tartalmi meghatározást ezekről, ezért megvizsgáltuk azt, hogy elégséges-e így a törvényi szabályozás, vagy az adatvédelmi követelmények érvényre juttatása érdekében ki kellene egészíteni a speciális eszközök tartalmi meghatározásával. Ehhez kapcsolódóan például azt teszteltük, hogy az elektronikus hírközlési eszközök rejtett ellenőrzésekor egyértelműen elhatárolható-e az elektronikus hírközlési szolgáltatás útján továbbított kommunikáció tartalma a kommunikációhoz járuló meta információktól. Ez azért lényeges, mert a kommunikáció tartalmának ellenőrzése az Nbtv. 56. § d) pontja értelmében külső engedélyhez kötött, ám a meta információké nem. A vonatkozó audit teszt koncepciója szerint az volt a vizsgálandó kérdés, hogy a különleges eszközalkalmazás gyakorlatában melyik kategóriának feleltethetők meg például a távbeszélő hívásfelépülést megelőzően esetleg továbbított jelek, valamint a csengetés. (Ezen kívül további, a jelen beszámolóban nem részletezhető audit tesztek is érintették az egyes speciális eszközök és módszerek törvényi meghatározottságának, illetve a törvényi definíció esetleges hiányosságának kérdéskörét.)

A tesztek arra mutattak rá, hogy a hatályos Nbtv. több speciális eszköz és módszer esetében nem tér ki adatvédelmi szempontból lényeges részletek meghatározására, ám a vonatkozó NBSZ belső normák eszközalkalmazással kapcsolatos részletszabályai, valamint az NBSZ által követett jogértelmezés összhangban van az adatvédelem követelményeivel, vagyis az adatvédelmi szempontból helyes gyakorlat mintegy pótolja a jogszabályból hiányzó részletszabályokat.

VIII.4.3.3. A titkos információgyűjtéssel kapcsolatos eljárási szabályok

E kérdéskör azért lényeges adatvédelmi szempontból, mert alkotmányos követelmény, hogy a különleges eszközök alkalmazásának eljárási rendje kellő garanciát nyújtson az egyén jogainak védelmére. A vonatkozó szabályozásnak precíznek, részletesnek és követhetőnek kell lennie, továbbá világossá kell válnia az eszközöket alkalmazó szerv hatáskörének, az intézkedések lényegének, azok gyakorlása módjának. Az audit során végzett tesztek szerint a szabályozás megfelel e követelményeknek, néhány kisebb hiányosságtól eltekintve. Így például az Nbtv. 57. § (2) bekezdés c) pontja szerint a TIGY külső engedély iránti előterjesztés tartalmazza a tevékenység kezdetét és végét napban meghatározva, ám az 58. § (4) bekezdése nem tisztázza, hogy az engedélyezőnek milyen pontossággal kell meghatároznia az engedély kezdő időpontját és határidejét, illetve olyan egzakt határidő-számítási előírás sincs a törvényben, amely egyértelművé tenné, hogy ha a külső engedély napokban határozza meg az időtartamot, akkor az alatt pl. a kezdőnap 0 óra 0 perctől a határidő utolsó napján 23 óra 59 perc végéig tartó időtartam értendő.

VIII.4.4. A bűnüldözési célú titkos információgyűjtés szabályozása

A titkos információgyűjtés külső engedélyezésének problematikája egy másik összefüggésben, a bűnügyi szabályozási tárgykör kapcsán is megjelent 2017-ben. A titkos információgyűjtés szabályainak új büntetőeljárási törvénnyel összefüggő módosításait tartalmazó törvénytervezet számos olyan új szabály törvénybe iktatását irányozta elő, amelyek összhangban vannak az Alkotmánybíróság 2/2007. (I. 24.) AB határozatában meghatározott alkotmányossági követelményekkel, ezért adatvédelmi szempontból támogatandók. A Hatóság fontos előrelépésként értékelte például azt a módosítást, amely sok év szabályozási adósságát törlesztve arra irányult, hogy a célszemély utólagos tájékoztatást kapjon arról, hogy vele szemben információgyűjtés folyt, amennyiben e tájékoztatás nem veszélyezteti a titkos információgyűjtés érdekét, továbbá a folyamatban lévő büntetőeljárás eredményességét. Azzal is egyetértettünk, hogy az előterjesztés kitért az eszközalkalmazás ellenőrzésére. A törvénytervezet szerint az ellenőrzési jogkör a bíróságot fogja megilletni. Ezzel kapcsolatban a Hatóság arra hívta fel a figyelmet, hogy az eszközalkalmazás végrehajtásának törvényességi ellenőrzésére a független bíróság nyilvánvalóan alkalmas lehet, ám a tervezett normaanyag több tekintetben hiányos volt. A törvényszöveg csak eshetőleges lehetőségként utalt arra, hogy a bíróság az alkalmazás során vizsgálhatja a bírói engedélyhez kötött eszközök alkalmazásának törvényességét. Nem volt világos, hogy ki, milyen feltételekkel, milyen szempontok mérlegelése alapján dönthet a vizsgálat elrendeléséről. továbbá mikor kötelező az eszközalkalmazás törvényességét ellenőrizni.

A tervezet nem válaszolta meg azt a kérdést sem, hogy honnan tudhatja meg a bíróság azt, hogy mely titkos információgyűjtés esetében merül fel olyan körülmény, ami törvénysértésre utal, és ezért a végrehajtás ellenőrzése szükséges. Ezzel kapcsolatban indokoltnak tartottuk felhívni a figyelmet arra, hogy konkrét ügyekben az információgyűjtés titkossága miatt az eszközalkalmazással kapcsolatos információk a bírósághoz sem juthatnak vissza, ezért feltételezhető, hogy a bíróság számára nem fog rendelkezésre állni az adott eszközalkalmazás törvényességi vizsgálatának szükségességét megalapozó információ. Mindezek alapján kérdésesnek véltük, hogy a szabályozás hatályba lépése esetén az ügyekkel egyébként is leterhelt bíróságok fognak-e élni az ellenőrzési jogkörükkel.

VIII.4.5. A tiltott adatszerzés büntetőjogi szankcionálása

Egy sajnálatos 2017-es esemény világított rá a tiltott adatszerzés büntetőjogi szabályozásának hiányos voltára. A sajtó számolt be arról, hogy rejtett kamerát találtak az MTVA székházának egyik irodájában, ám nem volt mód az elkövető felderítésére és büntetőjogi felelősségre vonására, mert a hatályos Btk. szerint az iroda nem minősült magánlakásnak, így az nem lehet tiltott adatszerzés elkövetésének helyszíne. A jogellenes rejtett megfigyelés és adatszerzés rendkívül súlyos információs alapjogi jogsérelmet okozhat, mert azzal az egyén magánszférájának legbensőbb, leginkább védendő területei is feltárhatók, ugyanakkor e tevékenység rejtettsége folytán az érintettnek nincs lehetősége arra, hogy a jogai védelmében fellépjen. A törvény az információs önrendelkezési jog, valamint a magánélet tiszteletben tartásához való jog védelme érdekében minden hasonló jogsértést szankcionál a büntetőjog eszközeivel is.

Minden hasonló, titkos információgyűjtéssel kapcsolatos eljárási szabály és büntetőjogi tényállás esetében olyan értelmezés irányadó a helyszínt jelölő „*lakás*” vagy „*magánlakás*” meghatározására, amely szerint a hétköznapi értelemben vett lakáson túl a nyilvános vagy a közönség részére nyitva álló helyen kívül minden más helyiség vagy terület, továbbá – a közösségi közlekedési eszköz kivételével – a jármű is lakásnak minősül. A Hatóság álláspontja szerint semmilyen ésszerű indoka nincs annak, hogy a tiltott adatszerzés büntetőjogi tényállása esetében ettől eltérve a „*magánlaksértés*” büntetőjogi tényállásánál használt lakásfogalom legyen irányadó, mert abból az következik, hogy büntetlenül maradhatnak olyan súlyos jogsértések, mint például az MTVA megfigyelési ügy. Ezért a NAIH egyetértett azzal, hogy a Legfőbb Ügyészség kezdeményezte a Büntető Törvénykönyv tiltott adatszerzésre vonatkozó tényállásának módosítását, továbbá az Igazságügyi Minisztérium közjogi jogalkotásért felelős helyettes államtitkárának írt levelében szintén kezdeményezte ezt.

VIII.5. Az adatkezelések rendszerét érintő nagy állami informatikai fejlesztési projektek

A személyes adatok védelmével kapcsolatos bejelentések kivizsgálásakor rendszerint az a kérdés merül fel, hogy jogszerűen kezelte-e adott adatkezelő a hozzánk forduló személy adatait, illetve érvényesíthette-e az érintett az adott adatkezeléssel kapcsolatos, az Infotv.-ben meghatározott jogait. Ezekben az esetekben az adatvédelmi jogi kérdés alanyi jog érvényesülésével összefüggésben jelenik meg.

Ezen túl van az adatvédelmi jognak egy konkrét személyhez kevésbé köthető vetülete, amikor az a Hatóság eljárása során eldöntendő kérdés, hogy adott nyilvántartás vagy más adatkezelés, illetve valamely konkrét adatkezelő tevékenysége általában, egészét tekintve összhangban van-e az adatvédelmi követelményekkel. Ebben az aspektusban vizsgálandó például az, hogy megfelelő-e az adatkezelő belső adatkezelési utasítása, vagy megfelelően védett-e egy személyes adatok kezelését végző informatikai rendszer az informatikai támadások ellen.

Végül meghatározható az adatvédelmi jognak egy olyan metszete is, amely az adatok hierarchiájának konkrét adatkezelésen és konkrét adatkezelőn túlmutató szférájában határoz meg jogi követelményeket. Ebben a szférában helyezhető el például az osztott információs rendszerek elve, az adathordozhatóság követelménye, valamint minden olyan további adatvédelmi szabály is, amely információs rendszerek közötti kapcsolatokra, vagyis az adatkezelések rendszerére vonatkozik. Az adatvédelemnek ez a területe egyre fontosabbá válik, hiszen az internet korában a technikai lehetőség adott az adatkezelések összekapcsolására, ami a fejlett információs társadalom körülményei közepette mindinkább elkerülhetetlenné válik. Ugyanakkor ez az adatvédelmi jogterület elméleti síkon, a normatartalmát és elveit illetően kevésbé tisztázott, mint például az érintettet megillető jogok. Érdemes elgondolkodni azon, hogy már évtizedekkel ezelőtt nagyjából egységes tartalommal nemzetközi egyezményekbe foglalták azt, hogy milyen feltételekkel korlátozható az érintett tájékoztatáshoz való joga egy demokratikus társadalomban, de máig nincs egységes európai válasz arra a kérdésre, hogy kötelezővé teheti-e egy állam a polgárai számára az egységes és univerzális személyazonosító jel használatát.

Jelenleg úgy tűnik számunkra, hogy az adatkezelések rendszerének adatvédelme nehezebben írható le konkrét adatvédelmi követelmények formalizált listájaként, mint például az *„érintett-adatkezelő”*, vagy az *„adatkezelő-adatfeldolgozó”* reláció. Ennek abban látjuk a fő okát, hogy az adatkezelések rendszere eseté-

ben a lehetséges adatkapcsolatok bármely viszonylata bonyolult műszaki-informatikai tartalommal bírhat, és ennek elvileg bármelyik apró részlete releváns lehet adatvédelmi szempontból. De természetesen nemcsak az apró részletek lehetnek lényegesek ebben a szférában, hanem a nagy összefüggések is. Például feltehető az a kérdés, hogy levezethető-e az alkotmányos államszervezési elvekből, így a hatalmi ágak elválasztásából olyan jogi követelmény, amely arra vonatkozik, hogy adott hatalmi ág, vagy állami szervezet informatikai rendszerei felett ki gyakorolhat ellenőrzést és ki (mely szervezet) nem, továbbá hol kell elhelyezni e rendszereket az államszervezeten belül? Ha levezethetők ilyen informatikai államszervezési követelmények, akkor tisztázandó, hogy mi ezeknek a viszonya az adatkezelések rendszerének adatvédelmi követelményeivel. Talán elvontnak tűnik ez a problémafelvetés, de a Hatóság a jogszabálytervezetek véleményezésekor, illetve a nagy összekapcsolt adatkezelések rendszerének vizsgálata során gyakran szembesül hasonló kérdésekkel. Tehát rendkívül komplex tárgykörről van szó, de nagy hiba lenne, ha az Alaptörvény által adatvédelmi ellenőrző jogkörrel felruházott Hatóság a várható nehézségektől visszariadva lemondana arról, hogy elméletileg megalapozott jogi válaszokat találjon az adatkezelések rendszerének adatvédelme körében felmerülő bonyolult problémákra. Ezért az a célunk, hogy az Alkotmánybíróság korábbi iránymutatásaira támaszkodva előrehaladást érjünk el az adatkezelések rendszerére vonatkozó adatvédelmi követelményrendszer kimunkálásában.

Magyarországon az adatkezelések rendszerének szférájában fontos mérföldkő volt az elektronikus ügyintézésről, valamint az állami adatkezelések interoperabilitásáról szóló törvény, amelynek lényegi szabályai 2018-tól lépnek hatályba, ám e terület nem ismeretlen a Hatóság számára, hiszen mind a törvényt, mind annak végrehajtási rendeleteit véleményezte, valamint munkatársai meghívottként részt vettek olyan kormányzati egyeztetéseken, amelyek az elektronikus ügyintézéssel kapcsolatos egyes adatkezelési és adatvédelmi problémák kerültek megvitatásra. Az elektronikus ügyintézés általánosan vett tárgykörébe beleértjük a Nemzeti Egységes Kártyarendszert, a személyazonosító jel helyébe lépő azonosítási módokról és a kódok használatáról szóló 1996. évi XX. törvény vonatkozó szabályait, valamint az önkormányzati ASP rendszert is. 2017-ben több kapcsolódó jogszabálytervezetet véleményeztünk, amelyek közül a Kormányzati Adattrezor létrehozására irányuló előterjesztés emelendő ki.

VIII.5.1. A Kormányzati Adattrezor

Az elektronikus ügyintézésről szóló törvény ad felhatalmazást a biztonsági mentések végrehajtási rendeleti szabályozására. E felhatalmazás alapján a Belügy-

minisztérium előkészítette a Kormányzati Adattrezorról szóló kormányrendelet tervezetét. Az előterjesztés értelmében az elektronikus ügyintézésre kötelezett szervek rendszeres adatmentésre kötelesek az informatikai rendszereikből, amelyet át kell adniuk megőrzésre a Kormányzati Adattrezor számára. A Kormányzati Adattrezor biztosítja a mentett adatállományok tárolását, vagyis az adatforrás szervek rendeltetésszerű működéséhez szükséges adatok megőrzését és visszaállíthatóságát arra az esetre, ha az adatátadó szervek valamelyikénél természeti katasztrófa, terrortámadás, vagy más ok folytán sérülnének vagy megsemmisülnének a feladatellátáshoz szükséges nyilvántartások.

A Hatóság úgy ítélte meg, hogy a Kormányzati Adattrezor létrehozása ésszerű, legitim célt szolgál, ám adatvédelmi szempontból kockázatos, ha a szinte a teljes közigazgatás, az egészségügyi ellátórendszer, a bíróságok, továbbá a közszolgáltatást végző társaságok adatállományainak biztonsági mentései egy szerv birtokába kerülnek. Kérdésként merült fel, hogy összeegyeztethető-e az osztott információs rendszerek alkotmányos elvével az, ha az állami szféra és a közszolgáltatók adatvagyona a Kormányzati Adattrezorban koncentrálódik. E kérdés nemcsak a személyes adatok védelmével összefüggésben vethető fel, hanem úgy is, hogy vajon összhangban van-e a hatalmi ágak elválasztásának a demokratikus jogállamisághoz köthető elvével az, ha a teljes közigazgatás adatvagyonán túl például a bírósági szervezetrendszer működése során kezelt adatok is egyazon szervhez kerülnek. Továbbá az esetleges adatvesztés, valamint az illetéktelen adathozzáférés veszélye is adatvédelmi kockázatot jelenthet.

A jelzett kockázatok kiküszöbölhetők azzal, ha úgy alakítják ki az archivált adatok központosított megőrzésének rendjét, hogy az adatokhoz kizárólag csak az a szerv férhessen hozzá, amely azokat a Központi Adattrezorba helyezte. Ez célszerűen oly módon történhet, hogy az adatforrás szerv az adatállományok elküldése előtt kódolja az archivált adatokat, hogy más ne tudjon hozzáférni azokhoz. A Belügyminisztérium által véleményezésre bocsátott tervezet előírta ugyan az adatok előzetes kódolását, de csak általánosságban, ezért a Hatóság javasolta a normaszöveg kiegészítését azzal, hogy az adatállományok átalakításához szükséges kulcsokat a Kormányzati Adattrezortól független szerv állítsa elő és közvetlenül – vagyis nem az őrzésért felelős szerv útján – juttassa el azokat az adatkezelőkhöz. A további javaslataink arra irányultak, hogy valamennyi adatkezelő szervezetet saját, egyéni kulccsal lássanak el. Egy kulcs ne legyen több alkalommal felhasználható és tilos legyen harmadik szerv vagy személy tudomására hozni. Továbbá meg kell határozni az adatkezelő szervezetek kulcs kezeléssel (biztonságos tárolással) kapcsolatos feladatait is, beleértve a kulcs kompromittálódására vonatkozó protokollt. A Hatóság javasolta a szabályozást akként pontosí-

tani, hogy az Adattrezorba helyezendő adatállományok átalakítását egyértelműen az adatkezelő legyen köteles elvégezni azok átadását megelőzően.

