



Nemzeti Adatvédelmi és
Információszabadság Hatóság



A NEMZETI ADATVÉDELMI ÉS INFORMÁCIÓSZABADSÁG HATÓSÁG
2019. ÉVI BESZÁMOLÓJA

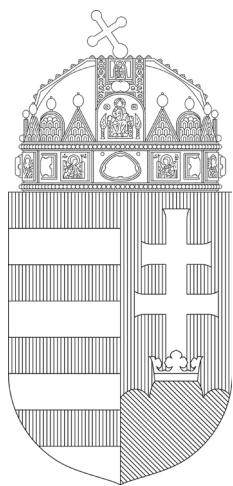
A Nemzeti Adatvédelmi
és Információszabadság Hatóság

Beszámolója

a 2019. évi tevékenységéről

B/8988

Nemzeti Adatvédelmi és Információszabadság Hatóság
Budapest, 2020



Bevezető

Köszöntöm a Tisztelt Olvasót!

Madách Imre után szabadon „*Be van fejezve a nagy mű, igen. A gép forog*”, de az alkotó nem pihen, hiszen hiába készült el az általános adatvédelmi rendelet az Európai Unióban, hátra van még két igen fontos művelet: a jogalkalmazás gyakorlati kimunkálása és a tudás átadása, közvetítése a szakmai és szélesebb közönség felé egyaránt.

A NAIH elnökeként és régi egyetemi oktatóként 2019-ben nagy hangsúlyt fektettem az adatvédelmi és információszabadsággal kapcsolatos ismeretek oktatására, azoknak az egyetemi képzésben való meghonosítására. Sajnos (hozzáteszem: erőfeszítéseink ellenére) a közoktatásban és a felsőoktatási alapképzésben az információs jogokkal kapcsolatos ismeretekre méltatlannul kevés figyelem esik – annak ellenére, hogy a digitális korban a magánszféra védelmére már a kiskorú felhasználókat is komolyan kellene nevelni! Ugyanakkor az egyetemi szakképzések területén óriási a piaci igény és kereslet az uniós adatvédelmi ismeretek megszerzésére és elmélyítésére.

Az ELTE Jogi Továbbképző Intézete 2014-ben indította adatbiztonsági és adatvédelmi szakjogász képzését: „*A kettő plusz egy féléves képzés célja, hogy az alapképzésben szinte meg sem jelenő adatbiztonság, adatvédelem, információszabadság, illetve a köz- és magánszféra adatkezelése területén felmerülő jogi problémákat a szakterület alaposabb megismertetésével, a NAIH gyakorlatára építve, felkészítse a jogászokat a hatósági-, illetve a peres és nemperes eljárások szakszerű vitelére.*”

A Nemzeti Közszolgálati Egyetemen 2019-ben indított Európai uniós adatvédelmi szaktanácsadó szakirányú továbbképzési szakon a cél „*olyan adatvédelmi szaktanácsadók képzése, akik alkalmazni tudják a GDPR rendelkezéseit az új, az EGT területén elvárt adatvédelmi szabályrendszer ismeretén keresztül.*”

A képzéseken zömében jogász végzettségű hallgatók vesznek részt (ügyvédök, bírók, köztisztviselők). Sokan a közigazgatásban dolgoznak, de rendvédelmi szervektől, a honvédségtől vagy akár a piaci szférából is érkeznek. A közösbennük, hogy minden nap munkájuk során szükségük van az információs jogok-

kal kapcsolatos joganyag alkalmazására, értelmezésére. Az ehhez szükséges tudás átadását elsősorban a NAIH szakértői biztosítják.

Szintén hasonló célt szolgált a 2019-ben első ízben elektronikus úton lebonyolított adatvédelmi tiszttiselők 2019. évi konferenciája, mely egy előzetes igényfelmérés eredményét figyelembe véve videóra vett előadások formájában közvetítí és osztja meg a NAIH szakmai ismereteit és tapasztalatait a szakmai közönséggel és a nyilvánossággal.¹

Az információszabadság területén 2019-ben is igyekeztünk olyan területeket „felderíteni”, átfogó tájékoztatást adni, ahol szükség van a felügyeleti szerv iránymutatására.²

Ezzel kapcsolatban megjegyzendő, hogy a közérdekű adatok nyilvánosságához fűződő alkotmányos alapjog szabályozási rendszere – a közérdekből nyilvános személyes adat fogalmának bevezetése óta – Magyarországon tulajdonképpen hosszú idő óta változatlan (ami természetesen nem azt jelenti, hogy a jogalkalmazás ne küzdene folyamatosan különféle régi-új problémákkal). Több évtizedes tapasztalataim alapján állítom, hogy valójában másfajta megközelítést igényel a közhatalom gyakorlásának nyilvánossága és a közpénzekkel való gazdálkodás nyilvánossága – ezekről a kérdésekéről pedig tudományos igényű viták keretében lehetne és kellene értekezni.

Szintén új helyzetet teremt mindenki információs jog tekintetében a megvalósult digitális környezet és az ezzel kapcsolatos kihívások köre, hiszen itt az adatkezelések minősége, gyorsasága, mennyisége bizony feszegeti a régi elvek kereteit. Elég, ha a közérdekű adatok kereshetőségének és elérhetőségének megköny nyítésére gondolunk, mely – optimális esetben – akár néhány másodpercre szűkíti azt a munkaidőt, ami papíralapú akták százainak átnézésével napokba vagy hetekbe tellett. A rendelkezésre álló digitális eszközökkel és megoldásokat pedig az alkotmányos alapjogok szolgálatába kellene állítani – minél teljesebb és magától értetődő módon!

Végül szót kell ejteni a 2018. szeptember 12-én az Európai Parlament által Magyarországgal szemben kezdeményezett úgynevezett 7. cikk szerinti, jogállamiságot vizsgáló eljárásról, melynek során civil szervezetek több ízben is hozzászólásaiakban azt vetik fel, hogy a NAIH nem tekinthető független intézménynek

a Hatóság elnökének kinevezési rendje miatt. A vádat egyetlen szakmai érvvel szeretném cáfolni e helyen: a Hatóság elnökének kinevezési rendje maradéktalanul megfelel a GDPR 53. cikk (1) bekezdésében meghatározott követelményeknek. Az adatvédelmi felügyeleti szerv vezetőjének a jelenleg hatállyos magyar szabályok szerinti kijelölésének rendjét az Európai Bizottság – éppen az adatvédelmi biztos megbízásának megszünésével kapcsolatban a civil szervezetek által hivatkozott kötelezettségszegési eljárást megelőzően – alaposan és minden elemére kiterjedően vizsgálta és e tekintetben semmilyen kifogást nem fogalmazott meg, azt az Európai Unió jogával összhangban állónak tartotta és egyébként a hivatkozott kötelezettségszegési eljárásnak e tárgykör nem is képezte részét. A NAIH részéről tehát ezt a felvetést – bár visszatérő vádaskodásról van szó – egyszer s mindenkorra megalapozatlannak ítélem.

Budapest, 2020. március 2.

Dr. Péterfalvi Attila

címzetes egyetemi tanár
a Nemzeti Adatvédelmi és Információszabadság Hatóság
Elnöke

1 <https://naih.hu/dpo-konferencia-2019.html>

2 <https://naih.hu/informacioszabadsaggal-kapcsolatos-tajekoztatok.htm>



I. A Hatóság működésének statisztikai adatai

I.1. Ügyeink statisztikai jellemzői

A GDPR kötelező alkalmazásának időpontja (2018.05.25) óta a 2019-es év az első teljes naptári év, amelynek ügystatisztikai elemzése információt adhat az új szabályozási környezetnek az adatvédelemi hatósági tevékenységre gyakorolt hatásáról.

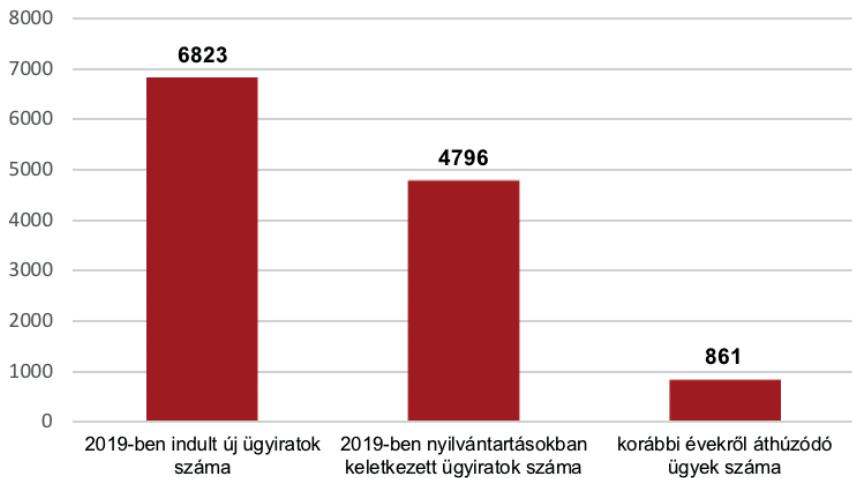
A Hatóság működésének számszerűsíthető bemutatását 2018-ban megnehezítette az évközben többször változott jogi környezet és a különböző szakfeladatok, nyilvántartások részleges átalakulása, illetve megszűnése. A 2019-es év ügystatisztikai adatainak bemutatásakor törekedtünk a 2019-ben tapasztalt változások megjelenítésére.

2019-ben a Hatóság elektronikus iratkezelő rendszerében 6823 db új ügy került iktatásra. A korábbi évekről áthúzódó ügyekkel (861 db) együtt 7684 db ügy volt folyamatban.

Az átalakult elektronikus nyilvántartó rendszerekben érkeztetett és iktatott iratok száma 4796 db volt.

2019-ben összesítve 11.619 ügy indult a Hatóságnál, a korábbi évekről áthúzódó ügyekkel együtt tehát 12.480 ügy volt folyamatban.

a Hatóság ügyszáma 2019-ben

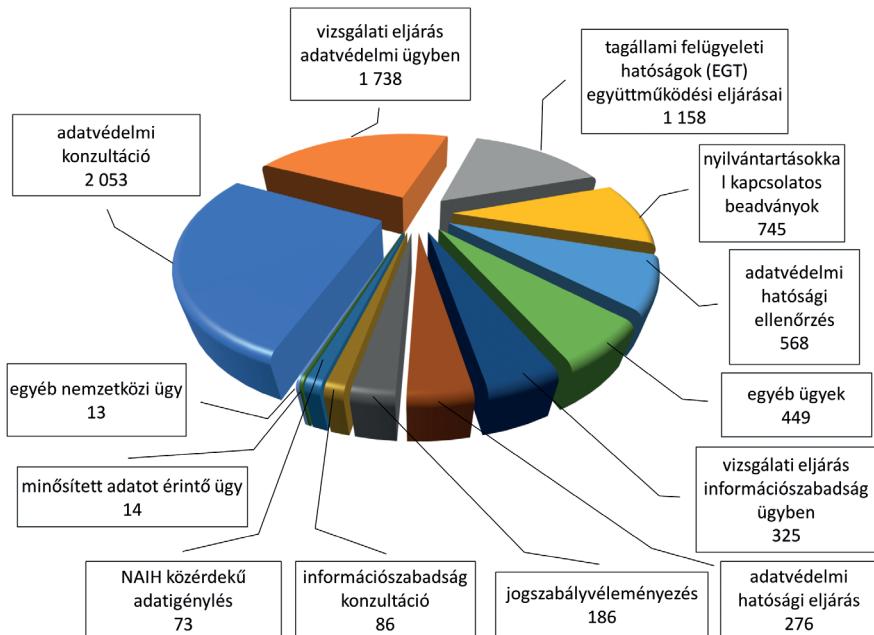


A Hatóság 2019-es ügyeinek száma (és annak változása 2018-hoz viszonyítva) ügykörönként

ügykör	2018	2019
adatvédelmi konzultáció	2.409	2.053
vizsgálati eljárás adatvédelmi ügyben	827	1.738
tagállami felügyeleti hatóságok (EGT) együttműködési eljárásai	606	1.158
nyilvántartásokkal kapcsolatos beadványok	1.305	745
adatvédelmi hatósági ellenőrzés	234	568
egyéb ügyek	131	449
vizsgálati eljárás információszabadság ügyben	375	325
adatvédelmi hatósági eljárás	67	276
jogszabály-véleményezés	195	186
információszabadság konzultáció	88	86
NAIH közérdekű adatigénylés	74	73
minősített adatot érintő ügy	15	14
egyéb nemzetközi ügy	85	13
folyamatban lévő ügyek összesen:	6.411	7.684
DPO nyilvántartásba érkezett elektronikus bejelentések	1.786	4.796
Éves ügyszám összesen:	8.197	12.480

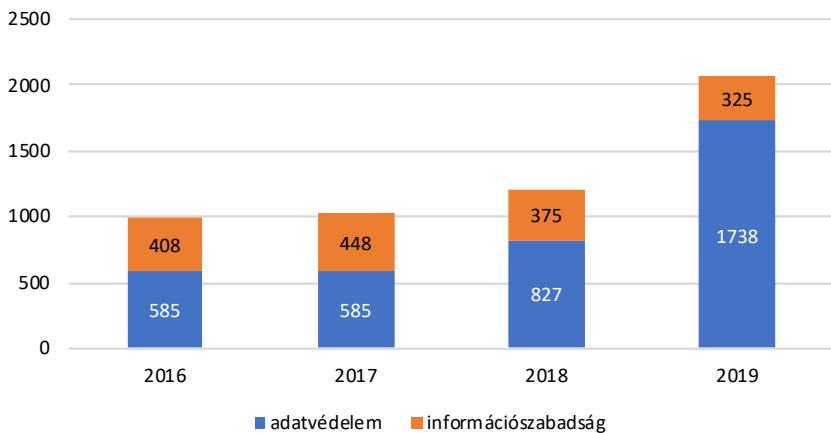
A Hatóság 2019-ben folyamatban lévő ügyei

(DPO nyilvántartás nélkül)



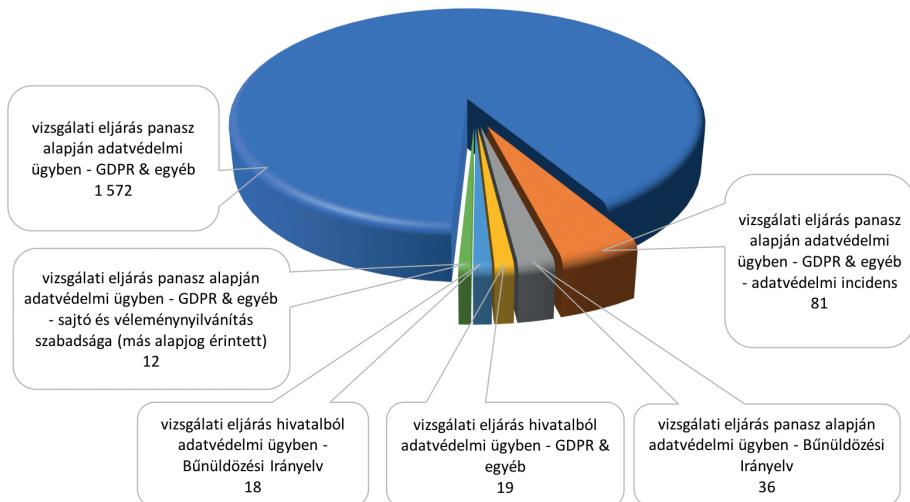
A konzultációs típusú ügykörbe tartozó ügyek száma 20%-kal csökkent, míg az adatvédelmi vizsgálati ügykörbe tartozó ügyek száma kétszeresére emelkedett 2018-hoz képest. A vizsgálati eljárások számának folyamatos emelkedését jól érzékeltetik a következő ábrák.

Vizsgálati eljárások száma



Az adatvédelmi vizsgálati típusú eljárások 2019-es számát ügytípusonként a következő kimutatás szemlélteti:

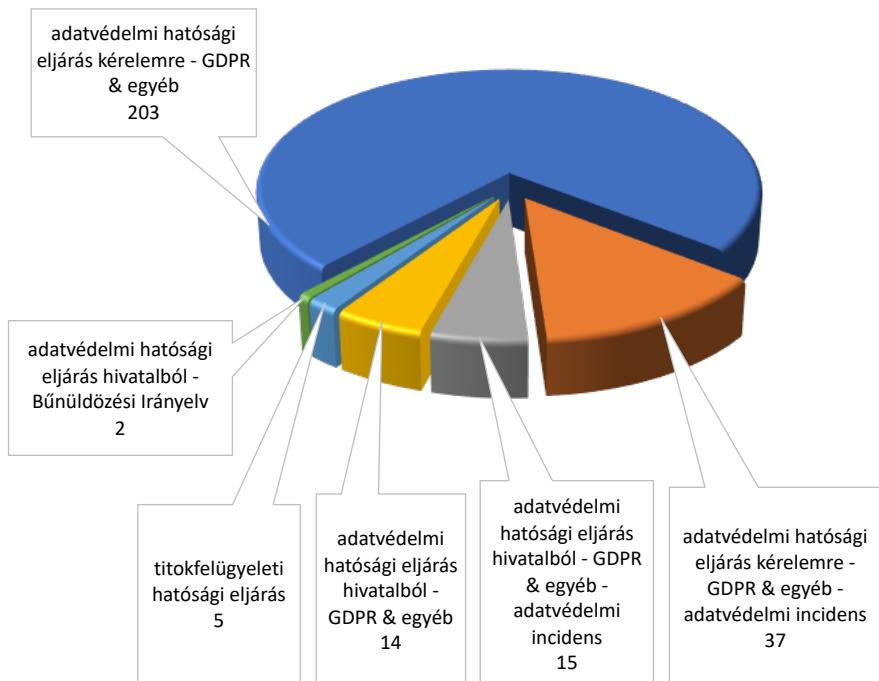
Adatvédelmi vizsgálati eljárások ügyféltypusonként



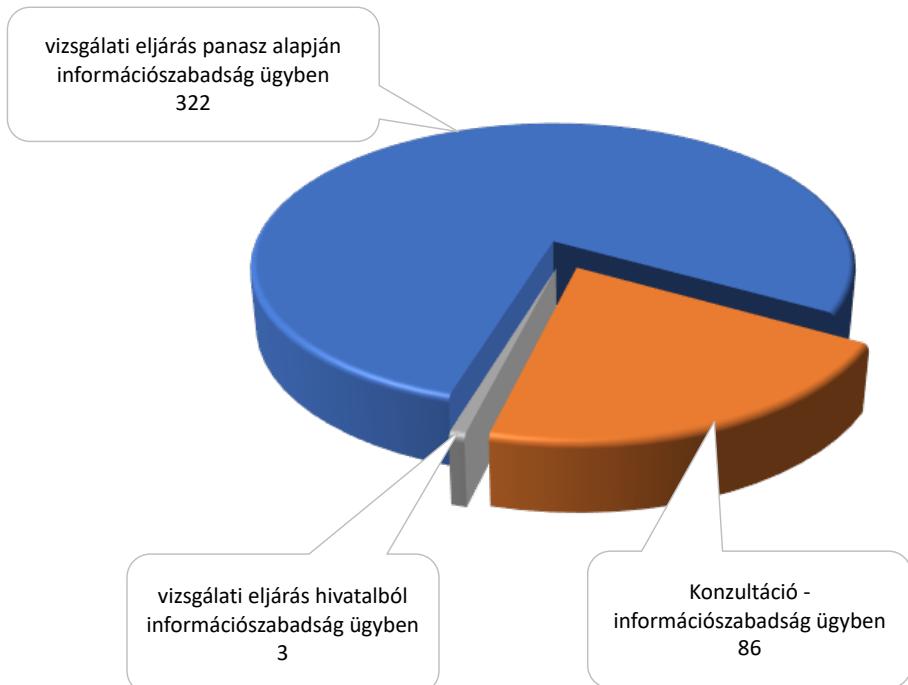
2019. évben az eljárásjogi környezet változása is mérhető eredményeket mutat. Az Ákr. hatályba lépése, illetve az Infotv. módosítása óta indult hatósági eljárások száma 2018-as 67 db -ról 276-re emelkedett. Ezzel az ügyszám emelkedéssel az ügyintézői terhelés is megsokszorozódott.

Ügytípus	Ügyszám (db)
adatvédelmi hatósági eljárás kérelemre - GDPR & egyéb	203
adatvédelmi hatósági eljárás kérelemre - GDPR & egyéb - adatvédelmi incidens	37
adatvédelmi hatósági eljárás hivatalból - GDPR & egyéb - adatvédelmi incidens	15
adatvédelmi hatósági eljárás hivatalból - GDPR & egyéb	14
titokfelügyeleti hatósági eljárás	5
adatvédelmi hatósági eljárás hivatalból - Bünöldözési Irányelv	2
Hatósági eljárások összesen:	276

Hatósági eljárások ügyféltipusonként



Információszabadsággal kapcsolatos ügyek ügykörönként



2019-ben a Hatóság telefonos ügyfélszolgálatára 2933 hívás érkezett, amely az előző évek adataihoz viszonyítva továbbra is emelkedést mutat. Megnövekedett azon érdeklődők száma, akik a GDPR alapján az óket mint érintetteket megillető jogok és érdekek védelmében – valamint az adatkezelővel szembeni eredményes fellépéshez – a Hatóság tájékoztatását, segítségét kérték. A Hatóság telefonos ügyfélszolgálata a GDPR-ban rögzített érintett jogok adatkezelő irányában történő gyakorlásának lehetőségeire, korlátaira és az adatkezelő válaszadási határidejére is felhívta a telefonálók figyelmét, emellett a számukra nyitva álló jogorvoslati lehetőségek kapcsán a Hatóság eljárásaival, a panaszok és kérelmek benyújtásának módjával összefüggésben is tájékoztatást adott.

Számos esetben kérték a Hatóság tájékoztatását ingatlantulajdonosok – illetve társasházban, lakásszövetkezeti lakásban élők – azzal kapcsolatban, hogy milyen jogi lehetőségeik vannak, ha a szomszédjuk az ő ingatlanjukat, bejáratí ajtajukat, esetleg a lépcsőházat is megfigyelő kamerát szerelt fel a saját ingatla-

nára. Sajnos sok esetben nem egyértelmű, hogy a vagyonvédelmi célú kamerák valóban jogosító módon kerültek-e kiépítésre, vagy azok látószöge ténylegesen csak a saját ingatlanra irányul – például mivel azt megfelelő kitakarási (maszkolási) beállítással látták el, vagy esetleg a felszerelt kamera csak álkamera volt. A telefonálók sok esetben már az illetékes jegyzőnél is próbáltak birtokvédelmi eljárást kezdeményezni, akik azonban az érintetteket a Hatósághoz irányították.

Gyakran érkeztek olyan hívások is, amelyek a munkavállalók kamerás megfigyelését érintették. Az esetek közös jellemzője, hogy az érintettek semmiféle vagy nem kellően részletes tájékoztatást kaptak az adatkezelés körülményeiről. Emellett sok esetben az adatkezelők érdeklödtek arról, hogy milyen módon végezhetnek jogoszerűen kamerás megfigyelést.

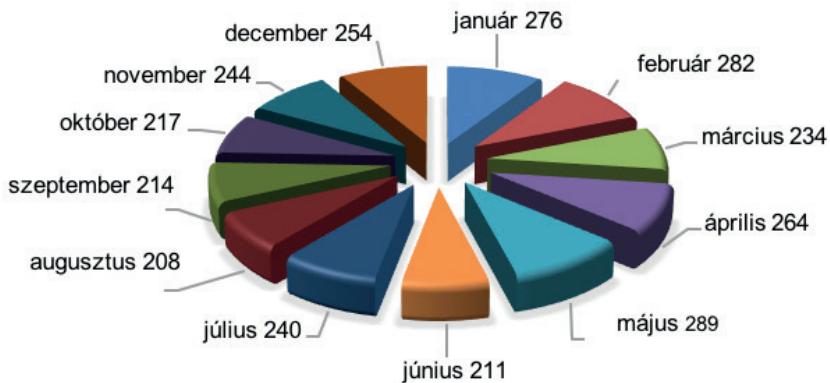
Az egyelőre csak angolul elérhető, az Európai Adatvédelmi Testület 3/2019. számú, a kamerás adatkezelési műveletekről szóló iránymutatása remélhetőleg segíteni tudja majd az adatkezelők megfelelését e területen.

Továbbra is számos kérdés érkezett azzal kapcsolatban, hogy milyen követelményeknek kell megfelelnie egy webshop indítását tervező személynek vagy szervezetnek, noha a Hatóság az adatvédelmi reformmal kapcsolatos állásfoglalásai között már 2018 nyarán elérhetővé tette a magánszemélyek által üzemeltetett honlapok adatvédelmi kérdéseiről szóló útmutatását.³

Végül, sok telefonáló azzal a problémával kereste az ügyfélszolgálatot, hogy tömegesen kap olyan zaklató jellegű, többnyire marketing célú elektronikus leveleket, esetleg SMS-eket, amelyek küldését nem kérte, azokra soha nem iratkozott fel. Sok esetben a levelek alján található internetes hivatkozássra történő kattintás ellenére sem lehet leiratkozni azokról vagy nincs is leiratkozási link. A Hatóság az őket érintettként a GDPR alapján megillető jogokon túl, arra is felszokta hívni a figyelmet, hogy a magyar nyelvű vagy egyértelműen hazai címzetteknek szánt elektronikus hirdetéssel összefüggő felügyeleti eljárás lefolytatására a Nemzeti Média- és Hírközlési Hatóság rendelkezik feladat- és hatáskorrel.

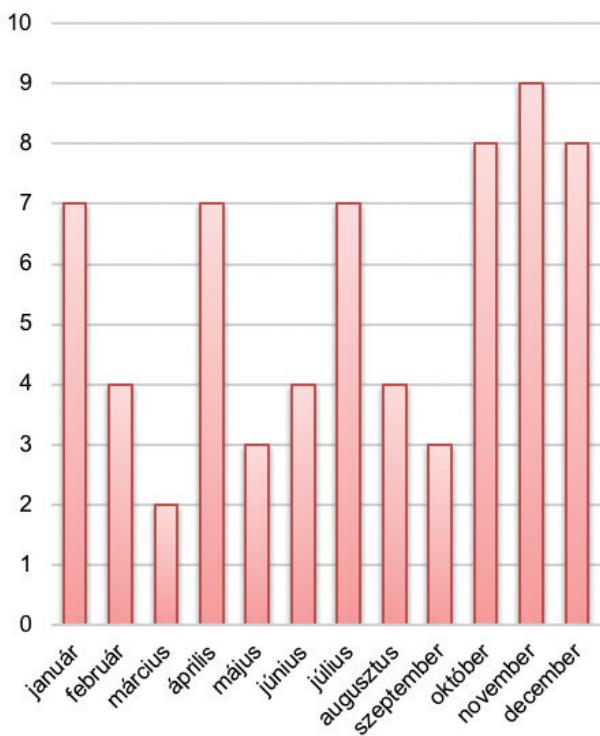
3 <https://naih.hu/files/2017-02-17-webaruhaz-tajekoztato-NAIH-2017-1060-V.pdf>

Telefonos ügyfélszolgálat 2019-ben (db hívás)



A GDPR alkalmazandóvá válását követő első évben a Hatóság személyes ügyfélszolgálatát 66 alkalommal vették igénybe – ez a 2018-as évehez képest mintegy 30%-os emelkedést jelent –, amelyek során az érintettek a személyes adatok kezelésével, illetve a közérdekű vagy a közérdekből nyilvános adatok megismeréséhez fűződő jogok gyakorlásával kapcsolatos jogszerelem miatti konkrét panaszukat terjeszthették elő vagy az eljárás irataiba való betekintési jogukat gyakorolták.

Személyes ügyfélfogadás 2019-ben (db)



A Hatóság honlapjáról elérhető elektronikus adatvédelmi tisztviselő bejelentő fejlületen 2019-ben 2400 új adatkezelő és adatfeldolgozó hozott létre fiókot, illetve több mint száz alkalommal érkezett a bejelentett tisztviselő, illetve az adatkezelő/adatfeldolgozó szervezet törlésére irányuló kérelem. Az adatvédelmi tisztviselő nevének (jogi személy esetén megnevezésének), elérhetőségének módosítását az adatkezelők és adatfeldolgozók a rendszerben létrehozott fiókjukon keresztüli új bejelentés benyújtásával kezdeményezhették, azonban a korábban rögzített adatok törlésére csak a tölük érkező írásbeli kérelem alapján van lehetőség.

I.2. Az adatvédelmi tisztviselők éves konferenciája

Az Infotv. 25/N. § rendelkezéseire tekintettel az adatvédelmi tisztviselők éves konferenciáját a Hatóság elnöke hívja össze, az a Hatóság és az adatvédelmi tisztviselők rendszeres szakmai kapcsolattartását szolgálja, célja a személyes adatok védelmére és a közérdekű adatok megismerésére vonatkozó jogszabályok alkalmazása során az egységes joggyakorlat kialakítása.

A szakmai kapcsolattartást tehát nem az adatkezelővel, hanem elsősorban a Hatósághoz bejelentett – 2019. év végéig mintegy 1850, feladatait több mint 4200 szerveztnél ellátó – adatvédelmi tisztviselővel összefüggésben írja elő a jogszabály. Ezért a konferencián történő részvételi lehetőség független attól, hogy az adatvédelmi tisztviselő mely szektorban működő szerveztnél vagy mi-lyen jogviszony keretében látja el tevékenységét, hiszen akár több különböző szerveztnél is kijelölhettek, illetve potenciálisan kijelölhetik e tisztségre.

Tekintettel arra, hogy a GDPR alkalmazandóvá válását követően a korábbinál jelentősen több résztvevő számára kell az egységes joggyakorlat kialakítása érdekében a képzést elérhetővé tenni, valamint a tisztviselői feladatok nem csak Magyarország területéről láthatók el, a mindenkiukat megillető részvételi jogra figyelemmel az adatvédelmi tisztviselők éves konferenciája ebben az évben első alkalommal elektronikus úton került lebonyolításra. Az e-tanulási megoldások alkalmazásával a konferencia az elhangzó szakmai ismeretek magasabb szintű hasznosulásához is hozzájárulhatott, hiszen az több alkalommal visszanézhető, annak előadásait a tisztviselők felhasználhatják akár belső képzéseik során is.

A Hatóság a szakmai együttműködés jegyében lehetőséget nyújtott az adatvédelmi tisztviselők számára is a konferencia-előadások tartalmának alakítására, ennek keretében 2019 októberében online kérdőíves rendszerben mért fel az adatvédelmi tisztviselők igényeit, szakmai felkészültségét és a szélesebb kört érintő – adatvédelemmel és információszabadsággal kapcsolatos – kérdéseiket, témafelvetéseiket.

I.2.1. Az előzetes kérdőíves felmérés eredményei

A 2019 októberi időállapot szerint a Hatósághoz bejelentett összes, mintegy 1797 tisztviselő elektronikus levélcímére elküldtük a Hatóság elnökének konferencia-felhívását és az ahhoz kapcsolódó kérdőívet. Mivel a kitöltők szinte ki-zárolag (97,7%-ban) az elektronikus levélben elérhető hivatkozáson keresztül érkeztek az oldalra, így feltételezhető, hogy valóban az adatvédelmi tisztviselő-

ket érte el a kérdéssor. A felmérés a várakozásokon felüli eredményt hozott, hiszen arra 488 kitöltés érkezett, azaz az összes bejelentett tisztviselő 27,15%-a élt a Hatóság felhívásában foglalt lehetőséggel.

Az önkéntes válaszadók több mint fele 1-3 éve foglalkozik kiemelten adatvédelemmel és lát el adatvédelmi tisztviselői feladatokat, közel 20% azonban csak néhány hónapja foglalkozik érdemben a területtel, míg 26% már több mint 3 éve foglalkozik adatvédelemmel. A válaszadók 43%-a információszabadsággal kapcsolatos feladatokat is ellát, így feltételezhetően jelentős részben a közszférában tevékenykednek, ugyanakkor kevesebb, mint a válaszadók 10 %-át alkalmazza olyan szervezet, amely az Infotv. hatálya alá tartozó (bűnuldözési, nemzetbiztonsági, honvédelmi célú) adatkezelési tevékenységet is folytat.

A tisztviselők ismereteinek naprakészsgére vonatkozó eredményekből kiderült, hogy az elmúlt egy évben a tisztviselők 70%-a egy-, vagy többnapos továbbképzés keretében bővítette adatvédelmi tudását, ugyanakkor több mint 20%, 100 tisztviselő úgy látja el tevékenységét, hogy egyáltalán nem vett részt adatvédelmi tárgyú képzésen.

Az elmúlt egy évben vett részt adatvédelmi tárgyú szervezett képzésen?	Válaszok	Arány
egyetemi	80	16.39%
több napos	182	37.3%
egy napos	156	31.97%
online	40	8.2%
Egyik sem.	100	20.49%
Más...	11	2.25%

A kérdőív kitöltőinek háromnegyedét a szervezete is támogatta adatvédelmi ismereteinek bővítése során, jellemzően szervezett képzéseken történő részvételüket biztosították és szakmai tartalmakra fizettek elő részükre.

Támogatta a szervezete az adatvédelmi és adatbiztonsági ismereteinek bővítését?	Válaszok	Arány
Munkaidő kedvezménnyel	69	14.14%
Belső képzéssel	86	17.62%
Szervezett képzéssel	209	42.83%
Szakmai tartalmakra történő előfizetéssel	106	21.72%
Egyik sem	126	25.82%
Más...	23	4.71%

Az önállóan is megszerezhető ismereteik vonatkozásában kiemelendő, hogy a válaszadók közel fele nem olvasta a Hatóság 2018. évi beszámolóját, emellett több mint 100 tisztviselőt nem érnek el a naih.hu honlapon közzétett friss, már a GDPR alkalmazandóvá válását követően közzétett határozatok, jelentések, közlemények. Ugyanakkor a válaszadók 78%-a legalább havonta látogatja a Hatóság honlapját.

Milyen gyakran keresi fel a www.naih.hu weboldalt?	Válaszok	Arány
Hetente vagy gyakrabban	195	39.96%
Havonta	185	37.91%
Ritkábban	94	19.26%
Soha	14	2.87%

Noha a GDPR-ban szereplő szerződéses jogalap online környezetben történő alkalmazásáról vagy éppen a kamerák alkalmazásával összefüggő adatkezelésről szóló iránymutatás is először az Európai Adatvédelmi Testület honlapján vált elérhetővé – mivel a GDPR utáni egységes joggyakorlat kialakítását célzó, társadalmi véleményezésre közzétett iránymutatás-tervezetek is még csak ezen a felületen érhetők el –, a tisztviselők 62%-a nem látogatja azt. Az oldalon az egyes tagállami felügyeleti hatóságok friss, bírság kiszabásával zároló döntéseinek angol nyelvű összefoglalása is elérhető, így hasznos forrásnak bizonyulhatnának az adatvédelmi területen tudományos kutatást végzők munkájához is.

Milyen gyakran keresi fel az Európai Adatvédelmi Testület honlapját?	Válaszok	Arány
Hetente vagy gyakrabban	58	11.89%
Havonta	129	26.43%
Ritkábban	214	43.85%
Soha	87	17.83%

A Hatóság megújuló honlapjának tartalmára irányuló javaslatok kapcsán a válaszadók jelentős többsége a KKV szektort érintő kérdés-felelet adatbázist, illetve kategorizált, témakör szerint szűrhető hatósági döntéseket látta legszívesebben, így a Hatóság kiemelt figyelmet fordít a kapcsolódó fejlesztésekre.

A tisztviselők tevékenysége kapcsán látható volt, hogy jelentős többségük teljesíti a GDPR 39. cikkében meghatározott feladatak közül az adatkezelő vagy az adatfeldolgozó, továbbá az adatkezelést végző munkatársak részére nyújtandó tanácsadási feladatait, szakmai álláspontjukat jellemzően kikéri a szervezetük vezetése. A többség azonban kinevezése óta nem folytatott vizsgálatot, auditot a belső adatvédelmi megfelelés kapcsán vagy azt nem dokumentálta, valamint azzal kapcsolatos tevékenységéhez nem készített tervet, amely azonban az elszámoltathatóság elvének érvényesülését, a szervezeten belül az adatvédelmi tudatosság szintjét és az átláthatóságot is javíthatná.

Adatvédelmi tisztviselővé kinevezése/megbízása óta a szervezeténél ...	Igen	Nem
véleményezett belső szabályozást, adatkezelést érintő tervezetet?	446	42
kikérte a szervezet vezetője/vezetése a szakmai álláspontját adatkezelést érintő kérdésben?	438	50
készített belső ellenőrzési (audit) tervet?	204	284
folytatott dokumentált módon belső ellenőrzést (auditot)?	192	296

A válaszok alapján az is látható, hogy a tudatosító képzések szervezése kapcsán sok helyen lehetnek hiányosságok, míg az érintett joggyakorláshoz kapcsolódó feladatok, illetve adatvédelmi hatásvizsgálatra vonatkozó igények még sok helyen nem merültek fel.

Adatvédelmi tisztviselővé kinevezése/ megbízása óta a szervezetnél ...	Igen	Nem
tartott adatvédelmi tudatosító képzést?	362	126
tartott adatbiztonsági tudatosító képzést?	279	209
közreműködött érintett joggyakorlással kapcsolatos választervezet elkészítésében?	277	211
folytatott adatvédelmi hatásvizsgálatot?	220	268

Összesen 173 olyan szakmai, jogértelmezési kérdés érkezett a Hatósághoz, amely a tisztviselők megítélése szerint közérdeklődésre tarthat számot. A kérdések nagyrészt a GDPR új jogintézményeit, a változó jogalapokat és az érintett joggyakorlás teljesítésének módját érintették, de érkezett kérdés a Hatóság eljárásai kapcsán, az Infotv. hatályára vonatkozóan és a 2018. május 25-én megszűnt adatvédelmi hatósági nyilvántartásba történő bejelentkezésről is.

I.2.2. Az adatvédelmi tisztviselők konferenciájának elektronikus oktatóanyagai

A Hatóság a kérdőíves felmérés eredményei, az adatvédelmi tisztviselők átlagos felkészültsége alapján meghatározta a konferencia tematikáját és összeállította a beérkezett kérdésekkel kapcsolatos iránymutatásokat is magába foglaló oktatónövényeket és írásbeli válaszokat.

2019. december 23-án a Hatóság honlapján létrehozott önálló felületen⁴ 10 oktatónövény került közzétételre, amelyekben a Hatóság elnöke, elnökhelyettese és munkatársai összesen több mint két óra időtartamban ismertetik a GDPR alkalmazásának első tapasztalatait. Mivel a kiküldött felmérés eredményei alapján először a gyakorlati példák bemutatását tartották hasznosnak az adatvédelmi

⁴ <https://naih.hu/dpo-konferencia-2019.html>

tisztviselők, így kiemelt hangsúlyt fektettek erre a konferencia előadói is a legfontosabb változások szemléltetésekor.

A köszöntőt követően a Hatóság elnöke elsőként a Hatóság eljárásai során történő bírságkiszabás szempontjait mutatta be két közelmúltbeli határozat kapcsán, összevetve azokat a 29. cikk szerinti adatvédelmi munkacsoportnak a 2016/679 rendelet szerinti közigazgatási bírság alkalmazásáról és megállapításáról (WP253) szóló iránymutatásával. Ezt követően a tisztviselők által egyik legtöbbet javasolt témát, a jogos érdeken alapuló adatkezelés és az érdekmérleges szempontjait, követelményeit ismertette.

A Hatóság elnökhelyettese az adatvédelmi incidens fogalmát, általános bemutatását követően az adatvédelmi incidensek kezeléséhez kapcsolódó feladatokat ismertette számos gyakorlati példa említésén keresztül és értelmezési kérdés megválaszolásával a 29. cikk szerinti adatvédelmi munkacsoport kapcsolódó irányutatása alapján. Ezt követően a harmadik előadásában a tisztviselők által az adatvédelmi hatásvizsgálat és a harmadik országba történő adattovábbítás kapcsán feltett kérdésekre tért ki.

A konferencia kapcsán készült előzetes felmérés eredményeit és az adatvédelmi tisztviselő kijelöléséhez kapcsolódó feladatokat, valamint a Hatóság honlapjáról elérhető adatvédelmi tisztviselő bejelentő rendszerrel kapcsolatos kérdésekre adott válaszokat a konferencia lebonyolításáért felelős Tanúsítási és Társadalmi Kapcsolatok Főosztályának vezetője mutatta be.

Az Adatvédelmi Főosztály adatvédelmi szakértője a Hatóság eljárásait mutatta be, valamint az érintett joggyakorlásra irányuló kérelmek azonosítását, elbírálsát és teljesítésének egyéb körülményeit vizsgálta, figyelemmel számos, 2019-ben zárt adatvédelmi hatósági eljárás tapasztalataira. Emellett a Hatósághoz a GDPR szerinti jogalapokkal kapcsolatban érkezett kérdéseket válaszolta meg, hivatkozva az Európai Unió Bíróságának joggyakorlatára és az Európai Adatvédelmi Testület által kiadott irányutatásokra is.

Végül az Európai Unió által finanszírozott STARII Projekt keretében a Hatóság által működtetett KKV Hotline útján a kis- és középvállalkozásoktól a Hatósághoz beérkező kérdések közül válaszolt meg néhány gyakran felmerülő kérdést a Hatóság projektasszisztens munkatársa.

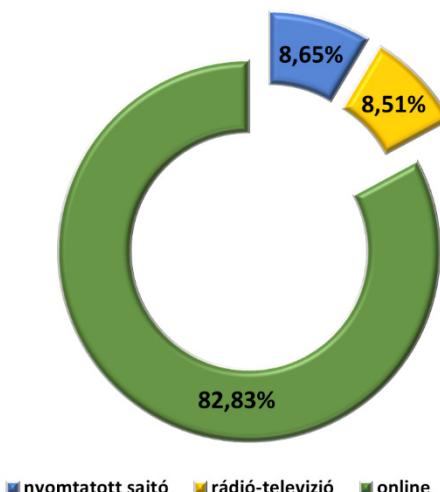
A videók egy évig maradnak a Hatóság honlapján lejátszhatók az MTVA Mediaklikk streaming szolgáltatásának köszönhetően, de az előadások várhatóan ezt követően is letölthetők maradnak a Hatóság honlapjáról.

A videók mellett az előadások során nem érintett, az adatvédelmi tisztviselők által beküldött további 25 adatvédelmi tárgyú és 7 információszabadság téma körben érkezett kérdésre a Hatóság írásbeli válaszokat tett közzé.

I.3. A Nemzeti Adatvédelmi és Információszabadság Hatóság megjelenése a médiában

A következőkben a Hatóság 2019. évi média megjelenéseit összegezzük. 2019. január 1. és december 31. között összesen 2808 hírt közöltek a médiaszereplők a Nemzeti Adatvédelmi és Információszabadság Hatóságról. A médiatípusok közül legtöbbször továbbra is az online médiában találkozhattunk a Hatóság tevékenységéről szóló híradásokkal, szám szerint 2326 alkalommal (82,83%). A nyomtatott sajtóban 243 esetben (8,65%), az elektronikus médiában pedig 239-szor (8,51%) szerepelt a NAIH.

A NAIH megjelenéseinek aránya a különböző médiumokban 2019-ben



Forrás: Observer Budapest Médiafigyelő Kft.

II. Az általános adatvédelmi rendelet alkalmazása

II.1. Adatvédelmi ügyek

A Hatóság ebben az évben is számos adatvédelmi kérdést, konzultációs beadványt választott meg, adatvédelmi vizsgálati eljárásokat és adatvédelmi hatósági eljárásokat folytatott le.

A hatósági eljárásokban hozott határozatok közül jelentősnek tekinthető azon határozatok száma, amelyek bíróság előtt is megmérettetnek. A Hatóság e tekinthetben sikeres évet zárt. 2019-ben öt esetben született jogerős bírósági döntés a Hatóság határozatának bírósági felülvizsgálata tárgyában. Az eljáró bíróságok az ügy érdemében minden esetben a Hatóság álláspontját osztották. Az öt befejeződött perből négy esetben a Hatóság pernyertes lett és a bíróság a Hatóság érvelését elfogadva a határozatot hatályában fenntartotta (NAIH/2019/167, NAIH/2019/214, NAIH/2019/2566, NAIH/2018/6248), míg egy ügyben (NAIH/2019/2074) a bírságkiszabás tekintetében új eljárásra utasította a Hatóságot.

II.1.1. Munkahelyi adatkezelések

1. A jogi szabályozás változásai

A jogszabályok általános adatvédelmi rendelet miatti felülvizsgálta keretén belül a 2019-es évre maradt számos (ágazati) adatvédelmi előírást tartalmazó jogszabály általános adatvédelmi rendelethez való „igazítása”. Ennek a folyamatnak a részét képezte a munka törvénykönyvről szóló 2012. évi I. törvény (a továbbiakban: Mt.) személyes adatok kezelését érintő rendelkezéseinek módosítása is.

A 2019. április 26. napjától hatályos főbb változások szerint a munkáltató által a munkavállalótól követelt nyilatkozatok, illetve adatok igazolása alapvetően okiratok bennutasával valósulhat meg, főszabályként megtiltva ezzel azt, hogy az okiratokról másolatokat készítsen a munkáltató.