Az Adattrezor adatfeldolgozó státusának tisztázását azért tartottuk szükségesnek, mert még az adatok leggondosabb tárolása mellett is előfordulhatnak olyan nem várt, de elvileg ki nem zárható események, mint például az Adattrezorba helyezett adatállományok megsérülése, törlése, elvesztése technikai vagy egyéb okból, vagy az Adattrezorban található adatállományok törvénysértő megszerzése olyan harmadik fél által, amely képes az adatok visszaalakítására. Lényeges, hogy az adatok megőrzéséért felelős szerv jogilag felelősségre vonható legyen ilyen helyzetben. Az Infotv. az adatkezelő és az adatfeldolgozó között osztja meg a jogi felelősséget, ezért az Adattrezornak legalább adatfeldolgozóként felelősséget kell viselnie az állományok szakszerű és jogszerű tárolásáért, annak ellenére, hogy az általa tárolt adatok tartalmát ő maga nem képes megismerni. A fenti észrevételeket a Belügyminisztérium elfogadta.

VIII.5.2. A közterületi megfigyelő rendszerek egységes informatikai rendszerbe integrálása

A Belügyminisztérium által közigazgatási egyeztetésre bocsátott, több törvény módosítását érintő előterjesztés arra irányult, hogy a jövőben a rendőrség, a közterület-felügyelet, a személyszállítási szolgáltatók, a közútkezelők, az útdíjszedők által, valamint a pénzügyi szolgáltatóknál rögzített kép- és hangfelvételeket egy a Belügyminisztériumnak alárendelt, központi állami szolgáltató szervhez kelljen továbbítani. A törvénytervezet szerint az adatkezelő szervezetek informatikai úton hozzáférést biztosítanak a törvényben feljogosított szervezetek számára és ezáltal „*az egyenként történő megkeresések mellőzhetők*”. Az előterjesztés akként mutatta be a tervezett szabályokat, hogy azok a jelenlegi jogi helyzetet lényegében nem változtatják meg, csupán a felvételek tárolási helyének megváltoztatásáról és az adatok megőrzési idejének egységesítéséről van szó. A Hatóság szerint az ország közterületeit figyelő kamerák képfolyamainak egy állami szerv számára történő kötelező átadása aligha lenne úgy értékelhető, hogy az adatvédelmi szempontból nem változtat a jelenlegi helyzeten. A képfolyamok központi tárolása megsokszorozná a megfigyelés, az adatgyűjtés és az adatok összekapcsolásának lehetőségeit, ezért adatvédelmi szempontból új helyzetet idézne elő. Továbbá a kamerákat működtető szervezeteknek sokkal kevésbé lenne lehetőségük arra, hogy a rögzített képfelvételek felhasználásának jogszerűségét ellenőrizzék, hiszen a rögzített állományok többé már nem lennének a birtokukban. Az adatkezelő szervezetek által üzemeltetett kamerarendszerek egységes adattárolási rendszerbe szervezése és

az adatokhoz való hozzáférés megkönnyítése folytán egy olyan, folyamatosan működő, készletező adatgyűjtést eredményező, titkos információgyűjtéshez felhasználható képi megfigyelőrendszer jönne létre, amely nagy földrajzi területet (a főváros kamerával megfigyelt közterületeit és az ország fontosabb közútjait) fedne le. Ezért a Hatóság szerint a tervezett központi rendszer csak akkor hozható létre, ha a szabályozás megfelelő garanciákat tartalmaz az adatok jogsértő felhasználásával szemben. Különösen fontos az adathozzáférések dokumentálása, valamint olyan ellenőrzési rendszer létrehozása, amely megfelelő visszatartó erővel bír a törvénytelen, aránytalan jogkorlátozással járó, jogsértő megfigyelésekkel szemben. Ezen kívül bizonyos közterületi helyszínek (például: templomok környezete), illetve események (például politikai demonstrációk) központosított, rejtett, adatrögzítéssel járó megfigyelésének lehetősége egyáltalán nem kívánatos.

VIII.5.3. A drónokkal végzett adatkezelés szabályozása

A gyors ütemű tudományos-technikai fejlődés időről időre olyan új műszaki-informatikai megoldások, eszközök, szolgáltatások elterjedését eredményezi, amelyek kihatnak az egyének életére és az információs jogok érvényesülésére. Az egyik ilyen viszonylag új jelenség a drónok alkalmazásának elterjedése. E folyamat nem teljesen új keletű, hiszen a Hatóság már 2014-ben közzétette ajánlásait a drónokkal végzett adatkezelés adatvédelmi követelményeiről. Emellett afelől sincs kétségünk, hogy a jövőben további jelentős fejlődés várható mind a technológiát, mind az alkalmazás elterjedését illetően. Már csak emiatt is fontos, hogy a 2017-es fejleményekről beszámoljunk.

A Nemzeti Fejlesztési Minisztérium 2017 elején hozta nyilvánosságra a pilóta nélküli légijárművek végrehajtási rendeleti szabályozására vonatkozó előterjesztést. Hatóságunk a véleményezés során egyetértett a szabályozás megalkotásának szükségességével, ugyanakkor azt javasolta, hogy a négy tervezetből álló csomag kerüljön kiegészítésre a drónokkal végzett adatkezelés szabályozásával, hiszen a pilóta nélküli légijárművek fő alkalmazási területe a megfigyelés és a légifényképezés. Ha a minisztérium elhanyagolná e tárgykör szabályozását, akkor félő, hogy az szabályozatlanul maradna. A Hatóság javaslatai a következőkre irányultak:

- A pilóta nélküli légijárművek adatvédelmi megítélése attól függ, hogy felszerelték-e képfelvételre, illetve képközvetítésre alkalmas eszközzel, és ha igen, az eszköz milyen felbontású és érzékenységű képérzékelővel, valamint optikával rendelkezik. Ezért javasoltuk ennek megfelelően differenciálni azt, hogy legalább milyen távolságra kell elkerülniük a dró-

noknak azon személyeket, illetve azoknak az otthonait, akik nem járultak hozzá a drónnal történő megfigyelésükhöz.

- A miniatürizálás előrehaladtával a jelenleg játékszernek tekintett, kis tömegű drónokon is elhelyezhetővé válnak nagy teljesítményű megfigyelőeszközök, ezért a könnyű drónok használatát is szabályozni kellene, ha azok nagy felbontású képfelvételre alkalmas kamerával rendelkeznek és a drónt kezelő személytől messzire reptethetők.
- A Hatóság szerint a magáncélú drónhasználat szabályozása mellett az állami szférában is ki kellene jelölni a drónokkal végzett adatkezelés jogi kereteit.
- Megfontolandó lenne, hogy a sajtó bizonyos könnyítéseket kaphasson az állami vezetőkkel és az állami rendezvényekkel kapcsolatos drónreptetési korlátozások alól. Mindezt nem azért, hogy a „*paparazzók*" szabadon tevékenykedhessenek, hanem azért, hogy a sajtó tehesse a dolgát a demokratikus közvélemény tájékoztatása és a közérdekű adatok terjesztése érdekében.
- Egyetértettünk azzal, hogy a drónokat napkeltétől napnyugtáig szabadjon reptetni, továbbá a drónt festéssel, vagy más módon jól láthatóvá kelljen tenni. Ez utóbbi azért lényeges, mert a halk és a környezetükbe olvadó drónok könnyen felhasználhatók lennének jogsértő megfigyelésre, vagy más illegális célra.
- A levegőben lévő drónról gyakran nem lehet megállapítani, hogy ki irányítja. Ezért egyetértettünk azzal, hogy a drónpilóta a drónreptetés közben köteles legyen a ruházatán elhelyezett piktogrammal jól láthatóan jelezni azt, hogy ő irányítja a drónt.
- Javasoltuk továbbá a drónpilóták képzési tematikáját és az állam által előírt drónpilóta vizsgakövetelményeket kiegészíteni az adatkezelési jogi és az adatvédelmi ismeretekkel.

IX. Titokfelügyelet, a minősített adatokkal kapcsolatos ügyek

Az úgynevezett titokügyek a Hatóság ügyportfóliójának heterogén részét alkotják. Az ide sorolandó ügyek mind a személyes adatok védelmével, mind a közérdekű adatok nyilvánosságával összefügghetnek. Eljárási jogi szempontból sem tekinthetők egységesnek, hiszen az Infotv.-ben meghatározottak közül a titokfelügyeleti hatósági eljáráson kívül például a vizsgálati eljárás, az adatvédelmi hatósági eljárás, az adatvédelmi audit, sőt a jogszabálytervezetek véleményezése során is felmerülhet olyan, információs alapjogot érintő kérdés, amely minősített adattal kapcsolatos. A Hatóság a nemzeti minősített adat esetében vizsgálhatja, hogy annak jogszerű volt-e a minősítése, illetve azt, hogy a minősítés sérti-e a személyes adatok védelméhez, vagy a közérdekű adat megismeréséhez és terjesztéséhez való jog érvényesülését. A külföldi minősített adat esetében a minősítés jogszerűségének ellenőrzése kívül esik a Hatóság hatáskörén.

A titokügyek a fentiekben vázolt sokféleségük ellenére olyan közös sajátosságokkal rendelkeznek, amelyek miatt mégis célszerű külön ügycsoportként kezelni őket. Elsősorban azért, mert a minősített adatok védelméről szóló 2009. évi CL. törvény (a továbbiakban: Mavtv.) a törvényben nevesített államérdekek által reprezentált közérdek védelme érdekében sajátos elveket, jogintézményeket és szigorúan betartandó korlátozó előírásokat határoz meg a minősített adatok védelme érdekében, amelyek a további, a jog által védett titokkategóriákra (például: banktitok, üzleti titok stb.) vonatkozó szabályoktól is jelentősen eltérnek. Néhányat felsorolunk a sajátosságok közül, a teljesség igénye nélkül:

- A minősítés a Mavtv.-ben részletesen szabályozott eljárás, amelyben nagy szerepet kap a formai és procedurális előírások maradéktalan betartása; ellenkező esetben az adat minősített jellege nem jön létre.
- A *„szükséges ismeret”* elve korlátozza azt, hogy kik férhetnek hozzá a minősített adatokhoz.
- A minősítés érvényességének időtartama alatt, vagyis a minősítés megszűnéséig vagy a minősített adat törléséig a minősítőt (jogutódlás esetén a minősítő jogutódját) illeti meg a legteljesebb rendelkezési jogkör a minősített adatot illetően, attól függetlenül, hogy az adat a minősítő birtokában van-e vagy azt másnak továbbította.

Van egy másik, gyakorlatias oka is a titokügyek külön ügycsoportként való kezelésének, mégpedig az, hogy a minősített adatokkal kapcsolatban olyan személyi, adminisztratív és műszaki biztonsági előírásoknak kell megfelelnünk,

amelyek a többi ügyre nem vonatkoznak. A „*Bizalmas*” és annál magasabb minősítésű adatok és iratok felhasználására csak a Mavtv. végrehajtási rendeletében meghatározott biztonsági követelményeknek megfelelő biztonsági területen kerülhet sor. A minősített adatokat tartalmazó iratanyagot ügyviteli szempontból teljesen el kell választani a többi irat kezelésétől. A minősített adatok készítésére és felhasználására szolgáló, úgynevezett TEMPEST informatikai rendszernek védettnek kell lennie a kompromittáló elektromágneses kisugárzás ellen. Csak olyan munkatárs dolgozhat minősített adatokkal, akinek a nemzetbiztonsági ellenőrzése megtörtént és az kockázati tényezőt nem állapított meg. A Hatóság a biztonsági követelményeknek való magas szintű megfelelés érdekében 2017-ben bővítette a biztonsági területét, intézkedett NATO TEMPEST Level A osztályú informatikai eszközök beszerzésére, valamint kezdeményezte a Kormányzati Rejtjelezett Gerinchálózathoz kapcsolását. Ezek után a 2017. évi titokügyekre áttérve a következőket emeljük ki.

IX.1. A kémper adatainak minősítése

Egy újságíró bejelentése alapján vizsgálta a Hatóság az úgynevezett kémper adatai minősítésének jogszerűségét. Korábban a sajtó bőséges tájékoztatást adott arról, hogy a Fővárosi Ítélőtábla 2017. szeptemberi jogerős ítéletében felmentette a kémkedéssel és bűnpártolással vádolt korábbi nemzetbiztonsági vezetőket, a korábbi titkosszolgálati minisztert és egy magánszemélyt. Az ügyet korábban is közérdeklődés övezte, ám a per tárgyáról csak keveset lehetett tudni, mert a bíróság az eljárás során minősített adatokat használt fel. Ugyanakkor különböző sajtóorgánumok ismeretlen forrásból származó, kétes megbízhatóságú információkat szivárogtattak a kémperben tárgyalt ügy vélt vagy valós részleteiről. A Hatóság úgy ítélte meg, hogy a felmentő ítélet visszamenőleg is kétségbe vonhatja a per során kezelt adatok legalábbis egy része esetében a minősítés szükségességét, továbbá egyetértett a bejelentővel abban, hogy a vádlottak közül voltak olyanok, akik kifejezetten a közhatalom gyakorlásával összefüggő minőségükben elkövetett cselekmények vádja miatt álltak bíróság előtt, így a közvéleménynek kiemelkedő alkotmányos érdeke fűződik a történtek megismeréséhez. A Hatóság megállapította, hogy a nyílt büntetőeljárást megelőzően a Nemzeti Védelmi Szolgálatnál (a továbbiakban: NVSZ) folytatták az ügy felderítését és az eljárás során gyűjtött adatok minősítése az NVSZ-nél történt meg. Ezt követően a Hatóság a minősítés részletes indokolását kérte a minősítőtől, valamint a helyszínen tanulmányozta a minősített adatokat tartalmazó iratokat. Ennek eredményeként megállapította, hogy a terjedelmes, több kötetnyi iratanyagban a szerteágazó felderítő tevékenység sok olyan részadata szerepel,

amelynek titokban tartásához továbbra is államérdekek fűződnek, így például a következők:

- Egyes adatok nyilvánosságra hozása esetén beazonosíthatóvá válna az információforrás. Ebben az esetben az információt szolgáltató személynek hátrányos következményekkel kellene számolnia. Ha a magyar bűnüldöző szervek nem tudnák titokban tartani a titkos információforrásaik kilétét, az a bűnüldözési érdek sérelmével járna, ugyanis kétséges, hogy bárki is vállalná a bűnüldöző szervekkel történő együttműködést, ha nem lehetne biztos abban, hogy személyazonossága titokban fog maradni.
- Az ügy egyes részleteit azért nem szabad nyilvánosságra hozni, mert az hátrányosan befolyásolhatná Magyarország külkapcsolatait.
- Az adatok nyilvánosságra kerülése esetén rekonstruálni lehetne a bűnügyi felderítő tevékenység konkrét részletes eljárásrendjét, módszertanát és a titkos információszerző képességek határait. Ha ez a potenciális célszemélyek tudomására jutna, az a későbbi felderítések eredményességét veszélyeztetné, vagyis bűnüldözési érdeket sértene.

Ugyanakkor a Hatóság szerint a felderítő tevékenység során gyűjtött és később a büntetőeljárásban a per tárgyát képező történések lényegének megismeréshez közérdek fűződik, amely erősebb, mint a nyilvánosság korlátozását alátámasztó szempontok. A már felsorolt körülményeken (a felmentő ítélet és a terhelt személyek korábbi közhatalmi beosztása) a nyilvánosság mellett szóltak még a következők is:

- A tényállás egy része már korábban kiszivárgott és a sajtó révén nyilvánosságot kapott. A széles körű nyilvánosság elé tárt részletek minősítésének fenntartása nyilvánvalóan szükségtelen.
- Az eljárásban egy magyar nemzetbiztonsági szolgálat külföldről történő befolyásolása merült fel. Ez olyan jellegű és súlyú ügy, amelyről a demokratikus közvéleményt tájékoztatni kell.

Az ellentmondás feloldása érdekében a Hatóság kiválasztott az iratanyagból egy olyan, a felderítő tevékenységet összegző jelentést, amely a kellő részletességgel taglalta az NVSZ információgyűjtő tevékenysége során feltárt tényállást, ám nem tartalmazott minősített adatot, ezért a minősítésének fenntartása már nem volt indokolt, majd ezt követően a titokfelügyeleti hatósági eljárásban hozott határozatában felszólította a minősítőt a hivatkozott jelentésben lévő adatok minősítésének megszüntetésére. A minősítő a Hatóság határozatával szemben a törvényes határidőn belül nem fordult a bírósághoz, ezért az iratban rögzített adatok minősítése megszűnt.

A titokfelügyeleti hatósági eljárás során olyan információk jutottak a tudomásunkra, amelyek szerint a Fővárosi Ítélőtábla előtt folyó per iratanyagában olyan minősített adatok is szerepeltek, amelyek minősítése nem a Nemzeti Védelmi Szolgálatnál történt. Ezen adatok esetében a minősítés jogszerűségét egy későbbi titokfelügyeleti hatósági eljárásban fogjuk ellenőrizni.

IX.2. A Soros György által támogatott civil szervezetekkel kapcsolatban gyűjtött adatok

Erősen polarizálja a közvéleményt és a politikai véleményformálókat a külföldön élő Soros György tevékenységének megítélése. Vannak, akik szerint az általa támogatott szervezetek révén leplezett befolyásszerzésre és az állami döntéshozatal befolyásolására törekszik, míg mások szerint ezek a feltételezések alaptalanok. Ilyen körülmények között nem csoda, hogy több eljárás is indult a Hatóságnál a Soros Györggyel és az általa támogatott civil szervezetekkel kapcsolatos adatokkal összefüggésben.

Németh Szilárd, az Országgyűlés Nemzetbiztonsági bizottságának alelnöke 2017. márciusában azt nyilatkozta egy híroldalként működő blognak, hogy a titkosszolgálatokhoz fordult, *„összegyűjtve a Soros-hálózattal együttműködő szervezetek nevét, kérve a tevékenységük teljes átvilágítását*". A nemzetbiztonsági szolgálatokról szóló 1995. évi CXXV. törvény (a továbbiakban: Nbtv.) nem hatalmazza fel a Nemzetbiztonsági bizottság alelnökét, hogy konkrét feladatot, hírigényt határozzon meg a nemzetbiztonsági szolgálatok számára, azért a Hatóság hivatalból eljárva tájékoztatást kért Németh Szilárd úrtól, hogy valóban az hangzott-e el, ami a blogban megjelent. Erre válaszul a nemzetbiztonsági bizottság alelnöke akként pontosította a blogbejegyzésben közzétetteket, hogy a rá irányadó jogszabályi rendelkezéseket ismerve és betartva, közvetlen utasítást intézkedésre soha nem adott a nemzetbiztonsági szolgálatok számára.

Titokfelügyeleti hatósági eljárás keretében ellenőrizte a Hatóság azt, hogy jogszerűen minősítették-e *„Szigorúan titkos!"* minősítési szintre azokat a Soros Györggyel és az általa támogatott szervezetekkel kapcsolatos adatokat, amelyeket az Országgyűlés Nemzetbiztonsági bizottsága zárt ülésen tárgyalt. Az eljárás során a Hatóság megismerte a zárt ülés jegyzőkönyvét, továbbá tisztázta, hogy az adatok minősítésére az Információs Hivatalnál (a továbbiakban: IH) került sor, ugyanis a Nemzetbiztonsági bizottság az IH-tól származó adatokat használt fel.

A tényállást megismerve a Hatóság arra a meggyőződésre jutott, hogy erős közérdek fűződik ahhoz, hogy a közvélemény a zárt ülésen elhangzottakat megismerve reális képet alkothasson arról, hogy hátrányos-e a magyar nemzetbiztonsági érdek szempontból Soros György és az általa támogatott civil szervezetek tevékenysége, vagy sem. Azonban két olyan nyomós indokra is fény derült, amelyek az adatok minősítésének fenntartása mellett szólnak:

1.) A Nemzetbiztonsági bizottság a zárt ülésen az IH, vagyis a külföldi hírszerzési feladatokat ellátó nemzetbiztonsági szolgálat által gyűjtött információkat tárgyalta. A Hatóság az IH főigazgatójának részletes indokolásával egyetértve azt állapította meg, hogy a zárt ülésen tárgyalt adatok nyilvánosságra hozása esetén következtetni lehetne arra, hogy az IH milyen titkos hírszerző pozíciókkal rendelkezik más országok felső állami, politikai és gazdasági döntéshozói körében. Ez ellehetetlenítené a magyar hírszerző tevékenységét, és ha a külföldi kémelhárító szolgálatok, illetve bűnüldöző szervek képesek lennének beazonosítani a magyar hírszerzés titkos információforrásait, akkor az érintett külföldieknek súlyos büntetőjogi retorziókkal kellene számolniuk az országukban.

2.) A zárt ülésen olyan vélemények és megállapítások hangzottak el más államok vezetésével és politikájával kapcsolatban, amelyek nélkülözték a diplomáciai udvariasság ismérveit, ezért a nyilvánosságra kerülésük zavart okozna Magyarország diplomáciai és külpolitikai kapcsolataiban.

Mindezek alapján a Hatóság úgy ítélte meg, hogy bár kívánatos lenne az eljárás tárgyát képező adatok minősítésének megszüntetése, azonban ennél nyomósabbak azok a nemzetbiztonsági és külpolitikai érdekek, amelyek a minősítés fenntartása mellett szólnak, ezért a titokfelügyeleti hatósági eljárást megszüntette.

IX.3. Az utólagos minősítés problematikája

Az egyik titokügy vizsgálata során az derült ki, hogy a minősítő nem az adatok keletkezését követően minősítette az adatokat, hanem évekkel később, ezért kérdésként merült fel, hogy elfogadható-e az a minősítési gyakorlat, vagy jogsértő. A Hatóság álláspontja a következő volt:

1.) Ha az adat minősítésének törvényben meghatározott feltételei fennállnak, úgy az adat minősítése nem halogatható. A minősítési eljárás késedelmes lefolytatása azért lenne hátrányos az információszabadság szempontjából, mert végső soron meghosszabbodna az adat keletkezésétől a közérdekű adat meg-

ismerhetővé válásáig (a minősítés megszűnéséig) terjedő időtartam. Ha a minősítő késedelmesen folytatja le a minősítési eljárást és olyan érvényességi időt határoz meg, amely ugyan a minősítéstől számított maximális érvényességi időn belül van, ám lényegesen meghaladja az adatok keletkezésétől számított, az adott minősítési szintre vonatkozóan a Mavtv.-ben meghatározott maximális érvényességi időtartamot, akkor ez a minősítés érvényességi idejének limitálására vonatkozó törvényi előírás megkerülésének tekintendő, amely az adat nyilvánosság előli elvonásának meghosszabbítása következtében sérti a közérdekű adatok megismeréséhez való jog érvényesülését. (Más ügyekben szerzett jogalkalmazási tapasztalataink szerint olyan is előfordult, hogy a minősítő egészen addig kivárt a minősítéssel, amíg adatigény érkezett a közérdekű adat megismerése iránt. Ilyen esetben egyértelműen megállapítható volt a minősítői jogkör visszaélésszerű alkalmazása.)

2.) A minősített adat kezelése során az általános iratkezelési előírásoknál szigorúbb személyi, fizikai, adminisztratív és elektronikus biztonsági előírások irányadók. A minősített adatokat tartalmazó adathordozókhoz történő hozzáférés, valamint az adatok felhasználása (továbbítás, sokszorosítás stb.) feltételekhez kötött és pontosan dokumentált. A titokvédelmi rezsim betartása csak akkor garantálható, ha az adatot a keletkezését (rögzítését, felvételét stb.) követően késlekedés nélkül minősítik azt. (A Mavtv. 6. § (6) bekezdése szerint a minősítési eljárás alatt álló adatot a minősítő döntéséig a kezdeményezett minősítési szintre vonatkozó személyi, fizikai, adminisztratív és elektronikus biztonsági szabályok szerint kell kezelni.)

Ha a minősítés később történik meg, akkor kérdéses, hogy az adat keletkezése és a minősítési eljárás megkezdése közötti időben ténylegesen ki fért hozzá az adatokhoz. Ha minősített adat illetéktelen személyhez kerül, akkor utólag már alig lehet bizonyítani azt, hogy az adat megszerzésére a minősítést megelőzően vagy azt követően történt. Az esetleges titoksértés megállapíthatóságával kapcsolatban ilyesféle jogbizonytalanság azért sem fogadható el, mert a minősített adattal való visszaélés büntetőjogi kategória.

IX.4. A paksi atomerőmű beruházás adatainak nyilvánossága

A Paks II. beruházás adatainak nyilvánosságával kapcsolatban számos bejelentés érkezett és érkezik a Hatósághoz. A beadványok sokféle adatra vonatkoznak, ide értve például a megvalósítási megállapodásokat, a tanácsadói szerződéseket és a beruházás előkészítésével kapcsolatos dokumentumok

megismerhetőségét. E bejelentésekkel kapcsolatban a Hatóság párhuzamosan több eljárást – vizsgálatot vagy titokfelügyeleti hatósági eljárást – indított, amelyek közül 2017-ben lezárásra kerültek a következők:

1.) A beruházás végrehajtási megállapodásainak ügyében több egyeztetésre került sor a minősítő képviselőivel, amelynek során tisztáztuk, hogy mely adatok védendők minősítéssel és melyek minősítése szüntetendő meg. Az eljárás folyamán a minősítő először a legalacsonyabb, „Korlátozott terjesztésű!" szintre csökkentette az adatok minősítését, majd az iratanyag nagy részének minősítését megszüntette. A fennmaradó adatok olyan, zömmel műszaki, biztonsági információkat tartalmaznak, amelyek minősítésének fenntartása továbbra is indokolt, ezért a Hatóság megszüntette az ügyben folytatott eljárást.

2.) A beruházás előkészítése során kötött több száz, részben minősített adatot, részben üzleti titkot is tartalmazó szerződés esetében a Hatóság több konzultáció és helyszíni vizsgálat keretében módszertani segítséget nyújtott az adatkezelő szervnek ahhoz, hogy a közérdekű adatok megismeréséhez való joggal összhangban vizsgálja felül a szerződéseket és tegye azokat hozzáférhetővé az adatigénylők számára. Ehhez a következőket kellett tisztázni az egyes szerződések esetében:

- a közérdekű adattartalom beazonosítása,
- üzleti titoktartalom meghatározása,
- az egyes speciális adatkörökre – például a környezeti adatok vagy az erőmű biztonsági adatok – vonatkozó jogi követelmények azonosítása,
- a nemzetbiztonsági érdekből védendő adatok problematikája.

A Hatóság ezen túl a következőkre hívta fel a figyelmet:

- A minősítés mindig konkrét adatra és nem teljes dokumentumra vonatkozik. A minősített adatot tartalmazó szerződések minősítéssel nem védendő részeit hozzáférhetővé kell tenni.
- A minősített adatot tartalmazó részek esetében sem szükségszerű a minősítés fenntartása. Ha a minősített adat védelméhez fűződő érdek már megszűnt, akkor a minősítést felül kell vizsgálni és meg kell szüntetni.
- A kitakarandó iratrészek esetében a teljes bekezdés, illetve mondat törlése helyett csak a valóban védendő információkat szabad megismerhetetlenné tenni az anonimizált másolaton.

A szakmai egyeztetéseket követően két ütemben, az első alkalommal mintegy 170, míg második alkalommal további mintegy 90 irat kiadása történt meg. Ezáltal az iratok egy része teljes egészében megismerhetővé vált, néhány dokumentum

azonban tartalmazott olyan, döntés-előkészítéssel összefüggő, illetve műszaki és védelmi-biztonsági jellegű adatokat, amelyek továbbra is védendők, ezért ezeket a védendő adatok nélkül, kivonatos formában küldték meg az adatigénylőknek. A vizsgálati eljárás tárgyát képező adatok kiadását az adatkezelő teljesítette, ezért a Hatóság az ügyben folytatott eljárást lezárta.

IX.5. A TIBEK és az ügyészség adatkapcsolata

A Hatóság egy konzultációs kérdés kapcsán értelmezte a Terrorelhárítási Információs és Bűnügyi Elemző Központ (a továbbiakban: TIBEK) Nbtv.-ben szabályozott adatigénylési jogosultságát az ügyészség által kezelt adatokkal összefüggésben.

A TIBEK Magyarország nemzetbiztonsági szolgálatainak egyike. Az Nbtv.-ben szabályozott adatkezelése két tekintetben tér el más nemzetbiztonsági szolgálatokétól. Egyrészt nem jogosult az általa kezelhető adatok megszerzéséhez titkos információgyűjtő tevékenység végzésére, másrészt pedig a törvényben meghatározott körben, az együttműködő szervek vonatkozásában közvetlen elektronikus adatkapcsolat útján szerzi be a tevékenysége ellátásához szükséges adatokat. A jelenlegi törvényi szabályozás szerint a TIBEK az Nbtv. általános adatkezelési előírásainak megfelelő megkeresés útján szerzi be azon adatokat, melyek a közvetlen elektronikus kapcsolat útján nem szerezhetők be, illetve melyek adatkezelői nem tartoznak a törvényben meghatározott együttműködő szervek közé, ahogyan az ügyészség sem tartozik ebbe a körbe.

A fentiekre tekintettel az Nbtv. 40. § (1) bekezdése alapján az általános szabályok szerint az adatok átadása akkor lehetséges az ügyészség részéről, ha a TIBEK az adatkérés célját megjelölte. Ennek hiányában nem lenne jogszerű a TIBEK adatkérése. Valamint az ügyészségről szóló 2011. évi CLXIII. törvény (a továbbiakban: Ütv.) 32. § (6) bekezdése alapján is megvan a lehetőség az adatok átadására azzal, hogy az Ügyészség kizárólag *„a kérelmező szerv által törvény alapján kezelhető adatok körére kiterjedően”* adhat át adatokat. A szabályozás tartalmát tekintve megállapítható, hogy nem az érintett bűncselekményi kör törvényi kijelölésére van szükség az adatok átadásánál, hanem az adatkérés céljának megjelölése elengedhetetlen.

A Hatóság megállapította, hogy az ügyészség és a TIBEK közötti együttműködési megállapodás megkötésének és az az alapján történő adatátadásnak a törvényi előírások megtartása esetén nincsen akadálya, tehát az adatkezelés alapvető szabályaira vonatkozó Infotv. és a fenti kógens szabályok megtartá-

sa mellett valósítható meg az adattovábbítás szabályozása az együttműködési megállapodásban.

Fontos kiemelni, hogy az Infotv. személyes adatok kezelésére vonatkozó rendelkezéseitől (személyes adatok védelméhez való jog korlátozásának szükségessége és arányossága; személyes adatok kezelésének célhoz kötöttsége; adatkezelés törvényessége és tisztességessége) érvényesen eltérni nem lehet, így az esetleges általános, keretjellegű megkeresés engedélyezési gyakorlat nem lenne összhangban a jogintézmény céljával, ezért joggal való visszaélést valósítana meg. Az adatszolgáltatást megalapozó körülmények adattovábbító általi mérlegelése bizonytalanságot eredményezhet arra vonatkozóan, hogy mikor szükséges az adatok továbbítása és mikor nem. Fontos hangsúlyozni, hogy mérlegelést kizáró módon, egyértelműen kell meghatározni, hogy mely körülmények alapozzák meg az adatkérés, illetve adattovábbítás szükségességét.

IX.6. A TEK adatigénylési jogosultsága

Az előbb ismertetetthez némileg hasonló ügyben, az Alapvető Jogok Biztosa által áttett beadvány alapján indított vizsgálati eljárás során az a kérdés merült fel, hogy milyen adatvédelmi követelményeknek kell megfelelnie a Terrorelhárítási Központnak (a továbbiakban: TEK) az adatigénylés során. A vizsgálat során megismert tényállás szerint a TEK részéről eljáró hivatásos állományú tiszt a helyszínen, az adatkezelő szerv (egy gazdasági társaság) telephelyén szóban közölte a TEK adatigényét. Ezzel kapcsolatban a Hatóság a következő javaslatokat fogalmazta meg a TEK főigazgatója számára:

– Az adatigénylés (az adatkezelés jogszerűségének ellenőrizhetősége és az adattovábbítás dokumentálhatósága érdekében) kizárólag írásban történhet.
– Az adatigénylésnek tartalmaznia kell az adatfelhasználás céljának és jogalapjának megjelölését.
– Az írásbeli megkeresésben pontosan meg kell jelölni a kért adatkört. Ezt az indokolja, hogy az adatátadónak joga és egyben kötelessége, hogy az adatigény teljesítése előtt meggyőződjön a hivatkozott cél- és jogalap fennállásáról. Ez természetesen nem azt jelenti, hogy az adatkezelő szerv jogosult lenne megismerni azt a konkrét tevékenységet, amely érdekében a TEK az adatokat igényeli. A rendvédelmi szervek és a nemzetbiztonsági szolgálatok adatkérései esetében, e szervek tevékenységének jellegére tekintettel az adatkérés konkrét céljának le-

írása helyett a cél megjelölése történhet a szerv adott tevékenységére, feladatkörére utaló jogszabályra hivatkozással. A jogalap megjelölése pedig – a meghatározott feladat ellátása érdekében – adatkérésre felhatalmazó jogszabályra, valamint a konkrét ügyszámra történő hivatkozással.
– Felhívtuk a figyelmet arra is, hogy az adatigénylésnek tartalmaznia kell a jogorvoslati jogról történő tájékoztatását is (vagyis hogy panasszal a szerv irányításáért felelős miniszterhez, valamint a NAIH-hoz bejelentéssel fordulhatnak, mely lehetőségek egymástól függetlenül fennállnak).

A jogorvoslattal kapcsolatban a TEK főigazgatója vitatta a Hatóság fenti álláspontját és azon a véleményen volt, hogy a TEK titkos információgyűjtés keretében történő adatigénylésével szembeni panasz kivizsgálására – speciális jogorvoslati rend érvényesülése miatt – a rendészetért felelős miniszter jogosult, ezért felterjesztette az ügyet a belügyminiszterhez. A Belügyminisztérium válaszában egyetértett a NAIH álláspontjával, mind a jogorvoslati rendre vonatkozóan (elismerve, hogy a panasz kivizsgálására mind a rendészetért felelős miniszter, mind a NAIH jogosult, a két hatáskör egymástól függetlenül és párhuzamosan is gyakorolható), mind abban a tekintetben, hogy a titkos információgyűjtés során alkalmazott adatigényléseknél milyen adatvédelmi szempontoknak kell érvényesülniük.

Az eljárás eredményeként a TEK tájékoztatta a Hatóságot, hogy – bár a szóban forgó adatkérés okafogyottá vált – a hasonló adatigényléseik tekintetében a NAIH tájékoztatása szerinti adatvédelmi szempontoknak megfelelő eljárásrendet fognak kialakítani és az adatigényeket tartalmazó megkereséseket a Hatóság által meghatározott tartalmi és formai követelményeknek megfelelően fogják végezni.

IX.7. A tömeges bevándorlás okozta válsághelyzet fenntartását szükségessé tevő információk nyilvánossága

Egy beadványozó azt kérte, hogy a Hatóság vizsgálja meg, szükséges-e fenntartani a tömeges bevándorlás okozta válsághelyzet fenntartása indokainak titkosságát.

A menedékjogról szóló 2007. évi LXXX. törvény 80/A. § (2) bekezdése kimondja, hogy az országos rendőrfőkapitány és a menekültügyi hatóság vezetőjének kezdeményezésére, az idegenrendészetért és a menekültügyért felelős miniszter

javaslatára a Kormány rendeletben rendelheti el a tömeges bevándorlás okozta válsághelyzetet. Ez a 41/2016. (III.9.) Korm. rendelet. A menedékjogról szóló törvény 80/A. § (3) bekezdése előírja az országos rendőrfőkapitány és a menekültügyi hatóság vezetőjének, hogy a tömeges bevándorlás okozta válsághelyzet feltételeinek fennállását folyamatosan kísérje figyelemmel, valamint a fent hivatkozott kormányrendelet 4. §-a előírja, hogy rendszeresen tájékoztassák a tömeges bevándorlás okozta válsághelyzet feltételeinek fennállásáról az idegenrendészetért és a menekültügyért felelős minisztert.