További változásokat szabályozza az Mt. azt, hogy milyen esetekben kezelhető a munkavállaló biometrikus adata, illetve bűnfügyi személyes adata. Az Mt. lényegében olyan érdekeket, eseteket határoz meg, melyek bekövetkezése esetén jogoszerűen kezelhetők ezen adatok, ha teljesül a szükségesség-arányosság követelménye és az adatkezelő is megfelelő jogalapra – döntően a jogos érdek-

re – hivatkozva folytatja adatkezelését. Ilyen eset lehet például, ha a munkavállalók vagy mások élete, testi épsége vagy egészsége súlyos vagy tömeges, visszafordíthatatlan sérelmének a veszélye áll fenn, ha a munkáltató mérgező vagy veszélyes vegyi vagy biológiai anyagokat tárol, vagy a munkáltató a Büntető Törvénykönyvről szóló 2012. évi C. törvény szerint legalább különösen nagy vagyoni értékű vagyontárgyat őriz. Az Mt. 11. § (1) bekezdés b) pontjában megjelölt törvényben védett jelentős érdekek a „különösen” szóból következően ugyanakkor csupán példaként értelmezendők, ezeken kívül a Hatóság adott esetben más törvényben védett érdekeket is elfogadhat, amennyiben az érdekmérlegelés során az adatkezelés szükségessége és arányossága igazolt.

A munkavállaló ellenőrzése körében lényeges változás, hogy a törvény módosítását követően a munkavállaló a munkáltató által a munkavégzéshez biztosított számítástechnikai eszközöt eltérő megállapodás hiányában kizárálag a munkaviszony teljesítése érdekében használhatja. Főszabályként tehát a munkavállaló magáncélra nem használhatja a munkavégzéshez biztosított számítástechnikai eszközt. Ennek a szabálynak a megsértése munkajogi jogkövetkezményekhez vezethet, azonban ennek ellenőrzése – még ha bizonyított is, hogy a munkavállaló magáncélra használta a számítástechnikai eszközt, – csupán a magánhasználat tényének megállapítására terjedhet ki, munkáltató a magáncélú adatokat, információkat nem ismerheti meg, csak a munkavégzéssel összefüggőeket. Ez következik abból a változatlan szabályból, hogy a munkavállaló a munkaviszonyal összefüggő magatartása körében ellenőrizhető. Mindez vonatkozik arra az esetre is, amikor a felek megállapodása alapján a munkavállaló a munkaviszony teljesítése érdekében a saját számítástechnikai eszközét használja.

Mindezen túl kiemelendő, hogy a munkavállaló személyiségi joga – így személyes adatok védelméhez fűződő joga is – akkor korlátozható, ha a korlátozás – így az adatkezelés – a munkaviszony rendeltetésével közvetlenül összefüggő okból feltétlenül szükséges és a cél elérésével arányos. A személyiségi jog korlátozásának módjáról, feltételeiről és várható tartamáról, továbbá szükségességét és arányosságát alátámasztó körülményekről a munkavállalót előzetesen írásban tájékoztatni kell. Ebből, továbbá az általános adatvédelmi rendelet szabályaiból következően a munkáltatónak megfelelő és átlátható módon tájékoztatnia kell a munkavállalót az adatkezelésről, illetve annak összes körülményéről.

2. E-mail fiók ellenőrzésével kapcsolatos ügyek

A Hatósághoz minden évben nagy számban érkeznek munkáltatói adatkezelést érintő panaszok. Ezek közül a 2019. évben két e-mail-fiók ellenőrzésével és egy elektronikus megfigyeléssel összefüggő ügy emelendő ki, amelyeket a Hatóság adatvédelmi hatósági eljárásban vizsgált.

Az egyik ügyben a kérelmező azt kifogásolta, hogy betegség miatti keresőképtelenségének időtartama alatt – távollétében – az íróasztal és számítástechnikai hozzáféréseit, eszközeit, valamint e-mail-fiókját ellenőrizték, az íróasztalán lévő dokumentumok fizikai elhelyezkedését megváltoztatták, továbbá minden ellenőrzésről fényképeket is készítettek, mely – álláspontja szerint – jogosultan adatkezelést és hozzáférést eredményezett. Lényeges, hogy elsődlegesen nem ellenőrzési célból, hanem – eredendően a kérelmező kifejezett kérelmére – a kieső munkatárs feladatai ellátása folyamatosságának biztosítása miatt került sor az e-mail-fiókhöz és a számítástechnikai eszközökhöz való hozzáférésre, és csak a kérelmező helyettesítése során észlelt hiányosságok miatt történt meg azok teljes ellenőrzése (NAIH/2019/769.).

A másik ügyben a kérelmező előadta, hogy egy kórházzal fennálló jogviszonya megszűnését követően tudomására jutott, hogy – engedélye nélkül – a kórházi elektronikus levelezése tudomása szerint törölt, valójában inaktivált fiókjai viszszsaállítását rendelte el a vezetés, mert kerestek egy dokumentumot. A kérelmező kifogásolta, hogy ennek során az inaktivált fiókokban bármelyik dokumentumához hozzáférhettek, bármely személyes adatát megismerhették, tekintettel arra, hogy magánlevelezéseit is azokon bonyolította le, ami engedélyezett volt számára (NAIH/2019/51.).

A NAIH/2019/769. számú ügyben a Hatóság alapvetően az e-mail-fiók ellenőrzését vizsgálta, és a jogos érdek jogalapja kapcsán tett a joggyakorlat alakítása szempontjából fontos megállapításokat.

A Hatóság a határozatában azt állapította meg, hogy a munkavállaló munkavégzése ellenőrzésének céljából végzett adatkezelés esetében az adatkezelés jogalapja a jogos érdek lehet.

A tényállás szerint a munkáltató az adatkezelést munkáltatói ellenőrzés kérében hajtotta végre, és az ezen ellenőrzéshez, valamint az ehhez szükséges személyes adatok megismeréséhez fűződő jogos érdekének fennállta megállapítható volt a jogi szabályozásból, az eljárás során tett nyilatkozataiból és

az azokat alátámasztó okirati bizonyítási eszközökből – az adatkezelőt súlyos pénzügyi és egyéb jogkövetkezmények fenyegették, amelyek elhárítása, illetve hatásainak mérséklése az adatkezelő haladéktalan lépéseinek megtételét tették szükségessé. A vizsgált esetben az e-mail fiókhoz és a számítástechnikai eszközökhöz való hozzáférésre elsődlegesen nem ellenőrzési célból, hanem a ki- és csökkenés munkatárs feladatai ellátása folyamatosságának biztosítása miatt került sor, és csak a kérelmező helyettesítése során észlelt hiányosságok miatt történt meg azok átvizsgálása a pénzügyi és egyéb jogkövetkezmények elhárítása érdekében, *ad hoc* módon.

Ezzel kapcsolatban ugyanakkor a Hatóság hangsúlyozza, hogy abból, hogy ebben az ügyben a jogos érdek jogalajának fennállását – az ügy valamennyi körülménye alapján – egy, az adatkezelő által előzetesen írásban lefektetett részletes érdekmérlegelési teszt hiányában is megállapíthatónak tartotta, nem következik, hogy az adatkezelőknek – az adatkezelő objektív felelősségeit és fokozott gondossági követelményét megfogalmazó elszámoltathatóság alapelvi követelményéből is fakadóan – ne lenne kötelezettsége az ilyen jogalapon folytatott adatkezelések esetében a jogalap megállapíthatóságához szükséges feltételek meglétét előzetesen és az adatkezelés során folyamatosan is ellenőrizni.

Ezen túlmenően a Hatóság mindenkor határozatában megállapította, hogy az e-mail fiók ellenőrzésekor a tiszteingeses adatkezelés elvéből következően főszabályként biztosítani kell a munkavállaló jelenlétét. A munkavállaló előzetes tájékoztatása és személyes – ha ez nem biztosítható, meghatalmazottja, képviselője – jelenléte az e-mail-fiók ellenőrzése, áttekintése, illetve az abban történő dokumentumkeresés során azért is szükséges, mert a munkavállaló és harmadik személyek különböző személyes adatai lehetnek a levelezőrendszerben, amelyek kezelésére a munkáltató – a személyes adat e jellege ellenőrzésén túl – nem jogosult. Ha az e-mail fiók áttekintése, ellenőrzése, adott esetben egy dokumentum keresése során a munkavállaló – képviselője, meghatalmazottja – jelen van, és jelezheti valamely személyes adatot tartalmazó e-mail tartalmának megtekintése előtt, hogy az magáncélú leveleket tartalmaz, akkor ezzel biztosító, hogy a munkáltató ne sértse meg ezt a tilalmat.

Az e-mail fiók áttekintésének körülményeitől függően ugyanakkor elköpzelhetők olyan helyzetek, amikor a munkavállaló személyes jelenléte objektív okokból nem biztosítható. A Hatóság – a főszabálytól eltérően – egyes helyzetekben ezért elfogadhatónak tartja azt is, ha a munkavállaló nincs jelen, például azonali intézkedést igénylő esetekben, táppénzen lévő vagy olyan volt munkavállaló esetén, akinek a munkaviszonya a munkáltatóval már nem áll fenn. Ebben az

esetben is azonban egyrészt tájékoztatást kell nyújtani a munkavállaló számára a tervezett munkáltatói intézkedésről, másrészt lehetőséget kell biztosítani számára arra is, hogy ha ő nem is, helyette meghatalmazottja vagy képviselője jelen legyen. Amennyiben ezen megelőző intézkedések – előzetes tájékoztatás és a munkavállaló vagy meghatalmazottja, képviselője jelenlétének biztosítása – ellenére a munkavállaló nem érhető el vagy nem jelenik meg sem személyesen, sem képviselője útján, akkor távollétében, független harmadik személy alkalmazásával is hozzá lehet férfi az e-mail fiókjához az azonnali intézkedések végrehajtása érdekében. Ilyen esetben is meg kell ugyanakkor minden tenni annak érdekében, hogy az e-mail fiók áttekintésének körülmenyei olyan módon legyenek rögzítve, hogy annak pontos menete, az annak során megismert adatok köre, azaz a ténylegesen elvégzett adatkezelési műveletek és azok jogoszerűsége utólag ellenőrizhető legyen. Mindez az elszámoltathatóság elvéből is következik.

Tekintettel azonban arra, hogy a két ügyben az adatkezelők semmilyen intézkést nem tettek meg annak érdekében, hogy a kérelmezők előzetesen tudomást szerezzenek az e-mail-fiókok ellenőrzéséről, a dokumentumkeresésről, illetve, hogy jelenlétéük biztosítva legyen, a Hatóság megállapította, hogy az adatkezelők megsértették a tiszteleges adatkezelés elvét.

A Hatóság figyelembe vette továbbá minden ügyben, hogy egyik adatkezelő sem rendelkezett belső szabályzattal az e-mail-fiókok használatára, ellenőrzésére vonatkozóan. Ezzel a kérdéssel szorosan összefügg a vonatkozó megfelelő szabályozás és az adatvédelmi követelményeknek való megfelelés biztosítása, mivel ekként biztosítható az általános adatvédelmi rendelet szerinti megfelelő technikai, szervezési intézkedéseknek való megfelelés. Az adatkezelés belső dokumentumban történő szabályozása, az adatkezelési műveletek rögzítése azért szükséges, mert az adatkezelések tervezésétől azok folytatásán át a célok megvalósulásáig tett valamennyi lényegi lépés adminisztrálását, dokumentálását is magában foglalja és egyben az adatvédelmi követelményeknek való megfelelés igazolására való képességet feltételezi. Ezen elv a gyakorlatban – többek között – az adatkezelők számára az általános adatvédelmi rendeletben előírtaknak megfelelő szabályzatok, eljárásrendek szakszerű rögzítését irányozza elő. A megfelelő technikai, szervezési intézkedések magukban foglalják a beépített és alapértelmezett adatvédelem teljesülését is, vagyis azt, hogy az elvek és az adatvédelmi követelmények érvényesülését garanciák beépítésével segíti elő az adatkezelő.

Noha a Hatóság álláspontja szerint a nem rendszeres, hanem azonnali ellenőrzések nél, dokumentumkeresések nél nem várható el, hogy a konkrét egyedi esetre is előzetes részletes belső szabályozás készüljön, azonban az minden-képpen elvárható, hogy az ilyen eseti ellenőrzések lehetőségével számolva előzetesen dokumentálják, szabályozzák az ilyen ellenőrzések lefolytatásának módját, azt, hogy az adott ellenőrzés során kinek, milyen hozzáférése lehet az érintett munkavállaló számítástechnikai eszközeihez, e-mail fiókjaihoz annak érdekében, hogy a munkavállalók világos, egyértelmű, a jelenlétéük biztosításának lehetőségére is kiterjedő információkkal rendelkezzenek.

3. Célhoz kötött adatkezelés elve a munkahelyi adatkezelésnél

Két érintett kérelemmel fordult a Hatósághoz, amelyben a munkáltatójuk adatkezelését kifogásolták. A beadvány szerint vezetői értekezleten a munkáltató olyan listát osztott szét, amely 51 alkalmazottnak egyesületi tagságra vonatkozó adatát tartalmazta. A listát munkavállalók bérnyilvántartási adatain végzett szűrés útján állították elő. A Hatóság adatvédelmi hatósági eljárás során megállapította, hogy a munkáltató a szakszervezeti egyesületi tagdíjnak a munkavállaló illetményéből történő levonása érdekében jogoszerűen kezeli az érintettek egyesületi-tagságra vonatkozó adatát. Ugyanakkor ez a felhatalmazás nem jelenti azt, hogy a díjlevonás érdekében kezelt adatok más célra is felhasználhatók lennének. A célhoz kötött adatkezelés elvének figyelembevételével a munkáltató adatkezelőként köteles arra, hogy az általa a munkavállalókról megismert adatokat a vonatkozó adatvédelmi szabályokkal összhangban kezelje, és mindenekelőtt biztosítsa, hogy egy-egy adatot a munkaszervezetén belül is csak az ismerhessen meg, aki arra jogosultként az adott adatkezelési cél megvalósításában szükségszerűen részt vesz. A Hatóság álláspontja szerint ennek megfelelően egyszerűt az érdekképviseleti tagságra vonatkozó adatokat kizárolag a munkáltató szervezetén belül bérszámfejtéssel foglalkozók ismerhetik meg, a munkáltatónak továbbá megfelelő szervezési és technikai intézkedésekkel kell gondoskodnia arról, hogy ezen adatokhoz mások – akár a vezető – megfelelő jogoszerű cél hiányában ne férhessenek hozzá. Másrészt az adatok a hozzájárulástól eltérő célra nem használhatóak. A személyes adatoknak a gyűjtésük eredeti céljától eltérő egyéb célból történő kezelése csak akkor megengedett, ha az adatkezelés összeegyeztethető az adatkezelés eredeti céljaival. Ezen cél tekintetében a munkáltatónak alkalmaznia kellett volna a GDPR 6. cikk (4) bekezdésében foglaltakat, és meg kellett volna állapítania, hogy az adatkezelés eredeti és ettől eltérő céljai összeegyeztethetők-e. A Hatóság álláspontja szerint a fent kifejtett eredeti céllal nem volt összeegyeztethető, hogy a munkáltatói jogköryakorlója a bérszámfejtéshez használt adatbázisból más célú felhasználás ér-

dekében érdekképviseleti tagságra vonatkozó lekérdezésre vonatkozó utasítást adott, és a lekérdezett adatakat listába szedve kezelte. Szintén megállapítást nyert a lekérdezett adatai továbbításának, a vezetők részére történő közlésének jogellenessége, miáltal a kérelmezők érdekképviseleti tagságra vonatkozó adatát az értekezlet résztvevői – közöttük a kérelmező felettese – jogoszerű felhatalmazás hiányában ismerték meg. A Hatóság 3.000.000 forint adatvédelmi bírságot szabott ki, amelyet a kötelezettségfizetett és a határozattal szemben bírósági felülvizsgálatot nem kezdeményezett. (NAIH/2472/2019)

II.1.2. Egyes fontos, érdekes ügyek

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

- munkahelyi adatkezelés
- „kamerás” ügyek
- egészségügyi adatkezelés
- követelés engedményezésével kapcsolatos adatkezelés
- követeléskezelők adatkezelése
- banki adatkezelés
- biztosítók adatkezelése
- hozzáféréshez való jog
- érintett jogok teljesítésének megtagadása, illetve elmulasztása

1. Munkahelyen rejtett kamerás felvételek készítése ellenőrzési céllal

A Hatósághoz bejelentések érkeztek, melyek szerint a bejelentők azt kifogásolták, hogy a közlekedési szolgáltatást nyújtó részvénnytársaság (a továbbiakban: BKV Zrt.) munkavállalóról a szolgáltatásvégzést ellenőrző részvénnytársaság (a továbbiakban: BKK Zrt.) megbízottai kézi kamera alkalmazásával több alkalommal rejtett kamerás felvételeket készítettek ellenőrzési céllal, több villamosnak a vonalán. A felvételeken a jármű vezetője teljes mértékben felismerhető, pontosan beazonosítható volt. A bejelentések szerint a felvételek a járművezetők tudomása nélkül kerültek rögzítésre, ahhoz hozzájárulásukat nem adták, illetve az ellenőrzésről tájékoztatást semmilyen módon nem kaptak. A bejelentések szerint az ezen ellenőrzés során feltárt esetleges jogszármazékok alapján a BKK Zrt. kötbérigényt érvényesít a BKV Zrt.-vel szemben. Amennyiben az ellenőrzés szabálytalanságot nem tár fel, a BKV Zrt. munkavállalója az ellenőrzésről sem-

milyen formában nem értesül. Amennyiben a BKK Zrt. jogisértést állapít meg, a BKV Zrt. ez alapján a munkavállalóval szemben prémiummegvonást alkalmaz.

Az ügyben vizsgálati eljárás indult. Noha a vizsgált időszak vonatkozásában az Infotv. rendelkezései voltak az irányadóak, azonban tekintettel arra, hogy az adatkezelés az általános adatvédelmi rendelet alkalmazásának kezdőnapjától, 2018. május 25. napjától is folyamatos volt, a Hatóság vizsgálta az adatkezelés mind az Infotv.-nek, mind az általános adatvédelmi rendeletnek való megfelelőségét.

A tényállás tisztázása során mindenki cég az adatkezelés jogalapjaként a Budapest közlekedésszervezési feladatainak ellátásáról szóló 20/2012. (III. 14. Főv. Kgy. rendelet (a továbbiakban: Kijelölő rendelet) 14. §-ának (6) bekezdésére hivatkozott, mely alapján a közlekedésszervező köteles az általa megrendelt szolgáltatások mennyiségét és minőségi színvonalát rendszeresen ellenőrizni. Szintén e jogszabályhely alapján a közlekedésszervező ennek keretében jogosult a szolgáltatók tevékenységét nyílt és rejtett úton, illetve próbaHASZNÁLAT útján is ellenőrizni. A közlekedésszervező a szolgáltató alkalmazottjának szabályszerű magatartása esetén jogosult a szolgáltatónál a közsziolgáltatási szerződésben meghatározott munkáltatói intézkedést kezdeményezni.

A Hatóság arra az álláspontra jutott a vizsgálat során, hogy amennyiben a BKV Zrt. által nyújtott szolgáltatások ezen ellenőrzését egy ellenőr végzi és szükséges a kézi kamerák alkalmazása, adott esetben el tudja fogadni azok alkalmazását megfelelő adatkezelési jogalap, továbbá garanciák és megfelelő tájékoztatás biztosításával.

A Hatóság álláspontja szerint ez a jogalap a BKK Zrt. esetében az általános adatvédelmi rendelet 6. cikk (1) bekezdés e) pontja lehet, mely szerint a személyes adatok kezelése közérdekű vagy az adatkezelőre ruházott közhatalmi jogosítvány gyakorlásának keretében végzett feladat végrehajtásához szükséges.

A közérdekű feladat ellátásához szükséges adatkezelés mint adatkezelési jogalap kapcsán azonban elmondható, hogy a hazai jogi környezet – így első sorban az Alaptörvény I. cikk (3) bekezdése – és az Alkotmánybíróság gyakorlata szerint az érintett alapvető jogait – így információs önrendelkezési jogát is – a jogalkotó csak a szükséges és arányos mértékben, valamely alapvető jog érvényesülése vagy valamely alkotmányos érték védelme érdekében, azaz közérdekből korlátozhatja. Ezért e jogalap alkalmazásához feltétel, hogy az adatkezelő a közérdekből elvégzendő feladata végrehajtásához szükséges adatkezelési tevé-

kenységét közérdeken alapuló célból jogszabály vagy uniós norma alapozza meg. Ezen jogszabályi rendelkezés ugyanakkor sok esetben csak az adatkezelő közzeladatát, eljárási mozgásterét és kötelezettségét határozza meg, az ehhez kapcsolódó adatkezelési műveletek részletes szabályait nem. Ha a jogalkotó ezen adatkezelésekre vonatkozó részletes szabályokat az Infotv. jelenleg hatályos 5. § (3) bekezdésének előírásait figyelmen kívül hagyva nem rögzítette, az adatkezelő az általános adatvédelmi szabályok – így különösen az alapelvet és a jogalap szükségességi mércéje – szerint köteles adatkezelési tevékenységét végezni, és annak jogoszerűségét az elszámoltathatóság elvének megfelelően igazolni.

A Hatóság a vizsgálati eljárásában megállapította, hogy mindezzel ellentétben az eljárás idején is és jelenleg is hatályos és releváns törvény, a személyszállítási szolgáltatásokról szóló 2012. évi XLI. törvény 35. § (1)-(2) bekezdése csupán azt tartalmazza, hogy az ellátásért felelős, azaz a Fővárosi Önkormányzat bármikor ellenőrizheti vagy megbízottja útján ellenőriztetheti a közlekedési szolgáltatót, azaz a BKV Zrt. közszolgáltatási szerződésben rögzített kötelezettségének teljesítését. Ugyanígy fogalmazott, illetve fogalmaz a Kijelölő rendelet, amelynek 14. § (6) bekezdése alapján a közlekedésszervező, azaz a BKK Zrt. köteles az általa megrendelt szolgáltatások mennyiségét és minőségi színvonalát rendszeresen ellenőrizni. A BKK Zrt. jogosult a szolgáltatók, így a BKV Zrt. tevékenységet nyílt és rejttet úton, illetve próbahasználat útján is ellenőrizni.

A Hatóság álláspontja szerint azonban e jogszabályi rendelkezések – mivel nem felelnek meg az Infotv. 5. § (3) bekezdésének – egyike sem ad – a hatályos magyar alkotmányossági és törvényi követelményeknek is megfelelő – jogalapot arra, hogy a BKK Zrt. akként ellenőrizze a BKV Zrt. által nyújtott szolgáltatásokat, hogy a BKV Zrt. munkavállalónak munkavégzését rejttet technikai eszközökkel rögzítve figyelje meg. A Hatóság a vizsgálati eljárásában többek között ezen indokok miatt ezt az ellenőrzést jogellenesnek minősítette.

A Hatóság álláspontja szerint, bár az adatkezelés célja jogoszerű és adott esetben az adatkezelés szükséges és arányos is lehet, szükséges, hogy a jogalkotó a jogszabályi környezet módosításával alkossa meg az adatkezelési szabályokat az Infotv. 5. § (3) bekezdésének megfelelően, annak érdekében, hogy az általános adatvédelmi rendelet 6. cikk (1) bekezdés e) pontja szerinti jogalap alkalma-zási feltételei maradéktalanul biztosítva legyenek.

A fentiekből következően a Hatóság ajánlással fordult a hatáskörrel rendelkező miniszteriumhoz és kezdeményezte a szabályozási tárgykörbe tarto-

zó jogszabály(ok) a jelzett jogalkotói kötelezettség teljesítéséhez szükséges és elégséges mértékben történő módosítását, kiegészítését. (NAIH/2018/127, NAIH/2019/4556)

2. Jogellenes kamerás megfigyelések

A Hatóság a 2019. év során számos – hatósági, illetve vizsgálati eljárást folytatott le jogellenes kamerás megfigyeléssel összefüggésben.

Ezek közül az egyik esetben a tényállás tisztázása során fény derült arra, hogy a bepanaszolt magánszemély nem önállóan, hanem egy magánnyomozással foglalkozó cég megbízásával figyelte meg a szomszédjában zajló tevékenységeket és az ott tartózkodó személyeket is. Az eljárás során feltárt tényállás és becsatolt bizonyítékok alapján kiderült, hogy a kamerát kifejezetten a szomszéd megfigyelése céljából szerelték fel, és az elkészült felvételeket a magánnyomozó társaság kezelte. Tekintettel arra, hogy a megfigyelés célját a megbízó határozta meg, míg annak eszközeiről, módjáról és a felvételek kezeléséről a társaság döntött – amely feladatát megbízási szerződés alapján végezte – megállapítható volt közös adatkezelői minőségük. Ugyan a bepanaszolt felek hivatkoztak arra, hogy tevékenységükön tájékoztatták a megfigyelt személyeket, azonban ez nem biztosít megfelelő jogalapot a megfigyelésre és nem teszi jogosítottá azt. A társaság megbízási szerződésében hivatkozott arra, hogy munkáját „az adatvédelmi törvényben leírtak szerint” végzi, azonban az ilyen jellegű megfigyelés folytatására semmiféle jogszabály sem ad felhatalmazást a magánnyomozóknak. A személy- és vagyonvédelmi, valamint a magánnyomozói tevékenység szabályairól szóló törvény ugyanis kimondja, hogy a magánnyomozó tevékenysége végzése során nem rendelkezik hatósági jogkörrel és azt is, hogy a magánnyomozó kép- és hangfelvételt csak a személyes adatok védelmére és a személyiségi jogokra vonatkozó szabályok megtartásával kezesséhet, illetve használhat fel. A Hatóság ezért megtiltotta a további megfigyelés folytatását, elrendelte annak megszüntetését és a jogellenesen készített felvételek megsemmisítését, valamint a társaságot 800.000,- Ft adatvédelmi bírság megfizetésére kötelezte. (NAIH/2019/3633)

3. Társasházban szomszéd által üzemeltetett kamera

Egy közös tulajdonú ingatlan területén, ahol több lakóház is van, az egyik lakó bejelentette, hogy a szomszédja kamerát szereltetett fel, amelynek a beállítási

szöge kifogásolható. A Hatóság az üggyel kapcsolatban vizsgálati eljárást indított. A szomszéd a megkeresésre nem válaszolt egyértelműen, illetve nem a kérdésre válaszolt, ezért a Hatóság hivatalból hatósági eljárást indított. A szomszéd a megindult hatósági eljárásra megküldte válaszait, egyúttal ő is bejelentést tett három további szomszédja ellen, tehát az ügyhöz kapcsolódóan még három hatósági eljárás indult. Az egyik eljárás tekintetében a Hatóság megállapította, hogy a szomszéd által üzemeltetett kamera látószöge közterületre, községi területre és magánterületre is irányul, ezért jogellenes adatkezelés történt, a többi szomszédra vonatkozó vizsgálat során a Hatóság nem talált jogosítést. (NAIH/2018/4761)

4. Az önkormányzat székhelyén üzemeltetett biztonsági kamerák adatkezelése

A kérelmező egy települési önkormányzat székhelyén üzemeltetett biztonsági kamerák adatkezelését kifogásolta. Ebben sérelmezte az épületben dolgozók megfigyelésének tényét, az erről történő előzetes tájékoztatás hiányát, azt, hogy ismeretlen – többek között – az adatkezelésért felelős személye, a felvételek rögzítésének időintervalluma, az adattárolás ideje, az ellenőrző személyzet jogosultságának terjedelme, a felvételkészítés normatív rendje. Honlapján is közöltettségi határozatában a Hatóság megállapította, hogy a kötelezettség megsértette a kérelmező GDPR szerinti jogait a képmása megfelelő tájékoztatás nélküli, jogellenes kezelésével. A hatósági eljárást a Hatóság hivatalból kiterjesztette az önkormányzat biztonsági kamerákkal kapcsolatos általános adatkezelési gyakorlatára. Ennek keretében megállapította, hogy az adatkezelő által megjelölt, GDPR 6. cikk (1) bekezdés f) pontja szerinti jogos érdek jogalapot közhatalmi szerv az általa végzett adatkezelés során nem alkalmazhatja a GDPR ezt kizáró rendelkezése miatt. A megfelelő jogalap a GDPR 6. cikk (1) bekezdés e) pontja lehet önkormányzat működésével összefüggő adatkezeléssel kapcsolatban. Ehhez azonban az adatkezelés szükségesége és arányossága is szükséges feltétel, valamint megfelelő előzetes tájékoztatást is kell nyújtani az érintettek számára. Ennek során többek között figyelembe kell venni azt is, hogy az önkormányzat területén politikai tevékenység is zajlik, valamint nemzetiségi önkormányzat is egy épületben található vele, így a szokásosnál is jelentősebb indokok támaszthatják csak alá a kamerák használatát. A Hatóság 2019. októberi határozatában megtiltotta a GDPR-be ütköző kamerás adatkezelés folytatását és 5 000 000 Ft adatvédelmi bírságot szabott ki. (NAIH/2019/2076)

Mindezek alapján jól látható, hogy a kép- és hangfelvétel készítésével kapcsolatos ügylek száma továbbra is jelentős. Ahogyan azt az előzőekben jeleztük, az

Európai Adatvédelmi Testület elfogadta a kamerás adatkezelési műveletekről szóló 3/2019. számú iránymutatását, amely a jövőben e területen az egységes jogalkalmazás elősegítését célozza, egyszersmind az adatkezelők számára is megfelelő tájékozódási pontot jelent adatkezelési műveleteik megtervezése és azok végrehajtása során.

5. Személyes adatok rögzítése az Elektronikus Egészségügyi Szolgáltatási Térben

A Hatósághoz 2019. során több beadvány érkezett az Elektronikus Egészségügyi Szolgáltatási Térrel (EESZT) összefüggésben. A megkeresésekben megállapítható, hogy a rendszer működésével kapcsolatosan nagyon sok a bizonytalanság az érintettek részéről. Több konzultációs jellegű, illetve vizsgálati eljárást kezdeményező beadvány is az EESZT-be történő adatfeltöltés megtiltására, illetve a már rögzített adatok törlésére irányuló kérést tartalmazott. A Hatóság az ezekre adott válaszaiban felhívta a figyelmet arra, hogy a személyes adatok EESZTben történő rögzítése ún. kötelező adatkezelés, melyhez megfelelő jogalapot biztosít az általános adatvédelmi rendelet, tagállami jogszabályként az egészségügyi és a hozzájuk kapcsolódó személyes adatok kezeléséről és védelméről szóló 1997. évi XLVII. törvény, valamint az EESZT-vel kapcsolatos részletes szabályokat tartalmazó 39/2016. (XII.21.) EMMI rendelet. Mindezek alapján azokat a kérelmeket, ahol az érintettek a Hatósághoz fordultak a személyes – köztük egészségügyi – adataik EESZT-be történő rögzítésének megtiltása vagy törlése érdekében, a NAIH elutasította. (NAIH/2019/6839, NAIH/2019/1852)

6. DNS-elemző szolgáltatások igénybevételének adatvédelmi veszélyei

2019 elején több újságíró is foglalkozott a családfakutatáshoz és etnikai származás vizsgálatához szükséges, egyre inkább elszaporodó hirdetésekkel, amelyek online megrendelhető és egyszerűen elvégezhető DNS-teszteket kínáltak. A Hatóság közleményben⁵ hívta fel a figyelmet ennek adatvédelmi veszélyire, amelyek részben a saját genetikai adatok nem az Európai Unióban található laboratóriumokba történő továbbításával járhatnak, másrészről arra is, hogy az eredmények nem csak a szolgáltatást igénybe vevő személyre vonatkozóan hor-dozhatnak egyedi információkat.

5 <https://www.naih.hu/files/2019-03-23-genetikai-adatok.pdf>

7. Beérkező hívások rögzíthetősége és a hívószám azonosítása lelki elsősegély telefonos szolgáltatóknál

Lelki elsősegély telefonszolgáltató új telekommunikációs rendszer kiépítésének adatvédelmi kérdéseiben, a beérkező hívások rögzíthetőségéről és a hívószám azonosíthatóságáról kérte a Hatóság állásfoglalását. A Hatóság kifejtette, hogy a krízishelyzetben lévők által a hívás során elmondottak alapján a hívott fél egészségügyi adatok birtokába jut, ezért adatkezelésének az egészségügyi adat kezelésére megszabott szigorúbb feltételeknek kell megfelelnie. Az adatkezelésnek rendelkeznie kell egy GDPR 6. cikkben felsorolt megfelelő jogalappal és egyben a 9. cikk (2) bekezdésének valamely pontjában meghatározott feltételnek is teljesülnie kell. A 9. cikk (2) bekezdés a) pontja az érintett kifejezett hozzájárulása esetén teszi lehetővé az egészségügyi adat kezelését. Fő szabályként tehát – a hívás megkezdésekor – be kell szerezni az érintett hozzájárulását. Hozzájárulás hiányában a hívást nem lehet rögzíteni és a beszélgetést és segítségnyújtást a hangrögzítés nélkül kell folytatni. A Hatóság álláspontja szerint a GDPR 9. cikk (2) bekezdés c) pontja – amely lehetővé teszi a hívószám azonosítását és helymeghatározást – csak közvetlen életveszély, krízishelyzet elhárítása érdekében alkalmazható. Az ezen alapuló adatkezelés azonban csak addig lehetséges, amíg a hívó fél állapota indokolja, illetve még részére a segítségnyújtást megszervezik vagy biztosítják, összhangban a GDPR 5. cikkében megfogalmazott alapelvekkel. A Hatóság azonban arra nem lát megfelelő jogalapot, hogy minőségbiztosítási vagy oktatási célból az érintett hozzájárulásának hiányában a rögzítést vagy a számkövetést elvégezzék. Ezen adatkezelés az adatkezelő jogos érdekére alapítva lenne végezhető a 6. cikkben foglalt jogalapok közül, azonban a GDPR 9. cikke e tekintetben nem tartalmaz az egészségügyi adat kezelésének főszabály szerinti tilalma alóli kivételt meghatározó rendelkezést. A hívó felek egészségügyi adatainak védelme, az ahhoz fűződő érdekkük, hogy állapotukról a hozzájárulásuk nélkül azonosítható módon mások ne szerezzenek tudomást, felülírja a szolgáltató minőségbiztosítási és egyéb érdekeit. (NAIH/2019/5042)

8. Fényképfelvétel készítése egészségügyi intézményben

Állásfoglalás iránti kérelemben a beadványozó arról érdeklődött, jog szerű-e az – az utóbbi időben terjedő – gyakorlat, amely állami vagy önkormányzati fentartású egészségügyi intézmény vezetőjének előzetes engedélyéhez köti, hogy az intézmény területén bárki fényképfelvételt készítsen. Ugyanebben a tárgyban az alapvető jogok biztosa is kérte a Hatóság véleményének kifejtését. A

Hatóság az állásfoglalásában kiemelte, hogy az állami és önkormányzati fenn-tartású egészségügyi intézmények közfeladatot látnak el. Az ezekben az intézményekben fennálló állapotok, körülmények, tárgyi feltételek olyan kérdéseket érintenek, amelyek közérdeklődésre tarthatnak számot, az ilyen intézményekben készült, személyes adatokat nem tartalmazó felvételek az Infotv. alapján közérdekként adatnak minősülnek, vagyis az ilyen felvételek készítése és nyilvánosságra hozatala az információs szabadság érvényesülése szempontjából nem kifogásolható. Amennyiben a felvételen természetes személyek is szerepelnek, a kérdésben figyelembe kell venni a személyhez fűződő jogokat. Az információs önrendelkezési jognak mint alapjognak része az adatkezeléshez történő hozzájárulás megadása, a Ptk-nak és a GDPR-nak megfelelően a kórházban tartózkodó személyek (akár beteg, akár hozzátartozó, akár munkavállaló) fényképezése fő szabalyként a beleegyezésükön alapulhat. Figyelemmel kell lenni továbbá arra, hogy egészségügyi intézményben betegként tartózkodó személyek képmásának rögzítése különleges adat kezelését is megvalósíthatja, mivel a fénykép utalhat az érintett egészségi állapotára, illetve a kép készítésének helye is tartalmazhat erre utaló információt (pl. intenzív osztályon, szakrendelő berendezéséi alapján, de akár várótermi folyosón a rendelő látható megnevezésével készített kép esetén stb.) A Hatóság megítélése szerint az információs önrendelkezési jog mint alkotmányos alapjog nem korlátozható az intézmény vezetője által. Így amennyiben a képen szereplő érintett kifejezetten hozzájárul egy-egy felvételen történő szerepléshez, önrendelkezése nem függhet az intézményvezető utasításától. A kép készítőjének felelőssége annak biztosítása, hogy a felvételen ne szerepeljen egy olyan egyéb személy sem, aki a képmásának rögzítéséhez, az adatkezeléshez nem adta hozzájárulását. A Hatóság álláspontja szerint a képfelvétel-készítés általános és teljes tiltása aránytalanul korlátozza az érintettek Alaptörvényben biztosított alapvető jogait. Az intézmény vezetője akkor jár el a jogok biztosítása érdekében az Eütv. 2. §-ának is megfelelően, ha az intézmény betegeit és az intézményben megforduló egyéb személyeket felvilágosító anyagokkal tájékoztatja az intézményben jól láthatóan, több helyen elhelyezve, illetve bármilyen egyéb módon, amellyel felhívják a betegek és a hozzátartozók figyelmét a más személyekről való felvételkészítés szabályaira, az érintettet megillető jogokra és a kép készítőjének kötelezettségeire. (NAIH/2019/2741, NAIH/2019/3406)

9. Kórházi ellátással kapcsolatos dokumentumok másolatának kiadása

Egy kérelmezőt 2015-ben baleset ért, melynek következtében kórházi ellátásban részesült. 2016-ban a kórházi ellátással kapcsolatban panasz nyújtott be, amely

alapján vizsgálati eljárás indult az érintett kórházban, valamint a Panasztörvény alapján szintén eljárás indult az ÁNTSZ-nél. A kérelmező 2019-ben, több alkalommal a vizsgálati eljárással összefüggésben keletkezett iratok és az ÁNTSZ által lefolytatott vizsgálati anyag hitelesített másolatainak megküldését kérte. A kórház a kért iratok megküldéséért térítési díjat állapított meg, arra tekintettel, hogy a kérelmező a kért iratokat a kórházból való távozáskor már megkaptá. A kérelmező a térítési díjat kifizette. A kórház a kért dokumentum másolatait a kérelmező részére a kérelem benyújtásától számított 84 nap múlva küldte meg. A Hatóság megállapította, hogy a kórház megsértette a GDPR 13. cikk (3) bekezdését azzal, hogy a kérelem beérkezésétől számított egy hónapon belül a kérelemmel kapcsolatban nem adott tájékoztatást, továbbá a GDPR 15. cikk (3) bekezdését azzal, hogy az utólagos teljesítés során az első másolat ingyeneségét nem biztosította és térítési díjat állapított meg. A kérelmező GDPR alkalmazandóvá válását követően benyújtott másolat kiadása iránti kérelmét ugyanis első hozzáférési kérelemnek kell tekinteni, ezért költség nem számolható fel. A Hatóság a másolatok hitelesített formában történő megküldésére vonatkozó kérést elutasította, tekintettel arra, hogy az általános adatvédelmi rendelet 15. cikkének (3) bekezdéséből és az 5. cikk (1) bekezdésének d) pontjából, az adatpontosság elvéből nem vezethető le az a kötelezettség, hogy a másolat valós tartalmát hitelesítéssel kell igazolnia az adatkezelőnek. A Hatóság az általános adatvédelmi rendelet 58. cikk (2) bekezdés d) pontja alapján, hivatalból utasította a kórházat arra, hogy az általa hivatkozott belső térítési díj szabályzatát az általános adatvédelmi rendelettel hozza összhangba. (NAIH/2019/5112)

10. Elhunyt személy egészségügyi dokumentációjához való hozzáférés

Az elhunyt személy elhalálzásának körülményeire és a halál okára vonatkozó, valamint a rá vonatkozó egészségügyi dokumentációban foglalt személyes adat kezelésére az egészségügyi adat és az egészségügyi dokumentációban foglalt személyes adat kezelésére vonatkozó kötelező európai uniós jogi aktusban vagy jogszabályban foglalt szabályokat kell alkalmazni. A személyes adatok kezelésére vonatkozóan 2018. május 25-től a GDPR határozza meg a főbb szabályokat. Ugyanakkor a GDPR tárgyi hatálya a (27) preambulumbekezdés alapján nem terjed ki az elhunyt személyekkel kapcsolatos személyes adatakra, így ezen adatok kezelésére vonatkozó szabályokat a tagállamok állapíthatnak meg. Magyarországon a GDPR által nyújtott lehetőséggel élve az elhunyt személyek személyes adatainak kezelésével kapcsolatban az Infotv. 2018. július 26-án hatályba lépett rendelkezései tartalmazzák az érintett halálát követően a személyes adatokkal összefüggő jogok érvényesítésére vonatkozó rendelke-

zéseket. Ez azonban – az érintett életében tett nyilatkozat hiányában – csak az elhunyt érintett közeli hozzájárulású számára és kizárolag a jogellenes adatkezelés megszüntetésének vagy korrekciójának lehetőségét teremti meg. Más jogi előírásokból fakadóan azonban lehetséges további adatmegismerési jogosultságok érvényesítése, így az egészségügyi dokumentációra, egészségügyi adatok megismerésére továbbra is az egészségügyi és a hozzájuk kapcsolódó személyes adatok kezeléséről és védelemről szóló 1997. évi XLVII. törvény (EÜak.) és az egészségügyről szóló 1997. évi CLIV. törvény (EÜtv.) vonatkozik. (NAIH/2019/5831)

11. Megőrzési időn túl kezelt személyes adatok

A kérelmező egy kölcsönszerződés miatt az adatkezelő bank ügyfele lett. A szerződés felmondásakor az elszámolt és fennmaradó tartozás mértékéről a bank és a kérelmező között véleményeltérés volt. A bank a követelését követeléskezelőre engedményezte. A levélváltásokat követően a követeléskezelő fizetési meghagyásos eljárást indított a kérelmezővel szemben, mely ellentmondás miatt perré alakult. A peres eljárásban a követelést alátámasztó banki iratokkal (folyószámla-kimutatás, egyenlegközlő) a követeléskezelő nem rendelkezett, azokat a bank nyújtotta be. Az első fokon eljárt bíróság szerint a követelés elővült, az ítéletet a másodfokú bíróság helybenhagyta. A kérelmező a másodfokú, jogerős ítélet kézhezvételét követően kért tájékoztatást arról, hogy milyen, banktitoknak minősülő adatait kezeli a bank, milyen egyéb személyes adatait kezelik, továbbá tájékoztatást kért az adatkezelés időtartamáról. A Hatóság megállapította, hogy a bank a megfelelő jogalapon kezelt adatkörön túlmenően olyan adatokat is kezel a kérelmezőről, melyekre a Számviteli törvény megőrzési kötelezettség teljesítését előíró rendelkezéseinek hatálya kiterjedt ugyan, azonban a megőrzési kötelezettség teljesítésére nyitva álló határidő már eltelt. Ilyen adatok: a kérelmező családi állapota, telefonszáma, munkáltatójának neve és telefonszáma, e-mail címe, valamint a lezárt folyószámlájához kapcsolódó adat. Hatályos szerződés hiányában az adatkezelő az előírt megőrzési időn túl kezelt személyes adatok vonatkozásában a GDPR 6. cikk (1) bekezdés a)-f) pontjaiban meghatározott jogalapok egyikének fennálltát sem tudta igazolni, ezért a Hatóság elrendelte azok törlését és a bankot 2.000.000,- Ft bírság megfizetésére kötelezte. (NAIH/2019/2113)

12. Tájékoztatás az adatkezelő kilétérről

Egy követeléskezeléssel kapcsolatos ügyben az érintett több kérelmet is benyújtott, két különböző, de az érintett kérelmek vonatkozásában közös adatkezelést folytató adatkezelőhöz. Az érintettnek küldött válaszlevélben nem volt arra vonatkozó utalás, hogy a választ küldő adatkezelő a másik adatkezelőhöz küldött érintett kérelemre válaszolt. Az érintett számára a levélben nem szerepelt semmiféle információ arra nézve, hogy az általa megkeresett adatkezelő továbbította az érintett kérelmét annak az adatkezelőnek, akitől végül választ kapott. Az érintettnek választ küldő adatkezelő azon érvelését sem fogadta el a Hatóság, hogy az átláthatóság követelményének azzal is eleget tett, hogy az érintettnek küldött leveleken mindenig szerepelt és szerepel az, hogy az érintett kérelmének a címzettje az érintettnek választ küldő adatkezelő MNB által jóváhagyott közvetítője, mivel ebből nem vonhatnak le következtetéseket az érintettek adatkezelői vagy adatfeldolgozói minőségére vonatkozóan. Az adatkezelő azon érvelése sem volt elfogadható, hogy az érintettnek tisztában kellett volna lennie az adatkezelés körülményeivel, mert „*folyamatos volt a kommunikáció*” az érintettel a több mint kilenc éve kezelt követelés miatt. Tekintettel arra, hogy az érintett számára a választ küldő adatkezelő nem nyújtott megfelelő előzetes tájékoztatást a törlési kérelmek elbírálására jogosult adatkezelő kilétérről és a válaszleveléből sem derült ki az érintett számára az, hogy az adatkezelő válaszlevele a másik adatkezelőhöz benyújtott érintett kérelem nyomán hozott adatkezelői intézkedés, a Hatóság megállapította, hogy a választ küldő adatkezelő megsértette az átlátható adatkezelés elvét. (NAIH/2019/4424)

13. Tájékoztatás az érintett személyes adatainak kezeléséről követeléskezelés esetén

Egy követeléskezelő a kérelem beérkezését követő egy hónapos határidőn belül nem adott tájékoztatást, majd a hatósági eljárásról való tudomásszerzést követően hiányos tájékoztatást adott az érintett személyes adatainak kezeléséről. A tájékoztatás nem tartalmazta, hogy a Számviteli törvény, a Hpt. és a pénzügyi intézmények, biztosítók és viszontbiztosítók, továbbá a befektetési vállalkozások és árutőzsdei szolgáltatók informatikai rendszerének védelméről szóló 42/2015. (III.12.) Korm. rendelet által előírt jogi kötelezettség teljesítésével összszefüggésben konkrétan milyen személyes adatokat kezel az érintett vonatkozásában. Ezzel lehetetlenné tette az érintett számára, hogy átlássa a rá vonatkozó személyes adatok kezelését, ezáltal megsértette a GDPR 5. cikk (1) bekezdés a) pontja szerinti átláthatóság elvét. Tekintettel arra, hogy az utólagos tájékoz-

tatás is hiányos volt, a követéskezelőt a Hatóság a GDPR 15. cikk (1) bekezdés a)-h) pontjában foglaltaknak megfelelő válasz adására és a követeléskezelőt 300.000,- Ft bírság megfizetésére kötelezte. (NAIH/2019/4424)

14. Pénzügyi vállalkozás befektetési szolgáltatások nyújtásával kapcsolatos adatkezelési gyakorlata

A Hatóság egy pénzügyi vállalkozás befektetési szolgáltatások nyújtásával kapcsolatos általános adatkezelési gyakorlatát vizsgálta. Az alkalmassági tesztekben felvett személyes adatak kezelése vizsgálatának két fő pontja a jogalap (GDPR 6. cikk) valamint a tájékoztatás (GDPR 13. cikk) volt. A befektetési vállalkozásokról szóló törvény alapján csak bizonyos befektetési szolgáltatások (befektetési tanácsadás nyújtása, portfólió-kezelés) igénybevétele esetén kötelesek a pénzügyi vállalkozások az alkalmassági tesztet kitölteni az ügyfelekkel. A vizsgált pénzügyi vállalkozás mindenkit kötött az alkalmassági tesztet az ügyfeleivel, ha azok olyan szerződést kötöttek vele, amely alapján jogosulttá váltak portfólió-kezelési vagy befektetési tanácsadási szolgáltatást igénybe venni. A pénzügyi vállalkozás nem vizsgálta, hogy a befektetési szolgáltatást és portfoliókezelést igénybe venni jogosult ügyfelei ténylegesen igénybe kívánják-e venni e szolgáltatásokat, vagy csak a szerződésből származó egyéb előnyök miatt választották ezt a szerződéstípust. A pénzügyi vállalkozás a befektetési szolgáltatást és portfólió-kezelést igénybe nem vevő ügyfelei alkalmassági tesztben megadott személyes adatait a jogos érdekére hivatkozással kezelte, az érdekmérlegelési tesztben azonban nem igazolta a saját jogos érdekeinek elsőbbségét az érintettek jogaival és szabadságaival szemben. Több különböző dokumentumban, részben eltérő tartalommal tájékoztatta az ügyfeleit az új befektetői (MiFID) kérdőívekben felvett személyes adatak kezeléséről. Egyik dokumentum sem tartalmazta, hogy bizonyos esetekben a pénzügyi vállalkozás a jogos érdeke alapján kezeli az ügyfelei alkalmassági tesztben megadott személyes adatait, ezzel ellehetetlenítve a tiltakozási jog gyakorlását. A bírságkiszabásnál a Hatóság az alábbi szempontokat vette figyelembe: a pénzügyi vállalkozás nem első alkalommal sérthette meg a GDPR rendelkezéseit, továbbá a figyelmeztetés nem lett volna arányos és visszatartó erejű szankció. Súlyosbító körülményként került értékelésre, hogy a jogszertés a vizsgált időszakban folyamatosan fennállt, illetve, hogy minden jogszertés az érintettek nagy számát érintette. A nem megfelelő tájékoztatás közvetetten akadályozta az érintettek tiltakozási jogának gyakorlását, továbbá a tájékoztatás átláthatatlansága súlyos jogszertésnek minősült, mivel olyan speciális szakmai kérdésekhez kapcsolódó adatkezelésről kellett a pénzügyi vállalkozásnak információval ellátnia az érintetteket, melyekhez az át-

lagos érintett más forrásból nem férhet hozzá. Enyhítő körülmény volt, hogy a pénzügyi vállalkozás a jogos érdeke alapján végzett adatkezelésének egyik céljaként, illetve az adatkezeléshez fűződő jogos érdekeként a befektetők védelmének fokozottabb biztosítását jelölte meg. (NAIH/2019/3107.)

15. Személyes adatok átadása követelés átadásával

Kérelmezők azt kifogásolták, hogy banki hitelt vettek fel egy pénzügyi intézménytől, azonban a fennálló követelést egy cég vásárolta meg, és a követelés átadásával a kérelmezők személyes adatait is továbbították az adatkezelőhöz. A kérelmezők álláspontja szerint a cég jogosulatlanul kezelte személyes adataikat, mivel nem volt engedélye követeléskezelési tevékenységre. A kérelmezők az ügyben a Magyar Nemzeti Bankhoz fordultak, mely piacfelügyeleti eljárást indított, és határozatában megállapította, hogy a cég az MNB engedélye nélküli követelésvásárlási pénzügyi tevékenységet folytatott. A kérelmezők álláspontja szerint az MNB eljárása során megállapították, hogy a cég a személyes adataikhoz is jogosulatlanul fert hozzá. A cég az engedményezési szerződés alapján a kérelmezőkkel szemben fennálló követelések jogosultjává vált, és a követelések érvényesítése, az adósok teljesítésre bírása érdekében, annak céljából kezeli személyes adataikat. Önmagában ezen adatkezelési cél jog szerűnek minősül. Tekintettel azonban arra, hogy az MNB piacfelügyeleti eljárásában megállapította, hogy a cég a kérelmezőket érintően is engedély nélkül végezte a követelésvásárlási tevékenységet, mely miatt el is tiltotta e tevékenység végzésétől, a Hatóság álláspontja szerint e jogellenesen végzett tevékenységgel összefüggő adatkezelés és annak célja is jogellenességet eredményezett. A Hatóság a kérellem jogellenes adatkezelés megállapítására vonatkozó részének helyt adott és megállapította, hogy a követeléskezelő nem megfelelő jogalap alapján, jogszerrülettel adatkezelési célból kezelte a kérelmezők személyes adatait a jogosulatlanul végzett követelésvásárlási tevékenysége során. A Hatóság a céget az általa végzett jogellenes adatkezelés miatt elmarasztalta. Elrendelte a kérelmezők személyes adatai kezelésének korlátozását, valamint megtiltotta az adatkezelőnek, hogy követeléskezelés céljából felhasználja azokat, és további szankcióként 1.000.000 forint adatvédelmi bírságot szabott ki rá. (NAIH/2019/1598)

16. A MOHOSZ adatkezelési gyakorlata a horgászkártya igénylési eljárása során

Több bejelentés érkezett a Hatósághoz, amelyben a bejelentők a Magyar Országos Horgász Szövetség (a továbbiakban: MOHOSZ) adatkezelési gyakorlatát kifogásolták a horgászkártya – online és személyes – igénylési eljárása során bekért, adóigazolványról készített fényképfelvétel vonatkozásában. Az ügyben vizsgálat indult. A MOHOSZ az adatkezelés jogalapjaként a szerződés teljesítéséhez szükséges adatkezelést, az érintett hozzájárulását és a MOHOSZ jogos érdekét jelölte meg, továbbá az adatkezelési tájékoztatója a számlán szereplő adatok tekintetében a számviteli jogszabályokra is hivatkozott. Az adatkezelés jogosításához a jogalap mellett azt a célt is meg kellett vizsgálni, amelynek elérése érdekében a MOHOSZ az okmánymásolatokat beérkezte, továbbá meg kellett ítélni, hogy ez az adatkezelés alkalmass-e az adott célra. A MOHOSZ által megjelölt adatkezelési célok: *ügyfél-azonosítás, személyes adatok egyezőségének ellenőrzése, kockázatelemzés*.

Az adóigazolvány másolatában szereplő adatok is személyes adatnak minősülnek. A Hatóság álláspontja szerint a MOHOSZ-nak sem személyazonosítási célból, sem számlázási célból nem törvényben előírt kötelezettsége az adóazonosító jel kezelése. Az adóazonosító jel nem jogszabály által előírt kötelező tartalmi eleme egy polgár részére kiállítandó számlának mint bizonylatnak. A Hatóság a vizsgálati eljárásban megállapította, hogy MOHOSZ az adóazonosító jel kezelésére nem rendelkezik törvényi felhatalmazással, ezért a Szaztv. 7. §-a értelmében kezelésének jogalapja csak az érintett hozzájárulása lehet, amennyiben az adatkezelésnek van jogosító célja. A Hatóság álláspontja szerint az adatkezelési tájékoztatóban megjelölt hozzájárulás nem megfelelő adatkezelési jogalap, mert az érvényes hozzájárulás egyik fogalmi eleme az önkéntesség, mely csak akkor valósul meg, ha az érintett szabadon, befolyástól mentesen jut az adatkezelésre felhatalmazást adó jognyilatkozat megtételére vonatkozó elhatározásra. Emellett a Szaztv. alapján a polgárt a hozzájárulás megadása, megtagadása, illetve visszavonása miatt hátrány nem érheti, márpédig nyilvánvalónan az önkéntességet kizáró befolyásnak, illetve hátránynak minősül az, ha az ügyfél a hozzájárulás hiányában nem tud regisztrálni.

A MOHOSZ az adóazonosító jel kezelésének „lehetséges” jogalapjaként a szerződés teljesítéséhez szükséges adatkezelést és a jogos érdekét is megjelölte. Ezek a „lehetséges” jogalapok alkalmazása azonban ellenétes a Szaztv.-ben írtakkal, mivel az azonosító kódok – köztük a természetes személyek adóazonosító jele – csak törvény felhatalmazása, ennek hiányában az érintett előzetes írásbeli hozzájárulása, illetőleg az ügyintézési rendelkezésben tett hozzájárulá-

sa alapján használhatók fel. Az adatkezelő jogos érdekére hivatkozással kapcsolatosan a Hatóság felhívta a MOHOSZ figyelmét arra, hogy az érintett alapvető jogai ebben az esetben elsőbbséget élveznek, pusztán az a tény, hogy egy esetleges visszaélést kívánnak ily módon megelőzni, nem elegendő ahhoz, hogy univerzális azonosítóként használják az adóazonosító jelet. Tehát a MOHOSZ az adóazonosító jelet nyilvántartási célból nem használhatja és a begyűjtött adóazonosító jel adatokat törölnie kell. (NAIH/2019/3620)

17. Származására vonatkozó különleges adat nyilvánosságra hozatala

2018-ban indult, de 2019-ben zárult az a vizsgálat, amelyet egy magánszemély azért kezdeményezett, mert kifogásolta, hogy egy alapítvány évkönyvének online változatában a név szerinti felsorolás mellett fel van tüntetve a tény, hogy ō nemzetiségi diákoknak felsőoktatásban adható ösztöndíjban részesült. A származására vonatkozó különleges adat nyilvánosságra hozatalára elmondása szerint a tanulmányi ösztöndíjról szóló szerződés aláírásakor nem adott hozzájárulást. Az adatkezelő együttműködésének hiányában a Hatóság a becsatolt iratok alapján bíráltá el a panaszt. A Hatóság megállapította, hogy az adatkezelés a személyes adatok védelméről és a közérdekkű adatok nyilvánosságáról szóló 1992. évi LXIII. törvény (Avtv.) hatálya alatt kezdődött, azonban minden adatkezelőnek a GDPR alkalmazására való felkészülés ideje alatt a GDPR (171) preambulum-bekezdése értelmében a korábban megkezdett adatkezelést összhangba kellett hozni a rendelettel. Mivel az adatkezelés 2019-ben is fennállt, ezért a származásnak mint különleges adatnak a nyilvánosan elérhető biztosítására a GDPR szabályai alkalmazandóak, és az adatkezelésnek a GDPR 6. ciklében foglalt jogalap mellett a 9. cikk szerinti korlátozásnak is meg kell felelnie, amely az adatkezelés jogosító céljához igazodik. A Hatóság álláspontja szerint az alapítvány átlátható működésének ellenőrzése a különleges adat nyilvánosságra hozatala nélkül is megvalósítható és biztosítható oly módon, ha az ösztöndíjat kapott hallgatók névsora egyébként elérhető papír alapon, és kérésre azt az érdeklődő rendelkezésére bocsátják. A bárki általi ellenőrzéshez elegendő mértékű a személyes adatok nélküli nyilvános információk közzététele, például hány fő, egyenként milyen összegben kapott támogatást, egyúttal utalva arra, hogy a részletes adatok a megadott helyeken megtekinthetők, különös tekintettel arra, ha az adatok nyilvánosságra hozatalára megfelelő jogalappal nem rendelkeznek. Azt, hogy az adatkezelés a GDPR 5. cikk (1) bekezdésnek megfelelően érvényes jogalappal, célhoz kötötten és az adattakarékkosság elvének eleget téve csak a cél eléréshez szükséges mértékű adattartalomra korlátozódik, az adatkezelő – válaszadás híján – nem igazolta, mint ahogy azt sem hogy jelenleg

az átláthatóság mint adatkezelési cél eléréséhez miért szükséges a különleges adatnak bárki számára történő hozzáférhetővé tétele. Amennyiben az eredeti iratok szerint a panaszos hozzájárulást is adott volna a nyilvánosságra hozatalhoz, ám azt a GDPR-ban biztosított jogával élve visszavonja, az adatkezelőnek a GDPR szabályai alapján akkor is felül kellett volna vizsgálna az adatkezelés jogoszerűségét, és megítélni, hogy a visszavont hozzájárulás ellenére az ellenőrizhetőség és átláthatóság mint adatkezelési cél érdekében történő adatkezelés milyen, a 6. cikkben foglalt és a 9. cikknek megfelelő jogalapon alapulhat. Mindezeknek megfelelően a Hatóság azt a megállapítást tette, hogy az alapítvány a panaszos nevének és származásának nyilvános megjelenítésére nem rendelkezett jogalappal. A panaszos a Hatóság válaszának kézhez vétele után tájékoztatta a Hatóságot, hogy a válaszra hivatkozással a Google-hoz fordult, és kérte a nyilvánosságra hozott adat eltávolítását, amelynek a Google eleget tett, így a keresőbe beírva a panaszos származására vonatkozó adat a továbbiakban már nem jelenik meg találatként. (NAIH/1101/2019)

18. Kezelt személyes adatok pontosságának vitatása

Egy panaszos olyan e-mailt kapott egy szolgáltatótól, amely a szolgáltató egy másik ügyfelének szolt. A problémát az okozta, hogy a két személyt ugyanúgy hívják és az e-mail címük is hasonló. A szolgáltató felé a panaszos jelezte a problémát, a szolgáltató ugyanakkor arra hivatkozott, hogy megkereste ügyfélét, azonban ügyfele kijelentette, hogy a nevéhez csatolt e-mail cím helyes, emiatt a szolgáltató nem tudta törlni az e-mail címet és a panaszosnak továbbra is küldték az e-maileket. Hosszas egyeztetést követően sikerült az ügyféllel megállapodni, hogy másik e-mail címet csatoljanak a nevéhez, így a probléma megoldódott. A panasz oka, hogy a Gmail nem tesz különbséget a „pont”-tal és „pont” nélkül írt e-mail-címek között. Emiatt kerülhetett sor arra, hogy a x.y@gmail.com e-mail-címmel regisztrált ügyfél e-mail-címére küldött számla elkészültének értesítését az x.y@gmail.com e-mail-címmel regisztrált panaszos (is) megkappa. A szolgáltató tájékoztatta a Hatóságot, hogy a jövőben rendszeresen ellenőrizni fogja azon előfizetői Gmail fiókos e-mail-címeit, ahol a különbség csak egy „pont”, és felveszi velük a kapcsolatot a további problémák elkerülése érdekében. A Hatóság felhívta a figyelmét arra, hogy a jövőben a személyes adatok pontosságának vitatása esetén a GDPR 18. cikk (1) bekezdés a) pontja szerint járjon el, amely szerint az adatkezelőnek korlátoznia kell az adatkezelést, amennyiben vitatott annak pontossága. A Hatóság felhívta az adatkezelő figyelmét a GDPR 32. cikk (1) bekezdésének megfelelő gyakorlat kialakítására. Ilyen gyakorlat lehet például, ha olyan Gmail e-mail címet szeretnének regisztrálni,

ahol csak egy „pont” az eltérés egy már meglévő Gmail e-mail címtől, azt ne engedje a rendszer regisztrálni. (NAIH/2019/776)

19. Adatkezelési tájékoztató nyelvi igényessége

Egy brit vállalkozás, a brit céggjegyzék szerint alvó cég, tehát nem végezhetne gazdasági tevékenységet, így Magyarországra sem nyújthatna szolgáltatást. A tulajdonos csehországi lakóhellyel rendelkezik, a panaszos Magyarországon él. A panaszolt cég adatkezelési tájékoztatójából peldaként idéznénk két bekezdést azzal a megjegyzéssel, hogy az Alaptörvény szerint Magyarország védi a magyar nyelvet. Az ügy érdekessége maga a nyelvromboló gúnytájékoztató. Idézet: „*Mindenki a mi cégeinkbe nagyon fontosnak és értekessnek tartsa a személyi adatok felhasználását és aszerint úgy is bánnunk velük. Kérjük Önöket figyelmesen olvasák el hogy hogyan állunk a személyes adatok megörzéséhez. Amennyiben valameik ponttal nemertenének együt, kerjük hogy értesícsenek minket.*” [...] „*A mi marketing kampányunkba csak is profilált és automatizált feldolgozást használunk annak a célnak az érdekelben hogy felalaljuk a mi céltot termékeinket és szolgáltatásainkat-szeretnénk fel kínálni aszt ami maguk számára releváns, és nem leterhelni feleslegeségekel. Nem használunk profilált (alakítót) sem automatizált feldolgozást automatikus döntésekkel amelyiek az Önök számára jogi következményekkel járnának vagy Önöket valamiben jelentős mértékben érintené.*” Az ügy tanulsága, hogy a nyelvi igénytelenség esetenként akadályozza, illetve lassítja a hatékony ügyintézést, egyszersmind nem felel meg a GDPR-ban rögzített, az adatkezelés átláthatóságával összefüggő követelményeknek sem. (NAIH/2020/83)

20. Választásokkal kapcsolatos adatkezelések

2019-ben számos panasz érkezett azzal kapcsolatban, hogy – a választásokhoz kapcsolódó ajánlásagyűjtésen kívül – nagy számban gyűjtötték személyes adatokat a választópolgároktól. Az adatok felvételére többnyire szímpatizánsi-adatbázis építése céljából, illetve egyes aláírásagyűjtésekhez, civil kezdeményezésekhez kapcsolódóan – kifejezetten és kinyilvánítottan is valamely meghatározott cél támogatása érdekében – került sor.

A Hatóság ezzel kapcsolatban a 2019 áprilisában kibocsátott, a választásokkal kapcsolatos adatkezelésekéről szóló ajánlásában⁶ hívta fel a figyelmet arra, hogy az adatgyűjtés minden esetben csak pontosan meghatározott, jogoszerű célból történhet. A cél megjelöléséről a tiszteességes adatkezelés követelményével összhangban kell gondoskodni, az nem lehet megtévesztő. Az ajánlásában a Hatóság külön kitért arra, hogy az ajánlások gyűjtésével egy időben, de attól eltérő célból (például szímpátia-adatbázis építés) történő adatgyűjtés önálló, a jelöltállításhoz kapcsolódótól eltérő célú adatkezelésnek minősül, amelyről ennéfogva az érintetteket ezen adatkezelési cél megjelölésével tájékoztatni kell. A Hatóság ezzel kapcsolatban kifejtette, hogy amennyiben a polgár kizárolag csak a politikai kezdeményezés (például helyi vagy országos petíciós cél) megvalósítása érdekében bocsátotta rendelkezésre adatait, úgy ezeket az adatokat törölni kell, amint az adatkezelés betöltötte célját, valamint akkor is, ha az adatkezelés célja meghiúsult. A legtöbb esetben azonban a kezdeményezés mellett az érintett a későbbi kapcsolattartás céljából is megadhatja a személyes adatait (különösen nevét, e-mail-címét, telefonszámát). Az így megadott elérhetőségi adatak kapcsolattartási célból történő felhasználása – amennyiben az érintett időbeli korlátozás nélkül bocsátotta azokat rendelkezésre – mindenkor jogoszerű, amíg az érintett nem kezdeményezi személyes adatai törlését az adatkezelőnél.

2019. szeptember 17-én postai úton beérkezett adatvédelmi hatósági eljárás lefolytatására irányuló kérelmében a Kérelmező (aki a kérelem benyújtásakor önkormányzati tulajdonú cégeknek volt az igazgatósági elnöke) előadta, hogy Budapest VIII. kerület önkormányzati képviselője (aki a 2019. októberi önkormányzati választásokat követően alpolgármester lett) 2019. szeptember 1-jén saját hivatalos (vagyis nem magáncélra használt) Facebook-oldalán közzétett bejegyzésében olyan, a Kérelmezőt ábrázoló fotót tett közzé, amelynek készítéséhez és közzétételéhez a Kérelmező nem járult hozzá. A Kérelmező előadta, hogy a fénykép készültének pillanatában a helyszínen azonnal felhívta a Kérelmezett figyelmét, hogy ne éljen vissza képmásával és azt ne hozza semmilyen közösségi oldalon nyilvánosságra, mert nem járul hozzá; a beszélgetésen jelen volt képfelvételen is látható kiskorú lánya, akinek bár az arcát kitakarták, de mivel megírták, hogy a képen is látható, így könnyen beazonosíthatóvá vált. A Kérelmező továbbá úgy nyilatkozott, hogy megpróbálta írásban is felvenni a kapcsolatot a Kérelmezettel a bejegyzés eltávolítása érdekében, kérésének azonban a Kérelmezett nem tett eleget.

6 https://www.naih.hu/files/ajanlas_valasztas_NAIH_2019_3061.pdf

A hiánpótlás és a tényállás tisztázáshoz szükséges nyilatkozatok beérkezése és értékelése után a Hatóság az ügyben 2020. március 4-én határozatot hozott, melyben megállapította, hogy

- A Kérelmező neve a képfelvétel készítésekor és közzétételekor közérdekből nyilvános adatnak minősült, ugyanakkor képmása nem tekinthető közérdekből nyilvános (személyes) adatnak az Infotv. 26. § (2) bekezdése alapján, tekintettel arra, hogy kinézete nem függ össze közfeladat el-látásával.
- A képfelvétel nem a választási hirdetmény megsemmisítésekor, hanem azt követően készült, azon nem a vélemezett jogosítás látható, ha-nem az, hogy a Kérelmező egy felismerhetetlen papírdarabbal a kezében átkel egy kijelölt gyalogátkelőhelyen. A képfelvételen tehát egyfelől a Kérelmező magán- vagy családi életének egy mozzanat látható, amely nem tekinthető nyilvános közéleti szereplésnek, és semmilyen összefüg-gésben nincs közfeladat ellátásával és a közügyek szabad vitatását biz-tosító alapjogok gyakorlássával, másfelől pedig a képfelvétel egyáltalán nem bizonyítja, hogy a bejegyzésben leírtak megfelelnek a valóságnak. Mindebből az következik, hogy a képfelvétel készítéséhez és közzététe-léhez szükség lett volna a Kérelmező hozzájárulására. A Kérelmezett által megjelölt véleménynyilvánításhoz, a választások tisztaságához és a választók kiegyensúlyozott tájékozódásához fűződő jog nem fogadható el érvényes jogalapként.
- A bejegyzésben közzétett képfelvételnek nincs külön a közügyek megvi-tatásához hozzájáruló többletinformáció-értéke, a nyilvánosság tájékoz-tatásához elegendő lett volna egy képfelvételt nem tartalmazó szöveges bejegyzés is.
- Sem a képfelvétel készítése, sem annak közzététele nem egyeztethe-tő össze a Kérelmezett által megjelölt céllal, nevezetesen egy jogosítő cselekmény rögzítésével és nyilvánosság elé tárással. Az eljárás során beszerzett nyilatkozatok és dokumentumok alapján nem volt megállapít-ható, hogy a képfelvétel készítéséhez és közzétételéhez fűződő érdek elsőbbséget élvezne a Kérelmező érdekeivel és személyes adatai védel-méhez fűződő jogával szemben, illetve, hogy az adatkezelés közérdekkü lenne, vagy a Kérelmezettre, mint adatkezelőre ruházott közhatalmi jo-gosítvány gyakorlásának keretében végzett feladat végrehajtásához lett volna szükséges.
- A Kérelmező érintett joggyakorlás keretében megjelölt igényeire a Kérelmezett semmilyen választ, tájékoztatást nem adott az általános adatvédelmi rendelet 12. cikk (3)-(4) bekezdéseiben meghatározott mó-don és időn belül. Nem fogadható el a Kérelmezett azon nyilatkozata,

miszerint azért nem válaszolt a Kérelmező megkeresésére, mert azt a kampány részének tekintette.

- A képfelvétel több hónappal a 2019. októberi önkormányzati választások után is elérhető maradt a Kérelmezett Facebook-oldalán, annak ellenére, hogy a Kérelmező 2019. novembere óta már nem tölti be az önkormányzati tulajdonú cégek igazgatósági elnöki tisztségét.

A Hatóság határozatában elmarasztalta és a bejegyzés eltávolítására kötelezte a Kérelmezettet, továbbá hivatalból 100.000 Ft adatvédelmi bírságot szabott ki vele szemben, mert a megfelelő jogalap és cél nélküli adatkezelés jelentősen érintette a Kérelmező magánszféráját. Emelett érintett jog gyakorlásával kapcsolatos jogosítás is megvalósult, a Kérelmezett az általános adatvédelmi rendelet több cikkét [5. cikk (1) bekezdés a)-c) pontjai, 6. cikk (1) bekezdése, 12. cikk (1)-(5) bekezdései, 15. cikk (1) bekezdése, 17. cikk (1) bekezdése] is megsértette, és a jogosítelmet a Kérelmezett szándékos magatartása idézte elő. [NAIH/2020/32 (NAIH/2019/6885)]

21. Tájékoztatás aláírásgyűjtéssel kapcsolatos adatkezelés esetén

A Hatóság egy további, az aláírásgyűjtéssel kapcsolatos adatkezelés jogosításának vizsgálatára indult eljárásában az adatkezelés körülményeiről történő tájékoztatással kapcsolatban kifejtette, hogy a megfelelő tájékoztatás az érintett hozzájárulás mint jogalap alkalmazása során központi szerepet betöltő fogalmi elem, amely a hozzájárulás valamennyi fogalmi elemének – úgy, mint önkéntesség, konkrétság, egyértelműség – érvényesüléséhez szorosan kapcsolódik. Ez szükséges ugyanis ahhoz, hogy az érintettek megfelelő információkkal rendelkezzenek arról, hogy pontosan mibe egyeznek bele, ismerjék az adatkezelés részleteit és gyakorolhassák a hozzájárulásuk visszavonásához való jogukat. A megfelelő tájékoztatáshoz kapcsolódan az általános adatvédelmi rendelet tartalmi és formai követelményeket is meghatároz az adatkezelők számára. (NAIH/2019/5062)

22. A benyújtó személyes adatainak kezelése elektronikus ügyintézés esetén

Több beadvány is érkezett a Hatósághoz azzal kapcsolatban, hogy az elektronikus ügyintézés során (például ePapír beadvány) a benyújtást végző képviselő (ügyvezető, ügyvéd stb.) azonosításhoz használt minden személyes adata a benyújtott kérelem részét képezi, és azt az ügy irataihoz fűzik és továbbítják az

adott ügyben minden félnek (például perben a másik félnek). Ezt az adatkezelést jogszabály írja elő kötelezően, és a Nemzeti Infokommunikációs Szolgáltató Zrt. (NISZ) a jogszabály szerint csak adatfeldolgozói szerepet lát el, az adatkezelés feltételeit nem határozhatja meg. Ezért a Hatóság 2019-ben kezdeményezte a Belügyminisztériumnál az elektronikus ügyintézés részletszabályairól szóló 451/2016. (XII. 19.) Korm. rendelet módosítását a GDPR szükségesség és arányosság követelményének történő megfelelés céljából. A Belügyminisztérium által a Hatóság kezdeményezése nyomán előterjesztett, és a Hatóság által véleményezett új rendelkezés alapján a benyújtó személyes azonosító adatait az azonosításához szükséges mértékben, a benyújtáskor végzett azonosítás végéig lehet csak kezelní. Ezen jogszabály-módosítás jelenleg is folyamatban van.

23. Az adatkezelő kötelezettségei hatósági megkeresés esetén

Egy adatkezelő az általa folytatott közigazgatási hatósági eljárásban megkereszettel fordult egy másik adatkezelőhöz abból a célból, hogy tájékoztatást kérjen a megelőző két évben – a folyamatban levő üggel kapcsolatosan – a megkeresett adatkezelő által hozott jogerős határozatokról. A megkeresett hatóság megküldte az üggel összefüggésben a döntései másolatát, melyek a megkereső hatóság előtt folyamatban levő üggel nem érintett személy személyes adatait is tartalmazták.

Egy hatósági megkeresés teljesítése az általános adatvédelmi rendelet 6. cikk (1) bekezdés e) pontja szerinti kötelező adatkezelésnek minősül. A megkeresés teljesítése során az általános közigazgatási rendtartásról szóló törvény (Ákr.) rendelkezéseit és az általános adatvédelmi rendelet szabályait is be kell tartani. Ezekből következően a megkeresett mint a személyes adatok kezelője pusztán annál fogva, hogy megkeresést teljesít, nem mentesül az alól a kötelezettség alól, hogy az adattovábbítás során az általános adatvédelmi rendeletnek az adatkezelés célhoz kötöttségére és az adattakarékosságra vonatkozó alapelvezet betartsa. A megkeresés teljesítése körében a megkereső hatóság van abban a helyzetben, hogy a saját ügyében a tényállás megállapításához szükséges adatok körét, köztük a személyes adatok körét meghatározza, így elsődlegesen az ő felelőssége – az említett jogi korátok között – abban a kérdésben döntení, hogy a megkeresés személyes adatokra vonatkozóan is szükséges-e. Ugyanakkor ez nem jelenti azt, hogy bármilyen hatósági megkeresést szükségszerűen és automatikusan olyannak kellene értelmeznie a megkeresettnek, mint amelyik a személyes adatok bármely körére válogatás nélkül kiterjed. A megkeresést teljesítő

adatkezelőnek adott esetben el kell végeznie a mérlegelést, és meg kell tennie a szükséges intézkedéseket (azaz például a megküldött jogerős/véleges határozatban a személyes adatok megismerhetetlenné tétele, az anonimizálást). (NAIH/2019/13)

24. Rendszám alapján a gépjárművek adatainak korlátlan lekérdezése

Az Alapvető Jogok Biztosa által áttett beadvány azt kifogásolta, hogy jogszabály-módosítás következtében a rendszám alapján a gépjárművek adatainak – köztük személyes adatoknak – korlátlan lekérdezése vált lehetővé, amely lehetőség – a beadványozó szerint – visszaélésekre adhat módot. A Hatóság válaszában rámutatott arra, hogy a jogalkotó a közúti közlekedési nyilvántartásról szóló 1999. évi LXXXIV. törvény preambulumának indokolásában jelezte, hogy a személyes adatok védelmére figyelemmel a törvény taxatíve meghatározza a nyilvántartható adatok körét, a nyilvántartás adatforrásait, az adatkezelés időtartamát, az adatszolgáltatás terjedelmét, korlátait, az adatigénylésre jogosultak körét, továbbá az adatvédelemre vonatkozó szabályokat. A Hatóság arra is rámutatott, hogy a jogszabály-módosítás a már létező adatigénylés lehetőségét bővíttette ki az elektronikus úton történő lekérdezéssel. Mivel a jogszabály-módosítás nem visszaélésekre ad lehetőséget, hanem ellenkezőleg, a közúti közlekedésben részt vevő gépjárművek adatainak elektronikus úton történő nyilvános, közvetlen és díjmentes ellenőrzését szolgálja, és további adatvédelmi relevanciája sem volt a beadványnak, vizsgálat nem indult. (NAIH/2019/1424)

25. Könyvtári dokumentumokban található személyes adatok közérdekű archiválása, illetve tudományos és történelmi kutatási célból történő kezelése

Egy megkeresésben a könyvtári dokumentumokban található személyes adatok közérdekű archiválása, illetve tudományos és történelmi kutatási célból történő kezelésével kapcsolatban kérték a Hatóság állásfoglalását. A könyvtárak gyűjteményének részét képező könyvtári dokumentumokban található személyes adatok tárolása, őrzése, digitalizálása adatkezelésnek minősül. Ezzel kapcsolatban érdemes azonban megjegyezni, hogy a GDPR-t nem kell alkalmazni az elhunyt személyekkel kapcsolatos személyes adatokra. A Hatóság álláspontja szerint a könyvtárak tevékenysége keretében végzett adatkezelés egyik lehetséges célja a közérdekű archiválás. A GDPR-t az archiválási célokat szolgáló adatkezelésre is alkalmazni kell, erre a (158) preambulumbekezdés is kifejezetten utal. A személyes adatokat tartalmazó dokumentumok digitalizálása és nyilvánosságra

hozatala is a GDPR hatálya alá tartozó adatkezelésnek minősül, így jogosításának elengedhetetlen feltétele, hogy a jogosítás célján túl legyen megfelelő jogalapja is. A Hatóság álláspontja szerint a könyvtárak törvényben meghatározott feladatai ellátásának során végzett adatkezelésének jogalapja a GDPR 6. cikk (1) bekezdés e) pontja lehet, mivel az adatkezelés közérdekű feladat végrehajtásához szükséges. A GDPR 89. cikk első bekezdése alapján a személyes adatok közérdekű archiválás céljából, tudományos és történelmi kutatási célból folytatott kezelését az érintett jogait és szabadságait védő megfelelő garanciák mellett kell végezni. Ez tehát azt jelenti, hogy magának az adatkezelőnek kell olyan módon kialakítani az adatkezelés folyamatait, hogy az megfeleljen a GDPR rendelkezéseinek. A GDPR kizárolag arra ad felhatalmazást a tagállami jogalkotónak, hogy az érintett jogok gyakorlását illetően eltérjen a GDPR szabályaitól, amennyiben az adatkezelés célja a közérdekű archiválás, sőt, maga a GDPR is tartalmaz ilyen kivétszabályokat. Kiemelendő a GDPR 17. cikk (3) bekezdése, amely szerint nem áll fenn az adatkezelő törlési kötelezettsége, ha az adatkezelés például közérdekből végzett feladat végrehajtásához szükséges, illetve a közérdekű archiválás céljából történő adatkezelések esetén, amennyiben az érintett törléshez való jogának gyakorlása valószínűsíthetően lehetetlenne tenné vagy komolyan veszélyeztetné ezt az adatkezelést. Ha az adatkezelés jogalapja a GDPR 6. cikk (1) bekezdés e) pontja, úgy az érintettet megilleti a tiltakozás joga is. Ha az érintett tiltakozik az adatkezelés – például a személyes adatait tartalmazó digitalizált újságcikk nyilvánosságra hozatala – ellen, az adatkezelő a személyes adatokat nem kezelheti tovább, kivéve, ha az adatkezelő bizonyítja, hogy az adatkezelést olyan kényszerítő erejű jogos okok indokolják, amelyek előbb séget élveznek az érintett érdekeivel, jogaival és szabadságaival szemben. Ezen mérlegelést az adatkezelőnek a tiltakozási jogát gyakorló érintett érdekeinek és jogainak figyelembevételével esetről esetre kell elvégeznie. A könyvtárak azonban ilyen esetekben sem módosíthatják a digitalizált könyvtári dokumentumok tartalmát, mivel feladatauk az állomány gondozása, megőrzése, amely együtt jár a dokumentumok integritásának megőrzésével is. (NAIH/2019/1342)

26. Költséghátralékkal rendelkező személyek nevének lépcsőházi kifüggesztése

A költséghátralékkal rendelkező személyek nevének lépcsőházi kifüggesztése visszatérő probléma. Az éves elszámolás elfogadásáról a társasházakról szóló törvény szerint a közgyűlés határoz. Szükségszerű tehát, hogy éves elszámolás benyújtásakor, illetve annak elfogadása érdekében a közgyűlés megismerhesse az elszámolásban szereplő adatokat, így a közös költséghez való hozzájárulás előírását és annak teljesítése mértékét a tulajdonostársak nevének feltünteté-

sével. Nincs tehát jogszabályi akadálya, hogy a tulajdonostársak megismerjék azon személyek kilétét, akik a közös költségek fizetésében hátralékkal rendelkeznek. A megismerés módja lehet például a postaládába dobbott lezárt tájékoztató, a könyvelésbe történő betekintés, vagy zárt (kizárolag a tulajdonostársak részvételével megtartott) közgyűlésen a hátralékkal rendelkező tulajdonostársak nevének és a hátralék összegének ismertetése. A természetes személy közös költségre vonatkozó hátralékának adatai a tulajdonostársak által megismerhető olyan adatok, amelyek azonban megtartják a személyes adat minőségüket, tehát a közös költségre vonatkozó személyes adatok kezelésekor, felhasználásakor érvényre kell juttatni az általános adatvédelmi rendelet célhoz kötött adatkezelés elvét is. Mivel a célhoz kötött adatkezelés elve miatt a közös képviselő és a tulajdonostársak a közös tulajdon üzemeltetésével kapcsolatban tudomásukra jutott adatokra vonatkozóan kötelesek a személyiségi jogokat tiszteletben tartani, és az ilyen adatokat célhoz kötötten felhasználni, a tájékoztatás akkor lehet jogoszerű, ha az a társasház költségvetésének megismeréséhez szükséges, továbbá nem teszi lehetővé azt, hogy a tulajdonostársakon kívül más, arra jogosultan személy is megismerhesse a személyes adatot tartalmazó közös költség elszámolást. A fentiekben részletezett okokból megállapítható, hogy sérti az adatvédelmi előírásokat a költséghátralékkal rendelkező személyek nevének lépcsőházban vagy más nyilvános helyen történő közzététele, mert a közzétett személyes adatokat a tulajdonostársakon kívül más személyek is megismerhetik. (NAIH/2019/2223)

27. Szülői felügyeleti joggal nem rendelkező szülő tájékoztatáshoz való joga

Egy szülői felügyeleti joggal nem rendelkező, gyermekétől különélő szülő a gyermek tanulmányi eredményeit nem tudja nyomon követni, mert a másik szülő az elektronikus napló használatához szükséges adatokat nem adta meg. A Hatóság álláspontja szerint a gyermek tanulmányi előmenetele a Ptk. szerinti, a gyermek sorsát érintő lényeges kérdés. A szülői felügyeleti joggal nem rendelkező szülőnek lehetősége van arra, hogy a gyermek tanulmányi előmenetelére vonatkozóan az iskolától, pedagógustól, valamint a másik szülőtől tájékoztatást kérjen. A Hatóság álláspontja szerint a szülői felügyeleti jogot nem gyakorló szülő csak azon információk megismerésére jogosult, amelyek a lényeges kérdések eldöntéséhez szükségesek. A Hatóság ugyanakkor nem jogosult annak megítélezésére, hogy a Ptk. szerinti lényeges kérdés eldöntése alapjául szolgáló tájékoztatás tartalma meddig terjed. Tekintettel arra, hogy jogbizonytalanságot okoz az, hogy az egyes intézmények eltérően értelmezik azt, hogy mely adatok kiadására jogosultak a tájékoztatás körében, illetve kötelesek-e a szülői felügyeleti jog

ellenőrzésére, ezért a Hatóság e kérdés vizsgálatára felkérte az alapvető jogok biztosát. (NAIH/2019/2202)

II.1.3. Határon átnyúló ügyek

A Hatóság a GDPR alapján együttműködik az Európai Unió többi tagállamában található adatvédelmi hatóságokkal. A Hatóság 2019-ben több száz határon átnyúló adatkezeléssel kapcsolatos eljárásban volt ún. érintett hatóság, amely az összes határon átnyúló eljárás körülbelül egyharmada, valamint voltak olyan, határon átnyúló adatkezeléssel kapcsolatos ügyek, melyekben főhatóságként járt el a NAIH. Ezen ügyeket az alábbiakban röviden ismertetjük.

1. Egy biztonsági szoftverekkel foglalkozó cég vírusirtójának ingyenes verziójával kapcsolatban a holland adatvédelmi hatósághoz nyújtottak be panaszt 2018. május 25-én. A panasz szerint az adatvédelmi beállítások az ingyenes verzióban le voltak tiltva, nem voltak átállíthatóak, ezzel a panaszos szerint sérültek a GDPR szerinti érintett jogok. Az ügyben a GDPR 56. cikke alapján az adatkezelő tevékenységi központja szerint illetékes cseh adatvédelmi hatóság járt el főhatóságként, és minden EU tagállam adatvédelmi hatósága érintettként közreműködött az eljárásban. A Hatóság a 2019. márciusi első döntéstervezettel kapcsolatban releváns és megalapozott kifogást terjesztett elő, mivel az eljárás tárgya és a jogkövetkezmények nem voltak megfelelően megjelölve. Ezt követően a cseh adatvédelmi hatóság bővítette a tervezet indokolását, és jelezte, hogy eljárási joga alapján egy második döntésben külön fogja a jogkövetkezményeket meghatározni. Emiatt a Hatóság a 2019. augusztusi új döntéstervezetet elfogadta.

A GDPR alapján minden – akár közvetetten – természetes személyhez köthető adat személyes adat, így a dinamikus IP cím és a cég által az adott végfelhasználói eszközhöz és az adott telepítéshez rendelt egyedi szám is. Megállapítást nyert továbbá, hogy az adatkezelő megsértette a GDPR 24. cikk (1) bekezdését, azaz nem tett megfelelő technikai és szervezési intézkedéseket annak biztosítása és bizonyítása céljából, hogy a személyes adatok kezelése a GDPR-al összhangban történik. (NAIH/2019/1257)

2. Egy panaszos amiatt fordult a Hatósághoz, mivel évekkel ezelőtt megadta személyes adatait egy nagy elektronikai cég televíziójának vásárlásakor azért, mert a regisztrációért cserébe további 1 év jótállási jogot biztosított számára

az adatkezelő. Tekintettel arra, hogy már a meghosszabbított jótállási jog is lejárt, kérte személyes adatai törlését. Az érintett jogok gyakorlására működtetett weboldalon az adatkezelő többek között valamilyen személyazonosító okmány szkennelt változatának feltöltéséhez kötötte az érintett kérelmének befogadását mind a törlés, mind más jogok gyakorlása esetén. Emiatt a Hatóság a GDPR alapján főhatóságként eljáró Egyesült Királyság Adatvédelmi Biztos Hivatala (ICO) eljárását kezdeményezte, és érintett hatóságként vett részt az eljárásban. Az ICO döntéstervezete szerint az adatkezelő felülvizsgálta eljárásait és arról határozott, hogy módosítja az érintett megkeresésekre vonatkozó gyakorlatát.

A fentiek alapján az ICO megküldte a Hatóságnak a döntéstervezetét, amely szerint nincs szükség további intézkedésekre. A Hatóság kifogásnak nem miőnősülő kisebb észrevételeket tett, pontosításokat javasolt a döntéstervezethez. (NAIH/2019/331)

3. A panaszos panasszal fordult a Hatósághoz, mely szerint egy álláslehetőségre pályázott egy nemzetközi bank magyarországi fióktelepéhez, azonban, mivel nem született megállapodás, kérte az adatkezelőt, hogy az összes rendszerből törölje személyes adatait. Az adatkezelő angol nyelvű válasza alapján a panaszos e kérelmének nem tettek eleget, mivel a belső szabályzatuk alapján az utolsó benyújtott álláspályázatától számított két évig megőrzik a pályázó személyes adatait. Az ügyben vizsgálat indult, és a Hatóság megkereséssel fordult az adatkezelő felé. A bank nyilatkozatai és a honlapján elérhető adatkezelési tájékoztatója alapján az adatkezelő központi ügyvitelének helye Londonban van, ezért a Hatóság a GDPR alapján főhatóságként eljáró Egyesült Királyság Adatvédelmi Biztos Hivatala (ICO) eljárását kezdeményezte. A Hatóság érintett hatóságként vesz részt az eljárásban. (NAIH/2019/2542.)

II.2. Az adatvédelmi incidensek bejelentése

A Hatóság előző évi beszámolójában az adatvédelmi incidensek bejelentésével, kezelésével kapcsolatban általános jellegű tájékoztatást nyújtott, valamint a leggyakrabban előforduló incidenstípusokat, illetve az azok megelőzésére, orvoslárára szolgáló intézkedéseket ismertette. Idén a Hatóság az elmúlt év valamelyen szempontból jellegzetes, tanulsággal szolgáló ügyének rövid összefoglalása mellett döntött, azzal a szándékkel, hogy az adatkezelők figyelmét az adatvédelmi incidensek kezelése során felmerülő kulcsfontosságú szempontokra irányítsa, az ügyekben ismertetett hibák és hiányosságok megelőzése érdekében.

1. A Hatóság egy általános iskolában történt incidens esetében a feltárt tényállás alapján megállapította, hogy 2018 decembere és 2019 februárja között az adatkezelő honlapján nyilvánosan elérhető volt egy, az iskolába járó gyerekek nevét, osztályát és egyéb, érzékenyebb személyes adataikat (például arra vonatkozó adat, hogy a gyermek halmozottan hátrányos helyzetű, hátrányos helyzetű, sajátos nevelési igényű, illetve rendszeres gyermekvédelmi kedvezményben részesül-e) tartalmazó táblázat. A dokumentum belső felhasználásra készült, ahhoz csak – felhasználónév és jelszó megadását követően – a nevelőtestületnek lehetett volna hozzáférése.