A Hatóság vizsgálati eljárást indított, és a fentiekre tekintettel a belügyminisztert kereste meg. A Belügyminisztérium válaszában arról tájékoztatta a Hatóságot, hogy az országos rendőrfőkapitány és a menekültügyi hatóság vezetője által előterjesztett jelentés nem minősül a Mavtv. szerinti nemzeti minősített adatnak és azt a Belügyminisztérium hozzáférhetővé is tette közérdekű adat megismerésére vonatkozó igény alapján. Bár ezzel az ügy további vizsgálata okafogyottá vált, ezért azt a Hatóság megszüntette. Érdemes megemlíteni, hogy ezt követően a 41/2016. (III. 9.) Korm. rendelet hatályának meghosszabbítására vonatkozó előterjesztés közigazgatási egyeztetésekor a Hatóság felhívta a Belügyminisztérium figyelmét arra, hogy a válsághelyzet elrendelésének meghosszabbításáról szóló döntés kiemelt közérdeklődésre tart számot, ezért az azt megalapozó információkat közzé kell tenni.

IX.8. A nemzetbiztonsági ellenőrzés során kezelt minősített adatok védelme

Egy magánszemély azért fordult a Hatóságunkhoz, mert névtelen gyalázkodó levelet kapott, amely olyan részleteket tartalmazott a magánéletéről és a családjáról, amelyekről vélelmezte, hogy titkos információgyűjtéssel szerezték meg. Korábban fontos és bizalmas beosztást töltött be, ezért számításba vette azt a lehetőséget, hogy a névtelen levél szerzője azokhoz az információkhoz juthatott hozzá, amelyeket a korábbi nemzetbiztonsági ellenőrzése során gyűjtöttek róla és a családjáról. Ezért annak kivizsgálását kérte, hogy hozzáférhetett-e illetéktelen személy a nemzetbiztonsági ellenőrzésének minősített adatot tartalmazó iratanyagához. A Hatóság vizsgálatot indított és az adatkezelőnél tartott helyszíni vizsgálat keretében ellenőrizte az adatkezelés körülményeit, így a kezelt adatok körét és azt, hogy illetéktelen személy hozzáférhetett-e jogosulatlanul a bejelentésben megjelölt személyes adatokhoz. A Hatóság a tényállás tisztázása érdekében a vizsgálat során az adatkezelőtől írásbeli és szóbeli felvilágosítást kért, az adatkezelő kezelésében levő, az üggyel összefüggésbe hozható iratok-

ba betekintett, az adatkezelés helyszínéül szolgáló helyiségbe belépett, valamint a vizsgált üggyel összefüggésbe hozható adatkezelést megismerte. Ennek eredményeként megállapítást nyert, hogy a nemzetbiztonsági ellenőrzés során gyűjtött adatokhoz csak ellenőrzött és dokumentált körülmények között lehet hozzáférni. A vizsgálat során nem merült fel olyan körülmény, amely illetéktelen adathozzáférésre utalt volna. Azt ugyanakkor nem lehetett kizárni, hogy a gyalázkodó levélben írt információk más forrásból, például az érintett ismeretségi köréből is származhattak. A biztonsági ellenőrzés adatainak kezelésével kapcsolatban jogsértésre utaló körülmény nem merült fel, ezért a Hatóság az ügyben folytatott eljárást megszüntette.

X. Nemzetközi kapcsolatok

2017-ben az összes uniós adatvédelmi hatóság leginkább a GDPR és az uniós Bűnügyi Irányelv új szabályozási rendszereire való felkészülésre koncentrált.

A Brexittel kapcsolatban a brit adatvédelmi hatóság megerősítette, hogy a jövőben is szorosan együtt kívánnak működni az uniós adatvédelmi munkacsoportokkal, az illetékes brit (digitális gazdaságért felelős) miniszter pedig elkötelezett a GDPR teljes körű alkalmazása mellett 2018 májusától. Ugyanakkor a Bizottság felhívta a nyilvánosság figyelmét arra, hogy 2019. március 30-tól az Egyesült Királyság a GDPR értelmében adatvédelmi szempontból úgynevezett harmadik országnak minősül, ennek minden következményével együtt.[62]

Számos bilaterális, regionális és nemzetközi tanácskozás témája volt egy-egy általános vagy részletszabályozás gyakorlati kidolgozásának problematikája. Ezek sorából is kiemelkedik a 2017 októberében Visegrádon megrendezett adatvédelmi hatóságok V4-es találkozója, ahol stratégiai és szervezeti kérdéseket vitattak meg a hatóságok vezetői; az osztrák adatvédelmi hatóság munkatársainak tartott, több fordulós GDPR-eset megoldó tréning, ahol meghívottként a magyar NAIH munkatársai is jelen lehettek; illetve a hollandiai tanulmányút[63], ahol a helyszínen ismerkedhettünk meg a 2016. január 1. óta működő adatvédelmi incidens jelentési rendszerrel (2016-ban a több, mint 6000 bejelentés 28%-a az egészségügyi, 20%-a a pénzügyi, 19%-a a közszféra, 8%-a a telekommunikációs szektort érintette.)

Az USA-Európai Unió között 2016. július 12-én megkötött, és az érvénytelenített Safe Harbour egyezmény helyébe lépő új adatvédelmi keretegyezmény, az ún. Adatvédelmi Pajzs Egyezmény (Privacy Shield) első éves felülvizsgálatát végző uniós delegáció egyik tagja a NAIH munkatársa volt. A felülvizsgálatról szóló jelentés elismeri ugyan a keretegyezmény jelentőségét (eddig több, mint 2400 amerikai vállalat kezdeményezte azt a hitelesítési eljárást, ami alapján felkerülhet a megbízható adatkezelők listájára), azonban még mindig nem nevezték ki az uniós állampolgárok adatvédelmi panaszait kivizsgálni hivatott ombudsmant és a szintén adatvédelmi tárgyú kormányzati ellenőrzéseket lefolytató Privacy and Civil Liberties Oversight Board-ban csak egy biztos van hivatalban az ötből,

62 http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=611943

63 A holland adatvédelmi hatóság 2017-ben a Microsoft Windows 10 operációs rendszerének vizsgálatánál számos jogsértő gyakorlatot fedett fel. Részletesen lásd: https://autoriteitpersoonsgegevens.nl/en/news/dutch-dpa-microsoft-breaches-data-protection-law-windowswindows-10

másrészt még mindig nem épült ki megnyugtató módon a nemzetbiztonsági célú adatkezelések – tömeges megfigyelések – uniós állampolgárokat érintő garancia rendszere.

Hosszú évek óta folyik az Európa Tanács 108-as adatvédelmi egyezményének modernizálásáról szóló tárgyalás. 2017-ben ezen a területen csak kisebb előrelépések történtek, de tovább folyt az egyeztetés az egészségügyi adatok kezeléséről vagy a rendőrségi adatkezelésekről szóló Európa tanácsi ajánlásokról, megszületett viszont a humanitárius tevékenységek adatvédelméről szóló kézikönyv[64], mely olyan, szó szerint létfontosságú kérdéseket tárgyal, mint például a háborús övezetekben hogyan kivitelezhető a veszélyeztetett segélyezettek személyes adatainak védelme vagy hogyan lehetséges az üzenetküldő alkalmazásoknál az adatok titkosítása.

Szintén kiemelkedő jelentőségű, hogy 2016-17-ben az Európa Tanács gyermekjogi bizottságának digitális jogokkal foglalkozó szakértői csoportja (CAHENF-IT) – melynek meghívás alapján a NAIH munkatársa is tagja volt – kidolgozta a tagállamoknak szóló ajánlás-tervezetét, amely a gyermekek jogainak előmozdításával és védelmével foglalkozik a digitális környezetben. A szigorú gyermekvédelmi normákat felállító anyag elfogadása 2018-ban várható.

Végül 2017-ben a nemzetközi panaszügyek sorában említésre méltó jelentőségű, mikor egy pakisztáni állampolgár arról tájékoztatta a Hatóságot, hogy Ügyfélkapu regisztrációja során adatai nem kerültek be az elektronikus ügyintézést igénybe vevő külföldiek személyi nyilvántartásába (3.NYT). Az ügyben indított vizsgálat során kiderült, hogy Magyarország külképviseletein nem volt mód a 3.NYT rendszerben történő regisztrációra, mert a külképviseleteken a kötelezően rögzítendő arcképmás és az aláírás vételezéséhez rendszeresített eszközök nem voltak azonosak az okmányirodákban alkalmazott eszközökkel, így a külképviseleteken használt biometrikus adatvételezésre alkalmas eszközök (G3) és a 3.NYT közötti adatátadás nem működött. A 3.NYT nyilvántartás vonatkozásában az adatkezelési és hatósági feladatokat ellátó Belügyminisztérium Nyilvántartások Vezetéséért Felelős Helyettes Államtitkársága arról tájékoztatta a Hatóságot, hogy 2017. év végére megvalósultak a Magyarország külképviseletein történő 3.NYT, illetve Ügyfélkapu regisztrációhoz szükséges informatikai fejlesztések.[65]

64 https://www.icrc.org/en/publication/handbook-data-protection-humanitarian-action
65 NAIH/2017/2692/I számú ügy.

X.1. Részvétel a 29-es Adatvédelmi Munkacsoport munkájában

A 29-es Adatvédelmi Munkacsoportnak[66], amely az Európai Unió adatvédelmi irányelvének 29. cikke alapján látja el elsősorban tanácsadói feladatait, a 2017-es volt az utolsó teljes éve. Az új adatvédelmi rendelet, a GDPR értelmében ugyanis helyét 2018 májusától az Európai Adatvédelmi Testület veszi át. A Munkacsoport 2017-ben elsősorban a GDPR-ra való felkészülésre összpontosította munkáját, és olyan iránymutatásokat fogalmazott meg, amelyek a rendelet gyakorlati alkalmazásához nyújtanak segítséget, mind az adatkezelőknek, mind a jogalkalmazó hatóságoknak.

Az iránymutatások az alábbi témákban születtek:

- Az adathordozhatóság jogáról
- Az adatvédelmi tisztviselőről
- A vezető hatóságról
- Az adatvédelmi hatásvizsgálatról
- Az adatvédelmi (közigazgatási) bírságról
- Az adatvédelmi incidens bejelentéséről
- Az automatizált egyedi döntéshozatalról és a profilozásról
- Az érintetti hozzájárulásról
- Az adatkezelés kapcsán az átláthatóságról
- A harmadik országba irányuló adattovábbítással összefüggésben több kérdésben is

Az iránymutatások angol nyelvűek és fokozatosan válnak az Unió valamennyi hivatalos nyelvén elérhetővé.

A Munkacsoport 2018-ban is bocsát ki új, illetve véglegesít korábban nyilvános konzultációra bocsátott iránymutatásokat, így válik teljessé az adatvédelmi hatóságok közös testületeinek tájékoztatása és állásfoglalása a rendelet kapcsán, illetve saját belső tevékenységéről, továbbá a tagállami adatvédelmi hatóságok közötti együttműködésről is fogalmaz meg iránymutatásokat, ezek gyakorlatilag a belső munkarend dokumentumai. Az itt említett iránymutatásokról a III. fejezetben is szóltunk.

A GDPR-ra való felkészülés jegyében 2017 nyarán Magyarországra látogatott a Munkacsoport francia elnöke, Isabelle Falque-Pierrotin, aki a felkészülés hazai állásáról tájékozódott és folytatott megbeszéléseket, valamint találkozott a Hatóság munkatársaival.

66 http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=50083

X.2. A 29-es adatvédelmi munkacsoport alcsoportjai

X.2.1. Együttműködési Alcsoport (Cooperation Subgroup)

Az Együttműködési Alcsoport feladata, hogy olyan dokumentumokat készítsen elő a Munkacsoport számára, amelyek a hatóságok közötti együttműködést segítik elő, de megjegyzendő, hogy például az egyes tagállamközi eljárások leíró dokumentumai nem kerülnek nyilvánosságra. Az alcsoport feladata volt, hogy az egyablakos ügyintézés, a kölcsönös segítségnyújtás és a közös műveletek eljárásait részletesen kidolgozza, ezzel kapcsolatban közös álláspontot alakítson ki. Szintén az Együttműködési Alcsoport készítette elő a közigazgatási bírságról szóló iránymutatást.

A GDPR végrehajtásával összefüggésben szintén dolgoz ki dokumentumrészeket, így az adatvédelmi incidens bejelentésével összefüggő nyomtatvány előkészítésében is részt vállalt. Az alcsoport feladata tehát azoknak a gyakorlati eszközöknek, formanyomtatványoknak, iránymutatásoknak az előkészítése, amelyek a GDPR gördülékeny és összehangolt végrehajtását elősegítik. Ez a tevékenység a többi alcsoporttal párhuzamosan a GDPR alkalmazása ideje alatt is folytatódni fog, így a korábbi dokumentumokat a gyakorlati tapasztalatok fényében szükség esetén módosítani, illetve kiegészíteni kell majd.

X.2.2. GDPR Végrehajtási Eljárások Alcsoport (Enforcement Subgroup)

A munkacsoport elsődleges célja 2017-ben, hogy a 29-es Adatvédelmi Munkacsoport által kidolgozott eszközökkel különböző valós/generált esettanulmányok útján tesztelje a GDPR három együttműködési rendszerét:

- kölcsönös segítségnyújtás (*„cooperation mechanism”*),
- a felügyeleti hatóságok közös műveletei (egységességi mechanizmus, különösen abban az esetben, amikor egy felügyeleti hatóság célja több tagállamban, nagyszámú érintettet jelentős mértékben érintő adatkezelési műveletekre vonatkozó joghatást kiváltó intézkedés elfogadása),
- a határokon átnyúló adatkezelések során felmerülő egyablakos ügyintézés (*„one-stop-shop”*).

Az alcsoport konzultációt kezdeményezett az adatvédelmi hatóságokkal és európai szintű felmérést végzett azon panaszügyek számáról, amelyek a jövőben a rendelet szerinti egységességi mechanizmus alá tartozhatnak. Az európai

adatvédelmi hatóságok hozzávetőlegesen 65.000 db panaszügyet kezeltek, amelyből 9000-11000 az egységességi mechanizmus alá tartozik és ezen ügyek főként valamely nemzetközi IT cég adatkezeléséhez köthetőek.

Az új adatvédelmi rendelet Unió-szerte következetes végrehajtásának biztosítása érdekében a felügyeleti hatóságokat minden tagállamban ugyanazokkal a feladatokkal és tényleges hatáskörökkel ruházza fel, ideértve a vizsgálati, a korrekciós és szankciós hatáskört és a szankciókat, valamint az engedélyezési és a tanácsadási hatáskört, különösen a természetes személyek panaszaival kapcsolatos ügyekben, továbbá – az ügyészi hatóságok tagállami jog szerinti hatásköreinek sérelme nélkül – az arra vonatkozó hatáskört, hogy a rendelet megsértése esetén az igazságügyi hatóságokhoz forduljanak és bírósági eljárást kezdeményezzenek.

A munkacsoport a Cooperation Alcsoporttal együttműködve iránymutatások megalkotását segíti elő a végrehajtás minél egységesebbé tételére, elősegítve ezzel egy egységes GDPR-alapú szempontrendszer kialakítását.

X.2.3. Nemzetközi Adattovábbítási Alcsoport (International Transfers Subgroup – ITS)

Kiemelt téma volt a Privacy Shield éves felülvizsgálatában a kereskedelmi vonatkozású kérdések vizsgálata, de a 2017-es munkát itt is alapvetően a GDPR-ra való felkészülés határozta meg:

- Korábbi WP 29-es dokumentumok (WP153-as és WP195-ös munkadokumentumok) táblázatos formában történő átdolgozása, segítséget nyújtva az adatkezelők és adatfeldolgozók számára a BCR kidolgozása és jóváhagyása során a BCR kötelező tartalmi elemeiről.
- Egy adott harmadik országban fennálló adatvédelem szint megfelelőségének elemzésével kapcsolatos vélemény, útmutatást nyújtva a 29-es Munkacsoportnak, illetve a Bizottságnak arról, hogy a GDPR alapján melyek azok az alapvető adatvédelmi szabályok, elvek, amelyek megléte elengedhetetlen a megfelelőségi határozat megszületéséhez.
- Harmadik országba történő adattovábbítás GDPR 49. cikk szerinti, különös helyzetekben alkalmazható jogalapok alkalmazására vonatkozó útmutató.

A fenti véleményeket a 29-es Munkacsoport 2018-ban véglegesíti és teszi közzé honlapján.

Az alcsoport szakértőinek közreműködésével emellett konkrét ügyekkel kapcsolatban számos, a WP 107-es munkadokumentum szerinti együttműködési eljárás lefolytatására is sor került. Az ennek eredményeként jóváhagyott BCR-ok listája megtalálható a 29-es Munkacsoport honlapján.

X.2.4. Határok, Utazás és Bűnüldözés Alcsoport (Borders, Travels and Law Enforcement Subgroup – BTLE)

Ez az alcsoport véglegesítette azt a dokumentum csomagot, amely ajánlásokat tartalmaz a Bűnügyi Irányelv fontosabb rendelkezéseinek értelmezésével, elemzésével kapcsolatban. Az Irányelv átültetése és alkalmazása szempontjából a legfontosabb kérdés, hogy az adott eljárásnak van-e valamilyen büntető vagy jogkorlátozó karaktere (*„punitive character and purpose”*). Az ülés egyetértett abban, hogy a gyakorlatban a nemzetközi bűnügyi bírói együttműködés és a tagállamokban a pénzmosás megelőzésével kapcsolatos elemző tevékenységet ellátó pénzügyi információs egységek (FIU-k) adatkezelései is az Irányelv hatálya alá tartoznak az olyan klasszikus bűnüldözési célú adatkezeléssel járó tevékenységek mellett, mint a büntető és szabálysértési eljárások lefolytatása, a büntetések végrehajtása, valamint a közrend és közbiztonság védelme.

Az alcsoportban megállapodás született arról, hogy ki kell dolgozni egy közös metodológiát a szabadságon, biztonságon és jog érvényesülésén alapuló térség nagyméretű IT-rendszereinek (SIS II, VIS, Eurodac, CIS, Europol IS) ellenőrzésével kapcsolatban, mivel adatvédelmi szempontból viszonylag sok átfedés van a rendszerek és az ellenőrzési mechanizmusaik között.