Az incidensről a Hatóság egy bejelentés alapján szerzett tudomást, az adatkezelő pedig legkésőbb a Hatóság végzésének készhevtelekor. Az adatkezelő azonban az esetet nem azonosította adatvédelmi incidensként, és az ezzel kapcsolatban fennálló, az általános adatvédelmi rendelet 33-34. cikkeiben rögzített kötelezettségeit sem teljesítette: nem végezte el az incidens kockázatainak elemzését, az adatvédelmi incidenst nem jelentette be a Hatóságnak, illetve a bejelentési kötelezettség alól kivételre sem hivatkozott. Emellett nem tett eleget azon kötelezettségének sem, mely alapján nyilván kell tartania az adatvédelmi incidenseket, feltüntetve az adatvédelmi incidenshez kapcsolódó tényeket, az incidens hatásait és az orvoslására tett intézkedéseket.

Hatórozatában a Hatóság megállapította, hogy a vizsgált adatvédelmi incidens magas kockázatúnak minősül, mivel az érintett személyes adatak jogosulatlan megismerése, nyilvánosságra hozatala azok jellegéből kifolyólag akár szociális hátrányt is eredményezhet, következésképpen az adatkezelő köteles lett volna tájékoztatni az érintetteket is haladéktalanul az adatvédelmi incidensről, az általános adatvédelmi rendelet 34. cikkében előírt tartalommal. Bár az adatkezelő az esetről egyébként értesítette az érintettek szüleit, illetve gondviselőit,

arra csak a tudomásszerzést követően több mint négy hónappal, és nem a rendeletben előírt tartalommal került sor. Szintén kockázatnövelő tényezőként került értékelésre, hogy az adatkezelő nem tudta megállapítani az incidens okát. A Hatóság az adatkezelő nyilatkozata alapján megállapította továbbá, hogy az nem alkotott külön szabályozást a bejelentkezést követően elérhető felület jogosultságaira vonatkozóan.

Az incidens értékelése során ugyanakkor a Hatóság enyhítő körülményként vette figyelembe a következőket:

- a) az eljárás során a Hatóságnak nem jutott tudomására olyan információ, amely arra utalna, hogy az érintetteket a jogszertés nyomán kár érte volna;
- b) a feltárt tényállásból arra lehet következtetni, hogy a jogszertés nem volt szándékos, azt az adatkezelő gondatlansága okozta;
- c) az adatkezelő első alkalommal sérтtette meg a személyes adatok kezelésére vonatkozó előírásokat;
- d) az adatkezelő a nyilvánosságra hozott listát a tudomásszerzést követően eltávolította a honlapjáról, ezáltal a bekövetkezett adatvédelmi incidens kockázatait orvosolta.

A fentebb vázlatosan ismertettek alapján a Hatóság határozatában megállapította, hogy az eljárás során feltárt jogszertések esetében a figyelmeztetés nem arányos és nem visszatartó erejű szankció, így – jelképes összegű – bírságot is kiszabott. (NAIH/2019/2238.)

2. Egy gyermekjóléti szerv egy munkatársa tévedésből 9 darab, személyes adatot tartalmazó dokumentumot tévesen egy hasonló feladatkörű, de más illetékes-ségi területű szociális intézmény részére postázott, így sérült az adatok bizalmas jellege. Az adatvédelmi incidens 18 személy (köztük kiskorúak is) következő személyes adatait érintette: azonosító adatok, elérhetőségi adatok, büntetett előélettel, bűncselekményekkel vagy büntetéssel, intézkedéssel kapcsolatos adatok, szociális azonosságra vonatkozó adatok, illetve az adatkezelő által folytatott, gyermekek védelmére irányuló eljárásokkal összefüggésben kezelt egyéb, a magánéletükre vonatkozó személyes adatok.

A téves címre történő postázás után öt nappal a téves címzett jelezte az esetet az adatkezelő felé, a küldemények pedig újabb nyolc nappal később érkeztek vissza hozzá. Az adatkezelő álláspontja szerint ekkor vált bizonyossá a téves postázás, így ezt az időpontot tekintette tudomásszerzésnek. Az adatvédelmi incidens Hatóság részére történő bejelentésére még ettől az időponttól számít-

va is több mint két héttel később került sor. Az adatkezelő azzal indokolta a késedelmes bejelentést, hogy a vezető beosztású tiszttviselője számára nem továbbították a visszaérkezett küldeményt, mivel időközben tartottak meg egy, az adatkezelő által szervezett rendezvényt, amelynek megrendezése az adatkezelő jogszabályban meghatározott alapfeladatának része; illetve a téves címzett maga is hasonló feladatokat ellátó, csak más illetékességgel rendelkező szerv. Az adatkezelő saját kockázatelemzése során még figyelembe vette, hogy bár az adatkör jelentős, azt csak kevesen, legfeljebb két személy ismerhette meg, aik titkotartásra kötelesek. Az elemzés eredményeként az adatkezelő megállapította, hogy az incidens közepes kockázatú, annak orvoslása céljából pedig ket-tős címzéskontrollt vezetett be, illetve intézkedett rendkívüli adatvédelmi oktatás megtartásáról, az érintettek tájékoztatását azonban nem tartotta szükségesnek.

A Hatóság a feltárt tényállás alapján arra a következtetésre jutott, hogy az incidens orvoslása az adatkezelő megfelelő intézkedéseket hozott, de az incidens bejelentésére nem került sor a GDPR által meghatározott határidőben. A Hatóság álláspontja szerint már akkor sor került az adatkezelő általi tudomás-szerzésre, amikor a téves címzett jelezte számára a téves címzés tényét. Ez alapján az adatkezelő tudomásszerzése és az adatvédelmi incidens bejelentése között 24 nap (az adatkezelő nyilatkozatában megjelölt időpont figyelembevétele esetén is 16 nap) telt el. A határozatában a Hatóság kötelezte az adatkezelőt, hogy tegye meg a szükséges intézkedéseket annak érdekében, hogy egy eset-leges jövőbeni adatvédelmi incidens bejelentése a rendeletben előírt határidőben megvalósuljon. A Hatóság a késedelem adatkezelő általi igazolását nem fogadta el: az incidens időben történő bejelentése előtt nem lehet akadály sem az, hogy az adatkezelőnek más jellegű kötelezettségei is vannak, sem az, hogy nem álltak rendelkezésre pontos információk, mivel a rendelet lehetővé teszi, hogy a bejelentésre szakaszosan kerüljön sor. A Hatóság hangsúlyozta azt is, hogy incidens észlelése esetén haladéktalanul értesíteni kell a megfelelő vezetési szinten lévő feletteset, hogy az incidenst kezelní és szükség szerint jelenteni lehessen.

A Hatóság továbbá figyelembe vette, hogy az adatkezelő az incidenssel kapcsolatos intézkedések megtételéről – így különösen a kockázatelemzésről – is csak késve intézkedett. Az incidens kezelése megkezdésének hiányában az incidensnek az egyes személyek jogait és szabadságait érintő tényleges kockázatai sem mérhetők fel kellőképpen, ami önmagában is kockázatot jelent.

- Enyhítő körülményként vette figyelembe a Hatóság, hogy
- a) amikor az incidenssel érintett szervezeti egység jelezte az esetet az adatkezelő adatvédelmi tisztviselője számára, akkor haladéktalanul megkezdte az incidenssel kapcsolatos kötelezettségek végrehajtását;
 - b) az incidens egy szervezeti egységnél történt gondatlan mulasztás eredménye, így a jogosítés nem vezethető vissza az adatkezelőnél fennálló rendszerintű problémára, illetve szándékosság gyanúja sem merül fel a jogosítéssel kapcsolatban;
 - c) az adatkezelő, bár nem indokolatlan késedelem nélkül, de bejelentette a Hatóság számára az adatvédelmi incidenst, és az egyéb, az adatvédelmi incidenst követően hozott intézkedéseiből is az következik, hogy általánosságban tisztában van az adatvédelmi incidens bekövetkezése esetén fennálló kötelezettségeivel.

A fentiek alapján a Hatóság szükségesnek tartotta bírság kiszabását.
(NAIH/2019/3854.)

3. Az adatvédelmi incidensek sok esetben a biztonsági intézkedések hiányára vagy a meglévő biztonsági intézkedések elégtelenségére vezethetők vissza, ezért döntő jelentősége van annak, hogy az incidensek lehetőség szerint megfelelő technikai és szervezési intézkedésekkel megelőzhetőek legyenek. A személyes adatok megfelelő biztonságát az adatkezelőknek a papíralapú adatkezelés során is biztosítania kell.

Egy egészségügyi intézmény egyik szakrendelőjéből egészségügyi dokumentáció részét képező ambuláns lapok eltűnésével valósult meg adatvédelmi incidens. Az incidensre valószínűsíthetően úgy került sor, hogy a takarítószemélyzet egyik tagja tévedésből hulladéknak tekintette az ambuláns lapokat tartalmazó irattartót, melyet az intézmény munkatársai a rendelő padlóján felejtettek. A dokumentumokban körülbelül 70 érintett személyes adatai, köztük egészségügyi adatok szerepeltek. Az adatvédelmi incidens fogalmának elemei közül csak az adatok elvesztése, az adatkezelő rendelkezése alól kikerülése valósult meg, az adatokhoz való jogosulatlan hozzáférésre vagy nyilvánosságra hozatalára utaló információ nem jutott az adatkezelő tudomására. Az adatkezelő az adatvédelmi incidens orvoslása céljából intézkedett a helyes dokumentációtárolási gyakorlat kialakításáról, illetve a személyes adatokat tartalmazó dokumentumok tárolására használt szekrények záratával és az irodai hulladéktárolás szabályainak betartásáról.

Az adatvédelmi incidens Hatóság felé történő bejelentésére csak akkor került sor, amikor megállapítást nyert, hogy az elveszett dokumentumok felkutatására irányuló vizsgálat nem vezetett eredményre, így az adatkezelő a bejelentési határidőt többszörösen túllépte. A Hatóság továbbá határozatában megállapította, hogy az érintettek incidensről való tájékoztatására sem került sor indokolatlan késedelem nélkül, és a tájékoztatás tartalma nem volt megfelelő. Az alkalmas szankció megállapításakor a Hatóság figyelembe vette továbbá, hogy az incidens a kezelt személyes adatok jellegéből, valamint az érintettek köréből fakadóan magasabb kockázatú, mivel azok jogosulatlan megismerése jelentős következménnyel járhat az érintettek számára. Ezek alapján az ügyben a Hatóság szükségesnek tartotta bírság kiszabását. (NAIH/2019/5743.)

4. Az incidens-bejelentő kórház egy védőnői szolgálat részére feladott, legfeljebb 10 várandós páciens laboratóriumi leletét tartalmazó postai küldeménye a Magyar Posta Zrt.-től sérülten, tartalom nélkül, műanyag tasakba csomagolva érkezett vissza az adatkezelő részére. Az adatkezelő a levelet nem könyvelt küldeményként adta fel. A postai küldeményben található személyes adatokat tartalmazó dokumentumok, laboratóriumi leletek elvesztek, megsemmisültek, azaz az eset az adatok véletlen megsemmisülését eredményezte. A leleteken a páciens neve, születési ideje, anyja neve, lakcíme, TAJ száma, illetve a laborvizsgálat eredményei szerepeltek. Az elveszett személyes adatok más forrásból is rendelkezésre álltak, az adatok rendelkezésre állása így tartósan nem sérült.

Az incidens bekövetkezésekor az adatkezelő minden postai küldemény postára adását kézbesítőkönyvben tartotta nyilván, de az incidens időpontjában olyan részletességű nyilvántartással nem rendelkezett, amelyből meg tudta volna állapítani, hogy az elveszett küldemény pontosan mely érintettek leleteit tartalmazta. Az adatkezelő nem tudta tájékoztatni az érintetteket, mivel a címzettel történő egyeztetés nem vezetett eredményre. Jövőbeli hasonló incidensek elkerülése végett az adatkezelő igazgatói utasításban intézkedett arról, hogy amennyiben egy lelet postai kézbesítése válik szükségessé, akkor azt ajánlott vagy tértive-vényes postai küldeményként kell feladni, illetve bevezetésre került egy nyilvántartás, amelyben a leleteket tartalmazó postai küldemények esetében rögzítésre kerül, hogy mely érintettek leleteit tartalmazza. A Hatóság az ellenőrzés során megállapította, hogy a feltárt körülmények alapján nem utal semmi sem arra, hogy sérült volna a személyes adatok bizalmas jellege, illetve a rendelkezésre állás sérült volna tartósan, a küldemény címzettjét értesítette az adatkezelő, így a rendelet 33-34. cikkeiben foglalt kötelezettségének eleget tett.

A rendelet 32. cikkében foglalt adatkezelés biztonsága kérdésben a Hatóság álláspontja szerint olyan dokumentumok továbbítása, amelyen teljesen beazonosítható módon szerepel az érintettek számos személyes adata – köztük egészségügyi adatok is – magasabb kockázatot jelenthet, amely szigorúbb intézkedéseket indokol az adatkezelő részéről. Az adatok biztonságát garantáló intézkedések meghatározása során az adatkezelőnek ezeket a magasabb kockázatokat figyelembe kellett volna vennie, és azokat úgy meghatározni, hogy garantálják azt, hogy a személyes adatokhoz jogosulatlan személyek ne férjenek hozzá, azok ne vesszenek el vagy semmisüljenek meg. Postai kézbesítés esetén a Posta szolgáltatásai közül az adatkezelőnek olyat kell igénybe venni, amely erre a célra alkalmas, például a könyvelt postai küldeményként történő feladást, amely esetében a Posta a címzett vagy az egyéb jogosult átvevő részére kézbesít.

A Hatóság álláspontja szerint tehát az incidens bekövetkezéskor az adatkezeléssel összefüggő intézkedések nem garantálták a kockázatokkal arányos adatbiztonságot, ezért a Hatóság megállapította, hogy az adatkezelő az incidenssel érintett adatkezelés vonatkozásában nem tett eleget a rendelet 32. cikke által előírt követelményeknek. (NAIH/2019/7998)

5. A Budapesti Rendőr-főkapitányság incidens bejelentése szerint egyik munkavállalója 2019. január 11-én, szolgálati feladatai ellátása során egy általa adattárolásra használt, 4 GB tárhellyel rendelkező pendrive-ot elveszített. Az adathordozón megtalálható volt a BRFK teljes nevesített személyzeti állománytáblája, továbbá a rendvédelmi szolgálati jogviszonyváltásra vonatkozó teljes személyügyi anyag elektronikus másolatban. Az adathordozó, valamint az azon található állományok semmilyen hozzáférés-védelemmel nem voltak ellátva, valamint a munkavállaló a dokumentumokat nem szolgálati, hanem magáncélra használt adathordozóra másolta át, hogy később a vezetői értekezleten részt vevő, munkáltatói jogkört gyakorló vezetők részére bemutassák. Az adathordozón található dokumentumokban 1733 érintett személy következő személyes adatai szerepeltek: születési név, születési idő, anyja neve, TAJ szám, beosztás, munkakör. Az adatkezelő munkavállalója az adathordozón nem alkalmazott semmilyen biztonsági intézkedést a tárolt adatokkal kapcsolatban, ezzel megszegve az adatkezelő Informatikai Biztonsági Szabályzatáról szóló 18/2018 (V.31) ORFK utasítást. Az adatkezelő nyilatkozata szerint bejelentés a pendrive megtalálásával, illetve az adatokkal való visszaéléssel kapcsolatban nem érkezett az adatkezelőhöz, az adatokhoz való jogosulatlan hozzáférés tényére utaló információ nem jutott az adatkezelő tudomására. Az adatkezelő valószínűsítette,

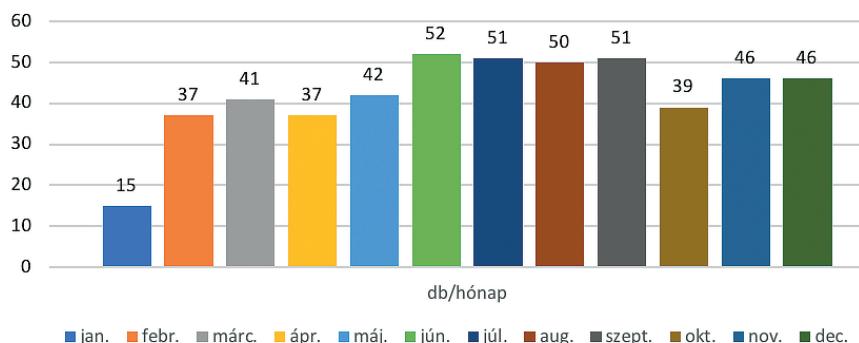
hogy az adathordozó az elveszítésének időpontjában fennálló időjárási körülmények miatt megsemmisült, így az adatok elveszítésén túl további biztonsági esemény nagy valószínűséggel nem történt.

A Hatóság az adatkezelővel egyetértett az incidens alapvetően kockázatos besorolásában, mert a pendrive-on tárolt adatok között megtalálhatóak voltak nem nyilvánosan hozzáférhető, illetve nem közérdekből nyilvános adatok is. A Hatóság kiemelte, hogy az adatvédelmi incidens fogalmának elemei közül csak az adatok elvesztése valósult meg jelen esetben, a további bizalmassági sérülésnek való kitettség kockázata azonban fennállt az ügyben, mivel az adathordozó és az azon tárolt adatok nem voltak semmilyen technikai intézkedéssel védve a jogosulatlan hozzáféréstől. A kockázatos adatvédelmi incidens bejelentésére nem került sor a rendelet 33. cikk (1) bekezdése által meghatározott határidőben. Az adatkezelő úgy nyilatkozott, hogy a pendrive elvesztésére valószínűleg 2019. január 11-én került sor, és aznap erről a munkavállaló rövid úton a szolgálati előlójáról is tájékoztatta, ezért a Hatóság megítélése szerint az adatkezelő általi hivatalos tudomásszerzésnek ez az időpont minősült. A Hatóság álláspontja szerint a tudomásszerzés idejének megítélése szempontjából elég, ha olyan érdemi ügyintéző/előlójáró tudomására jut az incidens bekövetkezésének ténye az adatkezelőnél, aki azt nem maga okozta, és akinek minden lehetősége és eszköze megvan a releváns döntéshozók, tisztviselő értesítésére.

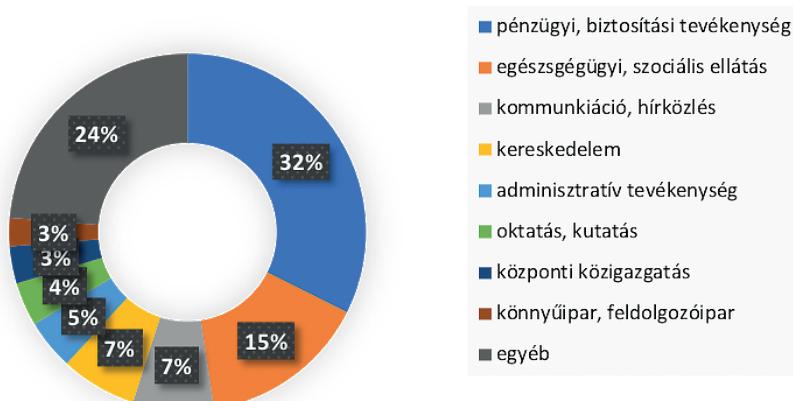
Az incidens-bejelentés késedelmes bejelentését az adatkezelő az eset teljes körű parancsnoki kivizsgálásával, valamint az ORFK-tól való állásfoglalás kérésével indokolta. A bejelentésre végül 2019. február 25-én került sor, mely alapján az incidensről való tudomásszerzés és a bejelentés között összesen 45 nap telt el, amely a rendelet által főszabályként előírt bejelentési határidő tizenötösrögs túllépését jelenti. A Hatóság nem fogadta el az adatkezelő indokait a határidő túllépére vonatkozóan, mert megítélése szerint az incidens kockázatértékeléséhez szükséges valamennyi tény és körülmény gyakorlatilag a pendrive valószínűsíthető elvesztése, a tudomásszerzés időpontja óta rendelkezésre állt. Az incidens időben történő bejelentése előtt az sem lehet akadály, ha nem állnak rendelkezésre pontos információk, mivel a Rendelet 33. cikk (4) bekezdése lehetséges, hogy a bejelentésre részletekben, szakaszosan kerüljön sor. Továbbá az adatkezelő adatvédelmi tisztviselőjének értesítése is bőven a tudomásszerzéstől számított 72 órán túl, 2019. január 28-án történt meg, mely elfogadhatatlan gyakorlatnak minősül a Hatóság szerint. A Hatóság továbbá megállapította, hogy az adatkezelő saját, belső utasításának rendelkezéseit sem tartotta be a kockázatértékelés, és az incidens-bejelentés vonatkozásában.

Az ismertettek alapján a Hatóság ötmillió forint adatvédelmi bírság megfizetésére kötelezte az adatkezelőt, és elrendelte a végleges határozatnak az adatkezelő azonosító adatainak közzétételével történő nyilvánosságra hozatalát. (NAIH/2019/2471)

*A 2019-ben bejelentett össz. 506 db incidens eloszlása
hónapok szerinti bontásban*



Incidensbejelentések megoszlása szektorok alapján 2019



II.3. Bíróság által felülvizsgált eljárások

A jelen beszámoló szerkesztésének időpontjában bírósági felülvizsgálat alatt álló ügyek közül a legérdekesebbeket ismertetjük.

1. Fesztiválokra történő beléptetés során végzett adatkezelés

A Hatóság adatvédelmi hatósági eljárásban (NAIH/2018/6248; NAIH/2019/55) vizsgálta a „Sziget” fesztivál és hasonló rendezvények beléptetés során folytatott adatkezelését. A Hatóság 2019 májusában hozott határozatában megállapította, hogy ezen rendezvényeken a beléptetés során végzett adatkezelés nem megfelelő jogalap alapján történt, illetve az nem felelt meg a célhoz kötött adatkezelés elvének, továbbá az érintettek nem kaptak megfelelő előzetes tájékoztatást a személyes adataik kezeléséről.

A Hatóság a 2018. május 25. napját követően végzett adatkezelés miatt harmincmillió forint adatvédelmi bírság megfizetését írta elő, továbbá elrendelte, hogy a beléptetés során végzett adatkezelését az adatkezelő hozza összhangba az általános adatvédelmi rendelet előírásaival.

A fesztivákat szervező gazdasági társaság a Hatóság határozatának bírósági felülvizsgálatát kezdeményezte, mert álláspontja szerint a Hatóság jogellenesen indította meg a hatósági eljárást, illetve a tényállást sem megfelelően tisztázta, így a Hatóság által meghozott határozat jogosítő.

A Fővárosi Törvényszék a Hatóság érvélését elfogadva a határozatot hatályában fenntartotta. Az adatkezelő a Kúria felülvizsgálatát kezdeményezte, mely eljárás még folyamatban van.

2. Az engedményezés jogalapjának bíróság általi megítélése

A követelésbehajtással foglalkozó vállalkozások gyakran hivatkoznak arra a Hatóság előtt, hogy az adósok személyes adatai kezelésének jogalapja a GDPR 6. cikk (1) bekezdés b) pontja szerinti szerződéses jogalap, mivel egy szerződésből eredtek azok a követelések, amelyeket később engedményezés útján megszereztek. A Hatóság megállapítása szerint a GDPR 6. cikk (1) bekezdés b) pontja szerinti jogalap – a szerződést kötést megelőző egyes lépések kivételevel – csak akkor alkalmazható, ha az adatkezelés a szerződés teljesítéséhez szükséges, tehát nem lehet kiterjeszteni ezt a jogalapot olyan adatkezelésekre, amelyekre a szerződés érintett általi nemteljesítése miatt előidézett helyzet or-

voslása érdekében, a szerződő felek rendes együttműködési kötelezettségből fakadó lépések megtételéhez van szükség. A szerződés teljesítése körébe eshetnek még azok a lépések, amikor az adatkezelő, aki a szerződést megkötötte az érintettel – tehát aki a szerződésben a másik fél – teljesítési késedelem esetén felszólítja az érintettet a teljesítésre. Azonban a GDPR 6. cikk (1) bekezdés b) pontja szerinti szerződéses jogalap már nem vonatkoztatható arra az esetre, ha az adatkezelő az elmaradt teljesítés miatt az érintettel szembeni követelését követelésbehajtással foglalkozó vállalkozásra engedményezi (azaz a problémát már a szerződésen kívül kívánja megoldani). Ilyenformán a követeléskezelő cégek és az adós között már szerződéses jogviszony nem áll fenn. Az engedményezés keretében történő adatátvétel jogalapja így csak más lehet, tipikusan az engedményes részéről a követelés saját részére történő érvényesítéséhez fűződő jogos érdeke.

A Ptk.-hoz fűzött indokolás szerint a követelések átruházására a tulajdonjog átruházásával azonos logika alapján kerül sor, tehát az engedményezés tulajdonképpen nem más, mint a követelés tulajdonjogának átruházása. Az engedményezéssel a követelés elválik az eredeti jogviszonytól, amelyből az származik, és az engedményes kizárolag a követelés és nem pedig az alapjogviszony vonatkozásában lép az engedményező helyébe. Azáltal, hogy az engedményezéssel a követelés elválik az alapjogviszonytól és az engedményes a követelés jogosultjává válik, a követelés engedményes általi érvényesítése, illetve az ahhoz kapcsolódó adatkezelés többé már nem azon szerződés teljesítése érdekében történik, amelyből a követelés eredetileg származott, mivel ebben az esetben az engedményesnek nem a saját, hanem az engedményező javára kellene érvényesíteni az engedményezés útján megszerzett követelést. Az engedményezéssel, amennyiben az ellenérték fejében történik, az engedményező kötelezettel szembeni követelése a vételár függvényében teljesen vagy részben megtérül. Az engedményes a követelés behajtása céljából saját érdekében és saját javára jár el, hiszen az engedményezéssel ő válik a követelés jogosultjává, és a követelés érvényesítése, az adósok teljesítésre bírása, valamint az ennek érdekében végzett adatkezelés az ő jogos érdekét, nem pedig az alapul fekvő szerződés teljesítését szolgálja. Mivel a követelés az engedményezéssel függetlenné vált a szerződéstől, az engedményezés útján követeléssel egyidejűleg megszerzett személyes adatok jogalapja nem lehet a GDPR 6. cikk (1) bekezdés b) pontja szerinti szerződéses jogalap.

A Hatóság ezen álláspontját a Fővárosi Törvényszék is megerősítette az ítéletében. Ez azonban nem feltétlenül jelenti azt, hogy az adósok személyes adatainak kezelésére nincsen jogalapja a követelésbehajtással foglalkozó vál-

lalkozásoknak. Amennyiben jogszabály által lehetővé tett követelésvásárlási tevékenységük keretében jutottak hozzá az adósok személyes adataihoz – természetes személyazonosító adatok, valamint a követelésre vonatkozó adatok –, úgy a jogoszerűen megszerzett követelések érvényesítéséhez, valamint az ehhez szükséges fenti adatok kezeléséhez fűződő jogos érdekének fennállta a jogi szabályozásból adódóan elvileg megállapítható. (NAIH/2019/2566)

3. Incidens-ügy a bíróság előtt

A Hatóság 2019. március 21-én kelt NAIH/2019/2668/2 számú határozatában megállapította egy politikai párt adatkezelővel szemben, hogy a párt egy általa kezelt, több mint 6000 érintett személy adatait tartalmazó adatbázist érintő adatvédelmi incidens vonatkozásában nem tett eleget a GDPR 33-34. cikkeiben foglalt incidens-bejelentési, nyilvántartásba vételi és az érintettek részére szóló tájékoztatási kötelezettségének. Ezért a Hatóság a pártot 11.000.000 Ft adatvédelmi bírsággal sújtotta.

A Hatóság az incidenssel kapcsolatos 2018. augusztusi közérdekű bejelentés alapján előbb hatósági ellenőrzést, majd később hatósági eljárást indított. A közérdekű bejelentés szerint egy hackerfórumon megtalálható volt egy olyan bejegyzés, amely a párt által üzemeltetett <http://web.dkp.hu> weboldalon található informatikai biztonsági (ún. SQLi) sérülékenységre hívja fel a figyelmet. A sérülékenységet kihasználva a bejegyzést író támadónak sikerült hozzáérnie egy adatbázishoz, amely a párt tagjainak és szímpatizánsainak számos személyes adatát tartalmazta (név, e-mail cím, felhasználó név, pártban betöltött funkció, gyengén titkosított jelszó). Az adatbázist a támadó publikálta a fórumon, továbbá elmondása alapján arra az adatkezelő figyelmét is felhívta. Az incident az adatkezelő azonban nem jelentette be a Hatósághoz és arról nem tájékoztatta az érintetteket sem.

A párt a hatósági eljárás során arra az álláspontra helyezkedett, hogy mivel a tárolt adatok már évek óta nem kerültek frissítésre, ezért azok elavultak és egy ilyen adatbázis nyilvánosságra kerülésével bekövetkező incident nem kell bejelenteni a felügyeleti hatóságnak és arról az érintetteket sem kell tájékoztatniuk. A Hatóság a határozatában az érintettek jogaira jelentett kockázat magas volta mellett érvelt, mivel az évek óta nem frissített adatokból is érzékeny következtetéseket lehet levonni a politikai véleményre, pártállásra. Ezen felül a gyenge jelszótitkosítás (MD5 algoritmus) használata is fokozott veszélyt jelenthet az érintettek magánszférájára nézve. A Hatóság ezért alkalmazandónak tekintette a GDPR incidenskezelésre vonatkozó előírásait a fenti esetre.

A párt a határozattal szemben bírósági felülvizsgálatot kezdeményezett a Fővárosi Közigazgatási és Munkaügyi Bíróság előtt. Keresetében arra hivatkozott, hogy mivel az incidenst kiváltó sérülékenység már a GDPR 2018. május 25-i alkalmazandó válása előtt (2018. áprilisától) fennállt, arra nem kell alkalmazni a rendelet adatvédelmi incidensek kezelésére vonatkozó előírásait. Ezen felül a bírság mértékének jogosságát is vitatta, annak arányossága, illetve a párt bevételi forrásainak figyelmen kívül hagyása miatt. A NAIH a kereset elutasítását kérte.

A bíróság elsőfokú ítéletében – a Hatóság álláspontját osztva – rámutatott arra, hogy a bekövetkezett adatvédelmi incidensre alkalmazni kell a GDPR incidenskezeléssel kapcsolatos előírásait, mivel a biztonsági sérülés az uniós rendelet alkalmazandóvá válása után is fennállt, illetve ekkor szerzett arról az adatkezelő párt is tudomást. A bírság mértékére vonatkozó szempontok újraértékelése kapcsán azonban az elsőfokú bíróság új eljárásra utasította a Hatóságot. Az elsőfokú nem jogerős ítélet ellen mind a felperes, mind a Hatóság fellebbezést nyújtott be a Kúriához mint másodfokú bírósághoz. A másodfokú eljárás 2020. év elején még folyamatban van.

4. A Hatóság bűnfüggelkívüli személyes adatok védelméhez fűződő jog megsértése tárgyában hozott határozatának kúriai felülvizsgálata

Egy újságíró egy levéltárban az adatkérő lapon a „[...], társa [...] – 1960” megjegyzést tüntette fel két ítélet megismerése vonatkozásában, amelyen a levéltár rögzítette, hogy „Csak támogatóival v. anonimizált másolatban adható ki.” A levéltár az elsőfokú bíróság ítéletéből tíz, a másodfokú bíróság ítéletéből három anonimizált oldalt bocsátott a kutató rendelkezésére. Ezt követően több médiafelületen arra vonatkozó cikkek jelentek meg, hogy az érintettet bűncselekmény elkövetése miatt jogerősen elítélték a hatvanas években.

A Hatóság a határozatában megállapította, hogy a levéltár jogellenesen biztosított hozzáférést az ítéletekhez és ezért hárommillió forint adatvédelmi bírság megfizetésére kötelezte. A Hatóság továbbá felszólította a levéltárat, hogy alakítsa ki olyan eljárási szabályokat, amelyek biztosítják a közokiratokról, a közlekedési szabályokról és a magánlevélzárti anyag védelméről szóló 1995. évi LXVI. törvény (a továbbiakban: Ltv.) 24. § (1) bekezdésének és (2) bekezdés a) pontjának megfelelő alkalmazását.

A Hatóság a határozata indokolásában kifejtette, hogy a levéltár nem teljesítette az Ltv. 24. § (2) bekezdés a) pontja szerinti kötelezettségét, mert nem ismerte fel, hogy az ítélet teljes egészében bűnügyi személyes adatnak minősül, mivel az elítélt személyek által elkövetett bűncselekményhez köthető információkat tartalmaz. A kutató az adatkérőlapon konkrét természetes személyeket jelölt meg, amely körülmény alapján a levéltárnak fel kellett volna ismernie, hogy a megjelölt személyekkel bármilyen anonimizálás mellett összefüggésbe hozhatók az ítéletek, így az Ltv. 24. § (2) bekezdés a) pontja szerinti anonimizálás nem lett volna alkalmazható. (NAIH/2016/2504/27/H)

A levéltár a határozat felülvizsgálatát kezdeményezte, mert álláspontja szerint helyesen alkalmazta a releváns jogszabályokat, mivel az ítéletek 1990 május 2-a előtt keletkeztek, nem esnek kutatási tilalom hatálya alá, így pedig anonimizálva a kutató rendelkezésére kellett bocsátania az ítéleteket, annak megtagadására az Ltv. 25. § b) pontja alapján nem volt lehetősége. A személyes adat minőség megállapításakor a szubjektív elem nem játszhat szerepet, az adat minősítése nem függhet attól, hogy az adott személy azt tudja-e meghatározott személyhez kötni vagy sem.

Az elsőfokú bíróság ítéletével a Hatóság határozatát hatályon kívül helyezte. Az elsőfokú bíróság szerint a hatósági értelmezésből az következik, hogy a levéltár a kutatói kérelmek elbírálása során a kutató rendelkezésére álló információk ismeretében tudná eldönteni, hogy a konkrét ítélet és az érintett között létrehozható, helyreállítható-e a kapcsolat vagy sem, azaz az anonimizált irat kiadható-e. Ilyen szubjektív tudattartalom vizsgálata azonban a kutatási kérelmek elbírálássát, és magát az anonimizálást tenné lehetetlenné. Az elsőfokú bíróság álláspontja szerint a személyes adat fogalma nem függhet a tudattartalomtól, azaz nem lehet különbséget tenni egy kutatási kérelem elbírálásakor aszerint, hogy a kutató milyen információval rendelkezik, mit tüntet fel a kérőlapon. A perbeli esetben az egyik érintett nevének megjelölése, annak gyakorisága folytán egy konkrét természetes személy azonosítására nem alkalmas, melynek következtében a Hatóság alaptalanul hivatkozott arra, hogy az érintett és az anonimizált másolatban kiadott ítéletek között a kapcsolat egy lépésben helyreállítható volt, melyet a levéltárnak fel kellett volna ismernie. A Hatóság olyan kiterjesztően értelmezte a személyes adat és a bűnügyi személyes adat fogalmát és minősítette a teljes ítéletet kizárolag az adott kutató adott kérelme szempontjából, azaz szubjektív tudattartalomtól függően bűnügyi személyes adatnak, amely értelmezés nem felel meg az Infotv. rendelkezéseinek. Az elsőfokú bíróság szerint az Ltv. 24. § (2) bekezdés a) pontjában foglalt anonimizálás megvalósíthatóságát a kutatás szempontjából kell értelmezni, azaz a kutatás anonimizált másolattal ak-

kor valósítható meg, ha az nem jár a szöveg sérelmével. (Fővárosi Közigazgatási és Munkaügyi Bíróság 13.K.32.793/2016/15)

A Hatóság az elsőfokú bíróság ítéletével szemben felülvizsgálati kérelmet terjesztett elő, mivel tévesnek tartotta az elsőfokú bíróság arra vonatkozó megállapítását, hogy a személyes adat fogalma nem függhet a tudattartalomtól, a kutató rendelkezésére álló információtól és az érintett neve nem alkalmas az azonosításra. A Hatóság – és az Adatvédelmi Munkacsoport személyes adat fogalmáról szóló 4/2007. számú véleménye – szerint a személyes adat minőséghez nem az kell, hogy mindenki azonosítani tudja az adott személyt, hanem elegendő, ha egy csoport képes az azonosításra, vagyis a szubjektív tudattartalom figyelembe veendő. Az adatkérő lapon a „[...], társa [...] – 1960” megjegyzés” szerepelt, tehát önmagában ebből megállapítható, hogy az azonosításra alkalmaság fennállt, hiszen nem pusztán egy gyakori személynévről volt szó, hanem két személy nevének és egy évszámnak a kombinációjáról. A Hatóság nem azt várja el, hogy egy levéltár minden esetben vizsgálja a kutató tudattartalmát. A Hatóság megállapításának lényege, hogy ha az adatkérő lapon valamely természetes személy azonosításához elégsges adattartalom kerül feltüntetésre, úgy hiába kerül az annak alapján kiadott dokumentumban bármilyen adat kitakarásra vagy törlésre, a fennmaradó kiadott információk a kitakarás ellenére kapcsolatba hozhatók lesznek az adatkérőlapon megjelölt személlyel, emiatt pedig az Ltv. szerinti anonimizálás ilyen esetben nem lehetséges. Ehhez a megállapításhoz nem volt szükséges a kutatónak kiadott kivonat részletes vizsgálata, hiszen kizárátható, hogy tizenhárom oldalon egyetlen adat vagy ténymegállapítás sem szerepelt volna. Tehát nem annak van jelentősége, hogy a kutató miről tudott, hanem annak, hogy az adatkérőlap tartalma lehetővé teszi-e meghatározott személyek azonosítását.

A levéltár az elsőfokú bíróság ítéletével szemben csatlakozó felülvizsgálati kérelmet, a Hatóság felülvizsgálati kérelmével szemben felülvizsgálati ellenkérelmet terjesztett elő. A csatlakozó felülvizsgálati kérelem szerint a Hatóság nem tett eleget tényfeltárási kötelezettségének, mivel elmulasztotta annak vizsgálatát, hogy az ítéletek kivonatolt részei személyes adatnak minősülnek-e.

A Kúria álláspontja szerint mind a felülvizsgálati kérelem, mind a csatlakozó felülvizsgálati kérelem alapos volt. A Kúriának abban az elvi kérdésben kellett állást foglalnia, hogy még élő természetes személyek bűnügyi személyes adatát tartalmazó büntetőítétek kutatása a védelmi idő lejárta előtt anonimizált másolattal megvalósulhat-e az Ltv. 24. § (2) bekezdés a) pontja alapján abban az

esetben, ha a kutató az ítéleteket az elítélték nevének és a bűncselekmény elkövetése évének feltüntetésével kéri ki.

A levéltár a védelmi idő ideje alatt a személyes adatot tartalmazó levéltári anyag kutatásának engedélyezése során a kutató által szolgáltatott információk (kutatói adatlap, adatkérő lap) és a kutatni kívánt levéltári anyag kutathatóságára vonatkozó törvényi előírások alapján dönti el, hogy a kutatás valamely kivételsszabály alapján engedélyezhető-e, vagy olyan törvényben meghatározott ok áll-e fenn, amelynek alapján a kérelem teljesítését meg kell tagadnia.

Az elsőfokú bíróság álláspontjával ellentétben, a kutatási kérelem elbírálásakor jelentősége van annak, hogy a kutatási kérelemben milyen adatok és információk szerepelnek, ugyanis, ha azok alapján az érintett azonosítható, akkor a levéltár bármennyire szakszerű és gondos anonimizálás mellett is bocsátja az ítéleteket a kutató rendelkezésére, a kutató a kutatni kívánt – személyes adatot tartalmazó – anyag tartalmát egy lépésben összefüggésbe tudja hozni a kérelemben megjelölt természetes személyvel. Ez ellentétes az anonimizált másolattal történő kutatás lehetőségét megteremteni kívánó jogalkotói céllal, így ilyen esetben az Ltv. 24. § (2) bekezdés a) pontja szerinti kutatás fogalmilag kizárt, következésképp nem engedélyezhető.

Helyes volt az elsőfokú bíróság arra vonatkozó megállapítása, hogy az érintett gyakori neve önmagában még nem elegendő az érintett azonosításához. Az adatkérő lapon azonban nem csupán az érintett neve, hanem egy büntetőügy két elítéltjének a neve és egy évszám kombinációja szerepelt. A Kúria a Hatóság döntésével megegyezően úgy ítélte meg, hogy ezek az információk már elegendő mértékük voltak az azonosításhoz, mivel a névhez kapcsolt további információk révén az érintett a többi azonos nevű személytől megkülönböztethetővé, ezáltal azonosíthatóvá vált.

A Hatóság nem a kutató tudattartalmának vizsgálatát várta el a levéltártól, hanem a kutatási kérelemben foglalt adatok alapján annak felismerését, hogy amennyiben a kutatási kérelemben valamely természetes személy azonosításához elegendő adattartalom kerül feltüntetésre, akkor a személyes adatot tartalmazó levéltári anyagban a védelmi idő fennállása alatt az anonimizált másolattal történő kutatás nem engedélyezhető.

A Kúria osztotta a Hatóság álláspontját abban, hogy a megítélendő jogkérdés szempontjából nem releváns, hogy milyen tartalmú anonimizált másolatot adott át a levéltár a kutatónak, mivel a perbeli esetben az anonimizált másolattal tör-

ténő kutatás engedélyezésére nem volt törvényes lehetőség. A jogszertés megállapításánál azonban kiemelt jelentőséggel bír, hogy a levéltár mit továbbított a kutatónak, jogszertést megállapítani csak a kutatónak ténylegesen átadott anonimizált másolatra vonatkozóan lehet. A Hatóság ezért e vonatkozásban nem tett eleget a tényállás-tisztázási kötelezettségének.

A felülvizsgálati eljárás során a Kúria megállapította, hogy az elsőfokú bíróság tévesen értelmezte az anyagi jogi szabályokat, ebből eredően a jogszertés hiányát illetően is téves következtetésre jutott, a tényállás-tisztázási kötelezettség Hatóság általi megszertését pedig tévesen hagyta figyelmen kívül. Tehát a Kúria az ügy érdemében a Hatóság álláspontját osztotta, a tényállás további tisztázása miatt pedig kötelezte új eljárás lefolytatására.

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

III.1. A személyes adatok Infotv. hatálya alá tartozó kezelésével kapcsolatos eljárások

A technikai fejlődés jelenleg tapasztalható és a belátható jövőbe extrapolálható tendenciái – például a képi megfigyelőrendszerök és a képi adattárolás költségeinek drasztikus csökkenése, a big data elemzési képességek fejlődése, a biometrikus adatkezelés és a mesterséges intelligencia alkalmazásának elterjedése, a mobil megfigyelésre alkalmas robotizált rendszerek (pl. drónok, robotjárművek) megjelenése –, valamint az ismertté vált fejlesztésekkel és tervezésekkel rendelkezésre álló információk alapján feltételezhető, hogy a jövőben az állami szervek az automatizált informatikai rendszerek révén egyre több helyszínen és egyre kifinomultabb módon lesznek képesek az érintettek magatartásának megfigyelésére, valamint ezzel kapcsolatban személyes adatok gyűjtésére.

A korábbi évekhez hasonlóan 2019-ben is azok a nagy informatikai rendszerek voltak a Hatóság figyelmének fókuszában, amelyek sok adatalannal összefüggésben tartalmaznak adatokat, országos léptékben működnek és rendszerint több adatkezelő szerv közreműködésével. Ilyen volt a korábbi beszámolóban említett, a megvalósítás egy közbenső fázisánál tartó „Szitakötő” projekt, vagy az okos városokban alkalmazandó újszerű szolgáltatások és megoldások előzetes tesztelése céljából megindított pilot projekt. A 2019-ben fókusza került adatkezelések közül több „kettős rendeltetésű”, azaz az elsődleges rendeltetésén túl van egy kevésbé ismert másodlagos, bűnüldözési vagy nemzetbiztonsági célja is.

III.1.1. A VÉDA rendszer

A VÉDA rendszert a rendőrség működteti. Elsődleges rendeltetése az, hogy technikai támogatást nyújtsa a közúti közlekedés szabályai betartásának rendőrség általi ellenőrzéséhez. A rendszer folyamatosan működő képfelvezői az ország közútjai felett, illetve mentén vannak elhelyezve. A kameráképek alapján automatizáltan történik a járművek rendszámának és más egyedi jellemzőinek felismerése, valamint a közlekedési szabályok megszegésének kiszűrése. Az adatokat – beleértve azon járművek adatait is, amelyek esetében a közúti

közlekedés szabályainak megszegésére utaló adat nem merült fel – harminc napig tárolják.

A Hatóság véleménye szerint a VÉDA rendszerrel végzett közlekedésrendészeti ellenőrzés legitim adatkezelési céllal bír, amelynek érvényesüléséhez társadalmi érdek fűződik. A rendelkezésére álló adatok alapján a rendőrség a közlekedésbiztonsági intézkedés jogi keretei között működteti a VÉDA rendszert, azonban kétség merült fel abban a tekintetben, hogy az országos kiterjedésű, automatizált adatgyűjtő rendszer alkalmazása megfeleltethető-e szabályoknak, ezért a Hatóság a helyzet tisztázása érdekében levélben kért további tájékoztatást a Belügyminisztérium közigazgatási államtitkárától. A jogi problémavezetés rámutatott, hogy a VÉDA rendszert az állampolgárok információs alapjogainak érvényesülése szempontjából vizsgálva az állapítható meg, hogy az adatvédelmi hatásprofilja több szempontból is eltér azokétől a rendőri intézkedésekkel (a továbbiakban: „klasszikus intézkedések”), amelyeknek az átfogó jogi szabályozására 1994-ben a Rendőrségről szóló 1994. évi XXXIV. törvényben (a továbbiakban: Rtv.) sor került. Főként a következő eltérések emelendők ki:

1. A klasszikus rendőri intézkedések során is sor kerülhet műszeres ellenőrzésre (pl. alkoholszonda, traffipax), azonban a VÉDA rendszerrel végzett technikai ellenőrzések kivételesek abból a szempontból, hogy az ellenőrzés helyszínén és az ellenőrzés időpontjában hiányzik a rendőrség személyes részvételle. Nincs személyes kontaktus az ellenőrzés alá vont személy és az ellenőrzést végző rendőr között, ezért esetleges, hogy az érintett tudomást szerez-e arról, hogy ellenőrzés alá vonták, továbbá arra sincs módja, hogy a tájékoztatási, hozzáférési és jogorvoslattal kapcsolatos jogait „*in situ*” gyakorolja.
2. Az ellenőrzés folyamata automatizált és a rendőrség részéről csak azon el-ellenőrzésekkel kapcsolatban kerül sor emberi tudomásszerzésre és döntéshozatalra, amelyeket a technikai rendszer potenciális szabályszegésként értékel. Kérdés, hogy ilyen körülmények között mennyiben tekinthető „*rendőri intézkedésnek*” az automatizált rendszer olyan mérése, amely során a gép által gyűjtött adatokat megőrizik ugyan, ám mivel azok nem utalnak közlekedési szabályszegésre, ezért nem is kerülnek emberi kiértékelésre. Ha az ilyen esetek rendőri intézkedésnek tekintendők, akkor például ki az intézkedő rendőr és mi az intézkedés helyszíne?
3. A VÉDA rendszerben párhuzamosan több helyszínen, folyamatosan történik az adatgyűjtés. Az automatizált adatkezelés csak minimális emberi felügyeletet igényel, ezért a klasszikus rendőri intézkedésekkel eltérően az élőmunka igény

nem hoz létre olyan szűk keresztmetszetet az adatgyűjtés és adatfelhasználás folyamatában, amely természetes határt szabna az ellenőrzési helyszínek számának növelésében, vagyis az állampolgárok rendőrség általi megfigyelésének kiterjesztésében.

4. Míg a klasszikus rendőri intézkedések adott helyszínhez köthetők, addig a VÉDA rendszer centralizált működésű: a sok helyszínről gyűjtött adatok tárolására és felhasználására központilag kerül sor, ezért adottak a technikai lehetőségek ahhoz, hogy a gyűjtött adatokat összekapcsolják egymással és más forrásból származó adatokkal. A VÉDA rendszer működése révén feltételezhetően országos léptékű, folyamatosan gyűlő, „big data” elemzésre alkalmas adattömeg jön létre, amelyből például járműhöz, illetve személyhez rendelt mozgásprofil és közlekedési szokásprofil hozható létre.

A VÉDA esetében nem vitatott a megfigyelés legitim célja, azonban a Hatóság szerint tisztázandó, hogy miként lehet egyensúlyt találni a megfigyeléshez fűződő közlekedésbiztonsági érdekek és a személyes adatok védelméhez, valamint a magánélet tiszteletben tartásához fűződő, az Alaptörvényben biztosított joguk érvényesülése között. Kulcsfontosságú a megfigyelőrendszerekre vonatkozó törvényi szabályozás jellege és tartalma, hiszen a jogi szabályozás jelölheti ki a technika alkalmazásának a kereteit. A VÉDA és a hasonló rendszerek kötelező adatkezelést valósítanak meg, ezért az érintett tájékoztatási és hozzáférési, valamint panasztételi jogára vonatkozó szabályok alkalmazása nem elégséges ahhoz, hogy gátat szabjon a túlzott mértékű adatgyűjtésnek. Az adatkezelésre vonatkozó szektorális szabályoknak kell meghatározniuk a személyes adatok védelmére vonatkozó specifikus garanciákat. A Belügyminisztérium a válaszában kifejezte a nyitottságát a VÉDA rendszerrel kapcsolatos adatvédelmi egyeztetés folytatására és szükség szerint a jogi szabályozás korrekciójára is. Az e tárgyban megkezdett konzultáció a beszámoló készítésekor még folyamatban van.

III.1.2. Az OIF arckép összehasonlítást elősegítő biometrikus alkalmazása.

A Hatóság bejelentés alapján vizsgálta az Országos Idegenrendészeti Főigazgatóság (a továbbiakban: OIF) informatikai rendszerét. Az OIF főigazgatójától kapott tájékoztatás értelmében az OIF által működtetett alkalmazás kizárolag állóképeken végez arcfelismerést és arckép-összehasonlítást, vagyis mozgóképeken, illetve kamera képfolyamokon nem. Az OIF a tevékenységére

vonatkozó ágazati törvények szerint kezel arckép adatokat, illetve az említett törvényekben előírtak szerint használja a hatáskörébe tartozó eljárások során rögzített arckép adatokat a személyazonosításhoz. Az arcképeket a körözési nyilvántartásból származó arcképekkel, valamint az Interpol, az Europol és az FBI közérdekből közzétett, vagyis nyilvánosan felhasználható, ezen szervek honlapján megtalálható, körözés alatt álló személyek arcképeivel is összehasonlítják az ismeretlen, vagy hamis személyazonosságú, illetve körözött személyek kiszűrése céljából. Az OIF rendszerének működése fél-automatikus, tehát ténylegesen nem személyazonosítást végez, hanem az összehasonlítandó arcképhez leginkább hasonló találatokat mutatja meg. A megjelenített találatok alapján az ügyintéző a magát igazolni nem tudó személyteljes szemben a szükségesnek ítélt intézkedést teszi meg, ezek megválasztásához járul hozzá az arckép-összehasonlítás eredménye.

A Hatóság megállapította, hogy az OIF eljárásaival érintett személyeknek tudomásuk van az arcképek elkészítéséről és felhasználásáról, vagyis az adatgyűjtés nem rejetten történik. Az OIF hatáskörébe tartozó eljárásokkal kapcsolatban azzal lehet számolni, hogy az érintett külföldiek egy része nem rendelkezik személyazonosító iratokkal és esetleg ellenérdekelt a valós személyazonosságának megállapítását illetően, ezért a személyazonosítás, illetve a személyazonosság ellenőrzés fél-automatikus gépi támogatása indokolt. A vizsgálat során nem jutott a Hatóság birtokába olyan információ, amely arra utalna, hogy az OIF nagy földrajzi területen folyamatosan működő, automatizált megfigyelést végző infrastruktúrát hozott volna létre. A gépi rendszerrel segített arckép-összehasonlítás, valamint az adatok hatósági célú felhasználása emberi munkát igényel. Az élőmunka igény olyan szük kereszmetszetet hoz létre az adatok felhasználásának folyamatában, amely kizára a tömeges, készletező jellegű biometrikus adatgyűjtést. A Hatóság az ügyben folytatott vizsgálatot lezártta, ugyanakkor kezdeményezte a Belügyminisztérium közigazgatási államtitkáránál olyan jogszabály-módosítás előkészítését, amely kifejezetten utal a külföldi bűnöldöző szervezetek által közzétett körözési adatokra az OIF adatforrásai között.

III.1.3. A rendőri igazoltatás során kiállított RK lap adattartalma

Az alapvető jogok biztosának a Magyarországon élő nemzetiségek jogainak védelmét ellátó biztos-helyettese egy sorozatos rendőri igazoltatással kapcsolatos, az Alapvető Jogok Biztosának Hivatalához érkezett állampolgári panasz kapcsán véleményt kért a Hatóságtól az Rtv., valamint a Rendőrség Szolgálati

Szabályzatának egyes, az igazoltatással kapcsolatos szabályairól. Az Rtv. szerint akkor kell az igazoltatott adatait rögzíteni, ha az további intézkedéshez, eljáráshoz szükséges, vagy egyéb körülmenyek ezt indokolják. Az adatok rögzítésére az ún. RK lap szolgál. Ugyanakkor a Szolgálati Szabályzat minden igazoltatás esetében előírja az igazoltatott személy és a bemutatott okmány adatainak ellenőrzését a Schengeni Információs Rendszerben, a körözési nyilvántartási rendszerben, valamint – szükség szerint a személyiadat- és lakcímnyilvántartásban vagy az okmány-nyilvántartásban. Az adatbázisból a lekérdezéseket dokumentálni szükséges, ezért a jelenlegi gyakorlat szerint minden igazoltatásról RK lapot töltenek ki, vagyis olyankor is sor kerül az érintett és a bemutatott okmány adatainak rögzítésére, ha az további intézkedéshez, eljáráshoz nem szükséges.

A Hatóság a válaszában emlékeztetett arra, hogy az Infotv. szerint személyes adat kizárolag egyértelműen meghatározott, jogoszerű célból, jog gyakorlása és kötelezettség teljesítése érdekében kezelhető. Az adatkezelésnek minden szakaszában meg kell felelnie az adatkezelés céljának, az adatok gyűjtésének és kezelésének tiszteességesnek és törvényesnek kell lennie. Csak olyan személyes adat kezelhető, amely az adatkezelés céljának megvalósulásához elengedhetetlen, a cél elérésére alkalmas. A személyes adat csak a cél megvalósulásához szükséges mértékben és ideig kezelhető. Az Infotv. 25/F. §-a automatizált adatkezelési rendszerek esetében elektronikus napló vezetését írja elő. Az Rtv. szerint a rendőrség által történő adatátvétel, valamint adatfelhasználás jogszerrűségéért az átvevő rendőri szerv vezetője tartozik felelősséggel. Az adattovábbítás tényét mind az adatátadó, mind az adatátvevő szervnél dokumentálni kell. Mindezek alapján a Hatóság megállapította a következőket:

A Szolgálati Szabályzat az igazoltatott személy és az általa bemutatott okmány háttérnyilvántartásból történő lekérdezéssel történő ellenőrzésének előírásával személyes adatok kötelező kezelését írja elő miniszteri rendeleti jogforrási szinten. Az Infotv. 5. § (1) bekezdés a) pontja szerint személyes adat kötelező kezelését törvény vagy – törvény felhatalmazása alapján, az abban meghatározott körben, különleges adatnak vagy bűnügyi személyes adatnak nem minősülő adat esetén – helyi önkormányzat rendelete közérdeken alapuló célból rendelheti el. Az Infotv. 5. § (3) bekezdése szerint kötelező adatkezelés esetén a kezelendő adatok fajtáit, az adatkezelés célját és feltételeit, az adatok megismérhetőségét, az adatkezelő személyét, valamint az adatkezelés időtartamát vagy szükségsége időszakos felülvizsgálatát az adatkezelést elrendelő törvény, illetve önkormányzati rendelet határozza meg. Az idézett törvényi szabályok értelmében a belügyminiszter rendelete nem írhat elő kötelező adatkezelést. Azonban azt is

figyelembe kell venni, hogy az Rtv. fentebb hivatkozott szabályai törvényi kere-
tet biztosítanak a rendőrség adatkezelésének, ide értve a rendőri intézkedés
során végzett adatkezelést és a háttérnyilvántartásokhoz való hozzáférést is.
Amint azt az Alkotmánybíróság vonatkozó AB határozatai kifejtik, nem az alapjо-
gokkal való bármifajta összefüggés esetén követelmény, hogy a szabályozandó
kérdésekről törvény rendelkezzen. Az alapjogokkal való közvetett és távoli ösz-
szefüggések szabályozására elegendő a rendeleti jogforrási szint is. Ezért az
igazoltatás során kötelezően elvégzendő nyilvántartás-lekérdezések Szolgálati
Szabályzatban történő előírása a jogforrási szint szempontjából elfogadható.
Ugyanakkor a Hatóság problematikusnak tartja, hogy a Szolgálati Szabályzat az
olyan igazoltatások esetében is kötelezően előírja a bűnuldözési szempontból
releváns háttérnyilvántartások lekérdezését, amikor nem bűnuldözési célból ke-
rül sor az igazoltatásra. Ilyen esetekben az adatok ellenőrzése nincs összhang-
ban az intézkedés törvényes céljával.

Amennyiben az igazoltatás során végzett lekérdezések szükségesek, úgy azo-
kat dokumentálni kell. A rendőrségi adatkezelő szervek és a rendőrség állo-
mányába tartozó, adatkezeléssel kapcsolatos feladatot ellátó munkatársak
felelősséggel tartoznak az általuk végzett adatkezelés jogoszerűségéért. Az
adatkezelő utólagos elszámoltathatóságának előfeltétele az adatkezelés – bele-
értve a nyilvántartás-lekérdezéseket – megfelelő dokumentálása. Az adatkeze-
lés dokumentálása a lekérdezéssel érintett személyek hozzáférési jogosultsága
érvényesítésének is előfeltétele. Tehát a személyes adatok lekérdezésének
dokumentálása szükséges, ám sem az Infotv., sem az Rtv. szabályai szerint
nem szükségszerű, hogy ez az RK lap kitöltésével történjen. Az adatkezelés
dokumentálására vonatkozó követelmények az Infotv. elektronikus napló vezetésre
vonatkozó szabályaiból [Infotv. 25/F. § (1) bekezdés], az érintett hozzáférési
jogának tartalmából (Infotv. 17. §), valamint az Rtv. 84. § (4) bekezdéséből
határozhatók meg. Ezt számba véve a Hatóság a készletező jellegű adatgyűjtést
elkerülendő indokoltnak tartotta felülvizsgálni a Szolgálati Szabályzat azon
pontját, amely a nem bűnuldözési célból végzett igazoltatások esetében is kö-
telezővé teszi a teljes háttérellenőrzést. Ezen kívül a Hatóság szorgalmazta az
igazoltatás dokumentálása informatikai támogatásának megvalósítását, amely
az adminisztratív teendők felgyorsításával mind az állampolgárok, mind az intéz-
kedő rendőrök számára előnyös lenne.

III.1.4. A fogvatartottak levelezésének ellenőrzése

A Hatóság állampolgári panasz alapján vizsgálta a Sátoraljaújhelyi Fegyház és Börtön (a továbbiakban: bv. intézet) levélküldemények kezelésével kapcsolatos adatkezelési gyakorlatát, amely szerint a fogvatartottak részére érkező leveleket a bv. intézet lefénymásolja és kizárálag a fénymásolatot adjá át a fogvatartottak számára. A levélküldemények eredeti példányát elzárva tartják, és ha a fogvatartott kéri, a látogatófogadás alkalmával átadják az általa megjelölt hozzátarozójának. Egyébként a bv. intézet elhagyásakor vagy szabaduláskor adják át számára a levélküldemény eredeti példányát. A bv. intézettől kapott tájékoztatás szerint azért volt szükség a levélküldemények kezelésének ilyetén kialakítására, mert korábban számos alkalommal azt tapasztalták, hogy az elítélték részére érkező levelek bódító, illetve kábító hatású anyaggal voltak átitatva, amelyet a fogvatartottak darabokra tépve elfogyasztottak, vagy cigarettába sodorták azokat.

A Hatóság elfogadta azt a magyarázatot, hogy a levélküldemények bv. intézet általi lemásolása és az eredeti levelek átmeneti visszatartása a fogvatartás rendjének fenntartását, továbbá az elítélték egészségi állapotának védelmét szolgálja, ugyanakkor rámutatott arra, hogy a levelek lemasolása, valamint az eredeti levélpéldányok elkülönített tárolása személyes adatok kötelező kezelésével jár, aminek összhangban kell lennie a kötelező adatkezelésre vonatkozó jogi szabályozási követelményekkel. Az Infotv. szerint a kötelező adatkezelés elrendelése törvényhozási tárgykörbe tartozik. Esetünkben a büntetések, az intézkedések, egyes kényszerintézkedések és a szabálysértési elzárás végrehajtásáról szóló 2013. évi CCXL. törvény (a továbbiakban: Btv.) tartalmazza a szektorális szabályokat. A Btv. 9. § (1) bekezdése rendelkezik az elítélték jogai gyakorlásának korlátozásáról. A Btv. 174. §-a tartalmazza a levelezés szabályait és annak korlátait. A részletszabályokat a 16/2014. (XII. 19.) IM rendelet (a továbbiakban: IM rendelet) határozza meg. Az említett jogforrások nem tartalmaznak a fogvatartottak leveleinek lemasolására és az eredeti példányok kezelésére vonatkozó szabályokat, ezért a Hatóság az Igazságügyi Minisztérium közigazgatási államtitkárának küldött állásfoglalásában szükségesnek láitta fent ismertetett, a kábítószerrel átitatott levélküldemények bv. intézetbe jutását megelőző küldeménykezelési gyakorlat, valamint az adatkezelés megfelelő dokumentálásának rendeleti szintű szabályozását, amely kizárálag a Btv. alapján felbontható és ellenőrizhető levélküldeményekre vonatkozhat. A nyilvántartásnak ki kellene terjednie legalább a levélküldemények egyedi azonosítójára, címzettjére, az utólagos átadás időpontjára és a levélküldemény átvevőjének azonosító adataira. Ha a levélküldeményt a fogvatartott kérése alapján a hozzátarozójának adják át, akkor a fogvatartott erre vonatkozó nyilatkozatát is meg kellene őrizni. A Hatóság

az adatminőség követelményére tekintettel annak előírását is javasolta, hogy a fogvatartottaknak átadandó levélmásolatok jól olvasható minőségen készüljenek. (NAIH/2019/5469.)

III.2. Az Infotv. hatálya alá tartozó adatkezeléseket érintő adatvédelmi incidensekkel kapcsolatos eljárások

III.2.1. A bűnüldözési, honvédelmi és nemzetbiztonsági adatkezeléseket érintő adatvédelmi incidensekkel kapcsolatos eljárások sajátosságai

A GDPR alkalmazandóvá válásával párhuzamosan az Infotv. joganyaga is kiengészült azokkal a szabályokkal, amelyek az Infotv. tárgyi hatálya alá tartozó bűnüldözési, honvédelmi és nemzetbiztonsági adatkezelésekkel összefüggésben értelmezik az adatvédelmi incidens fogalmát, valamint meghatározzák az adatvédelmi incidens kezelésének szabályait és a Hatóság ezzel kapcsolatos feladatait. A nemzeti szabályozás a bűnügyi adatvédelmi irányelv⁷ szabályait ülteti át. Jóllehet az Infotv. vonatkozó normaanyaga a szabályozás célját, valamint az alapvető jogintézményeket tekintve párhuzamos a GDPR adatvédelmi incidensekre vonatkozó szabályával, azonban a részletekben mutatkozó eltérések okán célszerű a Hatóság bűnüldözési, honvédelmi és nemzetbiztonsági adatkezeléseket érintő adatvédelmi incidensekkel kapcsolatos eljárásait külön tárgyalni. A nemzeti szabályozás sajátosságaival, valamint az Infotv. hatálya alá tartozó adatkezelések jellegéből adódó sajátosságokkal kapcsolatban a következők emelendők ki:

1. A bűnügyi adatvédelmi irányelv adatvédelmi incidensekkel kapcsolatos szabályainak általáltatási kötelezettsége csak a bűnüldözési célú adatkezelésekkel kapcsolatban áll fenn, ám a magyar törvényhozás – figyelembe véve az állam Alaptörvény I. cikk (1) bekezdésében előírt alapjogvédelmi kötelezettségét – az egységes adatvédelmi szabályozás érdekében úgy döntött, hogy az adatvédelmi incidensekkel kapcsolatos szabályok hatálya terjedjen ki a személyes adatok valamennyi, az Infotv. hatálya alá tartozó kezelésére. Ugyanakkor a szabályozás reflektál a nemzetbiztonsági szolgálatok tevékenységének titkosszolgálati jelleg-

7 az Európai Parlament és a Tanács (EU) 2016/680 Irányelv a személyes adatoknak az illetékes hatóságok által a bűncselekmények megelőzése, nyomozása, felderítése, a vádelpelrás 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

ére és a nemzetbiztonsági érdek érvényesítésének kiemelt prioritására, ezért a nemzetbiztonsági célú adatkezelések esetén – ha az nemzetbiztonsági érdekre tekintettel szükséges – a törvény lehetővé teszi, hogy az adatkezelő az érintett tájékoztatását, valamint a Hatóságnak történő bejelentést a nemzetbiztonsági érdek megszűnését követő időpontra halassza. [Az Infotv. a bünöldözési célú és a honvédelmi célú adatkezeléseket érintő incidensekkel kapcsolatban is megengedi, hogy törvény az érintett tájékoztatását a 16. § (3) bekezdésben foglalt feltételekkel és okokból kizárhassa, korlátozhassa vagy a tájékoztatás késleltetett teljesítését írja elő. Ez azonban nem érinti az adatkezelő Hatóság irányában fennálló bejelentési kötelezettségét.]

2. A bünügyi adatvédelmi irányelv 31. cikk (4) bekezdése szerint, ha az adatkezelő még nem értesítette az érintettet az adatvédelmi incidensről, a felügyeleti hatóság, miután mérlegelte, hogy az adatvédelmi incidens valószínűsíthetően magas kockázattal jár-e, elrendelheti az érintett tájékoztatását. Az Infotv. ezt oly módon ültette át a magyar jogrendbe, hogy nem az érintett tájékoztatásának elrendelésére hatalmazza fel a Hatóságot, hanem arra, hogy az adatvédelmi incidensről szóló bejelentés alapján megállapítsa, hogy az adatvédelmi incidens magas kockázata miatt az érintett tájékoztatása szükséges. Ám ez a lényeget tekintve ugyanarra az eredményre vezet, mint a bünügyi adatvédelmi irányelv 31. cikk (4) bekezdésében foglaltak, hiszen ha a Hatóság az előbb említett megállapítást közli az adatkezelővel, úgy az az Infotv. 25/K. § (4) bekezdése alapján köteles az érintettet tájékoztatni az adatvédelmi incidensről.

3. A bünöldözési, a honvédelmi és a nemzetbiztonsági célú adatkezelés jellegében sok tekintetben eltér azoktól a – jellemzően a gazdasági élet szereplői által végzett – adatkezelésekktől, amelyekkel kapcsolatban a GDPR határozza meg az adatvédelmi kereteket. Az előbbi adatkezelések esetében jellemzően állami szervek által végzett, kötelező adatkezelésről van szó, melyek esetében a vonatkozó magyar szektorális törvények meghatározzák az adatok kezelésének valamennyi lényeges elemét, ide értve például az adatok megőrzésének kereteit, az adatok továbbításának lehetséges útvonalait, valamint az érintettek jogait, illetve az érintett jogok korlátozásának feltételeit. E körülmények figyelembe vétele az adatvédelmi incidensek kockázatainak mérlegelésekor is szükséges. Az e körbe tartozó adatkezelések esetében egy adatvédelmi incidens nemcsak az érintett személy jogait és érdekeit sértheti, hanem egyúttal annak a – nyomós államérdeket megtestesítő – közfeladatnak az ellátását is, mely a személyes adatok kezelését szükségessé teszi. De a GDPR hatálya alá tartozó adatvédelmi incidensekkel összehasonlítva akár az is megemlíthető, hogy még egy gazdasági társaság által kezelt adatállomány esetében reális lehetőség, hogy illeték-

telenek azért próbálják megszerezni a társaság által kezelt személyes adatokat – például a vevők adatbázisát –, hogy azt direkt marketing célra vagy más gazdasági előny megszerzésére használják fel, a bűnuldözési, honvédelmi, vagy a nemzetbiztonsági célú adatkezelések esetében az ilyen jellegű veszély minimális, ezért az adatvédelmi incidens kockázatainak mérlegelésekor sokkal kisebb figyelmet érdemel.

III.2.2. A Hatóság bűnuldözési, honvédelmi és nemzetbiztonsági adatkezeléseket érintő adatvédelmi incidensekkel kapcsolatos eljárásainak tapasztalatai

A Hatóság által 2019-ben vizsgált közel két tucatnyi, az Infotv. hatálya alá tartozó adatkezeléseket érintő adatvédelmi incidenssel kapcsolatban a következők állapíthatók meg:

1. Az adatkezelők köre

A legtöbb bejelentés rendőri szervektől érkezett. Ez véleményünk szerint három okra vezethető vissza:

1. A rendőrség nagy létszámu, az egész országban jelen lévő szervezet, amely feladatainak ellátása során nagy szerepet kap a személyes adatok kezelése.
2. A rendőrségi adatkezelés jelentős hányada „terepmunka”, legyen szó például a rendőri intézkedésekéről vagy a házkutatásról stb. A bejelentések tapasztalatai szerint a külső helyszíneken fokozottan fennáll a lehetőség az adathordozók elvesztésére, vagy más, hasonló adatvédelmi incidens bekövetkezésére.
3. A rendőri szervek munkatársai fegyelmezetten látják el a feladataikat, továbbá a rendőrségi szervezeten belül erősek a kontrollmechanizmusok, ezért az esetleges adatvédelmi incidensek nem maradnak látenciában, hanem a vonatkozó jogszabályoknak megfelelően kezelik azokat, ide értve a Hatóságnak történő bejelentést is.

Területi megoszlásukat tekintve a rendőri szervek esetében Budapestről érkezett több bejelentés, de más megyék adatkezelői is jelentettek be incidenseket.

2. Az adatvédelmi incidensek okai

A vizsgált incidensek jellemzően szervezeten belüli, rosszhiszeműnek nem minősülő, gondatlan cselekmények voltak. Többnyire különböző adathordozók vét-

len (például a ruházatra rögzített tartóból kiesett az adathordozó, miközben a rendőr a bűnelkövetőt üldözte) vagy figyelmetlenségből történő elhagyása okozta az incidenseket. Előfordultak továbbá olyan esetek, amikor figyelmetlenségből ügyintézés, ügykezelés során kerültek továbbításra, hozzáférésre nem jogosult, harmadik személy számára személyes- és bűnügyi személyes adatok.

Egy esetben jelentett be az egyik rendőri szerv szervezetén belüli, rosszhiszeműnek minősülő cselekményt. Ezzel összefüggésben az adatkezelő büntetőfeljelentést is tett, az ügyészszég pedig hivatali visszaélés bűntett gyanúja miatt rendelt el nyomozást. Ez esetben az incidenst okozó személy jogosultságával visszaélve fert hozzá egy büntetőeljárással kapcsolatban kezelt személyes adatokhoz (köztük a gyanúsított személyes adataihoz), bűnügyi személyes adatokhoz. A jogosulatlan hozzáférés mellett felmerült a jogosulatlan felhasználás, az adatok harmadik személy részére történő továbbításának a gyanúja, ennek tiszta zása az ügyészszég által elrendelt nyomozás keretében történik.

3. Az adatvédelmi incidensekkel érintett adatok köre

Megállapítható, hogy a bejelentett incidenseknél az érintett adatfajták között zömében az érintettek személyazonosító adatai (név, természetes személyazonosító adatok, személyazonosításra alkalmas okmányok azonosító adatai, olykor azok másolata), lakcímadatok, továbbá a rendőri szerveknél bekövetkezett incidensek kapcsán a büntetőeljárásokkal kapcsolatos, bűnügyi személyes adatok (úgymint történeti tényállásban szereplő személyes adatok, vagy a büntetőeljárásban részt vevő személy eljárási pozícióját kifejező adat, esetleg az érintettel szemben tett rendőri intézkedésre utaló adatok) szerepelnek.

4. Az adatvédelmi incidens bejelentésének ideje

A tavalyi év során bejelentett, Infotv. hatálya alá tartozó adatkezeléssel összefüggő incidensbejelentések kapcsán elmondható, hogy az adatkezelők többnyire határidőben, azaz az incidens észlelését követő 72 órán belül teljesítették a bejelentési kötelezettségüket. Egy esetben hozzávetőlegesen egy nap késés sel történt meg a bejelentés. Előfordult továbbá olyan eset, hogy az adatkezelő nem megfelelően értelmezte az adatvédelmi incidensről történő tudomásszerzés időpontját. Ezzel kapcsolatban hangsúlyozandó, hogy a tudomásszerzés időpontjának nem az számít, hogy az adatkezelő szervezetén belül az adatvédelmi tisztviselőhöz mikor ért el az incidens bekövetkeztéről az információ,

azaz Ő mikor szerzett tudomást az incidensről. Ez csak abban az esetben esik egybe az adatkezelő által az incidensről való tudomásszerzés időpontjával, ha az incidenst maga az adatvédelmi tisztviselő észlelte. A Hatóság egy incidens kapcsán hozott határozatában kifejtette, hogy a tudomásszerzés idejének megítélése szempontjából az az irányadó, ha az adatkezelőnél olyan ügyintéző vagy elöljáró tudomására jut az adatvédelmi incidens bekövetkeztének ténye, aki azt nem maga okozta és minden lehetősége és eszköze megvolt a releváns döntéshozók, tisztviselő értesítésére. Innentől számított 72 óra áll az adatkezelő rendelkezésére, hogy az incidenst a Hatóságnak bejelentse.

5. Az incide ns orvoslására tett intézkedések

A Hatóság tapasztalata szerint az incide ns orvoslására tett intézkedések közzött az adatkezelők nagy hangsúlyt fektetnek az incidenst előidéző, adatkezelő személyi állományába tartozó személy felelősségre vonására. Az adatkezelő szempontjából természetesen az incide nsnek ez is velejárója. Adatvédelmi szempontból azonban az adatvédelmi incide nsből eredő esetleges hátrányos következmények mér séklését célzó és egyéb (például jövőbeli incide nsek meg előzését szolgáló) intézkedések relevánsak. Az adatkezelő személyi állományát érintően ilyen intézkedés lehet az adatvédelmi incide nsek elkerülését, bekövetkezett incide nsek gyors felismerését és a megfelelő intézkedések megtételét ismertető oktatás, figyelemfelhívás. Megjegyzendő, hogy általában ezeket is alkalmazzák az adatkezelők.

A Hatóság az incide nsek kapcsán azt is vizsgálja, hogy az incidenst megelőzően milyen intézkedések, eszközök szolgáltak az esetleges incide nsek megelőzésére, elkerülésére, továbbá, hogy az adatkezelő azonosított-e a működésében, munkafolyamataiban az incide n bekövetkezését lehetővé tevő hiányosságot. Amennyiben igen, tett-e intézkedéseket ezek kiküszöbölésére. Volt olyan példa, hogy az adatkezelő a bekövetkezett adatvédelmi incide n okán áttekintette az incide nssel érintett eljárásrendet, melynek eredményeként azonnali módosításra került a munkafolyamat rendje. A Hatóság ez esetben megállapította, hogy az adatkezelő szerv a munkafolyamat rendjébe épített adatvédelmi intézkedések révén, eljárását adatvédelmi szempontból megfelelően módosította.

Leginkább az iratkezelés folyamatára, a postázás során történő ellenőrzésre, az adathordozók megőrzésére, az azokon tárolt információk felülvizsgálatára vonatkozó előírások, intézkedések kerültek előtérbe, tekintettel arra, hogy a bejelentett incide nsek nagyrészt az adathordozók elhagyása vagy meghatározott

helyszínen hagyása, hozzáférésre nem jogosult személy részére történő megküldése tekintetében valósultak meg.

III.3. A Schengeni Információs Rendszer magyarországi ellenőrzése

III.3.1. A Schengeni Információs Rendszer

A Schengeni Információs Rendszer (SIS II) Európa egyik legnagyobb informatikai rendszere, amely a belső határok eltörléséből és a külső határok megszigorított ellenőrzéséből eredő biztonsági kockázatokat hivatott kezelni, elsősorban a hatékony adatmegosztás eszközével.

Az uniós szinten kiépített informatikai rendszer három részt foglal magába: központi rendszer, nemzeti rendszerek és kommunikációs infrastruktúra. A SIS II központi részének üzemeltetését az uniós EU-LISA Ügynökség látja el, míg a nemzeti részek üzemeltetéséért az egyes tagállamok felelnek. Magyarországon ezt a feladatot a Belügyminisztérium Nyilvántartások Vezetéséért Felelős Helyettes Államtitkársága (BM NYHÁT) – mint nemzeti N.SIS II Hivatal – látja el. A rendszerbe bevitt figyelmeztető jelzésekhez kapcsolódó kiegészítő információkat az Országos Rendőr-főkapitányságon működő SIRENE Iroda kezeli.

A SIS több tízmillió figyelmeztető jelzést (körözést) tartalmaz. A rendszerhez helyi szinten minden rendőr, valamint az adatokat a törvényes rend védelmével és a bűnuldözéssel kapcsolatos feladatai elvégzéséhez igénylő egyéb bűnuldöző hatóság és tiszttelviselő azonnali és közvetlen hozzáféréssel rendelkezik. A SIRENE irodák elsőlegesen a bűnügyi együttműködés szempontjából fontos adatok cseréjét bonyolítják, illetőleg koordinálják a határon átnyúló műveleteket. Ezen tevékenységük közben kiegészítő információkkal szolgálnak a figyelmeztető jelzésekkel kapcsolatban, valamint összehangolják a megfelelő intézkedéseket a SIS II-ben megjelenő figyelmeztető jelzésekre vonatkozóan.

A SIS II rendszer szigorú adatvédelmi szabályok alapján működik, amelyek betartását az Európai Adatvédelmi Biztos és a tagállami adatvédelmi hatóságok – Magyarországon a NAIH – rendszeresen ellenőrzik. Az adatokhoz való hozzáférés is korlátozott, azokhoz a szükséges és arányos mértékben, az uniós rendeletben és a nemzeti jogszabályokban megállapított célok érdekében a nemzeti

rendvédelmi, határőrizeti, vámügyi, igazságügyi, vízumrendészeti és gépjármű regisztrációs hatóságok férhetnek csak hozzá.

Az uniós és magyar adatvédelmi jogszabályoknak megfelelően mindenkinek joga van ahhoz, hogy kérelemre tájékoztatást kapjon arról, hogy a SIS II-ben milyen adatokat kezelnek róla, hogy a hibásan bevitt adat helyesbítését kérje, hogy a jogellenesen kezelt adat törlését kérje, illetve, hogy bírósághoz vagy az adatvédelmi hatósághoz forduljon személyes adataihoz fűződő jogainak védelme érdekében. Az érintetteknek jogában áll bármely schengeni tagállam nemzeti joga szerint illetékes hatóságához fordulni vagy bíróságához keresetet benyújtani. A rendszerbe bevitt adatok jog szerűségének vizsgálata azon tagállam nemzeti joga szerint történik, amely tagállamhoz a kérelmet benyújtja az érintett.

A magyar nemzeti jogszabály a Schengeni Információs Rendszer második generációja keretében történő információcseréről, továbbá egyes rendészeti tárgyú törvények ezzel, valamint a Magyar Egyszerűsítési Programmal összefüggő módosításáról szóló 2012. évi CLXXXI. törvény (a továbbiakban: SIS II tv.). A SIS II tv. szerint, ha bárki tájékoztatást kíván kapni arról, hogy adatai szerepelnek-e a SIS II-ben, vagy a SIS II-ben található adatok helyesbítését, törlését kéri, kérelmét benyújthatja – a meghatározott formanyomtatvány kitöltésével – bármely kormányhivatalban, rendőrkapitányságon, illetve magyar külképviseleten. A kérelmeket első fokon a SIRENE Iroda bírálja el, aki a kért tájékoztatást a nemzetbiztonság, a bűncselekmények megelőzése vagy üldözése, a büntetés-véghajtás biztonsága, továbbá mások jogainak védelme érdekében megtagadhatja. A SIRENE Iroda tájékoztatni köteles a kérelmezőt a tájékoztatásadás megtagadásának tényéről, jogalapjáról és a rendelkezésére álló jogorvoslati lehetőségekről.

III.3.2. Schengeni monitoring és értékelési mechanizmus

A Tanács 1053/2013/EU rendelete szabályozza a schengeni vívmányok alkalmazását ellenőrző értékelési és monitoring mechanizmust. Az értékelési mechanizmus célja a schengeni vívmányok – adatvédelem, külső határok, rendőri együttműködés, visszatérés, Schengeni Információs Rendszer, valamint vízumpolitika terén történő – alkalmazásának ellenőrzése a Schengeni térség tagállamaiban. A tagállamok és a Bizottság együttesen felelnek az értékelési mechanizmus véghajtásáért, azonban a Bizottság koordinálja az éves és többéves értékelési programok kialakítását, a kérdőívhöz és a látogatások idő-

beosztásának összeállítását, a látogatások lebonyolítását, valamint az értékelő jelentések és az ajánlások megszövegezését. Az értékelésekre kérdőívek és – előre bejelentett vagy be nem jelentett – helyszíni látogatások formájában kerül sor. Az előre bejelentett helyszíni látogatásokat minden esetben kérdőív kitöltése előzi meg.

1. Többéves értékelési program

A Bizottság ötéves időszakra szóló értékelési programot állít össze, legkésőbb hat hónappal a következő ötéves időszak kezdete előtt. A többéves értékelési programok tárgyát képező minden ötéves időszak során valamennyi schengeni tagállamot értékelni kell, minden évre vonatkozóan meghatározva az adott évben értékelendő tagállamok listáját.

2. Helyszíni látogatások és kérdőív

A helyszíni látogatásokért felelős csoportok a tagállamok által kijelölt szakértőkből és a Bizottság képviselőiből állnak. A résztvevő tagállami szakértők száma nyolc fő, a bizottsági szakértők száma maximum két fő lehet. A helyszíni csoportok vezető szakértőinek szerepét az egyik bizottsági képviselő és az egyik tagállami szakértő tölti be. A Bizottság felkérheti a Frontexet, az Europolt vagy az Európai Adatvédelmi Biztost (EDPS), hogy jelöljenek ki egy képviselőt, aki megfigyelőként részt vesz a helyszíni látogatáson. A Bizottság a tagállamokkal együttműködésben szabványkérdővet készít, amelyben ki kell térni a vonatkozó jogszabályokra, a schengeni katalógusban szereplő közösen elfogadott ajánlásokra és legjobb gyakorlatokra, a schengeni vívmányok végrehajtása tekintetében rendelkezésre álló szervezeti és technikai eszközökre, továbbá a statisztikai adatokra. A Bizottság minden év július 1-jéig megküldi a kérdőivet a következő évben értékelendő tagállamoknak, akik a kérdőív készhevítelétől számított nyolc héten belül megküldik válaszaikat a Bizottságnak.

3. Értékelő jelentések és ajánlások

A helyszíni csoport az értékelést követően értékelő jelentést készít, amelynek a látogatás során tett megállapításokon és a kérdőívre adott válaszokon kell alapulnia. Az értékelő jelentésben tett megállapításokat három fokozat szerint kell értékelni: 1) az értékelt tagállam eleget tesz az előírásoknak, 2) eleget tesz az előírásoknak, de az értékelt terület fejlesztésre szorul, 3) az értékelt tagállam

nem tesz eleget az előírásoknak. A Bizottság a helyszíni látogatást követő hat héten belül megküldi az értékelő jelentés tervezetét az értékelt tagállamnak, amely a tervezet kézhezvételét követő két héten belül észrevételeket tehet. A Bizottság a többi tagállammal történő egyeztetést követően fogadja el az értékelő jelentést, amelyet továbbít az Európai Parlamentnek.

Az értékelést végző szakértők ajánlásokat fogalmaznak meg az értékelő jelen-tésben az értékelés során azonosított esetleges hiányosságok kiküszöbölése céljából hozandó intézkedésekre vonatkozóan. Az ajánlások elfogadásától számított három hónapon belül az értékelt tagállam a Bizottság és a Tanács ren-delkezésére bocsátja az értékelő jelentésben feltárt hiányosságok korrekciója céljából készített cselekvési tervet. A feltárt hiányosságok súlyosságától és az orvoslásukra foganatosított intézkedések től függően a Bizottság előirányozhatja az előre bejelentett helyszíni látogatások megismétlését a cselekvési terv vég-rehajtásának ellenőrzése érdekében.

4. Magyar szakértők részvétete a Schengeni ellenőrzéseken

A tagállamok és a Bizottság együttesen felelnek az értékelési és monitoring mechanizmus végrehajtásáért, ami a gyakorlatban azt jelenti, hogy a helyszíni látogatásokért felelős csoportok a tagállamok által kijelölt szakértőkből és a Bizottság képviselőiből állnak. A tagállamok tehát kötelesek aktívan közreműködni, szakértőt kijelölni az értékelést végző csoportokba. Az adatvédelmi tárgyú schengeni ellenőrzéseken ennek megfelelően szakértőként részt vesznek a Hatóság munkatársai is. 2019-ben Csehország adatvédelmi tárgyú schengeni ellenőrzésén vett részt a Hatóság egyik munkatársa.

5. Magyarország adatvédelmi tárgyú Schengeni ellenőrzése

Magyarország Schengeni ellenőrzésére a Schengeni monitoring és értékelési mechanizmus 2014-2019 időszakára szóló értékelési program végén, 2019 őszén került sor. A 2019. október 7-11. között lefolytatott adatvédelmi tárgyú helyszíni ellenőrzés során a Bizottság képviselője és a tagállamok által kijelölt adatvédelmi szakértők meglátogatták a Hatóságot, mint az uniós és nemzeti – különösen a SIS II-vel és a vízumeljárásokkal kapcsolatos – adatvédelmi jog-szabályok megfelelő végrehajtásának felügyeletéért felelős illetékes nemzeti adatvédelmi hatóságot. A Hatóság munkatársai bemutatták a vonatkozó nemzeti szabályozást, előadást tartottak a Hatóság szervezetéről, hatásköreiől rész-

letezve a Hatóság függetlenségét biztosító jogi szabályozási, költségvetési és egyéb garanciákat. Bemutatták a Hatóság felügyeleti tevékenységét, ismertették a Schengeni Információs Rendszerhez, valamint a Vízuminformációs rendszerhez hozzáféréssel rendelkező szerveknél elvégzett adatvédelmi ellenőrzések eredményét. Ismertették továbbá az érintett jogok gyakorlásának menetét, a Hatósághoz érkező beadványokkal kapcsolatos ügystatistikát, a Hatóság honlapján és ügyfélszolgálati helyiségeiben elhelyezett információnyújtást szolgáló anyagokat, valamint a tagállami társhatóságokkal folytatott nemzetközi együttműködést is.

A helyszíni ellenőrzési program következő részeként ellátogatott a delegáció a Belügyminisztérium Nyilvántartások Vezetéséért Felelős Helyettes Államtitkárságán működő N.SIS II Hivatalhoz mint a SIS II nemzeti részének üzemeltetéséért felelős szervhez. A Hivatal munkatársai bemutatták a Hivatal tevékenységét, majd az üzemeltetésért és fejlesztésért felelős külsős cégek képviseletében jelen lévő kollégák előadásaira került sor, végül a delegáció meglátogatta az NS.CP szervernek és nemzeti interfésznek helyet adó szervertermet is. Az ellenőrzés ezután a SIRENE Irodánál mint a SIS II irányításáért, valamint annak bűnöldözési célú használatáért felelős illetékes hatóságnál folytatódott. A Teve utcában az Országos Rendőr-főkapitányság adatvédelmi tisztviselője tartott előadást, majd a SIRENE Iroda vezetője mutatta be a szervezet működését, feladatait és tevékenységük jogszabályi háttérét. A delegáció megtekintette a BRFK tevékenységirányító központját, valamint tett egy rövid látogatást a XIII. Kerületi Rendőrkapitányságon is. A program a Külügazdasági és Külügymenisztériumnál, valamint az Országos Idegenrendészeti Főigazgatóságon mint a Vízuminformációs rendszerhez hozzáféréssel rendelkező, valamint a vízumeljárások terén illetékes hatóságoknál folytatódott. A Külügazdasági és Külügymenisztérium Konzuli Szolgálatának bemutatkozása, valamint az adatvédelmi tisztviselő, a Konzuli Információs Rendszert üzemeltető szervezeti egység és a fejlesztők előadása után, a helyszíni ellenőrzést végző csoport a Külügazdasági és Külügymenisztérium központi szervertermét is megtekintette. Végül az Országos Idegenrendészeti Főigazgatósághoz is ellátogatott a delegáció, ahol bemutatásra került a nemzeti vízuminformációs rendszer architektúrája, üzemeltetése és fejlesztése. Szó esett az Informatikai Főosztály kapcsolódó feladatairól, az adatbiztonsági szabályzatnak való megfelelésről és a vízumügyekkel kapcsolatos idegenrendészeti eljárásokról.

A Főigazgatóság Schengeni Együttműködési Osztályának munkatársa ismerte a Schengeni Információs Rendszerrel összefüggésben végzett adatkezeléssel kapcsolatos feladataikat, a társhatóságokkal és a SIRENE Irodával

folytatott együttműködésüket, az érintett jogok gyakorlásának módjait, valamint a Főigazgatósághoz érkező kérelmek kezelésének menetét és a vonatkozó statisztikai adatokat. A program zárásaként sor került egy utolsó közös egyeztetésre a helyszíni ellenőrzést végző szakértői csoport tagjai és az összes érintett szerv képviselőjének részvételével, ahol lehetőség volt a fennmaradó kérdések tisztázására, és a Hatóság munkatársai megköszönhették mindenkinél az audit alatt nyújtott segítő együttműködést. A helyszíni ellenőrzésről a Bizottság munkatársa és a szakértői csoport elkészít az értékelő jelentés tervezetét, melyet megküld az értékelt tagállam Hatóságának. Az ellenőrzésben résztvevő szerzők észrevételeit tehetnek az értékelő jelentés tervezetben foglaltakat illetően. Magyarország adatvédelmi tárgyú Schengeni értékelése, vagyis az ellenőrzés tapasztalatainak összegzése és a jelentéstervezet véglegesítése jelenleg is folyamatban van.