Az Európai Bíróság 2017. július 26-án hozott ítéletében a Kanadába történő PNR adattovábbítások kapcsán a szükségesség és arányosság követelményének hiányát állapította meg több esetben. Az ítélet miatt az EU-CAN PNR Egyezmény újratárgyalása vált szükségessé. Az alcsoport elkezdte az ítélet elemzését és feldolgozását.

Az alcsoport ezen felül a Privacy Shield hatálya alá tartozó adattovábbításokkal kapcsolatban az érintettek hozzáférési jogának gyakorlására szolgáló egységes formanyomtatványokat is kidolgozott. Ezeket a nyomtatványokat a nemzeti adatvédelmi hatóságok honlapjain hozták nyilvánosságra az adott nemzeti nyelven. A bűnügyi/nemzetbiztonsági adatkezelésekkel kapcsolatos nyomtatvány magyarul elérhető a Hatóság honlapján.[67]

67 https://www.naih.hu/kuelfoeldi-adattovabbitas.html

X.2.5. Technológiai Alcsoport (Technology Subgroup – TS)

A TS lett kijelölve az adathordozhatósághoz, az adatvédelmi hatásvizsgálathoz, az adatvédelmi incidens jelentéshez és az adatvédelmi tanúsításhoz kapcsolódó iránymutatások előkészítésére. Ezek közül a legsürgősebb az adathordozhatóság témája volt, hiszen az adatkezelők számára ennek az új érintetti jognak az értelmezése nyújtja a legnagyobb segítséget. A dokumentumot a 29-es Munkacsoport társadalmi egyeztetésre bocsátotta, amely során a több, mint 600 oldalnyi észrevételeket is figyelembe véve alakult ki az iránymutatás végleges szövege.

Tekintettel arra, hogy több adatvédelmi hatóság is rendelkezett önálló módszertannal adatvédelmi hatásvizsgálat elkészítéséhez, az iránymutatás nem tartalmaz konkrét módszertani leírást, csupán egy általános követelményrendszert az adatvédelmi hatásvizsgálat módszertanával szemben támasztott alapvető követelményekről, továbbá utal a meglévő tagállami és nemzetközi standardizációs hatásvizsgálati módszertanokra. A társadalmi vitát követően beérkezett észrevételeket az alcsoport beépítette az iránymutatás végleges szövegébe.

Az adatvédelmi incidens jelentésekről szóló iránymutatás társadalmi egyeztetése 2018-ban is folyamatban van.

A tanúsításról szóló iránymutatást az alcsoport két külön témára – akkreditáció és az adatvédelmi tanúsítási mechanizmusok alapvető követelményei – bontotta, amelynek következtében két külön dokumentum készül. Az iránymutatások szövegezése folyamatban van.

A fentieken túlmenően az alcsoport véleményt bocsátott ki a munkavállalók ellenőrzésének alapvető adatvédelmi kérdéseiről, illetve az új ePrivacy Rendelet tervezetről, és levélben véleményezte a Bizottságnak az intelligens közlekedési rendszerekkel kapcsolatos szabályozási elképzeléseit, valamint az ICANN által fenntartott domain regisztrációs nyilvános adatbázisának adatvédelmi vonatkozásait. Mind a két előbb említett kérdésben jelentős előrelépést hozott a 29-es Munkacsoport levelekben megfogalmazott egységes fellépése.

X.3. Részvétel az Európai Unió közös adatvédelmi felügyelő testületeiben

X.3.1. A Schengeni Információs Rendszer Adatvédelmét Felügyelő Munkacsoport (SIS II SCG) és a NAIH schengeni ügyei

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 egy vegyes típusú koordinációs ellenőrző csoport létrehozását írja elő, amely SIS II koordinációs ellenőrző csoportként (Coordinated Supervision Group) alakult meg még 2013 folyamán és folytatta tevékenységét 2017-ben is.

Az EDPS 2017. május 2-án kiadott egy véleményt a SIS II rendszer jövőbeli működésével kapcsolatban, mivel a rendszer több új biometrikus azonosítót is kezelni tudna a jövőben: arckép, ujj- és tenyérnyomat, valamint DNS profil. Az EDPS kritikája szerint több esetben kérdéses az adatkezelések szükségessége (például: arcképrögzítésnél, az ujjnyomatok korhatárának 6 éves korra történő levitelénél, 5 éves tárolási idő előírásánál).

Az üléseken szó esett a European Search Portalról, mint folyamatban lévő fejlesztésről, mely az EU nagyméretű IT rendszereinek interoperabilitását kívánja megteremteni. A fejlesztés lényege, hogy egyszerre lehet annak segítségével keresni szinte az összes adatbázisban egy egységes felületen keresztül (SIS, VIS, Eurodac, ECRIS, ETIAS, EES). A hozzáférési jogosultságok elkülönítése a rendszeren belül úgy történne meg, hogy azon adatbázisban tárolt adatokkal kapcsolatban, amelyhez nem rendelkezik a felhasználó közvetlen hozzáféréssel, a rendszer csak egy van/nincs találat jelzést adna, így a felhasználó később már közvetlenül fordulhatna az adatkezelőhöz. A rendszer képes lesz arra is, hogy összehasonlítja az egyes adatbázisokban található adatokat és a hasonlóakat listázza (például a biometrikus adatok alapján).

Az ujjnyomatok fokozott beazonosítását lehetővé tévő AFIS-projekt végrehajtása megkezdődött, melynek első szakaszában 8 tagállam vesz részt (Magyarország nincs közte). 2018. július 4-től a tagállamoknak az új sztenderdeket kell alkalmazniuk az ujjnyomatokat illetően, továbbá a már meglévő NIST fájlokat is át kell konvertálni az új sztenderdeknek megfelelően. A konvertálást néhány tagállam már el is végezte, és összességében jól halad a folyamat.

A fentieken túl az Európai Bizottság szervezésében 2017-ben 7 tagállamban (DK, IS, SE, NO, ES, HR, UK) került sor schengeni adatvédelmi ellenőrzésre (SCHEVAL).

A NAIH-hoz 2017-ben 16 alkalommal fordultak a SIS II rendszerben tárolt személyes adatok kezelésével kapcsolatban felülvizsgálati kérelemmel. Ezek összesen 18 személyt – 7 koszovói, 3 magyar, 2 szerb, 2 algériai, 1 albán, 1 nigériai, 1 macedón és 1 amerikai állampolgárt – érintettek (az egyik beadványban 3 személy szerepelt). Felülvizsgálati eljárást 5 alkalommal indított a Hatóság, a többi esetben általános tájékoztatást nyújtott a beadványozóknak a Nemzeti SIRENE Irodához fordulás jogáról és menetéről. Az egyik felülvizsgálati eljárásban megállapította a NAIH, hogy a beadványozóval szemben elrendelt SIS figyelmeztető jelzést már törölték a rendszerből, ugyanakkor vele szemben a Bevándorlási és Menekültügyi Hivatal (BMH) által elrendelt nemzeti beutazási és tartózkodási tilalom van érvényben. A beadványozót tájékoztattuk a BMH-hoz való fordulás lehetőségéről.

A másik ügyben a beadványozó kezdeményezte a vele szemben elhelyezett SIS figyelmeztető jelzés törlését, a SIRENE Iroda azonban arról tájékoztatta, hogy magyarországi tartózkodási joga megszűnt, valamint tartózkodási kártyáját is visszavonták, és a BMH-nál másodfokon folyamatban lévő eljárás jogerős lezárásáig a beadványozóval szemben elrendelt norvég SIS figyelmeztető jelzés törlése nem indokolt. A vizsgálat során kiderült, hogy a külföldi panaszos nem hagyott fel magyarországi tartózkodási jogának gyakorlásával és érvényes tartózkodási kártyával rendelkezik, aminek következtében a BMH kezdeményezte a norvég SIS figyelmeztető jelzés törlését.

Egy további felülvizsgálati ügy kiindulópontja, hogy a panaszos Olaszországban egy gépkocsi nagykereskedésben vásárolt egy autót, aminek magyarországi forgalomba helyezésekor kiderült, hogy a korábbi rendszámának körözését az olasz hatóságok elrendelték. A magyar rendőrség a gépkocsi dokumentumait lefoglalta – így azt forgalomba helyezni a magyar tulajdonos nem tudta – és megküldte a budapesti Olasz Nagykövetségnek. A Nagykövetség tájékoztatása alapján a személygépkocsi korábban Olaszországban eltulajdonított rendszáma áll schengeni körözés alatt, maga a gépkocsi azonban nem. A NAIH közbenjárására a NEBEK az olasz forgalmi engedély körözését visszatérően ellenőrizte és megállapították, hogy a körözés visszavonására időközben az illetékes olasz hatóság intézkedett. Az illetékes magyar rendőrkapitányság saját hatáskörben is elvégezte az ellenőrzést és ezt követően kiállította a lefoglalás megszüntetésére vonatkozó iratokat, majd erről tájékoztatta a Nagykövetséget is. A fentiek után

a jóhiszemű magyar tulajdonos már forgalomba tudta helyeztetni a gépkocsit Magyarországon.

A NAIH 2017. áprilisában a helyszínen ellenőrizte a Belügyminisztérium Nyilvántartások Vezetéséért Felelős Helyettes Államtitkárságán belül működő N.SIS II Hivatalt, mint a SIS hazai üzemeltetőjét. Az ellenőrzés jogalapját a 2012. évi CLXXXI. törvény (SIS II törvény) 34. §-a, valamint a Schengeni Információs Rendszer második generációjának (SIS II) létrehozásáról, működtetéséről és használatáról szóló 2007/533/IB határozat (2007. június 12.) 60. cikkében foglaltak adták.

Az ellenőrzés során, valamint az előzetesen kiküldött kérdőív segítségével a NAIH munkatársai ellenőrizték az N.SIS II rendszer működtetésével összefüggésben az adatkezelés jogszerűségére meghatározott feltételek teljesülését, az adatbevitel módjait és jogalapját, az adatkezelési műveletek naplózását, az adatkezelés célhoz kötöttségének és arányosságának kérdéskörét, a feladat-meghatározásokat és végrehajtásukat, továbbá látogatást tettek a szerverteremben is, hogy a fizikai biztonságról is meggyőződjenek. A rendszer naplózásának általános vizsgálata céljából három SIS II-vel kapcsolatos konkrét panaszügy kapcsán lekérdezések is történtek. A kezelt adatkör, illetve a naplóadatok alapján jogszerűtlen adatkezelés nem volt tapasztalható.

Összességében megállapítható, hogy az N.SIS II Hivatal működése során eleget tesz a jogszabályi előírásoknak és az adatvédelmi keretrendszernek megfelelően fejti ki tevékenységét. Ugyanakkor a SIS II rendszerhez hozzáférést biztosító alkalmazás fejlesztésre szorul, valamint abban ki kell javítani egy olyan hibát, ami miatt az előző felhasználó általi lekérdezés adatai *„beragadnak”* a rendszerbe és azokat aztán az ugyanarról a munkaállomásról bejelentkező személy később láthatja.

X.3.2. Váminformációs Rendszer Adatvédelmét Felügyelő Munkacsoport (JSA Customs és CIS SCG)

A JSA Customs, mint az EU *„régi harmadik pillérébe”* tartozó adatokat kezelő váminformációs rendszert ellenőrző hatóság feladatai 2017. május 1. után integrálásra kerülnek a Vámügyi Információs Rendszer Koordinációs Ellenőrzési Csoportjába (CIS SCG). A JSA Customs hatóság tehát formálisan megszűnt, azonban eddigi feladatait és a hatáskörébe tartozó ügyeket a CIS SCG látja el.

Az Európai Csalás Elleni Hivatal (OLAF) képviselői prezentációt tartottak a CIS SCG-nek az úgynevezett Anti Fraud Information System (röviden: AFIS, ami

nem összekeverendő az Eurodac-kal kapcsolatos *„Automated Fingerprint Identification System”*-el amit szintén AFIS-ként rövidítenek) információbiztonsági beállításairól és szabályzatáról. A szabályzat kidolgozásába az OLAF belső adatvédelmi felelősét is bevonták. Az adatvédelmi incidenssel kapcsolatos bejelentések a belső adatvédelmi felelősön keresztül történnek. Az OLAF két évente felülvizsgálja a biztonsági policyt is, ha új fenyegetések jelennek meg, akkor frissítik a rendszert. A logok ellenőrzéséhez automatikus eszközeik is vannak. A rendszerrel kapcsolatban kifejlesztettek továbbá egy e-learning modult, ami a felhasználókat segíti a rendszer használatában.

A munkacsoport emellett elkészítette a nemzeti CIS ellenőrzésével kapcsolatos közös audit keretrendszer elnevezésű dokumentumot.

X.3.3. Eurodac Rendszer Adatvédelmét Felügyelő Munkacsoport (Eurodac SCG)

Az ujjnyomatokat tároló Eurodac rendszer adatvédelmi felügyeletét ellátó Eurodac SCG munkacsoportnak az eu-LISA[68] képviselője beszámolt a központi rendszer legújabb fejlesztéseiről. Jelenleg a rendszerben mintegy 7 millió rekord található, de cél, hogy a 10 millió bejegyzés tárolása se jelenthessen problémát a jövőben. A rendszerben található bejegyzések leggyakoribb hibái az ujjnyomatok rossz minőségéből erednek. Az Eurodac rendelet módosulásaival és a kapcsolódó jövőbeli fejlesztésekkel kapcsolatban az eu-LISA hatásvizsgálatot folytat le.

A munkacsoport összeállított egy kérdőívet a tagállamok számára az érintetti jogok gyakorlásával kapcsolatban. A kérdőívet a nemzeti adatvédelmi hatóságok fogják megküldeni az érintett nemzeti hatóságok részére, a válaszok összesítése után pedig ajánlásokat is tartalmazó jelentés fog készülni.

X.3.4. Vízuminformációs Rendszer Adatvédelmét Felügyelő Munkacsoport (VIS SCG)

Az eu-LISA képviselője beszámolt a központi rendszer legújabb fejlesztéseiről. Az ujjnyomatok minőségével kapcsolatban a statisztikákból az volt kiolvasható, hogy Magyarország az egyik legjobb hibaaránnyal viszi fel azokat (csupán 3,5% nem fogadható be). Az Európai Bizottság a 6 évnél idősebb gyermekek ujjnyoma-

68 European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice.

tai levételének szükségességével kapcsolatban jelenleg hatásvizsgálatot folytat (erre jelenleg már technikailag adottak a lehetőségek). Fontos új fejlesztés lesz továbbá, hogy az útlevél másolatát is fel lehet majd tölteni a jövőben a rendszerbe.

A hosszú idejű tartózkodásra jogosító vízumok és tartózkodási engedélyek adatainak VIS-be való feltöltésével összefüggésben nyilvános konzultáció indult,[69] amely 2018. február 9-ig tartott, és amelyben egy online kérdőív kitöltésével lehetett részt venni. Az ujjnyomat-vétel alsó korhatárának 12 évről 6 évre történő levitelével összefüggésben indított konzultáció 2017. november 9-én lezárult.

X.3.5. Europol Együttműködési Testület (Europol Cooperation Board)

Az Europol Együttműködési Testülete (Europol Cooperation) összesen három ülést tartott 2017-ben, amelyen Magyarországot a NAIH képviselte. Az első, áprilisi ülésre még a korábban az Europol független ellenőrzésével megbízott JSB Europol (Europol Közös Felügyeleti Hatóság) keretei között került sor. A legfontosabb változás az Europol tevékenységének független ellenőrzésével megbízott szerv működésében, hogy 2017. május 1-től az új Europol-rendelet[70] hatálybalépésével a Testület átvette az ilyen feladatokkal korábban megbízott JSB Europol feladatait, ezzel egy időben pedig a JSB Europol megszűntette működését. Az új Testület számára az Európai Adatvédelmi Biztos látja el az adminisztrációs és titkársági feladatokat, aki állandó képviselővel képviselteti magát az üléseken. A JSB Europol eddigi működésével kapcsolatos irat- és tudásanyagot átadták az EDPS-nek, a belső eljárási rendet a Testület első ülése véglegesítette és elfogadta.

2017. január végén a JSB delegáltjai részt vettek egy ellenőrzésen az Europolnál, amely során azt vizsgálták, hogy mennyiben tettek eleget a JSB eddigi ajánlásainak (több mint 80 ajánlás). A legtöbb esetben az ajánlások végrehajtása megtörtént, 38 esetben azok végrehajtása folyamatban van, négy esetben viszont nem történt még érdemi előrelépés. Általánosságban elmondható, hogy az Europolnál világos adatvédelmi kultúra alakult ki, komolyan veszi az adatvédelmi megfelelést és a JSB ajánlásait. Negatívum, hogy az adatok nagy mennyi-

69 https://ec.europa.eu/home-affairs/content/consultation-extending-scope-visa-information-system-vis-include-data-long-stay-visas-and_en

70 Az Európai Parlament és Tanács (EU) 2016/794 rendelete (2016. május 11.) a Bűnüldözési Együttműködés Európai Uniós Ügynökségéről (Europol), valamint a 2009/371/IB, a 2009/934/IB, a 2009/935/IB, a 2009/936/IB és a 2009/968/IB tanácsi határozat felváltásáról és hatályon kívül helyezéséről.

sége miatt azok nem voltak sokszor megszűrve és nem végezték el a megfelelő elemzéseket.

Mivel az új Europol rendelet alkalmazását Dánia – élve opt out jogával – népszavazáson elutasította, ezért az Europolos adattovábbítások szempontjából harmadik államnak fog minősülni. Ettől függetlenül Dánia ugyanúgy részt vesz az Europol munkájában és fenntartja nemzeti egységét is, az együttműködés azonban nem az új rendelet, hanem Dánia és az Europol közötti kétoldalú megállapodáson alapul.

A fentieken túl az EDPS ajánlást fogalmazott meg az Europol részére, mert az egyes adatkezelési célok nem elég egyértelműek. 2017. december 15-én az EDPS az olasz adatvédelmi hatóság közreműködésével ellenőrzést végzett az Europolnál, melynek során elsősorban az új Europol-rendeletnek való megfelelésre, valamint az információbiztonságra, az adatbiztonságra és az adatmegőrzésre fókuszáltak.