6. Az értékelési és monitoring mechanizmus felülvizsgálata folytán történt változások

A Bizottság összegezte az elmúlt időszakban (2014. november – 2019. december) elvégzett Schengeni ellenőrzések tapasztalatait, valamint felülvizsgálta az ellenőrzéshez használt szabványkérdőívet, és a tapasztalatok alapján módosította azt. Az új schengeni ellenőrzési kérdőív elfogadását megelőzte egy konzultációs folyamat, amelynek keretében a schengeni tagállamok észrevételeket tehettek az új kérdőívvel kapcsolatban. A módosításokkal az volt a cél, hogy gyorsítsák az értékelési folyamatot, gördülékenyebben menjen a gyakorlati kivitelezés, mind a helyszíni ellenőrzések, mind az utómunka tekintetében. A Bizottság összegyűjtötte az elmúlt öt évben előforduló leggyakoribb hibákat, hiányosságokat, valamint a példaként szolgáló jó gyakorlatokat is. A Schengeni Információs Rendszer koordinált adatvédelmi felügyeletét ellátó ún. SIS Coordinated Supervision Group a feltárt jó gyakorlatokból készít egy listát, hogy segítse az ellenőrzés előtt álló tagállamok sikeres felkészülését.

III.4. Részvétel az adatvédelmi hatóságok közös felügyeleti tevékenységében

III.4.1. Határok, Utazás és Bűnüldözés Szakértői Csoport (Borders, Travel and Law Enforcement Expert Group – BTLE)

A BTLE szakértői csoport mandátumot kapott az év elején a bűnügyi adatvédelmi irányelv 47. cikkéhez kapcsolódó iránymutatás elkészítésére, amely munka jelenleg is folyamatban van. A csoport emellett kidolgozta a szabadságon, biztonságon és jog érvényesülésen alapuló térség nagyméretű IT-rendszereinek ellenőrzési módszereit. 2019 decemberében, Brüsszelben megtartotta alakuló ülését az információs rendszerek közös felügyeletet ellátó bizottság (Coordinated Supervision Committee - CSC). A CSC feladatai között szerepel az információcsere, az ellenőrzések, vizsgálatok végzése, az 1725/2018/EK rendelettel kapcsolatos alkalmazási és értelmezési kérdések megvitatása, az adatai lanyok jogaival kapcsolatos problémák megoldása, valamint egyéb összhangolt megoldások kidolgozása. A szakértői csoportot 2019 áprilisában azzal kereste meg a LIBE Bizottság, hogy az Európai Unió információs rendszereit érintő jogszabály-módosítások⁸ kapcsán az Európai Adatvédelmi Testület (EDPB) állásfoglalását kérje. Az EDPB válaszában ismét kifejtette a már korábban is megfogalmazott aggályait az új rendszerrel – vagyis a különböző információs rendszerek összekötésével – kapcsolatban. A csoport a fentiekben túl megtárgyalta és előkészítette az Adatvédelmi Pajzs (Privacy Shield) Egyezmény harmadik éves felülvizsgálatáról szóló Európai Adatvédelmi Testület által írt je lentésnek a nemzetbiztonsági és bűnüldözési célú adatkezeléssel kapcsolatos részét. Ezzel összefüggésben a szakértői csoport megvitatta az Európai Központi Testület (EUCB) eljárásrendjét. A Privacy Shield Egyezmény értelmében ugyanis a mechanizmus felügyeletét ellátó ombudsman eljárásának egy fontos eleme, hogy a kapcsolattartó szerepet betöltő EUCB továbbítja az uniós állampolgárok panaszait az ombudsmannak. A szakértői csoport tervezett feladatain túl felmerült az utasinformációs adatoknak (PNR adatok) az Egyesült Királyságnak az Európai Unióból történő kilépését (Brexit) követő kezelésével

⁸ az Európai Parlament és a Tanács 2017. november 30-i (EU) 2017/2226 rendelete a tagállamok külső határait átlépő harmadik országbeli állampolgárok belépéserére és kilépésére, valamint beléptetésének megtagadására vonatkozó adatok rögzítésére szolgáló határegisztrációs rendszer (EES) létrehozásáról és az EES-hez való bűnüldözési célú hozzáférés feltételeinek meghatározásáról, valamint az Európai Parlament és a Tanács 2018. szeptember 12-i (EU) 2018/1240 rendelete az Európai Utasinformációs és Engedélyezési Rendszer (ETIAS) létrehozásáról, és a 2018/1241 rendelet az Europol rendelet módosításáról

kapcsolatos kérdés is. Néhány tagállami hatóság arról számolt be, hogy megke-resték őket az egyes légi fuvarozók és állásfoglalást kértek arra vonatkozólag, hogy a Brexit után mi lesz a jogosító eljárás a PNR adatok továbbítását (és úgy általában a PNR adatok kezelését) illetően az Egyesült Királyság vonatkozásá-ban. A szakértői csoport hasznosnak tartana egy közös állásfoglalást kiadni, de erre majd csak a Brexit-tel kapcsolatos nyitott jogi kérdések lezárását követően kerülhet sor.

III.4.2. A Schengeni Információs Rendszer adatvédelmét felügyelő munkacsoport (SIS II SCG)

A 2013. április 9-én hatályba lépett Schengeni Információs Rendszer második generációjának (SIS II) létrehozásáról, működtetéséről és használatáról szóló 1987/2006/EK számú európai parlamenti és tanácsi rendelet alapján működő koordinációs ellenőrző csoport (Supervision Coordination Group) 2019-ben is folytatta munkáját.

A munkacsoport a SIS II Rendelet 24-es cikke⁹ szerinti figyelmeztető jelzések bevitelének kritériumaival kapcsolatban összeállított egy kérdőívet a tagállamok eljárásai közötti különbségek felmérésére. A munkacsoport célul tűzte ki a SIS II Határozat 36. cikke¹⁰ alapján a személyekre és tárgyakra vonatkozóan rejtett ellenőrzés vagy célzott ellenőrzés céljából kiadott figyelmeztető jelzések keze-lésének vizsgálatát is. A munkacsoport megvitatta és elfogadta a következő idő-szakra (2019-2021) vonatkozóan összeállított munkatervét, amely a fentieken túl tartalmazza az egyes tagállami N.SIS Hivatalokkal szerződésben álló – jel-lemezűen technikai, üzemeltetési feladatokat ellátó – külső szolgáltatók munka-végzésének monitorozását, az adatvédelmi szempontoknak történő megfelelés érdekében. A munkacsoport a jogszabályi változásoknak megfelelően frissíti a – weboldalon elérhető – hozzáférési jog gyakorlásáról szóló tájékoztatóját és megvizsgálja az egyes tagállamok hozzáférési kérelmek kezelését érintő eljá-rását, különös tekintettel a kérelmet benyújtó érintett személyazonosságának ellenőrzésére. A munkaterv tartalmazza még az arcfelismerő rendszerek hasz-nálatáról szóló kérdés megvitatását, valamint a különböző tagállamok által a

9 Az Európai Parlament és Tanács 2006. december 20-i 1987/2006/EK Rendelete a Schengeni Információs Rendszer második generációjának (SIS II) létrehozásáról, működéséről és használatáról.

24 cikk: A beutazás vagy tartózkodás megtagadása esetén kiadandó figyelmeztető jelzés feltételei

10 A Tanács 2007. június 12-i 2007/533/IB Határozata a Schengeni Információs Rendszer második generációjának (SIS II) létrehozásáról, működéséről és használatáról. 36. cikk: A figyelmeztető jelzések kiadásának céljai és feltételei

Schengeni ellenőrzések kapcsán kapott leggyakoribb ajánlások közös összegyűjtését, amely a jövőbeni ellenőrzésekre való hatékony felkészülést szolgálja.

A Schengeni Információs Rendszert üzemeltető eu-LISA adatvédelmi tisztselője tájékoztatta a munkacsoportot, hogy az eu-LISA központilag frissítette a transzliterációs sztenderdeket, aminek eredményeként a rendszer könnyebben kezeli a különböző írásmódokból fakadó problémákat.

2019. december 3-án Brüsszelben került sor a koordinált felügyeletet ellátó bizottság (Coordinated Supervision Committee) alakuló ülésére. A bizottság létrehozásának alapvető célja, hogy a szabadságon, biztonságon és jog érvényesülésen alapuló térség nagyméretű IT-rendszereinek koordinált felügyeletét ellátó munkacsoportok rugalmasan alakíthassák a munkarendjüket. A 1725/2018/EK¹¹ rendelet (GDPR) 62. cikke szól a felügyeleti hatóságok összehangolt műveleteiről. Az első ilyen koordinált felügyeletet megvalósító rendszer, amely létrejött az Európai Adatvédelmi Testület egisze alatt, az IMI rendszer, melyet az Eurojust (2019) követett. A többi koordinált ellenőrzést folytató csoport (SIS II, VIS, Eurodac) átalakulása, illetve (EES, ETIAS, ECRIS-TCN) megalakulása folyamatban van.

A Hatósághoz 2019-ben 25 alkalommal fordultak a SIS II-ben tárolt személyes adatok kezelésével kapcsolatban. Ezen megkeresések többsége az érintett jogok gyakorlásával kapcsolatos kérdés volt (tájékoztatás kérés, törlés), amely esetekben a Hatóság általános tájékoztatást nyújtott a beadványozónak a SIRENE Irodához fordulás jogáról és menetéről, valamint a jogorvoslati lehetségekről.

III.4.3. A Vízuminformációs Rendszer adatvédelmét felügyelő munkacsoport (VIS SCG)

A Vízuminformációs Rendszer célja, hogy elősegítse a közös vízumpolitika végrehajtását, a konzuli együttműködést és a központi vízumhatóságok közötti konzultációt. A Vízuminformációs Rendszert használják a schengeni térség konzulátusain, ahol vízumot állítanak ki, valamint a határátkelőhelyeken, ahol a határőrök ellenőrzik a biometrikus vízummal rendelkező személyek személyazonosságát. A VIS célja, hogy segítségével beazonosíthatóak legyenek az olyan

11 az EURÓPAI PARLAMENT ÉS TANÁCS 2018. október 23-i (EU) 2018/1725 RENDELETE a természetes személyeknek a személyes adatok uniós intézmények, szervek, hivatalok, és ügynökségek általi kezelése tekintetében való védelméről és az ilyen adatok szabad áramlásáról, valamint a 45/2001/EK rendelet és a 1247/2002/EK határozat hatályon kívül helyezéséről

személyek, akik nem teljesítik a tagállamok területére történő beutazás, az ott tartózkodás vagy a letelepedés feltételeit. A Vízuminformációs Rendszerhez hozzáférnek ezért a bűnuldöző hatóságok, menekültügyi hatóságok, valamint az Europol is.

A Vízuminformációs Rendszer adatvédelmét felügyelő munkacsoport (Supervision Coordination Group) a 2019-es év folyamán készített egy felmérést a vízuminformációs rendszerhez hozzáféréssel rendelkező hatóságok állományának adatvédelmi képzésével kapcsolatban. A munkacsoport véglegesítette az előző (2017-2018) időszakra vonatkozó tevékenységi jelentését, valamint el-készítette a következő (2019-2021) időszakra vonatkozó munkatervét. A munkacsoport úgy döntött, hogy a SIS II rendszer ellenőrzéséhez használt metódus mintájára kidolgoz egy közös vizsgálati tervet, amely tartalmazza a vízuminformációs rendszer adatbiztonságával kapcsolatos – minimumkövetelmények való megfelelést felmérő – kérdőívet is. A munkatervben a csoport megjelölt olyan feladatakat is, amelyekkel kiegészíthető a tervezet, ilyen például a konzulátusokon végzendő koordinált helyszíni vizsgálatok lefolytatása, a VIS rendelet¹² 35. cikke szerinti önenellenőrzés, az adattörles előrehozásának (25. cikk szerint) monitorozása, vagy a 31. cikk szerinti eljárás¹³ ellenőrzése.

A Hatósághoz 2019-ben 3 alkalommal érkezett megkeresés a Vízuminformációs Rendszerrel kapcsolatban, amelyek általános tájékoztatás keretein belül kerültek megválasztásra, felülvizsgálati eljárást a Hatóság egyetlen esetben sem indított.

III.4.4. Az Eurodac Rendszer adatvédelmét felügyelő munkacsoport (Eurodac SCG)

A 603/2013/EU rendelettel létrejött az Eurodac rendszer, amely lehetővé teszi a Dublini rendeletet alkalmazó országok számára, hogy az Eurodac rendszerben tárolt ujjlenyomatok összehasonlításával megállapítsák, hogy melyik tagállam köteles a menekültügyi eljárás lefolytatására. Az Eurodac rendszerbe adatokat küldő tagállamoknak a személyes adatok védelme érdekében biztosítaniuk kell, hogy az ujjlenyomatok levétele, valamint az adatok feldolgozásával, továbbításával, tárolásával vagy törlésével kapcsolatos műveletek jogoszerűek legyenek.

12 az EURÓPAI PARLAMENT ÉS TANÁCS 767/2008/EK rendelete a vízuminformációs rendszerről (VIS) és a rövid távú tartózkodásra jogosító vízumokra vonatkozó adatok tagállamok közötti cseréjéről

13 Uo. 31. cikk: Adatok közzételese harmadik országokkal vagy nemzetközi szervezetekkel

Az Eurodac adatkezeléseket az Európai Adatvédelmi Biztos felügyeli, együttműködve a nemzeti felügyeleti hatóságokkal (Eurodac SCG).

Az Eurodac rendszert felügyelő adatvédelmi munkacsoport véglegesítette az érintett jogok gyakorlásáról készített jelentését, amely megtalálható az Eurodac SCG weboldalán. A csoport az Európai Unió Alapjogi Ügynökségével (Fundamental Rights Agency, FRA) közösen kidolgozott egy, az érintettek tájékoztatására szolgáló anyagot. A tájékoztató egy ikonokkal illusztrált és közzérhető nyelvezettel megfogalmazott brosúra, melynek célja, hogy minden az ujjnyomat-felvétel menetéről, minden az öket megillető jogokról megfelelő tájékoztatást nyújtson az érintettek számára. Kiemelt figyelmet kap a gyermekekkel történő kommunikáció és ikonok jelzik, hogy mely információt szükséges szóban és/vagy írásban megadni az ujjnyomatok felvételét megelőzően. A munkacsoport elkészítette a következő (2019-2021) időszakra vonatkozó munkatervét, amely tartalmazza a tagállamok által a nemzeti ellenőrzési tevékenységekhez használható közösen kidolgozott vizsgálati metódust, a rendszerhez hozzáféréssel rendelkező bűnüldöző szervekkel (az Europol-t is ide értve) kapcsolatos felmérést, valamint a téves jelzések vizsgálatát.

III.4.5. Váminformációs Rendszer adatvédelmét felügyelő munkacsoport (Customs Information System – Supervision Coordination Group) és az Europol Cooperation Board

A Hatóság képviselői 2019-ben is részt vettek a brüsszeli üléseken. Az előző évekhez hasonlóan továbbra is kiemelt téma volt a tanácskozásokon a FIU.net jövője, a SIENA-val való kapcsolata, továbbá szó esett a kiskorú gyanúsítottakra vonatkozó személyes adatok átadásáról és az Egyesült Királyságnak az EU-ból való kilépése után az Europol által kezelt adatokra vonatkozó jogi helyzet változásáról is.

IV. Információszabadság

IV.1. Bevezetés

Az Információszabadság Főosztályon 2019-ben összesen 663 ügy volt folyamatban, melyek közül 489 ebben az évben érkezett, 174 pedig az előző évről áthúzódó ügy volt. A Főosztály feladatkörébe tartozó, 2019-ben indult adatvédelmi hatósági eljárások száma 11 (olyan ügyek tartoznak ide, melyeknél érdemben felmerül a két információs jog ütközése vagy együththatása), a konzultációs jellegű ügyek száma 116.

Emellett 17 jogszabálytervezetet véleményezett a főosztály. Ezzel kapcsolatban megjegyzendő, hogy az Infotv. 38. § (4) a) pontja kifejezetten felhatalmazza a Hatóságot a közérdekű és közérdekből nyilvános adatok megismerését érintő jogszabály tervezetek véleményezésére, ami összhangban áll a jogszabályok előkészítésében való társadalmi részvételről szóló 2010. évi CXXXI. törvény 7. § b) bekezdésében szereplő szabályozással. Ez utóbbi törvény a jogszabály, mint közérdekű adat széles körű megismerését és a jogalkotásban való aktív társadalmi részvételt célozza.

Az állampolgárok érdeklődési köre a Hatósághoz 2019-ben beérkezett panasz-beadványok alapján továbbra is rendkívül szerteágazó: kiterjed a külföldiek ingatlanszerzési statisztikájától kezdve a sportágak és sportrendezvények állami támogatásán át az önkormányzati jegyzők illetményére – és sok egyéb más kérdésre. Ezekre is reagálva 2019 őszén a NAIH két nagy horderejű, részletes tájékoztatót is kibocsátott az önkormányzati működés, illetve a közbeszerzési adatok nyilvánosságáról¹⁴. A tematikus szakmai iránymutatások a Hatóság meggyőződése szerint hatékonyan hozzájárulnak a nyilvánosság és a jogalkalmazók számára fontos kérdések egyértelmű megoldásához és egységes alkalmazásához.

14 <https://www.naih.hu/informacioszabadsaggal-kapcsolatos-tajekoztatok.html>

/V.2. Nemzetközi kitekintés

Ahogy a brandenburgi információs biztos által évente megrendezésre kerülő potsdami nemzetközi információszabadság szimpóziumon is megfogalmazódott¹⁵: mindenki tudomásul kell vennie, hogy az átláthatóság sokszorosan is hatékonyságnövelő tényező, az ezzel ellentétes állami szándékok pedig kontra-produktív hatásúak.

A NAIH 2019-ben az elsők között nyert akkreditációt az egyetlen világméretű információszabadság-felügyeleti szerveket összefogó nemzetközi hálózatban, az Információs Biztosok Nemzetközi Konferenciája (International Conference of Information Commissioners, ICIC¹⁶ körében, ahol a Hatóság az operatív testület (ICIC Governance Group) munkájában annak megalakulása óta részt vesz.

A márciusban Johannesburgban megrendezett ICIC 2019¹⁷ (Információs Biztosok 11. nemzetközi konferenciája) eseményre több mint 50 országból érkeztek a résztvevők. A konferencia elnöke Adv. Pansy Tlakula asszony volt, aki a 2016-ban öt évre a parlament által jelölt, az államelnök által kinevezett, de működését még csak most kezdő Information Regulator of South Africa bizottság (a két információs jog érvényesülését felügyelő hatóság) elnöke. Pansy Tlakula asszony 1995-2002 között a Dél-Afrikai Emberi Jogi Bizottság elnöke és az Afrikai Emberi Jogi és Népek Joga Bizottság tagja, ez utóbbi minőségeben 2010-12 között az Információhoz való hozzáférésről szóló afrikai modelltörvény – amit azóta 23 afrikai ország törvényhozása használt mintának – speciális rapportőre.

A konferencia kiemelten foglalkozott a sérülékeny társadalmi csoportok érdekvédelmével és a zárónyilatkozat is kiemeli, hogy a sérülékeny csoportok számára létfontosságú, hogy amellett, hogy ők is jussanak hozzá a közérdekű információkhoz, a társadalmat is tájékoztatni kell speciális helyzetükön és igényeikről. Hangsúlyos volt a felügyeleti szerv státuszára vonatkozó különféle modellek bemutatása – önálló vagy közös jogvédelem az adatvédelemmel, függetlenségi kritériumok, külön törvény vagy közös jogi norma stb. A másik fő kérdéskör az adatvédelem-információszabadság egymásra való hatását érintette. Az afrikai információs biztosok többször hangsúlyozták, hogy a kontinensen az egyéni jogként érvényesülő személyes adatok védelméhez való jog egyértelműen háttérbe szorul a közösségi jogként funkcionáló információhoz való hozzájutás jogához képest. Ugyanakkor a kölcsönhatás növekvő jellege tagadhatatlan, megfigyelhe-

15 <https://www.lda.brandenburg.de/cms/detail.php/bb1.c.648047.de?highlight=Symposium>

16 <https://www.informationcommissioners.org/hungary>

17 <https://www.informationcommissioners.org/icic-2019/programme>

tő például a választási eljárások kérdéskörénél, az állami adatbázisok nyilvánosságánál vagy a közzeladatot betöltő személyek esetén.

A másik fontos nemzetközi súlyú esemény a tavaly első ízben Budapesten megrendezett, gyakorlati témákat napirendre tűző Case Handling Workshop folytatása: 2019-ben az esemény házigazdája a gibraltári felügyeleti hatóság volt¹⁸ és téma között szerepelt az információszabadság ügyekben versengő jogi rezsimek ütközésének kérdése, a kormányzat által üzleti vállalkozásokkal kötött szerződések vagy a segélyhívó szolgálatok munkájának átláthatósága.

IV.3. Fontos alkotmánybírósági döntések

Az Alkotmánybíróság több információszabadságot érintő határozatot hozott 2019-ben, melyek a hatósági jogértelmezésénél is kiemelkedő jelentőségűek.

3190/2019. (VII. 16.) AB határozat: Paks II. atomerőmű hatástanulmányainak nyilvánossága

Az Alkotmánybíróság – a NAIH/2017/2365/2/T állásfoglalását is figyelembe véve – elutasította a Szekszárdi Törvényszék „közérdekű adatkiadás megtagadása tárgyában” hozott ítélete elleni alkotmányjogi panaszt.

Az indítványozó a paksi atomerőmű bővítésével kapcsolatos összes hatástanulmány kiadását kérte az MVM Paks II. Atomerőmű Fejlesztő Zrt.-től, mely az adatigényt döntést megalapozó adatok korlátozható nyilvánosságára hivatkozással elutasította és ezt a bíróság is megalapozottnak találta. Az Alkotmánybíróság szerint egy törvénnyel kihirdetett kormányközi egyezmény értelmezésének a kérdése, hogy az információszabadság szempontjából mi minősül döntésnek. A bíróság jogértelmezése – ideértve a környezeti adatok körét is – megfelel az Alaptörvény rendelkezéseinek, mivel egy olyan nemzetbiztonsági és nemzetstratégiai fontosságú beruházást érintő tárgyalássorozatban, mint a paksi atomerőmű bővítése, a magyar tárgyaló fél és a magyar állam pozícióinak védelme szükségessé teheti a közérdekű adatok megismeréséhez való jog korlátozását.

¹⁸ <https://www.gra.gi/data-protection/press-releases/freedom-of-information-workshop>

3147/2019. (VI. 26.) AB határozat: közérdekből nyilvános adat „érintettjének” a közpénz felhasználására vonatkozó üzleti titoktartási kötelezettségéről

Egy sorozatszínész a Médiaszolgáltatás-támogató és Vagyonkezelő Alap által finanszírozott filmsorozat főszerepére megbízási szerződést kötött egy műsorgyártó gazdasági társasággal és kötbérfizetési kötelezettség terhe mellett vállalta, hogy megbízási díját üzleti titokként kezeli. A műsorgyártó felmondta a megbízási szerződést, a színész erre egy internetes lapnak nyilatkozott gázsijáról és a műsorgyártó ezért beperelte. Az első- és másodfokú bíróság, valamint a Kúria is kötelezte a színész a kötbér megfizetésére. Az Alkotmánybíróság nem foglalt állást arról, hogy a vitatott adat (a szerződésbe foglalt megbízási díj összegére vonatkozó, titoktartási kötelezettséggel terhelt információ) közérdekből nyilvános adatnak minősül-e, ennek megítélése ugyanis jogvita esetén bírósági hatáskör. Ugyanakkor leszögezte: a közpénzekkel gazdálkodó szervezetek pusztán titokvédelmi szerződéses kikötésekre hivatkozással nem zárkózhannak el közérdekből nyilvános adatok kiadásától.

3069/2019. (IV. 10.) AB határozat és a 3070/2019. (IV. 10.) AB határozat: a Kúria jogegységi döntéséhez beszerzett vélemények, állásfoglalások adatainak nyilvánosságánál a döntést megalapozó adat tartalmi vizsgálata kötelező

Az alapügyben az indítványozó – miután közérdekből adatigénylésének teljesítését elutasították – azt kérte a bíróságtól, hogy kötelezze a Kúriát a vonatkozó polgári jogegységi határozat előkészítésével kapcsolatban beszerzett szakértői véleményekkel kapcsolatos adatok kiadására.

Az Alkotmánybíróság a következőket állapította meg:

A köztisztviselők döntés-előkészítése szabadon, informálisan és a nyilvánosság nyomásától mentesen folyik. Ezért az aktanyilvánosság a végeredményre vonatkozik csak, a közbülső munkaanyagokra nem. Az a jogértelmezés, amely az igényelt dokumentumokat – tartalmukra tekintet nélkül – egészében véve döntés megalapozást szolgáló adatnak minősíti, s ilyen módon a dokumentumok megismerését meggátolja, a közérdekből adatok megismeréséhez való jog indokolatlan tág körű és ezáltal szükségtelen korlátozását engedi meg. A vizsgált ügyben megállapítható, hogy mivel a bíróság a külső véleményadók személyét és a vélemények tartalmát nem ismerte, a nyilvánosságkorlátozás tartalmi indokoltságának tényleges vizsgálata nélkül hozta meg döntését. Ezzel az igényelt dokumentumokat tartalmukra tekintet nélkül, egészében véve helyezte nyilvá-

nosságkorlátozás alá. A feltétlenül szükségesnél tágabb alapjog-korlátozásra lehetőséget adó bírói döntés pedig alaptörvény-ellenes.

13/2019. (IV. 8.) AB határozat: közérdekű adat definíciójának értelmezése, a közérdekű adat előállítási kötelezettségének határai

Az indítványozó tudományos kutató, aki közérdekű adatigénylés útján a legalább hét éve tartó polgári peres eljárások listájának és egyes adatainak (ügyszámok, keresetlevél benyújtásának időpontja, jogi személyek esetében a peres felek neve) rendelkezésre bocsátását kért a Kúriától, mely azonban arra hivatkozott, hogy a keresetlevél benyújtásának az időpontját nem tartja nyilván, ezért a kért adatsort nem tudja kiadni. Az Alkotmánybíróság hangsúlyozta: a nem visszaélésszerűen gyakorolt adatigénylés nem tagadható meg arra hivatkozással, hogy a kért adat hozzáférhetővé tételehez idővel vagy költséggel járó többletmunkára van szükség. Azonban ettől *elkülönítendő* az az eset, amikor az adatigénylés arra irányul, hogy az adatkezelő új adatokat szerezzen be, vagy az általa egyébként kezelt adatokból minőségileg más adatot, statisztikát vagy kimutatást állítson elő. A bírói igazságszolgáltatás mint különálló hatalmi ág működésének nyilvánossága alapvetően nem különbözik más, közpénzből finanszírozott szervezetétől. A Kúria feladata a bíróságok joggyakorlatának egységesítése és elsődlegesen a rendkívüli jogorvoslatok elbírálása. A keresetlevél beadásának időpontja és ahhoz kapcsolódóan az egész eljárás hét évi vagy azt meghaladó pertartama – bár kikövetkezhető a bírósági aktákból –, de nem a Kúria tevékenységevel vagy közfeladata ellátásával összefüggésben keletkező adat. A kiadni kért információ tekintetében a Kúria egyébként sincs monopolhelyzetben, mivel az elsőfokú bíróság az eljárási törvényekben meghatározott feladatai értelmében szükségképpen közreműködik a polgári peres eljárás minden lényeges pontjánál, tehát a keresetlevél benyújtásának időpontját is rögzíti. minden körülményt mérlegelve az Alkotmánybíróság az indítványozó alkotmányjogi panaszát elutasította.

29/2019. (XI. 4.) AB határozat: közfeladatot ellátó személy (jegyző) bírálhatósága a közösségi médiában – a valóság bizonyításának kérdése

Egy állampolgár 2011-ben több alkalommal egy közösségi portálon a saját fiókjához tartozó üzenőfalon a városi jegyzőt bíráló megjegyzéseket tett, egy képviselő-testületi közmeghallgatáson pedig kijelentette, hogy „*a jegyző kétszer is feljelentette őt, és a rendőrségen hamis tanúvallomást tett*”.

A jegyző által indított személyiségvédelmi perben a Kúria is helybenhagyta az előzetes bírói ítéleteket becsületsértés vétsége és folytatónak elkövetett rágalmasztás vétsége megállapításáról azzal az indokolással, hogy az elhangzottak kizárálag a terhelt és a sérült viszonylatában, nem pedig a város közélete szempontjából bírnak jelentőséggel, így közérdekű információk semmiképpen sem tekinthetők, és a közmeghallgatáson történő elhangzásukat jogos magánérdekként sem indokolta.

Az indítványozó alkotmányjogi panasza nyomán az Alkotmánybíróság 3263/2018. (VII. 20.) AB határozatában a Kúria felülvizsgálati eljárás keretében hozott, az első- és másodfokú bírói döntéseket hatályában fenntartó végzését megsemmisítette azzal, hogy a bíróság a releváns alkotmányossági szempontokkal összhangban hozta meg döntését, azonban az ebből levont alkotmányos következtetései helytelenek. A szólásszabadság határainak – kiváltképp buntetőjogi korlátozásának – értelmezése során az Alkotmánybíróság a „*becsületérzés sérelméné*” szigorúbb mércét határozott meg. A korábbi gyakorlaton alapuló, azt az Alaptörvény alapján továbbfejlesztő értelmezés szerint a közügyek vitájában a közhatalom gyakorlóját vagy közszereplő politikust érintő bírálat, értékítélet főszabály szerint nem lehet alapja jogi felelősségre vonásnak. A véleménynyilvánítás szabadságának alkotmányos határát e körben csak azok a közlések lépik át, amelyek az emberi méltóságot, azaz a méltóságnak az *emberi mivolt lényegét jogilag megragadó tartalmát* sértik. A támadott ítélet indokolásából pedig nem tüntek ki azok az indokok, amelyek alapján a szóban forgó tényállítás „*kizárálag a terhelt és a sérült viszonylatában, nem pedig a város közélete szempontjából bír jelentőséggel.*”

A Kúria a jogerős ítéletet azonban ismét hatályában fenntartotta és e végzésével szemben az indítványozó másodszor is alkotmányjogi panasszal fordult az Alkotmánybírósághoz, mely szerint nincs akadálya annak, hogy a véleménynyilvánítás szabadsága és a jó hírnév védelme közti mérlegelés eredményeképp a bíróság eltérő következtetésre jusson, mint a támadott döntés. Az indítványozó kifejezéseit a véleménynyilvánítás szabadsága védte, a bírálat ugyanis nem sérte tette az érintett közszereplő emberi méltóságának lényegi magját. Ugyanakkor azzal, hogy a Kúria támadott döntése *hatályában fenntartott olyan bírósági döntéseket, amelyek az indítványozó védett véleménynyilvánítását bűncselekménynek minősítették*, megsértette az indítványozó Alaptörvény IX. cikk (1) bekezdésében rögzített jogát. A hamis tanúzsára vonatkozó kijelentéssel összefüggésben az Alkotmánybíróság arra tekintettel tartotta az ott vizsgált bírói döntést alaptörvény-ellenesnek, hogy az nem rögzítette, a sérültre vonatkozó tényállítás miért került ki a közügyek vitájának a köréből. A közügyek vitája so-

rán lehetőséget kell adni a terheltnek arra, hogy a tényállásszerűen rágalmazást megvalósító állításának valóságát bizonyítsa. Mindezt nem pótolja, ha felülvizsgálati eljárás keretében (amikor új bizonyítékok felvételére nincs mód) a Kúria azt a következtetést vonja le, hogy a terhelti állítás valótlanúsága már megállapításra került. A véleménynyilvánítás szabadságának egyik garanciája, hogy a bíróságok az alapeljárás keretében is vizsgálják a terhelti állítás valóságtartalmát, és a terheltnek formalizált keretek között van lehetősége eljárási jogainak érvényesítésére. Az Alkotmánybíróság ezért a döntést ismét megsemmisítette és - az alkotmányogi kérdés jelentőségére tekintettel - elrendelte a határozat Magyar Közlönyben történő közzétételét.

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

Az Alkotmánybíróság 2019 őszén két döntésében is foglalkozott a közérdekű adatok kiadásával kapcsolatos költségtérítéssel:

AB határozat a közérdekű adat iránti igény teljesítéséért megállapítható költségtérítés mértékéről szóló 301/2016. (IX. 30.) Korm. rendelet (Rendelet) 4. § (4) bekezdése elleni utólagos normakontroll tárgyában (ügyszám: II/1808/2016.sz.)

Az 58 országgyűlési képviselő által támadott rendelkezés az adatigénylés teljesítésével összefüggő munkaerő-ráfordítás költségeként elszámolható óradíjat szabályozza. A képviselők szerint a támadott rendelkezés nem a tevékenységet végző munkatársak átlagos bérköltségét veszi alapul, a 4400,- forintos óradíj eltúlzott, a rendelkezés tehát sérti a közérdekű adatok megismeréséhez való jogot, mivel egy alapjog gyakorlását ellenérték megfizetéséhez köti. Az Alkotmánybíróság először is rámutatott arra, hogy az adatigénylés teljesítése során igénybe vett munkaerő-ráfordításért nem kötelező a költségtérítés megállapítása, és ha erre sor is kerül, sem az Infotv., sem a Rendelet nem határozza meg előre a munkaerő igénybevételéért felszámítható pontos összeget, az ugyanis a tényleges munkaerő-költségtől függ. Ezért megállapítható, hogy a rendelkezés, amely csupán az adatigénylés teljesítésével összefüggő munkaerő-ráfordítás munkaóránként felszámítható maximális összegét határozza meg, nem alaptörvény ellenes, sőt, a támadott rendelkezés bizonyos értelemben – a felső korlát bevezetésével – a közérdekű és közérdekből nyilvános adatokhoz való hozzájutást segíti, mert a rendelkezés megsemmisítése esetében az adatigénylők a fennállónál hátrányosabb helyzetbe kerülhetnének. Mindezekre

tekintettel az Alkotmánybíróság az országgyűlési képviselők utólagos norma-kontroll indítványát elutasította.

AB végzés a Kúria Pfv.IV. 22.218/2017/4. számú ítélete elleni alkotmányjogi panasz közérdekű adat kiadásával kapcsolatos költségtérítés tárgyában (ügyszám: IV/1013/2019.)

Az indítvány alapvetően a bírói jogértelmezés és jogalkalmazás kritikáját tartalmazta a papír alapú adatszolgáltatás postai úton történő kézbesítéséért felszámolt költségtérítéssel összefüggésben. Az adatigénylők sérelmesnek tartották a Rendelet alapján megállapított 680,- forintos postaköltséget, és először a NAIH-hoz fordultak, majd miután a NAIH nem állapított meg jogszabályt, a közérdekű adat kiadásával kapcsolatos költségtérítés megváltoztatása iránt pert indítottak. Érvelésük szerint a vonatkozó jogszabályok alapján csak az igényelt adatokat tartalmazó dokumentumról készült másolat megküldéséért számítható fel postaköltség, egyszerű – másolatot nem tartalmazó – válaszlevélre azonban nem. Vitatták továbbá, hogy két levél postaköltségének a megtérítésére lennének kötelesek. Az eljáró bíróságok azt állapították meg, hogy az Infotv. és a Rendelet előírásaival összhangban került sor a költségtérítés felszámítására, ugyanis a postai borítékba helyezett papír, amelyen a válasz szerepel, adathordozónak minősül. A költségtérítés összege szintén nem jogosító, miután a két kérelmező részére történő postázás kétszeres postázási költségét számították fel. Ezt követően fordult az indítványozó alkotmányjogi panasszal az Alkotmánybírósághoz, melynek véleménye szerint önmagában az, hogy az indítványozó az egyébként megindokolt, az indítványozó érveit elbíráló bírósági ítélet érvelését tévesnek tartja, nem alkotmányossági kérdés. A Rendelet értelmében munkaerőforrás-ráfordításként figyelembe vehető legfeljebb 4400,- forint összeget a Központi Statisztikai Hivatal által a jogszabály-előkészítés során szolgáltatott, a központi költségvetési szerveknél teljes munkaidőben alkalmasban álló köztisztviselőkre számított, egy munkaórára vonatkozó bruttó kereseti adatok alapján, annak a kerekítésével (a pontos összeg 4353,4 forint volt) határozták meg. Azért ehhez az összeghez igazították a jogszabályi előírást, mert közérdekű adatigénylés teljesítésére számos, jogállását, működési kereteit tekintve eltérő szervtípus köteles, és e szervek foglalkoztatottjai is eltérő jogalilási törvények hatálya alá tartoznak, de a jogalkotó előfeltevése szerint az adatigénylésekkel jellemzően központi államigazgatási szervek teljesítik, ezért az itt köztisztviselőként foglalkoztatott személyek átlagkeresetét indokolt alapul venni.

2019-ban a NAIH-hoz a költségtérítés jogalapját, vagy annak összegszerűségét vitató 32 állampolgári panasz érkezett. Az adatkezelők között érintett volt a Pénzügyminisztérium, a Magyar Nemzeti Bank, a Közbeszerzési és Ellátási Igazgatóság, önkormányzatok, kormányhivatalok, valamint állami és önkormányzati tulajdonú gazdasági társaságok, és közintézmények. A megállapított költségtérítés összegek tág határok között mozogtak: a pár tízezer forintos téTEL volt a leggyakoribb, de előfordult többszázezer forintos összeg, illetve néhány kirívó esetben milliós nagyságrendek is (Pécsi Sport Nonprofit Zrt.: 4.841.000.- forint; Magyar Honvédség Egészségügyi Központ: 3.805.000 forint; Országos Rendőr-főkapitányság: 2.966.575.- forint). A legmagasabb költségtérítést a Magyar Tenisz Szövetség közel 9 millió forint összegben állapította meg.

Lezárt ügyeink jelentős hányadában a vizsgálat eredményeképpen az adatigénylést az adatkezelő költségtérítés megfizetése nélkül teljesítette, vagy a téves kalkulációval alapuló költségtérítés összegét mérsékelté, illetve a már befizetett költségtérítést az adatkezelő az igénylők részére visszautalta. Ilyen módon zártultak le például a Magyar Nemzeti Bankkal, a Közbeszerzési és Ellátási Főigazgatósággal, a FEV IX. Ferencvárosi Vagyonkezelő és Városfejlesztő Zrt.-vel, illetve a Pest Megyei Kormányhivatal Érdi Járásai Hivatalával kapcsolatban indult vizsgálataink.

Ugyanakkor az elmúlt évben is indult több olyan vizsgálat, mely a beszámoló készítésének időszakában is folyamatban van, tekintettel arra, hogy az álláspontok többszöri levélváltás követően sem közeledtek egymáshoz. Az egyik ilyen ügyben a Pénzügyminisztérium 33.033,- forint összegű költségtérítést állapított meg az adatigénylés teljesítésével összefüggő 17 munkaóráért, illetve 36.510,- forint költségtérítést 19 munkaóráért. Mindkét ügyben a Hatóság úgy ítélte meg, hogy az adatigénylés összeállítása egy ilyen nagyságrendű szervezet esetében egyik esetben sem minősült aránytalan mértékű igénybevételnek (NAIH/2019/944, NAIH/2019/982).

Az adatigénylés teljesítése természetesen bizonyos mértékű munkaerő-ráfordítást szükségképpen igényel, ez a közérdekű adatok megismeréséhez fűződő alapjog intézményi biztosításának velejárója. A közzeladatot ellátó szerveknek azonban készen kell állniuk arra, hogy bármely tevékenységüket illetően érkezhet hozzájuk közérdekű, illetve közérdekből nyilvános adatok megismerésére vonatkozó igény. A Hatóság a NIF Nemzeti Infrastruktúra Fejlesztő Zrt. által megállapított 176.000.- forint esetében is hasonló megállapításra jutott, és az

adatkezelő egyet nem értése miatt a vizsgálat jelentés közzétételével zárult (NAIH/2019/507).

A bírósági (jogorvoslati) eljárásban a költségtérítés összegének megalapozottságát az adatkezelőnek kell bizonyítania, ezért is fontos a részletes, pontos kalkuláció és a költségek dokumentumokkal történő alátámasztása. A bíróság döntéssével az összeget megváltoztathatja, vagy a közfeladatot ellátó szervet annak megállapítása tekintetében új eljárásra kötelezheti.

A közérdekű adatok megismeréséhez való alkotmányos jog nem korlátozhatatlan alapjog, azonban a szabad véleménynyilvánításhoz való jog gyakorlásának egyik feltételeként és annak részeként kitüntetett alkotmányos védelemben részesül. Ez azt jelenti, hogy az információszabadságot korlátozó törvényeket is megszorítóan kell értelmezni. A Hatóság egy panaszos ügyében ebből fakadóan, valamint a Rendelet 4. § (3) bekezdésével összhangban úgy foglalt állást, hogy a szociális hozzájárulási adó mint a munkáltatói oldalon jelentkező közteher összege sem terhelhető át az adatigénylőre, így annak visszafizetésére szólította fel az adatkezelőt. A felszólításban foglaltaknak az ügyben érintett önkormányzat eleget tett. (NAIH/2019/5705)

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 költségeemet, amelyek a megállapított összeg megalapozottságát támasztják alá. A megfelelő tájékoztatás nagyban hozzájárul ahhoz, hogy az igénylő valóban megértse azt, hogy miért, milyen költségtérítést kell megfizetnie ahhoz, hogy a megismerni kívánt adatok birtokába jusszon.

A munkaerő-ráfordítás összegét a konkrét munkafolyamat alapján kell kiszámolni. A Hatóság több ízben is felhívta az adatkezelők figyelmét arra, hogy az indokolásban pontosan írják le azokat a munkafolyamatokat is, amelyek szükségessé válnak az adatigénylés sikeres teljesítéséhez. Az egyik ügyben az ORFK arról tájékoztatta az igénylőt, hogy a létszám- és a leszerelésre vonatkozó adatokat minden év január 1-jei állapotnak megfelelően kezeli a rendőrség a teljes rendőrségi hivatásos állományra kiterjedően. Így a szervenként és azon belül is havi bontású adatokat tartalmazó kimutatás összeállításához valamennyi érintett, munkáltatói jogkörrel rendelkező rendőri szerv bevonásával végrehajtható országos adatgyűjtés elvégzésére lenne szükség. Az ORFK ezzel pontosan megjelölte azt a körülményt, amely miatt az adatigénylés teljesítése a közfeladatot ellátó szerv alaptevékenységének ellátásához szükséges munkaerőfor-

rás aránytalan mértékű igénybevételével járt volna (NAIH/2019/4306). Érdemes ilyen esetekben az adatigénylőknek átgondolni azt is, hogy célszerű-e a közérdekű adatigénylést változatlan formában fenntartani. Az adatigénylők az adatkezelővel történt egyeztetést követően bármikor dönthetnek úgy, hogy módosítják azt a formát, illetve módot, ahogyan a közérdekű adatokat meg szeretnék kapni – természetesen úgy, hogy az adatigénylés a célját elérje – jelentősen csökkentve vagy akár teljesen ki is iktatva ezzel az adatigénylés költségvonzatát.

Egy másik ügyben a körfeladatot ellátó szerv jelentős mértékű (355.600,- forint) költségtérítést helyezett kilátásba pusztán azzal az indokkal, hogy „*a szerződések adatvédelmi szempontból való ellenőrzéséhez DPO (adatvédelmi tisztviselő) bevonására van szükség*”. A Hatóság ezzel kapcsolatban felhívta az adatkezelő figyelmét, hogy önmagában az a tény, hogy a szerződésekben szereplő egyes személyes adatokat anonimizálni kell és ezt a feladatot a DPO ellenőrzi, nem alapozza meg a költségtérítési igény jogosságát (NAIH/2019/5915).

Költségtérítéses ügyekben fontos azt is kiemelni, hogy az 5.000 forintot el nem érő költségtérítés megállapításakor az adatigénylés teljesítése nem köthető a meghatározott összeg előzetes megfizetéséhez, illetve az első 4 munkaóra eleve nem számolható fel [Rendelet 3. § (1) bekezdés]. Gyakran bizonytalanságot okoz, hogy nincs egyértelműen feltüntetve a költséggalkulációban, ha az említett 4 munkaóra már levonásra került.

IV.5. Fontos bírósági döntések

- I. Az államháztartás alrendszerébe tartozó valamely személlyel/szervezettel pénzügyi vagy üzleti kapcsolatot létesítő piaci szereplőnek számolni kell a nagyobb nyilvánossággal.
- II. Amennyiben a kérelem az igényelt adat konkrét beazonosításához szükséges minimális követelményeknek megfelel, a kérelemmel érdemben kell foglalkozni és szükség esetén – egyfajta aktív kötelezettséggé – az igénylőt pontosításra kell felhívni. (*Pécsi Ítélezőtábla Pf.III.20.036/2019/4.*)

Ha az adatkezelő a közérdekű adatok megismerése iránti perben nem tud olyan döntéshozatallal végződő eljárást bizonyítani, amelyben a megismerni kívánt adatokat felhasználják, eredménnyel nem hivatkozhat az adatok döntést megállapozó jellegére, illetve arra, hogy ezek megismerése a körfeladatot ellátó szerv törvényes működési rendjét vagy feladat- és hatáskörének illetéktelen, kül-

ső befolyástól mentes ellátását veszélyeztetné. A nyilvánosságkorlátozásra nem lehet alap egy jövőben, bizonytalan időpontban elkeszülő vélemény lehetősége. (*Fővárosi Ítéltábla 32.Pf.20.913/2018/4-II.*)

A közfeladatot ellátó szerveknek a közérdekű adatigénylések teljesítésekor alapesetben a normál napi működés keretében ingyenesen kell az igényelt adatokat az állampolgárok rendelkezésére bocsátaniuk. Az adatigénylés teljesítése bizonyos mértékű munkaerő-ráfordítást szükségképpen igényel, amely a közérdekű adatok megismeréséhez fűződő alapjog intézményi biztosításának a velejárója. Csak a négy munkaórát meghaladó munkaerő-ráfordítás költsége számítható fel az adatigénylővel szemben, az is csak akkor, ha az adatigénylés teljesítése a közfeladatot ellátó szerv tevékenységének ellátásához szükséges munkaerőforrás aránytalan mértékű igénybevételével járna. Ennek megítélése minden esetben az összes körülmény körültekintő mérlegelésével állapítható meg. (*Fővárosi Ítéltábla 8.Pf.20.420/2019/5.*)

I. A bírósági eljárás során nyilvánosságra került személyes és különleges adatok nem osztják a közérdekből nyilvános vagy közérdekű adatok jogi sorsát.

II. A peres eljárás tárgyalásának nyilvánossága nem azonos a periratok nyilvánosságával. A tárgyaláson az érdeklődők megjelenhetnek és a szóbeli eljárást figyelemmel kísérhetik, e jog azonban nem foglalja magában az iratok nyilvánosságát. A peres eljárás iratai – ide értve a tárgyalási jegyzőkönyveket is – nem hozhatók nyilvánosságra a bennük foglalt személyes adatok miatt általában akkor sem, ha egyébként az az eljárási cselekmény, amelyről készültek, nyilvánosan zajlott. (*BDT2005. 1277., Győri Ítéltábla Pf.I.20.238/2016/7., Fővárosi Ítéltábla 17.Pf.21.336/2017/7., Szegedi Ítéltábla Pf.I.21.182/2017/14.*)

Az Infotv. 27. § (3a)¹⁹ bekezdésének értelmezéséről:

„A másodfokú bíróság osztotta az elsőfokú ítélet álláspontját abban, hogy az alperes, mint az államháztartáson kívüli személy az anyagbeszállítói szerződések megkötése során saját vagyonával, saját kockázatára és felelősséggére gazzdál-kodik, amelynek során már az államháztartás alrendszerébe tartozó személlyel

19 Infotv. 27. § (3a) Az a természetes személy, jogi személy vagy jogi személyiséggel nem rendelkező szervezet, aki vagy amely az államháztartás alrendszerébe tartozó valamely személyel pénzügyi vagy üzleti kapcsolatot létesít, köteles e jogviszonnyal összefüggő és a (3) bekezdés alapján közérdekből nyilvános adatra vonatkozóan - erre irányuló igény esetén - bárki számára tájékoztatást adni. A tájékoztatási kötelezettség a közérdekből nyilvános adatok nyilvánosságra hozatalával vagy a korábban már elektronikus formában nyilvánosságra hozott adatot tartalmazó nyilvános forrás megjelölésével is teljesíthető.

lététesített üzleti megállapodás teljesítése érdekében jár el. Az Ítéltőtábla álláspontja szerint azonban nem annak van jelentősége, hogy ezzel új kötelelem keletkezett. Ezzel szemben arra helyezi a hangsúlyt, hogy a perbeli esetben az Európai Uniós forrásból finanszírozott beruházás keretében beépített összes alapanyag típusára, mennyiségére és a beszerzésének forrására, valamint költségére vonatkozó, az alperes és beszállítói közötti jogviszony keretében keletkezett adatok és a forrásként szolgáló közpénz közötti kapcsolat túl távoli és közvetett ahhoz, hogy annak részleteiről az alperes az Infotv. 27. § (3a) bekezdésének szabályai szerinti közérdekből nyilvános adatként tájékoztatást kell adjon. E szakasz nyelvtani értelmezése alapján is az jelenthető ki a másodfokú bíróság álláspontja szerint, hogy az adatszolgáltatási kötelezettség az államháztartás alrendszerébe tartozó személlyel pénzügyi vagy üzleti kapcsolatot létesítő személyt terheli, méghozzá a kettejük jogviszonyával összefüggő közérdekből nyilvános adatok vonatkozásában. Az alperes és az alvállalkozói közötti szerződések nem állnak összefüggésben az államháztartás alrendszerivel, azokra az Infotv. 27. § (3a) bekezdése szerinti adatkiadási kötelezettség nem értelmezhető.”

Fővárosi Ítéltőtábla 8.Pf.20.031/2019/5. sz. ítélete

IV.6. A közszolgálatban álló személyek közérdekből nyilvános adatai

A NAIH 2018-as beszámolójában külön alfejezetet szenteltünk a foglalkoztatták közérdekből nyilvános személyes adatai nyilvánosságának, az egyes adatfajták megismerhetőségének a különböző foglalkoztatásra irányuló jogviszonyokban.

E körben 2019 egyik fontos fejleménye, hogy 2019. január 1-jén hatályba lépett a kormányzati igazgatásról szóló 2018. évi CXXV. törvény (Kit.), amely egyes közszolgálati tiszttiselők (kormánytiszttiselők, állami tiszttiselők) jogviszonyára külön törvényt alkotott.

A közszolgálati tiszttiselőkről szóló 2011. évi CXCIX. törvény (Kttv.) 179. §-a egyértelműen felsorolja, hogy a hatálya alá tartozó foglalkoztatottak tekintetében mely adatok minősülnek közérdekből nyilvános adatnak (név, állampolgárság, a foglalkoztató államigazgatási szerv neve, a szolgálati jogviszony kezdete, a besorolási adatak, a munkakör, a vezetői kinevezés időpontjai, a címadományozásra és az illetményre vonatkozó adatak).

Ezzel analóg rendelkezést azonban sem a Kit., sem a csak 2020. május 1-jétől alkalmazandó, a különleges jogállású szervekről és az általuk foglalkoztatottak jogállásáról szóló 2019. évi CVII. törvény (a továbbiakban: Küt.) nem tartalmaz.

Ebből fakadóan előállt az a helyzet, hogy a közigazgatási szervek különböző törvények (Kttv., Kit., Küt.) hatálya alá tartozó foglalkoztatottjai tekintetében eltérő tartalmú nyilvánossági szabályok lehetnek alkalmazandóak. Így még egy a Kttv. alapján köszolgálatban álló foglalkoztatott tekintetében az előzőekben felsorolt adatok – ideértve az illetményt is – közérdekből nyilvánosak, addig ugyanezen adatok egy másik, hasonló munkakört betölthető, de a Kit. vagy a Küt. hatálya alá tartozó foglalkoztatott esetében – a Kit. és a Küt. rendelkezései alapján már nem minősülnek közérdekből nyilvános adatnak.

Ez egyszintű a Hatóság megítélése szerint homogén csoportba tartozó – Kit., Küt., Kttv. hatálya alatt álló – foglalkoztatottak igazolható alkotmányossági indok hiányában történő megkülönböztetéséhez, az egyenlő bánásmód követelményének sérelméhez vezethet, másrészt az Infotv. 26. § (2) bekezdésére tekintettel a jogbiztonságot sértő helyzetet is eredményez a jogalkalmazásban.

Az Infotv. 26. § (2) bekezdése alapján ugyanis közérdekből nyilvános adat a közfeladatot ellátó szerv feladat- és hatáskörében eljáró személy neve, feladatköre, munkaköre, vezetői megbízása, a közfeladat ellátásával összefüggő egyéb személyes adata.

A Hatóság ezen rendelkezéshez is kapcsolódó következetes gyakorlata alapján így az illetményre vonatkozó adat a közfeladatot ellátó szerv hatáskörében eljáró foglalkoztatott esetében közérdekből nyilvános adatnak minősül, e gyakorlattól való eltérésre – figyelemmel az Infotv. rendelkezéseire – a Kit. és a Küt. hatályba lépésével sincs ok.

Ugyanakkor a jogbiztonság szempontjából kerülendő, hogy a törvényben meg-határozott adatfajták körében nyilvánosságot előíró konkrét rendelkezés hiányában, az Infotv. 26. § (2) bekezdésében foglalt, a „közfeladat ellátásával összefüggő adat” terminus értelmezési tartományát az adatkezelő közfeladatot ellátó szerv egyedi mérlegelését igénylő, absztrakt jogértelmezésének körébe utalja a szabályozás.

A Hatóság jogalkalmazási tapasztalata is megerősíti az e jogi helyzből fakadó jogértelmezési nehézségeket. A Hatóság egy konkrét bejelentés kapcsán 2019-ben arra az álláspontra helyezkedett, hogy a Kit. hatálya alá tartozó kor-

mányhivatal vezetőjének, illetve a járási hivatal vezetőjének és helyetteseinek illetménye és jutalma az igényelt formában közérdekből nyilvános adat, tekintettel arra, hogy azok a közfeladatot ellátó személyek feladatkörének ellátásával egyértelműen összefüggnek. Az egyéb, szociális alapú juttatások azonban már nem minősülnek közérdekből nyilvános adatnak, ezekre vonatkozóan név szerinti adatszolgáltatás helyett csak személyazonosításra alkalmatlan módon, összesített adatszolgáltatás teljesíthető. (NAIH/2019/7257)

A Hatóság álláspontja a töretlen hazai jogalkalmazói gyakorlattal, illetve az Alkotmánybíróság korábbi döntéseivel továbbá a NAIH/2015/7163/2/V számú állásfoglalással egyezően továbbra is az, hogy a Ktv. 179. §-ában meghatározott adatkör a Kit. és a Küt. hatálya alá tartozó foglalkoztatottak esetében is közérdekből nyilvánosak.

Mindezek alapján a Hatóság javaslatot tett az Igazságügyi Minisztériumnak az egyértelmű jogi helyzet megteremtéséhez szükséges módosítások előkészítésére.

IV.7. Helyi közügyek – az önkormányzati testületek működésének nyilvánossága

2019 az önkormányzati választások éve volt és már a megelőző időszakban érezhetővé vált a felfokozott választópolgári érdeklődés a helyhatósági működés átláthatóságával kapcsolatban, illetve az új képviselők és polgármesterek is sok esetben fogalmaztak meg felvetéseket és tettek fel kérdéseket. Az önkormányzati testületek működésének nyilvánossága témajában készült NAIH tájékoztató teljes²⁰ és rövidített változata²¹ is elérhető honlapunkon, és a szakmai összeállítás a Belügyminisztérium által szerkesztett Önkormányzati Hírlevél útján valamennyi település önkormányzatához eljutott. A tájékoztató kiemeli az adatelv érvényesülését az iratellvel szemben, részletesen kitér a zárt ülés feltételeire, az önkormányzati képviselő adatmegismerési jogára, a szociális ügyek nyilvánosságára, az önkormányzati bérifikációkról kiadható információkra és eligazítást nyújt a kötelezően közzéteendő adatokról, valamint az anonimizálás kötelezettségéről.

20 https://www.naih.hu/files/NAIH-2019-6273-3--taj_önkormányzati_testületek_működésenek_nyilvanossagarol.pdf

21 https://www.naih.hu/files/Leporello--taj_önkormányzati_testületek_működésenek_nyilvanossagarol_roviditett.pdf

Az állásfoglalás hangsúlyozza: az önkormányzati képviselő önálló feladat- és hatáskörrel nem rendelkezik, képviselői munkája elsősorban a képviselő-testület és bizottságai döntési kompetenciájába tartozó egyes ügyek döntéseinek előkészítésében, végrehajtásuk szervezésében és ellenőrzésében való részvételt jelenti. A képviselő feladatai ellátása során kizárolag az adatkezelés szüksége és arányossága érvényesülésével, a szükséges mennyiségű adatot, a közfeladat ellátásának időtartama alatt kezelhet. Ez vonatkozik a képviselői mandátumot megelőző időpontban született zárt ülések jegyzőkönyveire, illetve a jegyző által vezetett szociális nyilvántartás adataiba történő betekintés esetére is: a képviselő kizárolag konkrét ügyben, a feladata ellátásához szükséges mértekben ismerheti meg a vonatkozó iratokat. (NAIH/2019/8161.) A feladataikhoz kapcsolódóan megismert védett adatok vonatkozásában a képviselők, bizottsági tagok azokról harmadik személynek nem adhatnak felvilágosítást, azokat nem továbbíthatják, megtekintésüket nem tehetik lehetővé.

Az adatbiztonság megvalósítása során a fő cél az adat illetékteleneknek történő továbbításának megakadályozása. Ez úgy is megvalósítható, ha az önkormányzati képviselő, bizottsági tag számára biztosított egy belső, zárt elektronikus levelezési kör, ezzel megakadályozható a dokumentum „külső” e-mail címre küldése, illetve továbbítása. (NAIH/2019/8337.)

Adatvédelmi szempontból további helyes gyakorlat, ha a zárt ülés előterjesztései az ülés résztvevői az érdemi döntést követően visszaszolgáltatják. Az ülést vezető személytől elvárható, hogy figyelmeztesse az ülés résztvevőit az ügyben elhangzott információk bizalmas kezelésére, az azzal kapcsolatos titoktartási kötelezettségre.

A zárt ülés előterjesztései és jegyzőkönyvét nem érinti közzétételi kötelezettség, kizárolag a zárt ülés anonimizált határozatait, illetve magát a döntést kell nyilvánosságra hozni. A Hatóság konzekvens álláspontja, hogy a zárt ülés adatai megismerésére irányuló adatigénylést nem lehet – érdemi vizsgálat nélkül– csupán arra hivatkozással elutasítani, hogy az adott kérdés megtárgyalása, illetve a döntés meghozatala zárt ülésen történt, ezért az emiatt nem megismerhető.

A testületi szerv ülésének nyilvánossága, vagy zártsága meghatározza az előterjesztések, az ott született döntések és a jegyzőkönyv nyilvánosságát is. A nyilvános üléseken elhangzott előterjesztések, nyilatkozatok, az ott történt események általában közérdekkű (illetve közérdekből nyilvános) adatnak minősülnek, ezért az erre vonatkozó adatok, információk (előterjesztések, meghozott döntések, szavazati arányok) főszabályként bárki által szabadon, korlátozás nélkül megismerhetők és terjeszthetők. Előfordulhat ugyanakkor, hogy a nyil-

vános testületi ülés dokumentumaiba (akár előre nem várható módon) megismerési korlátozás alá eső adat kerül. Ebben az esetben felismerhetetlenné kell tenni az érintett dokumentumokban a védeott adatot. Az adatok védelmének kötelezettsége a nyilvánosság ellenére, illetve emellett is megmarad.

Az önkormányzat vagyonával való rendelkezés esetén, továbbá az Mötv.²² 46. § (2) bekezdés c) pontjában felsorolt esetekben, ha a nyilvános tárgyalás az önkormányzat vagy más érintett üzleti érdekét sértené, a képviselő-testület – mérlegelesi jogkörével élve – zárt ülést rendelhet el. Az Alaptörvénnyel összhangban az Nvtv.²³ 7. §-a kimondja, hogy a nemzeti vagyon alapvető rendeltetése a közfeladat ellátásának biztosítása. A Hatóság az önkormányzati vagyonnal kapcsolatos előterjesztések zárt ülés keretében történő megtárgyalása kapcsán hangsúlyozza a széleskörű nyilvánosság biztosításának fontosságát, lehetőség szerint a zárt ülés elrendelésének mellőzését.

Az üzleti titok és az információszabadság ütközését feloldja az Infotv. 27. § (3) bekezdése, mely közpénzek felhasználása esetén közérdekből nyilvános adatoknak minősíti a „kvázi” üzleti titkokat. Ez esetben, ha a titokgazda kifejezetten megjelöli az üzleti titokra vonatkozó részeket és részletesen kifejti a védettség indokát az üzleti titok megőrzésére, az önkormányzat, mint szerződéses partnere azt nem hozhatja nyilvánosságra.

Az Mötv. 46. §-a rendelkezik a képviselő-testület ülésének nyilvánosságáról, a zárt ülés tartásának feltételeiről. Az Mötv. 2. §-a alapelvként deklarálja a képviselő-testületi ülések nyilvánosságát, melyet az Mötv. 46. § (1) bekezdésében további megerősítést kap. Emellett az egyes képviselő-testületeknek külön-külön, a saját működési rendjükben is meg kell határozniuk a nyilvánosság biztosításának módját, mely köti az önkormányzatot az adatok nyilvánosságra hozatalában. A nyilvános képviselő-testületi ülésen való részvétel több formában is történhet: leggyakrabban személyes jelenléttel, azonban egyre több önkormányzat alkalmazza a testületi ülések elő közvetítését – a helyi/önkormányzati televízió- vagy rádió csatornán, illetve interneten (az önkormányzat honlapján, közösségi oldalon) – a nyilvánosság biztosításának módjaként. Az ezeken a felvételeken szereplő közérdekből nyilvános személyes adatok az Infotv. 26. § (2) bekezdése alapján a célhoz kötött adatkezelés elvének tiszteletben tartásával terjeszthetők. (NAIH/2019/7890, NAIH/2019/8077, NAIH/2019/8173, NAIH/2019/8256, NAIH/2019/8337)

22 Mötv.: a Magyarország helyi önkormányzatairól szóló 2011. évi CLXXXIX. törvény

23 Nvtv.: a nemzeti vagyonról szóló 2011. évi CXCVI. törvény

IV.8. A közbeszerzési adatok nyilvánossága

A közbeszerzési eljárásokat közpénzekből gazdálkodó szervezetek, illetve bizonyos, nem versenyszférabeli vállalkozások (pl. energia- vagy vízszolgáltatók, tömegközlekedési vállalatok, postai szolgáltatók) indítják meghatározott értékhatáron felüli szolgáltatások, áruk vagy építési munkák beszerzésére. A közpénzek hatékony felhasználásának átláthatósága és nyilvános ellenőrizhetőségének biztosítása a közbeszerzési eljárás egyik kiemelt alapelve. A Hatóság határozott álláspontja szerint a közbeszerzési eljárásokban mind az ajánlatkérő cselekményei, mind az ajánlattevők által benyújtott iratok alapvetően közérdekű és közérdekből nyilvános adatokat tartalmaznak. A nyilvánosság és átláthatóság a kötelező közzététellel, iratbetekintéssel, illetve közérdekű adatigények teljesítésével biztosítható.

A közbeszerzési eljárás szakaszai:

- I. Előkészítő szakasz: közbeszerzési eljárások tervezése, éves közbeszerzési terv, közbeszerzési szabályzat elkészítése
- II. Közbeszerzési eljárás megindítása – ajánlattételi felhívás
- III. Kiegészítő tájékoztatás
- IV. Előzetes vitarendezés, iratbetekintés
- V. Beérkezett ajánlatok bontása
- VI. Az ajánlatok elbírálása (összegezés az ajánlatok elbírálásáról)
- VII. Hiánypótlás kérése
- VIII. Az ajánlattevők tájékoztatása az eljárás eredményéről (esetleges jogorvoslati eljárás, iratbetekintés)
- IX. Szerződéskötés a nyertes ajánlattevővel, teljesítés

Információszabadság szempontból meghatározó pont a nyertes ajánlattevő kiálasztásáról szóló döntés és a vele való szerződéskötés – ettől kezdődően a közbeszerzési eljárás adatai már nem minősíthetőek döntést megalapozó adatoknak. A törvény pontosan meghatározza, hogy kinek, mikor és milyen adatokat kell közzétenni az elektronikus közbeszerzési rendszerben (EKR) és a Közbeszerzési Hatóság honlapján. Így a közbeszerzési tervet, a szerződő felek megnevezését, a megkötött szerződésekét és szerződésmódosításokat, a teljesítésre vonatkozó adatot. A közzétett adatok elérési helye: <https://ekr.gov.hu/portal/kezdolap>.

A közbeszerzési eljárásra és a Közbeszerzési Döntőbizottság jogorvoslati eljárására az általános közigazgatási rendtartás szabályai alkalmazandóak, így az ajánlattételvők és más ügyfelek indokolt esetben, konkrétan megjelölt terjedelemben iratbetekintési jogukat, (korlátozások mellett) ez alapján gyakorolhatják. A Hatóság töretlen joggyakorlata szerint²⁴ a közérdekű adat megismeréséhez való jog mint alkotmányos jog azonban szélesebb körű jogosultság, mint a közigazgatási eljárási jellegű iratbetekintési jog. Önmagában az a tény, hogy a megismerni kívánt adatokat egyébként közbeszerzési eljárásban felhasználják, illetve annak során keletkeznek, nem fosztja meg azokat közérdekű adat jellegüktől, sőt, ezen adatok éppenséggel ettől válnak közérdekűvé. A döntéssel lezárt közbeszerzési eljárások esetében főszabály a nyilvánosság (ideértve például a nyertes ajánlattevő teljes ajánlatát – kivéve a védett üzleti titok köre – vagy a nem nyertes ajánlatok azon információit, amelyek szükségesek az összehasonlításhoz).

A védelmi és biztonsági célú beszerzési eljárás lezárását követően a beszerzések adatainak nyilvánossága vonatkozásában az Infotv. általános szabályai mellett a külön törvény speciális rendelkezéseit is alkalmazni kell. A közpénzekkel való gazdálkodás átláthatóságának érdekében az üzleti titok ebben a körben nem feltétlenül jelenti a nyilvánosság korlátját, ugyanakkor a törvény szűk körben lehetőséget ad a gazdálkodás eredményessége szempontjából fontos védett ismeretek (például technológiai eljárások, know-how, üzleti stratégiák stb.) titkosítására. A gazdasági szereplők jogos pénzügyi, gazdasági vagy piaci érdeke felülírhatja az információk megismerhetőségéhez fűződő közérdeket, ezt azonban minden egyedileg, szigorú mérlegelés útján kell előntení.

IV.9. Döntés megalapozását szolgáló adat

A NAIH állásfoglalása szerint (NAIH/2019/1824) az adatkezelő jogosan tagadta meg a közérdekű adatigénylés teljesítését, mikor egy panaszos azt kérdezte az ORFK-tól, hogy 2018. december 12-től milyen rendőrségi mozgások történtek a tüntetések miatt (az adatigénylő napi bontásban kérte, hogy mely települések ről vezényeltek fel Budapestre rendőröket, hány rendőrt vezényeltek fel – településsenként lebontva) és összesen hány rendőr vett részt a rendfenntartási műveletekben és ők milyen „fokozattal” rendelkeztek.

24 Lásd NAIH beszámoló 2018, 118. oldal

Az ügy megítélésében a Fővárosi Bíróság két korábbi ítélete is alkalmazható:

- „az egyes rendőri egységek konkrét létszámadatai, a rendelkezésre álló technikai eszközök nagysága, típusa, valamint a rendőrségi rádióforgalmazás során használt elnevezések ismerete olyan tényeket, körülményeket tartalmaz, amelyek valóban alkalmasak lehetnek későbbi döntés előkészítésére.” Valamint „az összesített erő-eszközkiadatás, a tömegdemonstrációval kapcsolatban keletkezett többletfeladatok költségeiről szóló kimutatás, [...] az eseménynapló olyan adatokat tartalmaz, amely megismerése alkalmas lehet a szerv törvényes működési rendjének feladat- és hatáskörének illetéktelen külső befolyástól mentes ellátásának veszélyeztetésére.” (19.P24/882/2009/14)
- „a műveletekben résztvevő egységek pontos létszáma, különböző rendőrségi hívószámok, valamint az egyes egységekhez kapcsolható technikai eszközök leírása esetében megalapozott a döntés előkészítésében való felhasználásra történő hivatkozás” és annak megjelölése, hogy a Rendőrség minden személyi erőkkel rendelkezik a létesítmény és esemény biztosításánál, illetve az egységekhez minden technikai eszközök csatolhatók, valóban alkalmas lehet további hasonló esetekben a döntés előkészítésének előmozdítására, illetve a szerv törvényes működési rendjének vagy feladat- és hatáskörének illetéktelen, külső befolyástól mentes ellátására. (19.P.24.246/2010/9)

Egy másik ügyben egy civil szervezet kereste meg az Emberi Erőforrások Minisztériumát (EMMI) és kérte, hogy küldje meg számára azt a minisztériumi választ, melyet az Alapvető Jogok Biztosának a különösen veszélyeztető időjárási viszonyokra („Vörös Kód”) alkalmazott hajléktalanellátással kapcsolatos vizsgálata során tett ajánlására adott. Az EMMI szerint ez a minisztériumi válaszlevél nem minősül közérdekkének, így nem tárgya a közérdekkű adatigénylésnek. A vizsgálat során az EMMI arra is hivatkozott, hogy a dokumentum döntés megalapozását szolgáló adatokat is tartalmaz, és mivel az adatigénylő a teljes dokumentum rendelkezésre bocsátását kérte, nem volt lehetőség az adatigénylés teljesítésére.

Egy újabb megkeresésre – amely a döntés-előkészítő adatok e minőségének alátámasztását kérte – az EMMI kifejtette, hogy álláspontjuk szerint az alapvető jogok biztosáról szóló 2011. évi CXI. törvény alapján az ombudsmani ajánlásokra a vizsgált hatóság által adott válasz mindaddig nem minősül közérdekkű adatnak, amíg az alapvető jogok biztosa a jelentésben feltárt alapvető jogokkal kapcsolatos visszásság megszűnéséről tájékoztatást nem ad, ezt megelőzően közbülső munkaanyagokról beszélhetünk csak, melyek a konkrét esetben egy jelenleg is előkészítő szakaszban lévő – a hajléktalanellátással kapcsolatos – jogszabály-tervezet anyagához kapcsolódnak, ezért a minisztériumi álláspont

megismerése a jogszabály-tervezet előkészítői álláspontjának a későbbi döntések előkészítése során történő szabad kifejtését veszélyezteti.

A Hatóság állásfoglalásában egyértelműen hivatkozott arra, hogy az alapvető jogok biztosa elősegíti az emberi jogok érvényesülését és védelmét, ennek során társadalmi tudatformáló, felvilágosító tevékenységet végez és együttműködik azon szervezetekkel és nemzeti intézményekkel, amelyek célja az alapvető jogok védelmének előmozdítása. Az alapvető jogok biztosa az általa lefolytatott vizsgálatról nyilvános jelentést készít, amely tartalmazza a feltárt tényeket, az ezeken alapuló megállapításokat és következtetéseket. A nyilvánosságra hozott jelentés nem tartalmazhat személyes adatot, minősített adatot, a törvény által védett titkot és hivatás gyakorlásához kötött titkot. A nyilvános jelentéssel kapcsolatban meghozott intézkedések rövidítőben szóló, illetve a jelentésre adott egyéb válaszok szintén nyilvánosak, bárki által megismerhető közérdekű adatok. Továbbá a vizsgálati eljárás során megismert, az EMMI Szociális Ügyekért és Társadalmi Felzárkózásáért Felelős Államtitkárának levele nem tartalmazott olyan tényeket/adatokat, melyek nyilvánosságra hozatala az EMMI törvényes működési rendjét vagy feladat- és hatáskörének illetéktelen külső befolyástól mentes ellátását, így különösen az adatot keletkeztető álláspontjának a döntések előkészítése során történő szabad kifejtését veszélyeztette volna. Ugyanakkor tartalmazott olyan megállapításokat, amelyek megismerhetőségére széles körben nagy érdeklődés mutatkozna a hajléktalanok védelme érdekében. A NAIH felszólítására az EMMI arról tájékoztatta a Hatóságot, hogy az alapvető jogok biztosának az AJB-809/2018. számú jelentésében megfogalmazott ajánlásaira adott miniszteri válaszlevelet az adatigénylő rendelkezésére bocsátotta. (NAIH/2019/1626)

IV.10. TAO támogatások

A Hatósághoz több olyan beadvány érkezett, mely a társasági adóról és osztályadóról szóló 1996. évi LXXXI. törvény (TAO törvény) 22/C. §-a alapján nyújtott juttatások (TAO támogatások) területét érintik. A TAO támogatások – „elérhető” adóbevételeként – közpénznek, és a velük való gazdálkodásra vonatkozó adatok közérdekű adatnak minősülnek [Alaptörvény 39. Cikk (2) bekezdés; Kúria Pfv.IV.21.175/2017/14.; Kúria Pfv.IV.21.135/2017/10.].

A TAO támogatást adó gazdálkodó szervezetek ugyanis – jogszabályi felhatalmazás alapján – társasági adójuk egy meghatározott részét nem fizetik be a költségvetésbe, ezáltal az állam adóbevételeiről mond le, s azt közvetett módon

– általa meghatározott célok finanszírozására – állami illetve sportági szakszövetségi ellenőrzés mellett átirányítja. A TAO támogatás felhasználásával kapcsolatos adatok akkor is közpénzre vonatkoznak, ha ezen összegek ténylegesen nem kerülnek be a költségvetésbe, hanem az állam által meghatározott irányba „*eltérítik*” őket. A TAO támogatás közpénz jellegét támasztja alá az – EUMSZ. 288. Cikke szerint kötelező – Európai Bizottság C (2011) 7287. számú határozat 20., 58., 65. és 82. bekezdése is. A támogatás közpénz jellegét támasztja alá az is, hogy amennyiben a támogatott nem, vagy nem az adókedvezményt biztosító cérla használja fel a támogatást, úgy azt a 107/2011. (VI.30.) Kormányrendelet 14. § (2) bekezdése alapján nem a támogató, hanem az állam részére kell viszszafizetni.

A Kúria Pfv. IV. 21.175/2017. számú ítéletében kimondta, hogy az adózás rendjéről szóló 2003. évi XCII. törvény (a továbbiakban: Art.) 2016. október 24-én hatályba lépett módosítása a visszaható hatállyú jogalkotás tilalmának alkotmányos alapelvére figyelemmel az azt megelőzően keletkezett adatok esetében nem alkalmazható, vagyis a nyilvánosság korlátjákról az adótítokra való hivatkozás nem fogadható el. A Kúria ítélete alapján tehát ebben az időszakban télesen, külön-külön megismerhető, hogy a felajánló adott kedvezményezett részére mekkora összegű támogatást nyújtott. A módosítást követően keletkezett adatok esetében a jelenleg hatállyos Art. (2018. január 1-jén hatályba lépett az adózás rendjéről szóló 2017. év CL. törvény, mely a fentiekkel egyezően tartalmazza az adótítok szabályokat) alapján minden esetben végezzenek el egy érdekmérlegelési tesztet. Ennek során részletesen indokolják meg, hogy a konkrét esetben a közpénz felhasználásnak átláthatóságához fűződik-e nagyobb közérdek, vagy az esetlegesen adótítonak minősülő adatok titokban tartásához. Vegyék számba azokat a szempontokat, amelyek alapján az adatkiadás sértené az adózó vagy a kedvezményezett üzleti érdekeit, magánszféráját. A Hatóság felhívja az adatkezelők figyelmét arra, hogy az Infotv. 31. § (2) bekezdése szerint a megtagadás jogosultségét és a megtagadás indokait az adatkezelőnek kell bizonyítania. Hangsúlyozandó, hogy az Art. az adójogi jogviszonyokban a támogatás „*felajánlásának*” folyamatával kapcsolatban határoz meg adótítonak minősülő adatokat. Amennyiben a közérdekű adatigénylés nem a támogatást nyújtó adózókkal összefüggésbe hozható adatok megismerésére irányul, hanem a támogatás felhasználására, az adatigénylés adótíkokra való hivatkozással jogosről nem utasítható el.

IV.11. Labdarúgó akadémiák

A Hatóság egy ügyében a bejelentő azt kifogásolta, hogy a Magyar Labdarúgó Szövetség (MLSZ), valamint a Beruházási, Műszaki Fejlesztési, Sportüzemeltetési és Közbeszerzési Zrt. (BMSK Zrt.) megsértette a közérdekkű és közérdekből nyilvános adatok megismeréséhez fűződő jogukat, mivel nem adta ki azokat a részbeszámolókat, amelyek leadására az érintett labdarúgó, illetve sportakadémiák fejlesztésére kötött támogatási szerződések kötelezik az érintett klubokat. Az MLSZ mint törvényben meghatározott feladatokat ellátó és különleges jogosítványokat gyakorló országos sportági szakszövetség, valamint a BMSK Zrt. is közfeladatot ellátó szervnek minősül, így a kezelésükben lévő és tevékenységükkel összefüggésben keletkezett adatok főszabály szerint közérdekkű és közérdekből nyilvános adatok. Az érintett sportklubok mint kedvezményezettek az MLSZ-nek, mint támogatónak tartoznak (rész)beszámolási és elszámolási kötelezettséggel, de – az MLSZ nevében – a (rész)beszámolókat és elszámolásokat a BMSK Zrt. mint lebonyolító fogadja, ellenőri és őrzi meg. Így az MLSZ adatkezelőnek, a BMSK Zrt. pedig az MLSZ által megbízott és irányított adatfeldolgozónak minősül.

A Hatóság a vizsgálat eredményeképpen megállapította, hogy az MLSZ megsértette az adatigénylő közérdekkű és közérdekből nyilvános adatok megismeréséhez fűződő jogát és felszólította az MLSZ-t, hogy az adatigénylés tárgyát képező dokumentumokat küldje meg az adatigénylő részére. Az MLSZ a Hatóság felszólításának eleget téve négy akadémia esetében az adatigénylők részére elérhetővé tette (kiadta) a BMSK Zrt. részére benyújtott valamennyi elszámolási iratot, a további öt akadémia vonatkozásában azonban azt a tájékoztatást adta, hogy lezárt, kiadható részbeszámoló nem áll rendelkezésre, mivel a részbeszámolók ellenőrzése vagy még folyamatban van, vagy a kedvezményezett a BMSK Zrt. (többszöri) felhívása ellenére sem nyújtotta be a beszámolót vagy pótolta annak hiányait. Ennek a mulasztásnak a vizsgálata, megítélése azonban már nem tartozik a Hatóság feladat- és hatáskörébe. (NAIH/2019/1111)

Egy másik ügyben a bejelentő egy labdarúgó akadémia beruházási koncepciója másolatának kiadására irányuló adatigénylés EMMI általi elutasítását („az igényelt adat jövőbeli döntések megalapozását szolgálja”) kifogásolta. A Hatóság álláspontja szerint azonban a Kormány által jóváhagyott beruházási koncepciót e későbbi döntések nem érintik, következésképpen a beruházási koncepció nem döntés megalapozását szolgáló adat, így e közérdekkű adat nyilvánosságát az Infotv. alapján nem lehet korlátozni. A döntés megalapozására az EMMI kizárolag addig az időpontig hivatkozhatott volna, amíg a beruházási koncepció elké-

szült, tekintettel arra, hogy a koncepció végleges, jóváhagyott formája maga a döntés. Az a körülmény, hogy a koncepció jóváhagyását követően a beruházás végrehajtása folyamatban van, már nem korlátozza az adat nyilvánosságát, feltéve hogy a végrehajtás sikerét az adatok kiadása meghiúsítaná, ám az ügy tárgyát képező adatigénylés vizsgálata során erre utaló körülmény nem merült fel. (NAIH/2019/4445)

IV.12. Börtönszabályzatok

A jogalkotásról szóló 2010. évi CXXX. törvény felhatalmazása szerint a Büntetés-végrehajtás Országos Parancsnoka (BVOP) normatív utasításban szabályozhatja a vezetése, az irányítása vagy felügyelete alá tartozó szervek szervezetét és működését, valamint tevékenységét és ezeket a szabályzatokat – a minősített adatot tartalmazók kivételével – közzé kell tenni. Erre figyelemmel a BVOP utasítások főszabály szerint bárki számára elérhetők, azokat a fogvatartottak is jogosultak megismerni. Mivel elektronikus ügyintézéshez való joguk a szabadságvesztés végrehajtása alatt szünetel, a fogvatartott a BVOP utasítás megismerésére irányuló kérelmével fordulhat a fogva tartás helye szerinti intézethez is, vagy kérheti a szabályozó kinyomtatását és átadását kapcsolattartójától vagy jogi képviselőjétől. Ezzel szemben a szakutasítások, körlevelek, egyéb belső szabályozók a szakirányítási feladatok olyan, a szervezet személyzetének címzett szabályozási eszközei, melyek a büntetés-végrehajtási szervek minden nap tevékenységének általános, technikai jellegű rendezést igénylő kérdéseire adhatóak ki, amennyiben jogszabály vagy közjogi szervezet szabályozó eszköz a kérdéskört nem szabályozza, illetve közjogi szervezet szabályozó eszköz kiadása nem kötelező. A különféle jogtárakban és a büntetés-végrehajtási szervezet honlapján valamennyi BVOP utasítás (a minősített adatot tartalmazók kivételével) elérhető. A szakutasítások, körlevelek és egyéb belső szabályozó eszközök nem minősülnek közjogi szervezet szabályozó eszköznek, ezért közzétételük nem kötelező, így a BVOP jogosult dönten arról, hogy közzé kívánja-e tenni azokat. Mivel szakutasítások közzététele biztonsági jellegű kockázatot jelenthet a büntetés-végrehajtási szervezet működési rendjére, a tiltott tárgyak nagyszámú bejutásának a megakadályozása és a korrupciós bűncselekmények megakadályozása érdekében döntött úgy a BVOP, hogy a biztonsági intézkedéseit minden területen megszigorítja, a már közzétett szakutasításokat felülvizsgálja, és szükség esetén módosítja, illetve a továbbiakban nem teszi közzé szakutasításait. (NAIH/2019/4389)

IV.13. Környezeti információk

A Hatóság a környezeti információkat jelentőségüknek megfelelően „minősítetten” közérdekű adatokként kezeli, hiszen a környezeti információhoz való hozzáférés nélkül az állampolgárok nem tudják megfelelően érvényesíteni az egészséges környezethez fűződő, Alaptörvényben rögzített jogukat. Éppen ezért fontos hangsúlyozni, hogy a környezet védelmének általános szabályairól szóló 1995. évi LIII. törvény (Kvt.) alapján a környezetterheléssel, környezet igénybevételel, környezet veszélyeztetéssel összefüggő adatokat nem csak a közfeladatot ellátó, vagy közpénzből gazdálkodó szervezeteknek, hanem minden szervezetnek, gazdasági társaságnak ki kell adnia.

2019-ben a Hatóság több olyan környezeti információval kapcsolatos ügyet is vizsgált, ahol fel kellett hívni a közfeladatot ellátó szervek figyelmét a környezeti információ fogalmának a lehető legtágabb értelmezésére – amit alátámaszt az Aarhusi Egyezmény (kihirdette a 2001. évi LXXXI. törvény) végrehajtási útmutatója, az Egyezmény Jogérvényesítő Bizottságának és az Európai Bíróságnak a joggyakorlata is.

Egy ügyben azért nem teljesítették a zajmérési adatokra vonatkozó adatigénylést, mert azok még nem voltak kiértékelve. Előfordulhat, hogy a nyers adatok kiértékelése, validálása az eredeti adatuktól eltérő eredményre vezet, de a nyers adatok is környezeti információk²⁵, melyek kiadásakor az adatigénylőt tájékoztatni kell a feldolgozás hiányáról. (NAIH/2019/5627)

Egy másik ügyben az önkormányzat azért nem bocsátotta az önkormányzati képviselők rendelkezésére az Országos Meteorológiai Szolgálattól megrendelt légszennyezettségi vizsgálati jegyzőkönyvet, mert „megállapításaiból nem lehet messzemenő következtéseket levonni”. A jegyzőkönyv megállapította, hogy „az erősen rákkeltő benzo-(a)-pirén koncentrációja 4 napon is meghaladja a napi határértéket, a legszennyezetebb napon elérte ennek közel négyzerszerét is. [...] Figyelembe kell vennünk azonban, hogy messzemenő következtéseket nem szabad levonni ilyen rövid mérési programból, a szennyező források megbízható meghatározásához hosszú távú mérésre, esetleg további komponensek vizsgálatára lenne szükség”. A Hatóság hangsúlyozta, hogy az adatkiadásnak nem feltétele, hogy az adat alkalmas legyen következtetések levonására. (NAIH/2019/7779)

²⁵ Lásd az Egyezmény Jogérvényesítő Bizottsága ACCC/C/2010/53 sz. ügyben hozott döntését

Az olyan esetekben, amikor az adatkezelőnek mérlegelési jogköre van, a környezeti információk nyilvánosságához fűződő közérdeket különösen jelentős súllyal kell figyelembe venni. Többek között erre hívtuk fel egy megyei jogú város önkormányzatának figyelmét, amikor nem akart kiadni egy környezeti adatokat tartalmazó megvalósíthatósági tanulmányt és költséghaszon elemzést. A Megvalósíthatósági Tanulmány az Integrált Közlekedésfejlesztési Operatív Program „Fenntartható városi közlekedés fejlesztése és elővárosi vasúti elérhetőség javítása a kevésbé fejlett régiókban” című pályázati felhívás kapcsán készült és egyértelműen környezeti információkat is tartalmazott, mert a környezettel összefüggő intézkedések és programok, valamint a környezeti elemekre, környezetterhelésre valószínűleg hatással lévő tevékenységek és költséghatékonyiségi, valamint más gazdasági elemzések is ilyennek minősülnek a nyilvánosság környezeti információkhöz valóhozzáférésének rendjéről szóló 311/2005 (XII.25.) Korm. rendelet 2. § e) pontja alapján. Egy olyan projekt, amely akár évtizedekre meghatározza egy város közösségi közlekedésének fejlesztési irányait, jelentősen kihat a városban élők környezetére, a levegő minőségére, a zajszintre. Fontos környezeti információ, hogy megfelelően „árazzák-e be” a környezeti értékeket és hogyan építik be a környezetterhelés okozta költségeket a környezetre hatást gyakorló döntésekhez felhasznált költséghaszon elemzésekbe. A költséghaszon elemzések, megvalósíthatósági tanulmányok nyilvánossága tehát biztosítja annak átláthatóságát, hogy egy projektről való döntéshozatal során figyelembe vették-e a környezeti költségeket és értékeket. Ráadásul a Megvalósíthatósági Tanulmány számos kibocsátási adatot is tartalmaz, amelyek nyilvánosságára még a környezeti információkra alkalmazandó általános szabályuktól is szigorúbb szabályok vonatkoznak, megelőzve a személyes adatok, üzleti titkok, adótitkok védelméhez fűződő érdekeket is. (NAIH/2019/1016)

A kibocsátási értékekkel kapcsolatos másik ügyben egy budapesti kerületi polgármesteri hivatal által megrendelt akusztikai szakvéleményt igényelt a helyi lakosok egy civil szervezete. A polgármesteri hivatal elutasította az adatigényt arra hivatkozva, hogy az akusztikai szakvélemények záradékai szerint azok „üzleti titkot és szellemi terméket képeznek”, illetve a szerzői jog hatálya alá tartoznak, így a szerzők hozzájárulásához kötik a szakvélemények nyilvánosságát. A Kvt. a helyi önkormányzatok környezetvédelmi feladatai közé sorolja a helyi zajvédelmi szabályok megállapítását, a fővárosban a fővárosi kerületi képviseleti-testület alkothat rendeletet a helyi zajvédelmi szabályok megállapításáról. A polgármesteri hivatal köteles elemezni, értékelni a környezet állapotát illetékeségi területén, és arról évente legalább egyszer tájékoztatni a lakosságot. Az akusztikai szakvélemények elkészítésére a hivatal adott megbízást, a vizsgálat célja a kerület utcái zajszintjének vizsgálata volt és a zaj csökkentésére vonat-

kozó intézkedési tervre javaslattétel. Az előbbiek alapján az akusztikai szakvélemények közérdekű adatok, mivel egy közfeladatot ellátó szerv kezelésében vannak, e szerv közfeladatának ellátásával összefüggésben keletkeztek és a szakvéleményekért a megrendelő közpénzből fizetett. Az akusztikai szakvélemények nem csak az Infotv. alapján, hanem a Kvt. szerint is közérdekű adatok. A Kvt. 12. § (2) bekezdése kimondja, hogy „*mindenkinek joga van a külön jogszabályban meghatározott környezeti információkat – mint közérdekű adatokat – megismerni*”. A 311/ 2005. (XII. 25.) Korm. rendelet 2. § b) pontja pedig a környezeti információk körébe sorolja a „*környezetterhelésre, ideértve a zaj [...] környezetbe történő közvetlen vagy közvetett kibocsátására*” vonatkozó információt.

A szerzői jogi korlátozással kapcsolatban megjegyzendő, hogy a szerzői jogról szóló 1999. évi LXXVI. törvény (Szjt.) nem korlátozza a szerzői jogi védelem alatt álló művek közérdekű adatként való megismeréséhez fűződő jogot, a 15/A. § csupán az igény teljesítésének módjára enged meg az Infotv.-ben foglaltaktól szigorúbb eljárási szabályokat: a *szerzői jogi védelem alatt álló mű közérdekű adatként vagy közérdekből nyilvános adatként való megismerésére irányuló igény a szerző személyhez fűződő jogainak védelme érdekében az adatot kezelő közfeladatot ellátó szerv az adatigénylő által kívánt forma és mód helyett – az adatigénylés teljesítésére rendelkezésre álló határidőben – a mű közérdekű adat vagy közérdekből nyilvános adatot tartalmazó részei megtekintésének lehetővé tételevel teljesíthető*.