X.3.6. Távközléssel foglalkozó nemzetközi adatvédelmi munkacsoport (International Working Group on Data Protection in Telecommunications - IWGDPT)

A munkacsoport 2017-ben véleményt fogadott el az e-learning megoldások során kezelt személyes adatokról; a domain regisztrációs nyilvántartást vezető ICANN whois adatbázisának adatvédelmi kérdéseiről; a titkosszolgálati adatgyűjtés nemzetközi alapelveiről; a firmware és szoftver frissítések és az elszámoltathatóság adatvédelmi alapelvének a kérdésköréről; a határon átnyúló bűnüldözési adatigényléssel kapcsolatos kérdéskörökről.

A 2018-as tavaszi ülés házigazdája a NAIH lesz, az ülést 2018. április 9-10-én Budapesten tartjuk meg.

X.3.7. Délkelet-európai Rendőri Együttműködési Egyezmény (Police Cooperation Convention for Southeast Europe - PCC SEE)

Az Egyezményhez Magyarország a 2012. évi XCII. törvény 2012. december 11-ei hatályba léptetésével csatlakozott. Az Egyezmény célja, hogy növelje a biztonságot a térségben és felkészítse a nyugat-balkáni országokat az európai uniós tagságra. A Szerződő Felek fokozzák együttműködésüket a közbiztonságot fenyegető veszélyek elhárítása, valamint a bűncselekmények megelőzése, felderítése és rendőrségi nyomozása során. Az Egyezmény végrehajtására lét-

rehozott legfőbb döntéshozó szerv, a Miniszteri Bizottság adatvédelmi munkacsoportjában a NAIH is tagként szerepel. Az adatvédelmi munkacsoport a 2016. decemberi ülésére elkészítette a kapcsolódó adatvédelmi végrehajtási egyezmény tervezetét, melyet 2017. május végén Belgrádban véglegesítettek a szerződő államok adatvédelmi és bűnüldöző hatóságaitól beérkezett vélemények és megjegyzések mentén. A végrehajtási egyezmény kihirdetésével, illetve annak a szerződő államok nemzeti jogába történő implementálásával kapcsolatban egyelőre nincs további információ.

X.3.8. TFTP Megállapodás

Az Európai Unió és az Amerikai Egyesült Államok 2010. június 28-án írta alá *az Európai Unió és az Amerikai Egyesült Államok között az Európai Unióból származó pénzügyi üzenetadatoknak a terrorizmus finanszírozásának felderítését célzó program céljából történő feldolgozásáról és az Amerikai Egyesült Államok részére való átadásáról szóló megállapodást* (TFTP Megállapodás). A 2010. augusztus 1-jén hatályba lépett megállapodás keretein belül a felek pénzügyi adatok millióit kezelik és továbbítják évente. A TFTP Megállapodás az uniós és nemzeti szabályokkal összhangban adatvédelmi garanciákat is tartalmaz az uniós állampolgárok személyes adatainak védelme érdekében. Ilyen a TFTP Megállapodás 15. cikke szerinti tájékoztatáshoz, valamint a 16. cikk szerinti helyesbítéshez, törléshez és zároláshoz való jog is.

Egy magyar állampolgár eljárást kezdeményezett a NAIH-nál a TFTP rendszerben kezelt adatairól történő tájékoztatás céljából. Az Amerikai Egyesült Államok Pénzügyminisztériuma (Department of Treasury) arról tájékoztatta a NAIH-ot, hogy a panaszt megvizsgálták és nem tapasztaltak jogsértést a személyes adatok kezelésével kapcsolatban. A konkrét tájékoztatását arról, hogy kezelik-e a panaszos személyes adatait azonban megtagadták, mivel az erről való tájékoztatás a TFTP Megállapodás 15 (2) cikkében[71] szabályozott korlátozás alá esik, továbbá a tájékoztatás ellentétes lenne az USA Információszabadság törvényének (Freedom of Information Act) 522. § (b) (1), illetve (b)(7)(E) pontjaival. A fenti jogszabályhelyek alapján az érintett személy tájékoztatása azzal kapcsolatban, hogy az amerikai szervek kezelik-e személyes adatait, jogosan tagadható meg

71 TFTP Megállapodás 15 (2) cikke: *„A megállapodás alapján kezelt személyes adatokról szóló tájékoztatást a nemzeti jog közérdekből korlátozhatja a bűncselekmények megelőzése, felderítése, vizsgálata és üldözése céljából, továbbá a nemzetbiztonság és a közbiztonság védelme céljából, az érintett személy tájékoztatáshoz fűződő jogos érdekének figyelembe vételével."*

a bűnüldözés és a terrorizmus elleni harc, valamint a nemzetbiztonsági kockázatok kiküszöbölése céljából. A tájékoztatás akkor is megtagadható, ha az érintett szervek egyébként nem kezelik azon személy adatait, aki a tájékoztatás kérést előterjesztette. Az adatalany részére a tájékoztatás megtagadásával kapcsolatban a szervnek nincs bővebb indokolási kötelezettsége sem az amerikai törvények, sem a TFTP Megállapodás alapján. A magyar panaszos a döntés ellen fellebbezést jelentett be. Fellebbezése indokaként előadta, hogy az USA-ban sosem járt, továbbá nem egyértelmű a tájékoztatás alapján, hogy adatait a külföldi hatóságok kezelik-e. Feltételezi, hogy adatait a tájékoztatás ellenére kezelik, mivel a megtagadásnak csak ekkor lenne értelme. A fellebbezést az USA Pénzügyminisztériumának Magánszféra-védelem, Átláthatóság és Nyilvántartásért felelős Helyettes Államtitkára (Deputy Assistant Secretary for Privacy, Transparency and Records) bírálta el és a döntést helybenhagyta, kiemelve, hogy hasonló megkeresésekkel kapcsolatban mind az USA, mind az EU állampolgárait ugyanazon jogok illetik meg, így a válasz tartalma nem függ attól, hogy a kérvényező amerikai vagy európai állampolgár. A döntéssel kapcsolatban a panaszost megilleti a bírósághoz fordulás joga az USA Columbia Szövetségi Körzetének (District of Columbia) szövetségi bírósága előtt.

X.4. A NAIH nemzetközi projektjei

X.4.1. Macedón projekt

Az EUROPAID által *finanszírozott „Support to access to right on protection of personal data in Macedonia”* pályázat keretében, amelyben a NAIH konzorciumi partnerként vesz részt, 2017-ben is folytatódtak a szakértői tanulmányutak a Macedón Köztársaságban. A három NAIH szakértő témái: nemzetközi adatvédelmi együttműködés, a két információs jog összhangjának megteremtése, valamint a bíróságok, ügyészségek és az ombudsman adatkezeléseinek egyes kérdései. A projekt részeként a Macedón Adatvédelmi Hatóság munkatársai 2017 júliusában egy budapesti látogatás során közvetlenül megismerhették a Hatóság belső működését és eljárásait, valamint látogatást tettek a Magyar Telekom Nyrt.-nél, ahol a vállalat belső adatvédelmi felelősével konzultáltak.

X.4.2. STAR Project

2017 novemberében a budapesti kick-off találkozóval kezdetét vette az új uniós adatvédelmi projektünk – STAR Project *(Support Training Activities on the data protection Reform)* – megvalósítási szakasza. A 24 hónapos projekt az Európai

Unió társfinanszírozásában valósul meg, partnerek a NAIH mellett a brüsszeli Vrije Universiteit (VUB) és a brit Trilateral Research Ltd. (TRI), célja a GDPR-hoz kapcsolódó, adatvédelmi hatóságok és adatvédelmi tisztviselők részére szóló képzési anyagok összeállítása és tesztelése. A projekttel kapcsolatban a https://projectstareu.wordpress.com/ weboldalon találhatók további információk.

XI. Mellékletek

XI.1. A NAIH emlékérem kitüntetettjei 2017-ben

I. Pokorni Zoltán, pedagógus, a Budapesti XII. Kerületi Önkormányzat polgármestere, a Hegyvidéki ONvédelmi program kidolgozása és végrehajtása miatt kapta 2017-ben a NAIH emlékérmet.

Pokorni Zoltán a Hegyvidéki Önkormányzat vezetőjeként munkatársaival együtt egy olyan komplex jogtudatosító, érzékenyítő helyi programot alkottak és tartanak fenn, melynek célja, hogy a fiatalok digitális világban történő létezését, megnyilvánulásait megfelelő módon előkészítsék és felkészítsék az érintett gyermekeket, szüleiket és pedagógusaikat a lehetséges veszélyekre és a jövőbeni kihívásokra.

A digitális világ számos előnyt kínál a gyermekeknek mind a tanulás, mind a világban való eligazodást szolgáló kommunikáció terén, ugyanakkor sok olyan veszélyforrás is jelen van, ami negatívan befolyásolhatja érzelmi-értelmi fejlődésüket. Ezért nagyon fontos minden olyan gyermekekkel kapcsolatos oktatói-nevelői munka és tevékenység, mely az internet tudatos és okos használatára tanít. A NAIH nem csak saját, de más szervezetek kezdeményezéseit is figyeli, támogatja, és e téren is kiemelkedő jelentőségűnek ítélte egy budapesti önkormányzat tudatosító programját.

A Budapesti XII. kerületi Önkormányzat Hegyvidéki ONvédelem programja komplex megközelítéssel, elkötelezett szakemberek bevonásával, a gyermekek-pedagógusok-szülők célcsoportként történt meghatározásával hosszú távon vállalja fel céljának elérését. Infografikai kisfilmek, plakátok, tájékoztató szórólap, szülői akadémiák, kortárs mentorprogram és akkreditált pedagógus képzés életre hívásával (és finanszírozásával) hatékonyan és kreatív módon hajtja végre programját, példát mutatva ezzel más állami szereplőknek is.

Fontos, hogy itt nem egy kampányról van szó, noha a programnak számos kampányeleme is van, hanem egy olyan rutint próbálnak kialakítani a kerület iskoláiban, minden évben egy meghatározott időponthoz kötve, ami az összes érintettet egyszerre szólítja meg. A kezdeményezés évente ismétlődően a pedagógusok számára szeretne meghirdetni és finanszírozni egy speciális képzést, a gimnazisták számára kialakítani egy úgynevezett kortársképzést, mely egy men-

tori képzési programmal zárul és ehhez csatlakozik a szülők bevonásával egy szülők akadémiája típusú párbeszéd.

A 2016-os program előkészítése tudományos felméréssel kezdődött, az önbevalláson alapuló kérdőívek segítettek feltérképezni a problémákat és kiderült, hogy a szülők mennyire téves feltevésekben élnek a gyermekeik internethasználatával kapcsolatban. Például a szülők csupán 6%-a gondolja, hogy gyermekük internetes kommunikáció során idegennel lépett kapcsolatba, míg a valóságban ez az adat 21%.

A program részei: a figyelemfelkeltő kommunikáció, a pedagógusok számára egy 60 órás akkreditált képzés, kerekasztal-beszélgetések alapján szerveződő szülői akadémiák és fiatalabb korosztálynak szóló *„nagyon okos kortársképzés”*, hiszen egyértelmű, hogy egy „*okosakat mondó*” idősebb gyermek felé leginkább nyitott és befogadó a kisebb gyermekekből álló célközönség.

A honlapon megtalálható kisfilmek, tájékoztató anyagok és a program szervezése mögött is komoly munka és komoly erőforrás áll. A program a helyi közösség jövőjére koncentrál, a jövő generációk digitális biztonságával és képzésével foglalkozik. Reményeink szerint ez a vállalkozás mintaadó lesz nem csak más közösségek előtt, de országos szinten is.

Pokorni Zoltán és Péterfalvi Attila

Ezért a Nemzeti Adatvédelmi és Információszabadság Hatóság Emlékérem adományozásáról szóló 19/2012. sz. NAIH szabályzat alapján az ezüst emlékérmet Pokorni Zoltán, a Hegyvidék Önkormányzat polgármestere (képviselve a programban részt vevő munkatársait is) kapta az internetes adatvédelemmel, valamint a fiatalok biztonságos és jogtudatos internethasználatával kapcsolatos ismeretek népszerűsítése érdekében végzett kiemelkedő tevékenységért.

II. Az Információszabadság napja alkalmából Dr. Molnár Katalin, Budapest Főpolgármesteri Hivatal Főjegyzői Irodájának vezetője, belső adatvédelmi felelőse kapta 2017-ben a NAIH emlékérmet.

Dr. Molnár Katalin és Dr. Péterfalvi Attila, a NAIH elnöke

Molnár Katalin 2003. októberétől dolgozik a Fővárosi Önkormányzat Főpolgármesteri Hivatalánál, kezdetben adatvédelmi ügyintézőként, majd 2006. májusától belső adatvédelmi felelősként. 2011-ben megbízott irodavezető lett, 2014-ben a Főjegyzői Iroda vezetésére kapott megbízást. 2010-ben szakmai tanácsadó címet kapott. Feladatai közé nem csupán az adatvédelem szabályai érvényesülésének felügyelete, de a közérdekű adatigénylések teljesítése, az információszabadság biztosítása is beletartozik.

Amint más közfeladatot ellátó szerveknek, úgy a Főpolgármesteri Hivatalnak is, sőt közjogi intézményi helyzeténél fogva még inkább kiemelt feladata, hogy a kezelésében lévő adatok érdemi tartalmáról a közvélemény értesüljön, annak jelentős részét nyilvánosságra hozzák, valamint a napi szinten jelentkező közérdekű adatigényléseket is érdemben, a törvényben rögzített határidőn belül megválaszolják.

Molnár Katalin több mint tíz esztendeje egyeztetéseken, a napi ügyek intézése és koordinálása során, valamint belső oktatások keretében a gyakorlatban azért is dolgozik, hogy az információszabadság jelentőségét a dolgozók felismerjék, az adatvédelem mellett az információszabadság szabályai megfelelően érvényesüljenek az 1000 fős Hivatalban.

A nyilvánosságnak a közérdekű adatigénylés lehetőségének megteremtése mellett másik fő pillére a közzétételi kötelezettség jogintézménye. Az a kívánatos gyakorlat, hogy a közfeladatot ellátó szervek honlapjukon pontos tartalommal és naprakészen jelenítsék meg a tevékenységükre és gazdálkodásukra vonatkozó – törvényben nyilvánosságra szánt adatokat. A díjazott érdeme (is) hogy a Pénzügyi Rendszerük össze van kötve az e-Információszabadság rendszerrel, így nemcsak az 5 millió Ft feletti szerződéseinek adatait teszik közzé, hanem ezen összeghatár alattiakat is, így a szerződéseik sokkal nagyobb hányada ismerhető meg anélkül, hogy az adatigénylőknek aktívan adatigénylést kellene benyújtaniuk. Előremutató kezdeményezésük példaértékű más közfeladatot ellátó szerv számára is.

XI.2. Belső adatvédelmi felelősök konferenciája

A Hatóság 2017-ben is megszervezte a Belső Adatvédelmi Felelősök Konferenciáját, amelynek témája értelemszerűen az új adatvédelmi szabályozásra való felkészülés volt. A Konferencia első részében a GDPR-ral összefüggő kérdések, így az érintetti jogok, az adatvédelmi incidens jelentése, a jogalapok kérdésköre, valamint a szankciórendszer átalakulása volt napirenden.

A Bűnügyi Irányelvvel kapcsolatban a Konferencia második részében az érintetti jogok érvényesüléséről, a Hatóság hatásköréről, az adatvédelmi incidensről és hatásvizsgálatról, továbbá a hatóságok közötti együttműködésről és a közösen felügyelt adatkezelésekről hangzottak el előadások.

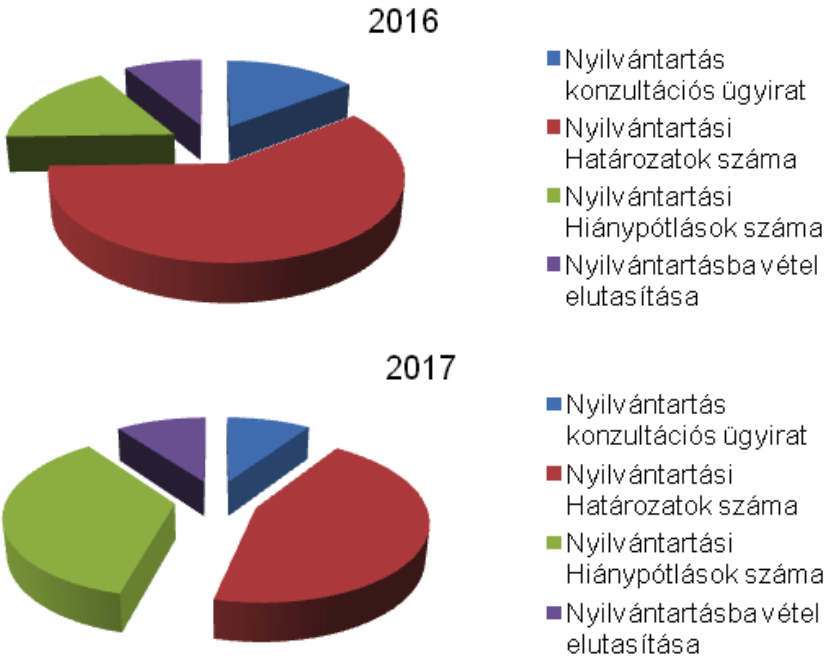
A Konferencia iránti érdeklődés nagy volt, több, mint kétszáz belső adatvédelmi felelős regisztrált. Tekintettel arra, hogy a Hatóság és az adatkezelők közötti kapcsolattartás és együttműködés bevált formája a Konferencia, várhatóan a GDPR alkalmazásának idején, 2018 májusát követően is rendszeresen megszervezi majd a Hatóság.

XI.3. Az adatvédelmi nyilvántartás és IT

2017-ben az adatvédelmi nyilvántartással kapcsolatos teendők ellátása az Informatikai, Ügyviteli és Nyilvántartási Főosztály feladatkörébe tartozott. A kérelmek feldolgozását és a kapcsolódó operatív feladatokat 2017-ben két fő látta el.

Az adatvédelmi nyilvántartás ügyiratszám statisztikája

	2016	**2017**
Nyilvántartás konzultációs ügyirat	2.983	2.522
Nyilvántartási Határozatok száma	12.275	11.890
Nyilvántartási Hiánypótlások száma	3.437	9.614
Nyilvántartásba vétel elutasítása	1.766	2.702
Nyilvántartási ügyek összesen:	**20.461**	**26.728**



Az előző évekhez képest tovább csökkent a papír alapon beérkezett kérelmek száma, ami mindössze 6%-a az összes kérelemnek. Az adatkezelések adatvédelmi nyilvántartásba történő bejelentésének menetében a már bejelentett adatkezelések módosításának, törlésének, valamint a hiánypótlások teljesítésének módjában a korábbi évekhez képest nem történt változás.

Mint arról már a beszámoló korábbi fejezeteiben is említést tettünk, az általános adatvédelmi rendelet (GDPR) nem tartalmaz az Infotv. jelenlegi szabályozásához hasonló, a tagállami adatvédelmi hatóságok által vezetendő, országos adatvédelmi nyilvántartásra vonatkozó szabályokat. A GDPR 30. cikke az adatkezelők, illetve az adatfeldolgozók kötelezettségévé teszi, hogy a felelősségi körükbe tartozóan végzett adatkezelési tevékenységekről nyilvántartást vezessenek.

Ez azt fogja jelenteni, hogy az adatkezelőknek, adatfeldolgozóknak a GDPR kötelező alkalmazásával, saját maguknak kell nyilvántartást vezetniük adatkezeléseikről, amit nem kell bejelenteniük az adatvédelmi hatósághoz. Tehát a jelenlegi adatvédelmi nyilvántartásba történő bejelentési kötelezettség 2018. május 25-étől megszűnik.

XI.3.1. A NAIH általános adatvédelmi rendelet alkalmazására történő felkészülését 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 terheinek csökkentését célzó projektek között jön létre az Integrált Jogalkotási Rendszer (a továbbiakban: IJR).

A projekt keretében valósul meg a NAIH európai uniós kötelezettségeiből adódó jogszabályváltozást követő ügyviteli és eljárásrendi harmonizációja, információtechnológiai modernizációja.

2017. áprilisában több hónapos előkészítés után írtuk alá, az 1585/2016. (X. 25.) Korm. határozat alapján az IJR projekt Támogatási Szerződés 1. számú módosítását, amely a konzorciumi partnerek között nevesíti a Hatóságot, illetve a projekt által támogatott és a GDPR-ban szereplő feladatokat. A NAIH konzorciumi partnerként csatlakozott az IJR projekthez, figyelembe véve annak alapvető céljait és eszközrendszerét.

A projekt eredményeként létrejön a NAIH számára egy integrált, többnyelvű, intelligens ügyintéző és határozat-előkészítő modul, valamint sor kerül az adatvédelmi incidens-bejelentő rendszer teljes körű fejlesztésére, továbbá a rendszer informatikai, IT biztonsági és szervezeti implementációjára is.

A projekt keretében kialakítunk egy olyan, mind az Uniós, mind a hazai elvárásoknak megfelelő rendszert, amely képes az eddigiekhez képest összetettebb és nagyságrendileg nagyobb ügyintézési terhelés professzionális kezelésére, valamint a hatósági határozatok tervezetei előkészítésének, mind a magas jogi minőségi, mind a hibátlan szakmai idegen nyelvi (szaknyelvi) szempontból megfelelő, standard támogatására és végrehajtására.

Fontos, hogy a jelzett határozat-előkészítő modul logikai megközelítésében illeszkedik a GovLex jogszabály-előkészítő modulhoz. Ugyanakkor mind szerkezetében, mind elemeiben eltér attól: az elkülönülő fejlesztés egyszerre képez egy integráns, mégis különböző alrendszert az IJR más alkalmazásaitól.

Létrejön továbbá az adatvédelmi incidensek bejelentésére szolgáló ügyfél rendszer, hiszen az új szabályozás (GDPR) 2018. május 25-től kötelezővé teszi az adatvesztéssel, illetéktelen hozzáféréssel járó adatvédelmi incidensek bejelentését. Az illetékes tagállami adatvédelmi hatóság, azaz a NAIH nem csupán

fogadja, hanem értékeli is a bejelentéseket. A bejelentés tartalma, valamint a beszerezhető 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.

A megjelölt informatikai rendszer-fejlesztésekkel párhuzamosan – a bővítés keretében – meg kell teremteni a szükséges informatikai, elsősorban adatbiztonsági IT bővítéseket, illetve a szervezeti infrastruktúrát (átfogó szervezetfejlesztéssel) és információbiztonsági minőségbiztosítást.

A NAIH alrendszereinek a projektben történő kiépítése során a Hatóság a hardware infrastruktúrát saját forrásból biztosítja. A NAIH jogállásából eredően a projekt célja, hogy független, önálló szakrendszer és infrastruktúra jöjjön létre.

A NAIH IJR alrendszerek funkcióinak csak azon része futhat a KAK-ban (kormányzati adatközpontban) üzemelő infrastruktúrán, mely funkcionálisan is az IJR alaprendszerben helyezkedik el. Ezek a funkciók teljesen elkülönülnek a NAIH IJR alrendszer többi szakrendszeri moduljától.

A NAIH IJR alrendszer egy fejlesztés alatt álló szakrendszer, mely kizárólag a NAIH feladatait lefedő jogalkalmazási feladatokat fogja ellátni. Az IJR alaprendszertől biztonságtechnikai és jogszabályi okokból leválasztva, de egyes pontokon mégis integrált funkciókkal valósul meg a közeljövőben.

XI.4. Az elutasított adatigénylések és tájékoztatási kérelmek

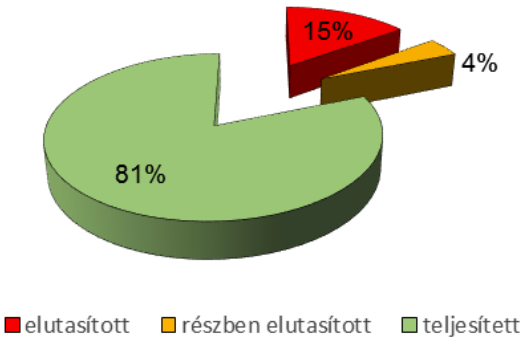
XI.4.1. Az elutasított és teljesített adatigénylésekről, valamint az elutasítások indokairól való tájékoztatási kötelezettség teljesítése

Az Infotv. 30. § (3) bekezdésének második fordulata alapján az adatkezelő az elutasított közérdekű adatigénylésekről, valamint az elutasítások indokairól nyilvántartást vezet, és az abban foglaltakról minden évben január 31-éig tájékoztatja a Hatóságot.

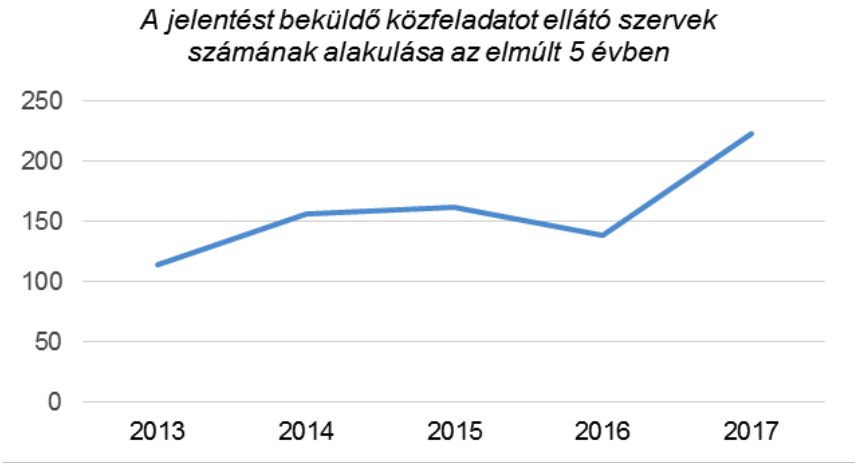
A Hatósághoz 2018. február 21-éig 223 adatkezelő tett eleget az Infotv. 30. § (3) bekezdése szerinti tájékoztatási kötelezettségének.

A közérdekű adatra, illetve a közérdekből nyilvános adatra vonatkozó adatigénylés				
elutasított (db)	részben elutasított (db)	teljesített (db)	összes (db)	adatkezelők száma
552	150	3016	3718	223

A közérdekű és a közérdekből nyilvános adatigénylések teljesítésére/elutasítására vonatkozó 2017. évi statisztikai adatok



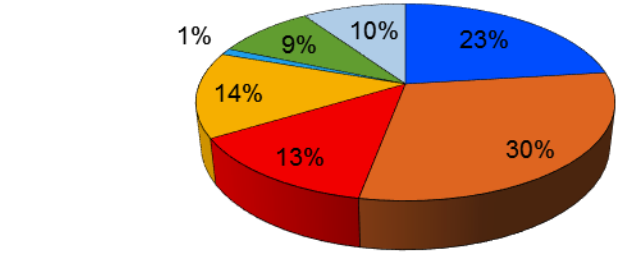
A 2016. évi statisztikai adatokhoz képest elmondható, hogy javult a közfeladatot ellátó szervek közérdekű adatigénylések teljesítésének tendenciája, hiszen 5 %-kal csökkent az elutasított kérelmek aránya, és emellett 5 %-kal nőtt a teljesített adatigénylések aránya.



A grafikon adataiból látható, hogy az elmúlt 5 évben miként változott a közfeladatot ellátó szervek jelentéstételi kötelezettségének teljesítése.

Elutasítási indok	Hivatkozások száma
nem közérdekű vagy közérdekből nyilvános adatra vonatkozott az adatigénylés	128
az igényelt adat nem áll rendelkezésre	166
az igényelt adatok a törvény értelmében nem nyilvános adatok	74
az igényelt adat esetében a megkeresett szerv nem minősül adatkezelőnek	78
a nyilvánosságot korlátozó határidő nem telt el	6
az igényelt adatok döntés megalapozását szolgáló adatoknak minősülnek	50
egyéb indok	53

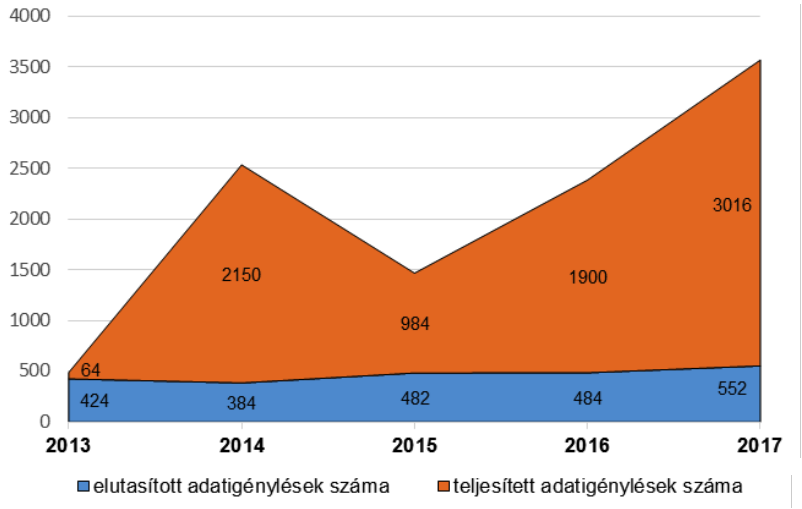
Adatigénylések elutasítási okainak megoszlása 2017



- nem közérdekű vagy közérdekből nyilvános adatra vonatkozott az adatigénylés
- az igényelt adat nem áll rendelkezésre
- az igényelt adatok a törvény értelmében nem nyilvános adatok
- az igényelt adat vonatkozásában a megkeresett szerv nem minősül adatkezelőnek
- a nyilvánosságot korlátozó határidő nem telt el
- az igényelt adatok döntés megalapozását szolgáló adatoknak minősülnek
- egyéb

A 2015. év visszaesése mellett emelkedő tendenciát mutat a benyújtott adatigénylések és a teljesített adatigénylések száma, ami arra utal, hogy az adatigénylők aktivitása fokozódott.

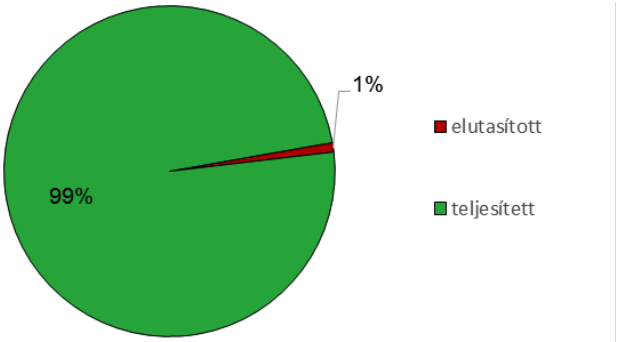
A közérdekű adatigénylések elutasításának, illetve teljesítésének alakulása az elmúlt 5 évben



XI.4.2. Az érintett tájékoztatáshoz való jogának érvényesülése

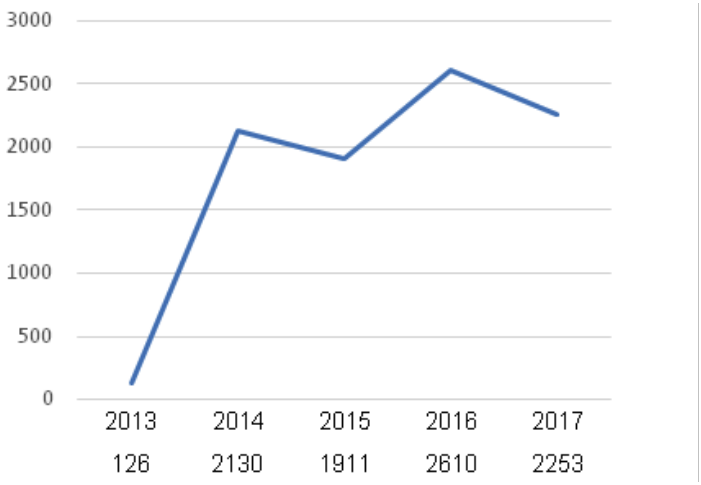
Az Infotv. 14. §-a értelmében az érintett kérelmezheti az adatkezelőnél a személyes adatai kezelésére vonatkozó tájékoztatást, illetve személyes adatainak helyesbítését, törlését, illetve zárolását. A tájékoztatás megtagadásáról az adatkezelő az Infotv. 16. § (3) bekezdése alapján a tárgyévet követő év január 31-éig a Hatóságot értesíti.

Az érintett személyes adataira vonatkozó tájékoztatások 2017. évi alakulása



A fenti grafikon alapján elmondható, hogy a tájékoztatást nyújtó adatkezelők az érintett tájékoztatására irányuló kérelmét 99%-ban teljesítették.

Az érintett tájékoztatására vonatkozó elutasíttott kérelmek számának alakulása az elmúlt 5 évben



XI.5. A Hatóság 2017. évi gazdálkodása

A Nemzeti Adatvédelmi és Információszabadság Hatóság működésének és gazdálkodásának hatodik évét is magunk mögött tudhatjuk 2017. december 31-ével.

XI.5.1. A bevételi előirányzat és teljesítési adatai 2017. évben

A NAIH 2017. évi költségvetése, eredeti előirányzata 642 300eFt volt, melyből a kiemelt személyi előirányzat 411 800eFt, a munkáltatói járulék és szociális hozzájárulás előirányzat 103 000eFt, a dologi kiadások kiemelt előirányzata 105 900eFt, a felhalmozási célú előirányzat 21 600eFt.

A 2017. év módosított előirányzata 739 482eFt volt, mely tartalmazza az eredeti előirányzatot, az 50 319eFt kötelezettségvállalással terhelt 2016. évi maradványt, valamint a KÖFOP-1.0.0-VEKOP-15-2016-00029 pályázatból származó, 25 000eFt egyéb bevételt. Ezen kívül az egyéb működési célú 10 268eFt bevételt, az egyéb szolgáltatások bevételét, mely 4 080eFt, valamint a kiszámlázott 1 114eFt bevételt, valamint az Arcades projekt elszámolás utáni 2 505eFt bevételét. A bérkompenzáció összege 930eFt volt. Az erre vonatkozó számokat a következő táblázat mutatja:

Megnevezés	**Eredeti előirányzat**	**Módosított előirányzat**	**Teljesítés**	**Kötelezettséggel terhelt 2017. évi maradvány**
Eredeti előirányzat	642 300			
Egyéb működési célú támogatások (KÖFOP)		25 000	25 000	
Közhatalmi bevételek		2 926	2 926	
Szolgáltatások bevételei		4 080	4 080	
Kiszámlázott forgalmi adó bevétel		1 114	1 114	
Árfolyamnyereség		40	40	
Egyéb működési bevételek		10 268	10 268	
Egyéb működési c. átvett pénzeszköz (ARCADES)		2 505	2 505	
2016. évi költségvetési maradvány		50 319	50 319	

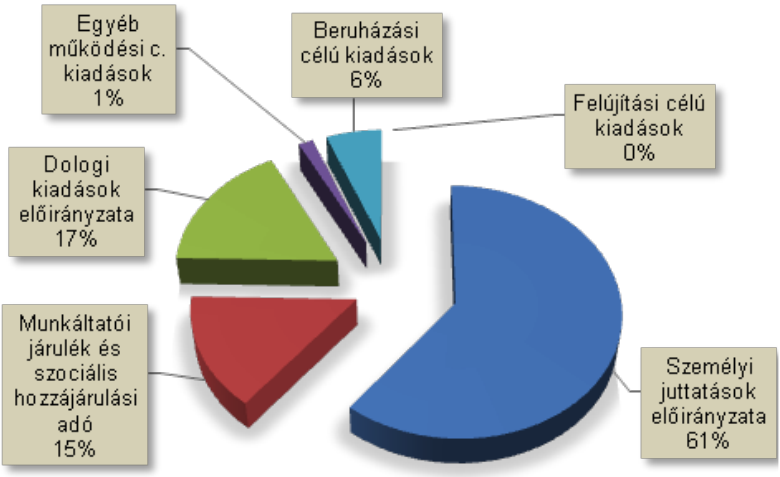
Központi, irányító szervi támogatás	*642 300*	*643 230*	*643 230*	
ebből: bérkompenzáció, garantált bérminimum		*930*	*930*	
Bevételi előirányzatok mindösszesen:	***642 300***	***739 482***	***739 482***	**–**
Személyi juttatások előirányzata	411 800	428 970	407 762	21 208
Munkáltatói járulék és szociális hozzájárulási adó	103 000	104 159	98 615	5 544
Dologi kiadások előirányzata	105 900	130 722	114 749	15 973
Egyéb működési c. kiadások	–	10 629	10 629	–
Beruházási célú kiadások	19 100	63 484	40 169	23 315
Felújítási célú kiadások	2 500	1 518	–	
Kiadási előirányzatok	***642 300***	***739 482***	***671 924***	***67 558***

XI.5.2. Kiadási előirányzatok és teljesítési adatai

A 2017. évi költségvetés eredeti előirányzata 642 300eFt volt. A módosított bevételi előirányzat 737 482eFt, melyből a teljesített személyi előirányzat kiadása 428 970eFt. A munkáltatói járulék és szociális hozzájárulási adó kiadások teljesítése 98 615eFt. A dologi kiadások összesen 114 749eFt-ot tettek ki. A beruházási kiadások mértéke 40 169eFt, az egyéb működési célú kiadások összege pedig 10 629eFt volt.

A következő grafikon a módosított előirányzatok teljesült kiadásait mutatja %-os megoszlásban:

Teljesített kiadási előirányzat megoszlása 2017



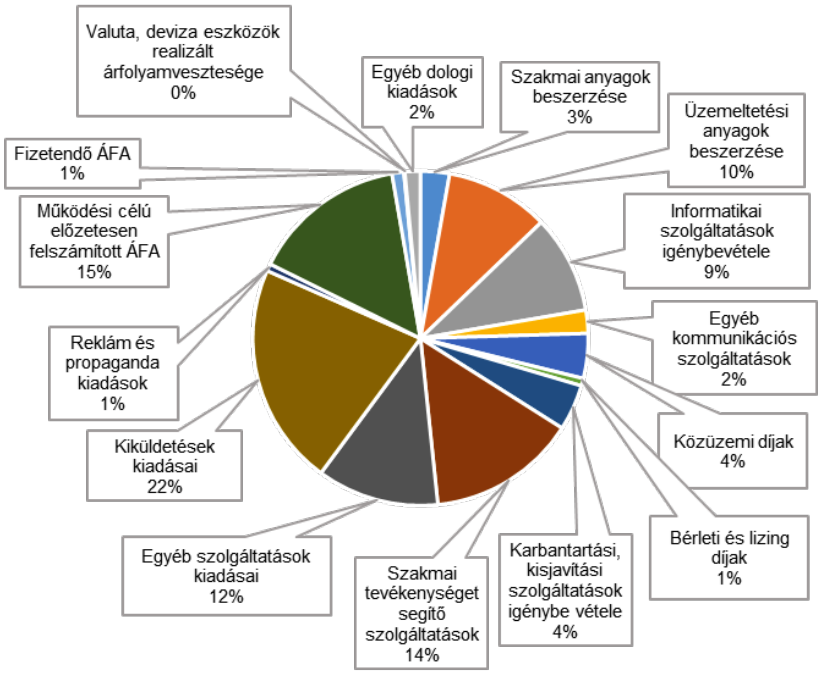
A 2017. évi módosított előirányzatok 61%-a a személyi juttatások kiadásaként teljesült. A munkáltatói járulék és szociális hozzájárulási adó 15% volt a teljes kiadáshoz mérten. A kiemelt dologi előirányzatok az összes módosított költségvetés 17%-át tették ki. A beruházási célú kiadások a teljes költségvetés 6%-a mértékéig teljesült. Az egyéb működési célú kiadások aránya 1% volt.

A kötelezettségvállalással terhelt 2017. év végi maradvány 67 558eFt volt. Ebből a KÖFOP-1.0.0-VEKOP-15-2016-00029 pályázat maradványa 25 000eFt, 2017. évben nem volt ebből a forrásból kifizetés, mivel a pénzügyi teljesítése a Hatóságot érintő szerződés módosításához volt kötve. A beruházás közbeszerzési eljárás elhúzódása miatt 23 315eFt lekötött maradvány keletkezett.

XI.5.3. A dologi kiadások megoszlása

A következő diagram a teljesült kiadási előirányzatok rovatrend szerinti %-os megoszlását mutatja.

A dologi kiadások megoszlása 2017



A dologi kiadások legnagyobb részét a kiküldetési kiadások teszik ki, mely 24 686eFt, azaz 22%. A GDPR 2018. évi bevezetése miatt jelentősen megnövekedett az uniós utak volumene.

A működési célú előzetesen felszámított Áfa – mivel a Hatóság nincs visszaigénylő pozícióban –, 15%-a teljes dologi kiadásnak, mely 17 153eFt. A szakmai tevékenységet segítő szolgáltatás kiadásainak értéke 16 439eFt.

Az üzemeltetési anyagok értéke 11 483eFt, valamint az informatikai szolgáltatások igénybe vételéért 10 880eFt-ot fizetett ki a Hatóság. A közüzemi díjakért Hatóságunk mindösszesen 4 970eFt-ot fizetett ki.

XI.5.4. A bírságbevételek alakulása

A Hatóság által kiszabott és befolyt bírság 68 010eFt volt, mely teljes egészében a központi költségvetés bevétele.

XI.5.5. A Hatóság létszámának alakulása

A Hatóság 2017. december 31-i munkaügyi létszáma 77 fő volt. A létszámbővülés a 2018-tól alkalmazandó általános adatvédelmi rendeletre való felkészülés miatt már év végén megindult. A nagyobb személyi erőforrás bővítés 2018. év elejétől várható.

XI.6. Fényképek a Hatóság eseményeiről

A 2016-os beszámoló sajtótájékoztatója a Parlament épületében

E-commerce Expo 2017, NAIH stand

XI.7. A Hatóság elnökének részvétele szakmai konferenciákon, rendezvényeken 2017-ben

2017. január 13. – Párizs – International Workshop on Post-Mortem Data Protection – Fate of our personal data after decease

2017. január 19-20. – Firenze – Ch@rterClick! Workshop – roundtable discussions

2017. február 22-24. – Berlin – Meeting of FOI Commissioners and Ombudsmen - roundtable discussions

2017. február 28. – Budapest, Stefánia Palota – Biztonságpiac 2017 Konferencia és Kiállítás – A biztonság fejlődése az IT információbiztonság az adatvédelmi szabályok tükrében/pódiumbeszélgetés

2017. március 8. – Budapest – Ernst & Young Konferencia – Adatvédelmi szabályozás a technológiai fejlődés tükrében

2017. március 23-24. – Krakkó – V4 DPA's meeting – roundtable discussions

2017. március 31. – Budapest, Müpa – CIO-fórum 2017 – Adatvédelmi szabályozás a technológiai fejlődés tükrében

2017. április 4. – Budapest, Ernst & Young Konferencia – Adatvédelmi szabályozás a technológiai fejlődés tükrében

2017. április 10. – Kaposvár – Dél-dunántúli Közigazgatási és Munkaügyi Regionális Kollégium teljes ülése – Az adatvédelem időszerű kihívásai

2017. április 27-28. – Ciprus, Limasszol – Európai Adatvédelmi Biztosok Tavaszi Konferenciája – kerekasztal beszélgetések

2017. május 2. – Budapest, Telekom Székház – a Telekom kiemelt német ügyfelei vezetőinek tartott konferencia – New data protection era – challenges and duties for the Hungarian DPA

2017. május 3. – Budapest – mySec GDPR konferencia – Adatvédelmi szabályozás a technológiai fejlődés tükrében

2017. május 4-5. – Brüsszel – European University Association Expert Group meeting - Open Access/roundtable discussions

2017. május 9. – Budapest – AIDA Magyar Nemzeti Szekciójának konferenciája – Az új adatvédelmi szabályozás aktuális kérdései, kihívásai és a biztosítás

2017. május 17-18. – Tbilisi, Grúzia – 19th Meeting of the Central and Eastern European Data Protection Authorities – Data processing by law enforcement sector/roundtable discussion

2017. május 24. – Budapest - KPMG Adatvédelmi Konferencia – Az új Európai Adatvédelmi Szabályozás és a magyar vonatkozásai

2017. május 25-26. – Budapest, Ludovika Campus – Eljárási jog az Európai Unióban? – a ReNEUAL Modell szabályok értékelés, avagy az Európai Unió közigazgatási eljárási kódexe a magyar kutatók szemszögéből – tudományos és szakmai konferencia – A magyar adatvédelmi hatóság eljárásai a GDPR alapján

2017. május 26-28. – Pozsony – GLOBSEC 2017 Forum – roundtable discussions

2017. május 29. – Budapest, Pázmány Péter Katolikus Egyetem, Jog és Államtudományi Kar, „Titkos információgyűjtés és a magánszféra védelme" című konferencia – A Nemzeti Adatvédelmi és Információszabadság Hatóság szerepe a titkos információgyűjtés ellenőrzésében

2017. június 6. – Budapest – Az Általános Adatvédelmi Rendelet (GDPR), Változó szabályozás, új kihívások c. rendezvény – Technológiai fejlődés és adatvédelem

2017. június 13. – Budapest - ISACA Konferencia – Adatvédelem a technológiai fejlődés tükrében

2017. június 16. – Budapest – Adózás Európában – XI. Nemzetközi Adókonferencia – Digitalizáció és biztonság: adatvédelmi korlátok

2017. június 29. – Budapest – MNV Zrt. Fórum – GDPR

2017. július 4. – Kecskemét – „Big data" IV. Public Relations Akadémia – Az információszabadság jelentősége, társadalmi funkciói

2017. július 5. – Budapest – Információszabadság Konferencia – Az információszabadság jelentősége, társadalmi funkciói

2017. július 6. – Miskolc – Magyar Könyvtárosok Egyesülete 49. Vándorgyűlés – A személyes adatok kezelése a könyvtárak életében – aktuális kérdések

2017. szeptember 7-8. – Észtország, Tartu – E-Volution of Data Protection – roundtable discussion

2017. szeptember 11. – Budapest – ITOSZ/Az EU Általános Adatvédelmi Rendeletének alkalmazása a gyakorlatban szakmai konferencia – Általánosságban a GDPR hazai alkalmazásáról/nyitó előadás

2017. szeptember 20-21. – Manchester – International Conference for Information Commissioners in Manchester – roundtable discussion

2017. szeptember 25-29. – Hong-Kong – 39th International Conference of Data Protection and Privacy Commissioners – Hungary's first-hand experiences of how profound change to the political system affected the establishment of the new fundamental rights

2017. október 2. – Tatabánya – Magyar Könyvtárosok Egyesülete Szakmai Napok – A személyes adatok kezelése a könyvtárak életében 2018-tól

2017. október 5. – Balatonföldvár – Belügyminisztérium Országos Katasztrófavédelmi Főigazgatóság Hivatalának rendvédelmi adatvédelmi szakmai napok – Az új adatvédelmi rendelet

2017. október 5-6. – Eger – Az Európai Jogi Szaktanácsadó Bírák Egyesületének tudományos konferenciája – Az EU új adatvédelmi reformjának hatása a magyar jogra

2017. október 8-10. – Visegrád – Visegrad V4 Meeting – DPA's – roundtable discussions

2017. október 10. – Budapest – BM Adatvédelmi előadás sorozat – Aktualitások az információszabadság körében, felkészülés az adatvédelmi rendelet, a GDPR alkalmazására.

2017. október 16. – Budapest – Kúria Teljes Ülés – Az új Európai Adatvédelmi Szabályozás és a magyar vonatkozásai

2017. október 16-17. – Varsó – 20th anniversary of the personal data protection law in Poland – Effectiveness of privacy regulations – Hungarian experiences

2017. október 19. – Budapest – GDPR – az Európai Unió új adatvédelmi szabályozása a gyakorlat tükrében konferencia – Az új Európai Adatvédelmi Szabályozás és a magyar vonatkozásai

2017. október 24. – Budapest – Magyar Honvédség IV. Adatvédelmi Továbbképzés – Az új Európai Adatvédelmi Szabályozás és a magyar vonatkozásai

2017. október 25. – Budapest – IVSZ konferencia – Az új Európai Adatvédelmi Szabályozás és a magyar vonatkozásai

2017. október 25. – Budapest – PPKE JÁK Díszterme – Az Alaptörvény VI. cikkének érvényesülése a jogrendszeren belül konferencia – Személyiségi jogi problémák a NAIH gyakorlatában

2017. október 26. – Budapest – „Új adatvédelmi rendelet – a GDPR hazai alkalmazása" konferencia – Az új Európai Adatvédelmi Szabályozás és a magyar vonatkozásai

2017. november 6-9. – Portugália, Lisszabon – Web Summit – roundtable discussions

2017. november 27. – Balatonföldvár – NBSZ vezetői állományának továbbképzése, Adatvédelem és információbiztonság – A Nemzetbiztonsági Szakszolgálat auditjának értékelése

2017. november 30. – Budapest – 16. Országos Kegyelet és Emlékezet Konferencia – A kegyelet és az emlékezés kultúrája a digitalizáció korában, az adatvédelem és az információszabadság tükrében

2017. december 5. – Budapest – BRFK Konferencia – Az új Európai Adatvédelmi Szabályozás és a magyar vonatkozásai

X.8. 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 Délkelet-európai Rendőri Együttműködési Egyezmény kihirdetéséről szóló 2012. évi XCII. törvény, 2012. december 11-től hatályos.
- A jogalkotásról szóló 2010. évi CXXX. törvény.
- A jogszabályok előkészítésében való társadalmi részvételről szóló 2010. évi CXXXI. törvény.
- A menedékjogról szóló 2007. évi LXXX. törvény.
- A pedagógiai szakszolgálati intézmények működéséről szóló 15/2013. (II.26.) EMMI rendelet.
- A tömeges bevándorlás okozta válsághelyzet Magyarország egész területére történő elrendeléséről, valamint a válsághelyzet elrendelésével, fennállásával és megszüntetésével összefüggő szabályokról szóló 41/2016. (III.9.) Korm. rendelet.
- ÁFA tv., az általános forgalmi adóról szóló 2007. évi CXXVII. törvény.
- Alaptörvény, alkotmány: Magyarország Alaptörvénye (2011. április 25.)
- Általános adatvédelmi rendelet lásd: GDPR.
- Avtv., a személyes adatok védelméről és a közérdekű adatok nyilvánosságáról szóló 1992. évi LXIII. törvény.
- Ávtv., az állami vagyonról szóló 2007. évi CVI. törvény.
- Az Európai Parlament és a Tanács 765/2008/EK rendelete (2008. július 9.) a termékek forgalmazása tekintetében az akkreditálás és piacfelügyelet előírásainak megállapításáról és a 339/93/EGK rendelet hatályon kívül helyezéséről.
- Bit., a biztosítási tevékenységről szóló 2014. évi LXXXVIII. törvény.
- Btk., a Büntető Törvénykönyvről szóló 2012. évi C. törvény.
- Bűnügyi 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.

- Eurodac rendelet, (EUROpean DActylographic Comparison system) az Eurodac létrehozásáról szóló 2725/2000/EK Tanácsi Rendelet, és 2015. július 20-ával az azt felváltó, jelenleg is hatályos 603/2013/EU Parlamenti és Tanácsi Rendelet.
- Europol rendelet, az Európai Parlament és Tanács (EU) 2016/794 rendelete (2016. május 11.) a Bűnüldözési Együttműködés Európai Uniós Ügynökségéről (Europol), valamint a 2009/371/IB, a 2009/934/IB, a 2009/935/IB, a 2009/936/IB és a 2009/968/IB tanácsi határozat felváltásáról és 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.
- 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.
- Kkvtv., a kis- és középvállalkozásokról, fejlődésük támogatásáról szóló 2004. évi XXXIV. törvény.
- Költségtérítési rendelet, a közérdekű adat iránti igény teljesítéséért megállapítható költségtérítés mértékéről szóló 301/2016. (IX. 30.) Korm. rendeletet.
- Mavtv., a minősített adat védelméről szóló 2009. évi CLV. törvény.
- MNBtv., a Magyar Nemzeti Bankról szóló 2013. évi CXXXIX. törvény.
- Mt., a Munka Törvénykönyvéről szóló 2012. évi I. törvény.
- Nbtv., a nemzetbiztonsági szolgálatokról szóló 1995. évi CXXV. törvény.
- Nvtv., a nemzeti vagyonról szóló 2011. évi CXCVI. törvény.
- Pmt., régi, 2017. június 26. napjáig hatályos, a pénzmosás és a terrorizmus finanszírozása megelőzéséről és megakadályozásáról szóló 2007. évi CXXXVI. törvény.
- Pmt., új, a pénzmosás és a terrorizmus finanszírozása megelőzéséről és megakadályozásáról szóló 2017. évi LIII. törvény (2017. június 26. napjától hatályos).
- Ptk. új, a Polgári Törvénykönyvről szóló 2013. évi V. törvény.

- SIS II törvény, a 2012. évi CLXXXI. törvény, a Schengeni Információs Rendszer második generációja keretében történő információcseréről, továbbá egyes rendészeti tárgyú törvények ezzel, valamint a Magyary Egyszerűsítési Programmal összefüggő módosításáról.
- SIS II, a Schengeni Információs Rendszer második generációjának létrehozásáról, működtetéséről és használatáról szóló 1987/2006/EK számú európai parlamenti és tanácsi rendelet.
- Szaztv., a személyazonosító jel helyébe lépő azonosítási módokról és a kódok használatáról szóló 1996. évi XX. törvény.
- Szvtv., a személy- és vagyonvédelmi, valamint a magánnyomozói tevékenység szabályairól szóló 2005. évi CXXXIII. törvény.
- Thtv., a társasházakról szóló 2003. évi CXXXIII. törvény.
- Ütv., az ügyészségről szóló 2011. évi CLXIII. törvény.

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)