A Hatóság a fentiek alapján megállapította, hogy az adatkezelő megsértette a bejelentő közérdekű adatok megismerésére vonatkozó jogát, amikor nem engedett betekintést a bejelentő által igényelt akusztikai szakvéleményeknek a mérései eredményekre és zajtérképekre vonatkozó részeibe. A polgármesteri hivatal a felszólítást követően teljesítette az adatigényt. (NAIH/2019/2549)

Az „ügyfél-minőség” kérdéséről szólt az az ügy, melyben a panaszos egy végleges természetvédelmi hatósági engedélyről szóló határozatot, valamint egy nemzeti park igazgatóságnak a határozathoz adott véleményét (NP vélemény) igényelte egy kormányhivataltól. Az adatigénylés elutasítását azzal indokolták, hogy az adatigénylő nem minősül ügyfélnek az általános közigazgatási rendtársról szóló 2016. évi CL. törvény (Ákr.) 10. § (1) bekezdése alapján. A Hatóság felszólításaiban kifejtette, hogy az Ákr. nem tartalmaz korlátozó rendelkezést a közérdekű adatok konkrét körének nyilvánosságára vonatkozóan, az Ákr. 33. §-ában szabályozott iratbetekintési jogot nem szabad összekoverni a közérdekű adatok megismeréséhez való joggal, az ott megfogalmazott korlátozás a közérdekű adatokra nem vonatkozik. A végleges határozatok nyilvánosságát – mely-

nek jogalapját az Infotv. adja – azonban még maga az Ákr. is kiemeli 33. § (5) bekezdésében. Emellett a természetvédelmi hatósági engedély és a NP vélemény környezeti információkat tartalmaz. Az Európai Bíróság a C-321/96 sz. ügyben (Mecklenburg-ítélet) kimondta, hogy bármilyen aktus, amely egy környezetvédelmi ágazat helyzetét hátrányosan befolyásolja vagy védi környezeti információ. Nem szükséges, hogy ez az aktus egy eljárást lezáró határozat legyen, azaz a természetvédelmi hatóság (közbenső) állásfoglalása környezeti információ, feltéve, hogy befolyásolja az építési tervezetet jóváhagyó határozatot. Egy fokozottan védett természeti területre vonatkozó természetvédelmi hatósági engedély és a terület értékeit számba vevő nemzeti parki vélemény nyilvánosságához, az eljárás átláthatóságához fűződő közérdekkal kiemelten fontos, ezért a Hatóság a kormányhivatalt többször is felszólította az adatigény teljesítésére, melyre végül is sor került. (NAIH/2019/78)

A környezeti információk közzétételével kapcsolatban fontos megjegyezni, hogy sokféle környezeti információt többféle szerv kezel, így az állampolgároknak nehez eligazodniuk abban, hogy milyen környezeti információt honnan igényelhetnek. Ezért különösen elvárható, hogy a környezeti információval rendelkező szervek betartsák a közzétételre vonatkozó kötelezettségeiket [lásd Kvt. 12. § (3) bekezdése, 311/ 2005. (XII. 25.) Korm. rendelet 3. § f) pontja és 4. §-a] különös tekintettel a környezeti információk jegyzékének közzétételére. A korábban ismertetett légszennyezettségi vizsgálati jegyzőkönyvvel kapcsolatos ügyben a Hatóság az önkormányzatot felszólította a környezeti információk közzétételével kapcsolatos kötelezettségei teljesítésére is. Az önkormányzat eleget tett a Hatóság felszólításának és közzétette a környezeti információk jegyzékét, továbbá honlapjára feltöltötte a légszennyezettségi vizsgálati jegyzőkönyvet is.

IV.14. Média- és internetes nyilvánosság

A Hatóság Szervezeti és Működési Szabályzatának értelmében az Információszabadság Főosztály feladatai közé tartozik az olyan adatvédelmi ügyek intézése is, ahol a személyes adatok védelméhez való jog mellett valamely más, az adatok nyilvánosságával összefüggő alapvető jog (így különösen a közérdekű vagy közérdekből nyilvános adatok nyilvánosságához vagy a sajtó és véleménynyilvánítás szabadságához fűződő alapvető jogok) együttes vagy egymásra figyelemmel történő érvényesülése vagy ütközése merül fel. 2019-ben adatvédelmi hatósági eljárásban két esetben került sor (bírságkiszabás nélkül) az adatkezelőt elmarasztaló határozathozatalra, két ügyben az eljárást

megszüntettük, a többi ügy pedig még folyamatban van. Jellemzően internetes nyilvánosság – közösségi média – a vélemezett jogosítések színtere. Ezzel kapcsolatban szeretnénk felhívni a figyelmet, hogy a kifogásolt tartalmakat, oldalakat, csoportokat, profilokat első körben az adatkezelő (Facebook) felé ajánlott jelenteni és itt lehet kérni azok törlését is.²⁶

Az egyik NAIH határozat²⁷ megállapította, hogy egy nagyközség polgármesteri hivatalának honlapján a zárt képviselő-testületi ülésen hozott döntésekről szóló polgármesteri beszámolót – jogellenesen – úgy tettek közre, hogy az önkormányzattal munkaügyi perben álló volt munkatárs személyes adatait nem takarták ki és az érintett törlés iránti kérelmét is elutasították arra való hivatkozással, hogy a zárt ülésen hozott képviselő-testületi döntés nyilvános, így a polgármester kötelező napirendi pontként jogoszerűen nyújtott tárgyilagos tájékoztatást a zárt ülésen hozott döntésről. Jelen ügyben azt kellett mérlegelni, hogy egy köztisztviselő munkaviszonyának megszüntetése miatt indult peres eljárás közvetlenül kapcsolódik-e az önkormányzat tevékenységéhez, működéséhez. Önmagában az a tény, hogy a polgármesteri hivatal mint közeladatot ellátó szerv munkaügyi perben áll(t) egy volt köztisztviselőjével, a hivatal szempontjából közérdekű adatnak minősül, vagyis a munkaügyi per ténye a perlő volt köztisztviselő személye megismerhetőségét lehetővé tevő adatok nélkül nyilvánosságra hozható, de az érintett személyes adatait felismerhetetlené kell tenni – ahogyan ezt a már hivatkozott NAIH önkormányzati tájékoztatója is javasolja.

A másik határozatban szintén elmarasztaltuk azokat a magánszemélyeket, akik a Facebookon a panaszosok személyes adatait tartalmazó bírósági ítéletet és ügyészségi határozatot posztoltak. A bejegyzések láthatóságának (ismerősökre történő) korlátozásával kapcsolatban a Hatóság megjegyezte, hogy az adatkezelés ebben az esetben sem tekinthető az ún. háztartási célú adatkezelésnek²⁸, mivel az iratokat nem maguk az érintettek töltötték fel és az adatkezelők több mint 1000 ismerőssel rendelkeznek a közösségi oldalon, akik így mind hozzáférhettek a dokumentumokhoz. (NAIH/2019/69)

Ugyanakkor egy másik ügyben egy jegyző azzal a kérdéssel fordult a Hatósághoz, hogy az Önkormányzatot érintő bírósági ítéletet a felperes megoszthatja-e a Facebook közösségi oldalon. A bírósági határozatok nyilvánosságát biztosítan-

26 A FB regisztráció és bejelentkezés nélkül is elérhető súgóközpontjának a „Szabályok és jelentések” menüpont „Visszaélés jelentése” alpontról információt található arról, hogy milyen esetekben és hogyan lehet bejelentést tenni a közösségi oldalhoz.

27 https://www.naih.hu/files/NAIH_2019_3114_hatarozat.pdf

28 GDPR 2. cikk (2) bekezdés c) pontja

dó, a Bírósági Határozatok Gyűjteményével kapcsolatos feladatokról, többek közt a közzéteendő határozatok köréről, a közzététel eljárási szabályairól, illetve a személyes adatok védelméről a bíróságok szervezetéről és igazgatásáról szóló 2011. évi CLXI. törvény (a továbbiakban: Bszi.) 166. § (2) bekezdése részletezi azt, hogy – amennyiben törvény másként nem rendelkezik – a Bírósági Határozatok Gyűjteményében közzétett határozatból nem kell törölni:

- a) az állami vagy helyi önkormányzati feladatot, valamint jogszabályban meghatározott egyéb közeladatot ellátó szerv és – ha törvény kivételt nem tesz – az e minőségében eljáró személy családi és utónevet, illetve neveit (a továbbiakban együtt: nevét), továbbá beosztását, ha az adott személy az eljárásban közeladatának ellátásával összefüggésben vett részt,
- b) a meghatalmazottként eljárt ügyvéd vagy kamarai jogtanácsos, továbbá a védő nevét,
- c) az alperesként perveztes természletes személy nevét, továbbá jogi személy vagy jogi személyiséggel nem rendelkező szervezet nevét és székhelyét, ha a határozatot olyan ügyben hozták, amelyben jogszabály alapján közérdekű igényérényesítésnek helye van,
- d) az egyesület vagy alapítvány nevét, székhelyét és képviselőjének nevét,
- e) a közérdekből nyilvános adatot.

A szóban forgó (foglalkoztatási jogviszony jogellenes megszüntetése miatt indult) eljárásban hozott bírósági ítélet a felperes nevét és lakcímét, a felperes képviseletében eljáró ügyvédi iroda nevét, székhelyét és ügyvédjének nevét, az alperes (önkormányzat) nevét és székhelyét, az alperes képviseletében eljáró ügyvéd nevét és székhelyét, valamint a község polgármesterének nevét tartalmazza. Tekintettel arra, hogy a felperes – saját elhatározásból ki nem takart – adatait leszámítva a megjelenítendő adatok az Infotv. értelmében közérdekű, illetve közérdekből nyilvános adatnak minősülnek, mely adatokat a Bszi. hivatkozott rendelkezése alapján akkor sem kellett volna törölni, ha az ítélet a Bírósági Határozatok Gyűjteményében került volna közzétételre, a Hatóság álláspontja szerint az ítélet felperes általi közzététellel adatvédelmi szempontból nem kifogásolható. (NAIH/2019/2631)

IV.15. Keresőmotorok

A Google Search keresőmotor találati listájáról történő eltávolításra irányuló kérelmek elutasításával kapcsolatos panaszok esetében nem alkalmazandó a GDPR által bevezetett egyablakos ügyintézési mechanizmus, vagyis az ilyen

ügyekben nem az ír adatvédelmi hatóság (mint a Google fő európai tevékenységi központjának helye szerinti felügyeleti hatóság) folytatja le az eljárást, hanem az a nemzeti adatvédelmi hatóság, amelyhez a panaszt benyújtották.

A „felejtéshez való joggal” kapcsolatban a GDPR kivételeket is meghatároz:

- ha az adatkezelés a véleménynyilvánítás szabadságához, valamint a tájékozódáshoz való jog (a tágan értelmezett információsabadság) gyakorlása céljából szükséges
- közérdek indokolja az adatkezelés szükségességét
- védendő magánérdekek (vagyis az adatok adatkezelés jogi igények előterjesztéséhez, érvényesítéséhez, illetve védelméhez szükségesek)

A Hatósághoz 2019-ben is számos olyan beadvány érkezett, amelyben a panaszosok azt kifogásolták, hogy a Google a kérelmük ellenére nem törölt bizonyos URL-eket a Google Search keresési találatai közül. Több esetben a Google elfogadta azt a hatósági érvelést, hogy valójában nem áll fenn közérdek az érintett törléshez fűződő jogával szemben. Érkezett olyan beadvány is, amelyben az érintett nevének egy politikai párttal való összekapcsolását sérelmezte, vagyis valójában nem a megjelölt URL eltávolítását szerette volna elérni, hanem csupán azt, hogy a Google törölje a keresőmotorból a nevéhez kapcsolt kifejezést. A Hatóság megállapította, hogy az érintett nevének a kifogásolt kifejezéssel történő összekapcsolásának megszüntetése nem okoz érdeksérelmet a Google-nek és nem korlátozza sem a véleménynyilvánítás szabadságát, sem a közvélemény tájékozódáshoz való jogát. A Hatóság felszólítására a Google a panaszos nevéhez kapcsolt kifejezést törölte a keresőmotorból. (NAIH/2019/7821)

Több érintett panaszos – akiknek az adatai a cégnyilvántartásban szerepelnek – kifogásolta, hogy a google.com internetes keresőbe beírva a nevüket a keresőprogram az érintettek nevét, „*anya nevét*” és a lakkímét a találati listában azonnal hozzáférhetővé teszi, a disztribútori szerződéssel rendelkező szervezet honlapját találati helyként megadva. A Hatóság az ügyben azzal az ajánlással fordult az igazságügyi miniszterhez, hogy tekintse át a cégnyilvántartásban kezelt közérdekből nyilvános személyes adatok hozzáférésének, terjesztésének és kereshetőségének szabályait. Külön kiemelendő az internetes keresőmotorok számára biztosított hozzáférés és az adattakarékkosság elvének olyan szintű érvényesülése, amely a cégnyilvántartás eredeti céljait – az üzleti élet átláthatóságát és tisztességeségét – arányosan képes biztosítani úgy, hogy a cégedatok, köztük személyes adatok közvetlen hozzáférése differenciált, a szükségesség és az arányosság követelményét szem előtt tartva érvényesüljön. 2019-ben az IM foglalkozott a cégnyilvánossági szabályok felülvizsgálatával –

ugyanakkor a sajtó által is ismertetett jogszabályi módosítások, mely alapján a cégnyilvántartás adataihoz való hozzáférés regisztrációhoz és díjfizetéshez kötötté vált volna, nem valósult meg – és az ajánlásban kifogásolt IM rendelet²⁹ módosítására az előzetes tervekkel ellentétben nem került sor.

IV.16. Az adatigénylő személyének kérdése

Több konzultációs beadvány is érkezett már a Hatósághoz, melyek az adatigénylő kilétének tisztázását célozták:

„Kötelezettségi-e adat kiadására a közzeladatot ellátó szerv egy olyan kérelem alapján, amelyből a kérelmező személye nem azonosítható be?

Mely adatok azok, amelyek minimálisan elégsgesek egy kérelmező egyértelmű beazonosításához?

Tekintettel arra, hogy a kérelmezők soha nem tüntetik fel sem a kérelmük, sem az azt követő adatfelhasználásuk célját, a jogszabály alapján a kérelmező köteles-e bármely célt megjelölni a kérelmében?”

Az Infotv. – Alaptörvényből eredő – alapvető előírása, hogy „bárki” benyújthat igényt közérdekű vagy közérdekből nyilvános adatok megismerésére, anélkül, hogy személyét illetően (vagy egyéb vonatkozásban is akár) igazmondási és/ vagy indokolási kötelezettsége lenne. A bárki kategóriájába valamennyi termésszes, illetve jogi személy vagy jogi személyiséggel nem rendelkező szervezet is beletartozik. Azonban abban az esetben például, amikor a szervhez olyan postai levélben érkezik egyedi adatigénylés, amelyen semmilyen azonosító adat nincs feltüntetve, úgy előfordulhat, hogy az adatigénylést nem lehet teljesíteni. minden egyes adatigénylés során esetről-esetre kell vizsgálni a körülményeket, és amennyiben más módon, akár elektronikus közzététellel eleget lehet tenni az érdeklődésnek, úgy azt az utat kell választani. A fentieket összefoglalva tehát: az adatkezelő nem jogosult a személyazonosság ellenőrzésére és nem kérhet nyilatkozatot sem az adatkérés céljáról, sem az igénylő motivációjáról.

29 Az ingyenes céginformációról szóló 47/2007. (X. 20.) IRM rendelet 5. § (3) bekezdése értelmében:

(3) Az (1) bekezdésben meghatározott adatok interneten működő keresőprogramok útján is megismerhetőek. Ebben az esetben az adatok megismeréséhez név és jelszó használata nem szükséges.

V. A Hatóság jogalkotással kapcsolatos tevékenysége

V.1. A jogi szabályozással kapcsolatos ügyek statisztikai adatai

Az állásfoglalások száma jogforrási szint szerinti bontásban			
Jogforrás/év	2017	2018	2019
Törvény	82	72	61
Kormányrendelet	89	47	49
Miniszteri rendelet	94	55	41
Kormányhatározat	33	40	34
Egyéb (Ogy. határozat, utasítás, stb.)	23	17	29
Összesen	321	231	214

Ami a Hatóság által véleményezett jogszabály-tervezetek és jogszabályok számát illeti, 2019-ben is folytatódott a több éve tapasztalható tendencia, vagyis a véleményezés céljából megküldött tervezetek számának csökkenése. Ennek oka nem ismert, de a következő tényezők szerepe feltételezhető:

1. A korábbi tapasztalatok szerint kevesebb jogszabály megalkotására kerül sor azokban az években, amikor országgyűlési képviselői vagy önkormányzati választásokat tartanak.
2. A GDPR a korábbi állapothoz képest szűkíti az adatkezeléssel kapcsolatos tagállami jogalkotás mozgásterét, ugyanis a 6. cikk (2) bekezdése értelmében a tagállamok akkor tarthatnak fenn, vagy vezethetnek be a GDPR adatkezelésre vonatkozó szabályai alkalmazásának kiigazítására irányuló szabályokat, ha az adatkezelés az adatkezelőre vonatkozó jogi kötelezettség teljesítéséhez, vagy közérdekű vagy az adatkezelőre ruházott közhatalmi jogosítvány gyakorlásának keretében végzett feladat végrehajtásához szükséges. E szabálynak való megfelelés 2018-ban még jogszabályalkotást igényelt, hiszen hatályon kívül kellett helyezni azokat a jogi normákat, amelyek kívül esnek a GDPR által meghatározott tagállami jogi szabályozási keretekben. A dereguláció és a magyar jogszabályok GDPR-hoz igazításának befejezését követően a jövőben már főként azzal a hatással lehet számolni, hogy mivel a GDPR bizonyos adatkezelési jogalapokkal összefüggésben nem teszi lehetővé a nemzeti szintű jogi szabályozást, ezért e tárgykörökben kevesebb jogszabály megalkotására kerül sor a jövőben.

3. A Hatóság számba vette azt a lehetőséget is, hogy esetleg azért csökken a véleményezés céljából megküldött előterjesztések mennyisége, mert a jogi szabályozásra irányuló tervezetek előkészítését végző miniszteriumok elmulasztják bevonni a Hatóságot a személyes adatok védelmével és a közérdekű adatok nyilvánosságával kapcsolatos tervezetek egyeztetésébe, ám a szúrópróbaszerű ellenőrzés azt mutatta, hogy e tekintetben nem romlott a helyzet a korábbi évekhez képest.

A véleményezés céljából megküldött tervezetekhez tett észrevételek összes ügyszámhoz viszonyított aránya 2019-ben is a korábbi évekhez hasonlóan alakult. Az észrevételek között nőtt az információszabadsággal kapcsolatosak hányada, de az összképet tekintve továbbra is az adatvédelemmel kapcsolatos észrevételek számosága a meghatározó.

Észrevételek jellege	Észrevételek száma		
	2017	2018	2019
Adatvédelemmel kapcsolatos	461	487	323
Információszabadsággal kapcsolatos	28	22	39
Egyéb	92	79	78
Összesen	581	588	440

V.2. A jogszabályok társadalmi egyeztetésével kapcsolatos tapasztalatok

A Hatóság azt észlelte, hogy 2019. folyamán jelentősen lecsökkent az előkészítés alatt álló jogszabálytervezetek hozzáférhetősége a nyilvánosság, az állam-polgárok számára. Ez azért is meglepő, mert a jogszabályok előkészítésében való társadalmi részvételről szóló 2010. évi CXXXI. törvény szerint a társadalmi egyeztetés során biztosítani kell, hogy a véleményezési folyamatban a véleményeknek – különös tekintettel a hátrányos helyzetű, társadalmi-gazdasági szempontból marginalizált csoportok véleményére – a lehető legszélesebb köre jelenjen meg. A jogszabályok előkészítése során biztosítani kell az egyeztetések átláthatóságát, azok minél teljesebb körű nyilvánosságát. A jogszabálytervezetek általános egyeztetési formája a honlapon megadott elérhetőségen keresztül biztosított véleményezés. A törvény 5. §-a értelmében társadalmi egyeztetésre bocsátandó tervezetek esetében általános egyeztetés tartása minden esetben

kötelező. Az általános egyeztetés során közzé kell tenni a honlapon a társadalmi egyeztetésre bocsátott tervezetet, koncepciót, valamint a tervezettel együtt a jogalkotásról szóló törvényben meghatározott előzetes hatásvizsgálat összefoglalóját. A tervezet a kormányzati szervekkel való egyeztetésre bocsátás-sal egyidejűleg úgy kell közzétenni, hogy megfelelő idő álljon rendelkezésre a tervezet érdemi megítéléséhez és a vélemények kifejtéséhez. A közzétett tervezeteket a közzétételtől számított egy évig nem lehet a honlapról eltávolítani. Korábban is előfordult – még ha ritkán is – olyan eset, hogy téves jogértelmezés vagy adminisztratív hiba folytán elmaradt egy-egy tervezet közzététele vagy késve került sor arra, ám 2019-ben azzal szembesültünk, hogy a tervezetek Kormány honlapján történő közzététele szinte teljesen megszűnt.

A jogszabályok előkészítésében való társadalmi részvételről szóló törvényben meghatározott közzétételi szabályok alkalmazásában mutatkozó zavart azért nem szabad figyelmen kívül hagynunk, mert a jogszabály-tervezetek társadalmi egyeztetésre bocsátása nem valamiféle kegy vagy kényelmi szolgáltatás az állam részéről, hanem – mint azt a fentebb hivatkozott törvény preambleuma ki-nyilvánítja – azzal, hogy a társadalom legszélesebb rétegei bekapcsolódhatnak a jogszabályok előkészítésébe, a közjó érdekében elősegítik a jogi szabályozás sokoldalú megalapozását, ezzel pedig a jogszabályok minőségének és végrehajthatóságának javítását, amelyek együtt a jó állam elengedhetetlen feltételei. Az említett törvény tervezetét az Országgyűléshez benyújtó igazságügyi miniszter a T/1382. számú törvényjavaslat általános indoklásában találóan, szállóigei tömörséggel úgy foglalta össze e gondolatot, hogy „az emberek véleménye nem akadály, hanem maga a megoldás”.

A Hatóság töretlenül képviselt álláspontja szerint a jogszabály-tervezetek tartalma olyan közérdekű adat, amely nyilvánosságához nyomós közérdek fűződik. Az Alkotmánybíróság a 32/1992. (V. 29.) AB határozatában kifejtette, a közérdekű információkhoz való szabad hozzáférés a közhatalmat gyakorló szervek tevékenysége ellenőrizhetőségének alkotmányos biztosítéka. A nyilvánosság a közhatalom demokratikus működésének a próbája. A közérdekű adatok megismerhetősége tehát a közhatalom, a közügyek intézésének áttetszőségét mint alapvető demokratikus intézmény garanciálását is jelenti. A közérdekű adatok nyilvánossága és az azokhoz való hozzáférhetőség ezért a demokratikus jogállamiság alapvető alkotmányos biztosítéka. A 34/1994. (VI. 24.) AB határozat indokolása pedig leszögezte, hogy az információszabadság, a közhatalom gyakorlásának nyilvánossága, az állam és a végrehajtó hatalom tevékenységének átláthatósága, ellenőrizhetősége feltétele a bírálat jogának, a kritika szabadságának, a szabad véleménynyilvánításnak. Ez az alapjog tehát – az alkotmányos

korlátok megítélésével összefüggésben – legalább annyi alkotmányos védelmet élvez, mint az „anyajog”, a véleménynyilvánítás szabadságjoga. A nyílt, áttetsző és ellenőrizhető közhatalmi tevékenység, általában az állami szervek és a végrehajtó hatalom nyilvánosság előtti működése a demokratizmus egyik alapköve, a jogállami államberendezkedés garanciája. A nyilvánosság próbája nélkül az állam polgáraitól „elidegenedett gépezetté”, működése kiszámíthatatlanná, előreláthatatlanná, kifejezetten veszélyessé válik, mert az állam működésének átláthatatlansága fokozott veszélyt jelent az alkotmányos szabadságjogokra.

A Hatóság a rendelkezésére álló eszközökkel élve a jogszabály-tervezetek közigazgatási egyeztetése során jelzi az egyeztetésért felelős minisztériumnak azt, ha elmaradt az adott előterjesztés közzététele, valamint a saját honlapján (<https://naih.hu>) havonta közzéteszi a véleményezett jogszabály-tervezetekre vonatkozó állásfoglalásait.

V.3. Az Európai Unió adatvédelmi reformjához kapcsolódó jogszabály-módosítások

Jóllehet a GDPR alkalmazandóvá válásával, valamint az Infotv. bűnügyi adatvédelmi irányelvvel történő harmonizálásával kapcsolatos szektorális törvény-módosítások nagy részére már 2018-ban sor került, ám a szükséges korrekciók egy része áthúzódott 2019-re. A tárgyével kapcsolatban a következők emeldők ki:

1. Az egyes törvényeknek az Európai Unió adatvédelmi reformjával összefüggő módosításáról szóló előterjesztés több törvényt érintő módosításokat foglalt össze egy nagy „salátatörvény” csomagba, amely jellegéből adódóan sokféle jogi szabályozási kérdést és problémát vetett fel, amelyek egyeztetése már korábban megkezdődött és 2019-ben tovább folytatódott. A Hatóság egyebek mellett fenntartotta a kutatás és közvetlen üzletszerzés célját szolgáló név- és lakcím-adatok kezeléséről szóló 1995. évi CXIX. törvény (a továbbiakban: Kkt.) tekintetében korábban tett észrevételét. Eszerint a GDPR alkalmazandóvá válására tekintettel Kkt. érdemi felülvizsgálata és deregulációja szükséges, figyelembe véve azt, hogy a közvetlen üzletszerzés jogalapját a GDPR rendszerében tipikusan a 6. cikk (1) bekezdés f) pontja képezi, márpédig az ilyen adatkezelési jogviszonyok tekintetében az adatkezelés feltételeinek szabályozására a tagállami jogalkotónak nincsen jogosultsága. A Hatóság megfontolni javasolta Kkt. hatályon kívül helyezését azzal, hogy az adatszolgáltatással kapcsolatos szabályok

szükség szerint a polgárok személyi adatainak és lakcímének nyilvántartásáról szóló 1992. évi LXVI. törvénybe lennének beépíthetők.

Az említett salátatörvényben az igazságügyi alkalmazottak szolgálati jogviszonnyáról szóló 1997. évi LXVIII. törvény kapcsán arra mutatott rá a Hatóság állásfoglalása, hogy kötelező adatkezelés esetén az adatkezelés jogalapja nem lehet az érintett hozzájárulása. (NAIH/2019/835)

2. A Hatóság bejelentés alapján vizsgálta a mező- és erdőgazdasági földek forgalmáról szóló 2013. évi CXXII. törvénnel összefüggő egyes rendelkezésekről és átmeneti szabályokról szóló törvény személyes adatok kezelésére vonatkozó szabályait, melyek nyomán megkereste az agrárminisztert, a törvény korrekcióját kezdeményezve. Az állásfoglalás jelezte, hogy az említett törvény nem határozza meg kellő pontossággal a személyes adatok kezelésének célját, továbbá rámutatott arra, hogy a GDPR-ból eredő szabályozási követelményekre tekintettel csak kötelező adatkezelésként írható elő az adatok nyilvántartása, ám a kötelező adatkezelési jogviszonyokkal összefüggésben kerülendő a normaszövegenben szereplő kodifikációs megoldás, vagyis az, hogy az adatkezelő szerv a személyes adatokat „jogosult kezelní”, ugyanis az adatkezelő ténylegesen nincs és nem is lehet döntési helyzetben az adatok kezelését illetően, hanem azt a szükséges adatkör tekintetében a törvénynek elő kell írnia, és ettől az adatkezelő szerv nem térhet el. Ezért a Hatóság azt javasolta, hogy a kifogásolt szabályozási konstrukció helyett a kötelezően kezelendő adatfajták taxatív felsorolása kerüljön a törvénybe. (NAIH/2019/2067)

3. A társadalombiztosítás ellátásaira jogosultakról, valamint ezen ellátások fejedezetéről szóló törvény tervezetének véleményezése során többek között az érintett jogok szektorális törvényben történő szabályozásának jogi lehetőségeit kellett tisztázni. A Hatóság ezzel kapcsolatban felhívta a figyelmet arra, hogy a GDPR azon szabályait, amelyek az érintett hozzáférési jogát biztosítják, az adatkezelésről szóló tagállami törvényben nem szükséges és – az uniós jog sérelme nélkül – nem is lehetséges megismételni. Az állásfoglalás ez esetben is kitért arra, hogy a kötelező adatkezelést előíró törvényben kerülendő az adatok nyilvántartására és továbbítására vonatkozó szabályok feltételes módú megfogalmazása (pl. „kezelheti”, „továbbíthatja”). Ezek helyett a kötelező adatkezeléssel kapcsolatos feladatok és kötelezettségek szabályozandók a törvényben. (NAIH/2019/7480)

4. Több csomagküldő szolgáltató cég is a Hatósághoz fordult, felvilágosítást kérve a kereskedelmi tevékenységek végzésének feltételeiről szóló 210/2009. (IX.

29.) Korm. rendelet 17. §-ának (2) bekezdésében foglaltakkal kapcsolatban. E jogszabályhely a következőket írta elő: „Ha a csomagküldő kereskedőnek az információs önrögzítési jogról és az információszabadságról szóló törvény értelmében az adatvédelmi nyilvántartásba be kell jelentkeznie, a csomagküldő szolgáltató – a külön jogszabályban előírt tájékoztatási követelményekben előírtakon túl – köteles a termék ismertetőjében, illetve a termékről szóló tájékoztatóban feltüntetni az adatvédelmi nyilvántartási számát.”. Az idézett normaszöveg anakronisztikus szabályt tartalmazott, hiszen az adatvédelmi nyilvántartásra vonatkozó szabályok az EU adatvédelmi reformjához kapcsolódóan deregulálásra kerültek. Bár az adatvédelmi nyilvántartás és az abba való bejelentkezés kötelezettség megszűnése miatt az idézett jogi norma ténylegesen már semmiféle adat feltüntetési kötelezettséget nem keletkeztetett, a Hatóság a jogi helyzet csomagküldő szolgáltatók számára is megnyugtató rendezése érdekében kezdeményezte a felesleges szabály hatályon kívül helyezését. (NAIH/2019/5137)

V.4. A nagy adatkezelők és adatkezelési rendszerek

1. A Belügyminisztérium közigazgatási államtitkára arról a tervezetről kért átláthatóságot a Hatóságtól, amely szerint a gazdasági és egyéb szempontból elmaradott települések felzárkóztatásának keretében, a közbiztonság javítása érdekében olyan településeken is megteremtenék a térfogatot kamerarendszerek kiépítésének jogi lehetőségeit, amelyeken nem működik helyi közterület-felügyelet, ezért a térfogatot telepítése a hatályos törvényi keretek között nem lehetséges. A tervezet szerint az ilyen településeken a jegyző feladatkörébe kerülne a képi megfigyelőrendszerrel végzett adatkezelés.

A Hatóság az ügyben kiadott állásfoglalásában egyetértett azzal, hogy a közterületi képi megfigyelőrendszer működése akkor is hozzájárulhat a bűnmegelőzéshez, illetve a bűnuldözéshez, ha a kameráképek figyelemmel kísérése nem folyamatos, hanem csak olyankor kerül sor a felvételek utólagos felhasználására, ha a nyomozóhatóság valamely bűncselekménnyel kapcsolatban adatot igényel a települési önkormányzati képi megfigyelőrendszer harminc napra viszszamenőleg rendelkezésre álló képfolyamaiból. Feltételezhető, hogy a potenciális bűnelkövetők számára visszatartó erővel bír, ha tudomást szereznek e lehetőségről. A Hatóság ugyanakkor jelezte azt, hogy a képi megfigyelőrendszer működtetése és az adatok felhasználása törvényi szintű szabályozást igényel, hiszen a személyes adatok kötelező kezelését települési önkormányzati

rendelet nem írhatja elő. A Belügyminisztérium ennek megfelelően előkészítette a szükséges törvénymódosítást. (NAIH/2019/6074)

2. A modern információs társadalmak működése erősen függ az infokommunikációs infrastruktúrák, az informatikai rendszerek és szolgáltatások hozzáérhetőségétől és megfelelő működésétől, ezért a fejlett államokban alapvető szuverenitási és nemzetbiztonsági kérdésként merül fel a kiberbiztonság fenntartásának igénye. A kibervédelem megerősítése az adatbiztonság erősítése révén a személyes adatok védelméhez is hozzájárul, ezért a Hatóság egyetértett a Polgári Információ- és Kiberbiztonsági Központ létrehozásával, amelyet egy 2019-ben véleményezett kormány-előterjesztés irányzott elő.

Az állam és az ország informatikai biztonságához és védelméhez nemzetbiztonsági érdek fűződik, továbbá a nemzetbiztonsági szolgálatoknak rendelkezniük kell olyan kifinomult informatikai képességekkel, amelyek a kibervédelemhez is szükségesek, ezért általában véve nem kifogásolható, ha a kibervédelem központi intézménye a nemzetbiztonsági szolgálatok szervezeti rendszerén belül jön létre. Ugyanakkor egy ilyen jellegű szervezetifejlesztés érzékeny, továbbgondolásra érdemes kérdéseket is felvet. Például felmerülhet az a kérdés, hogy ha egy nemzetbiztonsági szolgálat a kibervédelmi feladatai ellátása céljából hozzáférést kap valamennyi fontos magyar állami és esetleg nagyvállalati informatikai rendszerhez, valamint az ezekben tárolt adatokhoz, akkor vajon mi a garancia arra, hogy ez hosszú távon nem fog olyan helyzet kialakulásához vezetni, amikor a nemzetbiztonsági szolgálat a kibervédelem céljából megszerzett hozzáféréseket egy átfogó titkos megfigyelési infrastruktúra létrehozásához használja fel. Törvényes keretek között, megfelelő adatvédelmi garanciák alkalmazásával természetesen egy demokratikus jogállamban is jogosről végezhető a nemzetbiztonsági és a búnöldözési célú titkos információgyűjtés, ám az e célból hozzáférhető adatforrások és adatok mennyiségi növekedése, valamint az adatok feldolgozásának és felhasználásának automatizálása idővel olyan, a személyes adatok védelmével és a demokratikus jogállamisággal kapcsolatos kockázatokhoz vezethet, amelyek kezelésére a jelenlegi jogi garanciarendszer nem feltétlenül elégsséges. Ezért fontos, hogy a kibervédelmi tevékenység a más nemzetbiztonsági feladatok ellátásától elválasztva történjék és ezt megfelelő független külső kontroll ellenőrizze.

A magyar kibervédelem jövőbeli szerepének meghatározása és lehetséges tevékenységeinek tervezése során felmerült az a lehetőség, hogy ne csak védekező jellegű kiberműveletekre kerülhessen sor, hanem offenzív jellegűekre is, elsősorban a kibertámadások elhárítása céljából. A Hatóság álláspontja sze-

rint a kibertámadó műveletek információs alapjogi keretei törvényi szabályozást igényelnek. Törvényi szintű szabálynak kell meghatároznia, hogy milyen területeken, milyen körülmények között lehetséges valamely kibertámadó művelet végrehajtása, illetve milyen cél elérése érdekében engedélyezhető ilyen művelet. Megfontolandó olyan szabályok megalkotása, amelyek korlátozzák az olyan offenzív kiberműveleteket, amelyek például a magyar állami szervek, a pártok, az egyházak, a civil szervezetek, a sajtó, vagy a közvélemény befolyásolását eredményezhetik. A Hatóság egyetért azzal, hogy az offenzív kiberműveletek a külső engedélyhez kötött eszközök között legyenek elhelyezve a nemzetbiztonsági szolgálatokról szóló törvény szabályozási rendszerében. (NAIH/2019/2443)

3. Az egyes törvények honvédelmi kérdésekkel összefüggő módosításáról szóló törvény közigazgatási egyeztetésre bocsátott tervezete a potenciális hadkötelesek, a hadkötelesek és a kiképzett tartalékosok adatai esetében egységes, centralizált, békeidőben is vezetett, sok adatforrás felhasználásával frissített nyilvántartás létrehozását irányozta elő. A Hatóság ezzel kapcsolatban emlékeztetett arra, hogy a tervezett szabályozás szükségességéről rendelkezésre álló információk elégtelen volta miatt nincs módja megalapozott véleményt alkotni arról, hogy szükségesek-e a tervezett adatgyűjtés egyes elemei; ha igen, akkor milyen tartalmú, részletességű és gyakoriságú adatgyűjtésre van szükség; továbbá összhangban van-e a tervezett szabályozás a törvénymódosítás deklarált céljával. Ezt követően a Honvédelmi Minisztérium és a Magyar Honvédség hadkiegészítési és adatvédelmi szakembereivel folytatott konzultáció során megállapítást nyert, hogy egy esetleges mozgósítás olyan rövid határidejű feladatokkal jár a Magyar Honvédség számára, amelyek végrehajtása szükséges sé teszi a hadkiegészítési adatbázis folyamatos vezetését békeidőben is.

A nevezett törvénytervezet a honvédelmi célból gyűjtött biometrikus adatok kezelését is érintette. A törvény oly módon szabályozza ezen adatok gyűjtését, hogy az adatkezelést a Katonai Nemzetbiztonsági Szolgálat (a továbbiakban: KNBSZ) végzi, ám az adatok felvételében a Honvédség erői adatfeldolgozóként közreműködnek. A nemzetbiztonsági szolgálatok feladatait és a szolgálatok által végzett adatkezelés szabályait a nemzetbiztonsági szolgálatokról szóló 1995. évi CXXV. törvény (a továbbiakban: Nbtv.) határozza meg, ezért a Hatóság azt javasolta, hogy a KNBSZ honvédségi adatkezelésről szóló törvényben szabályozott, a biometrikus adatok kezelésével kapcsolatos feladatai oly módon kerüljenek meghatározásra, hogy azok összhangban legyenek a Nbtv. vonatkozó szabályaival. A Hatóság által javasolt módosítások kiterjednek a biometrikus adatok felvételének törvényi feltételeire, a biometrikus adatok külföldre továbbításának szabályaira, valamint a biometrikus adatok megőrzésének határide-

jére. Ez utóbbi neuralgikus kérdés. A Hatóság fenntartotta azt a már a 2018-as törvénymódosítás alkalmával is hangsúlyozott álláspontját, hogy a biometrikus adatok 50 éves kötelező megőrzése ellentétes a személyes adatok célhoz kötött kezelésére vonatkozó elvvel és nyilvánvalóan készletező adatgyűjtést ír elő a KNBSZ számára, ezért a Hatóság javasolta a kötelező tárolási időtartam differenciált csökkentését például adatfajták, érintett kategóriák, adatkezelési célok szerint.

A véleményezésre bocsátott törvénytervezet minősített adatok külföldre továbbítása tekintetében olyan eljárásrendet határozott meg, amely a Hatóság szerint elengedhetetlen a minősített adat védelméről szóló 2009. évi CLV. törvényben foglaltakkal. (A közigazgatási egyeztetés során a kifogásolt rész korrekciója megtörtént.)

Végül a Hatóság a törvénytervezetre vonatkozó állásfoglalásában jelezte a HM számára, hogy a törvénymódosítás valószínűsíthetően magas kockázatú adatkezelésre vonatkozó szabályokat tartalmaz, például az egészségügyi adatok és a biometrikus adatok kezelését illetően. Az Infotv. előírja, hogy ha a tervezett adatkezelés magas kockázatú, úgy előzetes konzultációt kötelező folytatni a Hatósággal. Kötelező adatkezelés esetén az előzetes konzultációt az adatkezelést előíró jogszabály előkészítője a jogszabály-előkészítési eljárás keretei között kezdeményezi és folytatja le. Bár a véleményezett kormány-előterjesztés tartalmazott „Kockázatkezelés” és „Adatvédelmi hatások” részeket, ám ennek másfél oldalnyi terjedelme és vázlatos kifejtése nem volt arányban a tervezett adatkezelés volumenével és komplexitásával, ezért a Hatóság az adatvédelmi hatások megalapozott felmérése érdekében javasolta az adatvédelmi hatásvizsgálat kiegészítését, ezzel kapcsolatban hangsúlyozva, hogy a jogszabály-tervezet előterjesztőjének feladata és felelőssége az, hogy az előzetes adatvédelmi hatásvizsgálatot elvégezze, valamint az Infotv.-ben meghatározott határidőre tekintettel időben kezdeményezze a konzultációt e téma keretében a Hatósággal.

4. A Hatóság a Terrorterhelésről szóló körfeliratban a feladat végrehajtás magasabb szintű ellátásához szükséges eszközbeszerzések forrásainak biztosításáról szóló kormányhatározat tervezetéből szerzett tudomást a drónok mobil megfigyelőplatformként (például járódrónként) történő alkalmazására vonatkozó tervről. A Hatóság az elkövetés célszerűségét nem vitatva rámutatott arra, hogy az minden bizonnal túlmutat a kép- és hangfelvétel készítésnek a Rendőrségről szóló 1994. évi XXXIV. törvényben (a továbbiakban: RtV.) meghatározott hatályos szabályain, ezért a tervezett fejlesztések megvalósítására csak annyiban kerülhet sor, amennyiben azokat a vonatkozó törvény a személyes adatok védelmének követelményeivel összhangban lehetővé teszi.

A Hatóság javasolta, hogy a drónok újszerű felhasználási módozatait lehetővé tevő jogi szabályozás előkészítése során készüljön el a tervezett adatkezelés előzetes adatvédelmi hatásvizsgálata. (NAIH/2019/3734)

5. Egy 2019-ben előkészített törvénymódosítás lehetővé tette a rendőrség számára az igazoltatás során az intézkedés alá vont személy arcképmás alapján, gépi arcfelismerés támogatással történő azonosítását. A módosítások célja a személyi szabadság korlátozásával járó előállítások számának csökkentése, a személyazonosítás egyszerűbbé és gyorsabbá tétele, az intézkedés hatékony-ságának növelése volt. (A kormány-előterjesztés indokolása szerint az azonosítás informatikai támogatása az ismeretlen személyazonosságú holttestek azonosításához is alkalmazható lehet.) Az azonosítás folyamata a következő-képpen zajlik: ha az igazoltatott személy nem tudja a személyazonosságát igazolni, mert nincs nála személyazonosító igazolvány, úgy az intézkedést végző rendőr a nála lévő NOVA.mobil alkalmazással ellátott eszközzel fényképfelvételt készít az intézkedés alá vont személyről. Az alkalmazás ez alapján az arckép alapján felajánl öt, a központi biometrikus arcképprofil-nyilvántartásból nyert találatot, amelyek közül a rendőr helyben eldönti, melyik egyezik meg az igazoltatás alá vont személlyel. Ezután az alkalmazás letölti a központi személyiadat- és lakcímnyilvántartásból az arckép alapján kiválasztott személy igazoltatáshoz szükséges adatait. Az arcképfájlokat a mobileszköz átmenetileg tárolja, majd automatikusan törli. A NOVA.mobil alkalmazás a Rendőrség által alkalmazott Robotzsaru rendszer része. A Robotzsaru rendszerben végzett minden műveletről naplóállomány készül.

A Hatóság megállapította, hogy az adatkezelés a rendőri intézkedéshez szükséges adataik kezelését könnyíti meg. Az alkalmazás működése féleautomatikus, vagyis az igazoltatott személy azonosságának megállapítását nem a szoftver végzi, hanem az intézkedő rendőr. Az élőmunka igény olyan szűk keresztmet-szetet hoz létre az adataik felhasználásának folyamatában, amely nem teszi lehetővé a tömeges adatgyűjtést. (NAIH/2019/4523)

V.5. Az információszabadsággal kapcsolatos jogi szabályozási tervezetek

A cégnyilvánosságról, a bírósági cégejjárásról és a végelszámolásról szóló 2006. évi V. törvény (a továbbiakban: Ctv.) ingyenesen hozzáférhető céginformációra vonatkozó rendelkezése 2019. október 1-jétől úgy módosult, hogy az ingyenes

céginformáció keretében havi tíz lekérdezés megengedett, amely a céginformációs szolgálat honlapján előzetes regisztrációt követően vehető igénybe. A Ctv. azt is előírta, hogy az „*ingyenes céginformáció nem eredményezheti a cégszolgáltató egészének, illetve annak jelentős részének megszerzését*”. A törvényhez fűzött indokolás szerint „*annak érdekében, hogy az internetről elérhető ingyenes céginformációs szolgáltatást ne lehessen visszaélésre igénybe venni, a Ctv. a céginformációt igénylő azonosítását írja elő*”. A Hatóság a törvénymódosításról kiadott állásfoglalásban hangsúlyozta, hogy az ismertetett módosítások nem szolgálják az átláthatóságot, valamint a tulajdon (a hitelezők) védelmét, továbbá a korrupció elleni küzdelemmel foglalkozó magánszemélyek és civil szervezetek, újságírók adatokhoz való hozzáférésének lehetőségeit jelentősen behatárolják. A Hatóság kétségesnek tartotta a törvénymódosítás szükségeségét, ugyanis a törvénymódosításhoz készített előterjesztés nem támasztotta alá konkréatumokkal azt, hogy milyen visszaélések történtek a nyilvános cégedadokkal, amelyek a kifogásolt korlátozást szükségessé tették. A Hatóság azt is jelezte, hogy az adatokhoz való hozzáférés korlátozása, illetve fizetőssé tétele az egyéb cégedatok, például a cégek beszámolói tekintetében is jelentős visszalépést jelent a korábbi, a széles körű nyilvánosságot ingyenes hozzáféréssel biztosító rendelkezésekhez képest. (NAIH/2019/8645)

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

VI.1. A titkos megfigyelési feladatok ellátását és a személykörözést elősegítő informatikai rendszer

A Hatóság bejelentés alapján indított vizsgálatot a Nemzetbiztonsági Szakszolgálat (a továbbiakban: NBSZ) által a körözési nyilvántartási rendszerről és a személyek, dolgok felkutatásáról és azonosításáról szóló 2013. évi LXXXVIII. törvényben (a továbbiakban: Körtv.) említett, személyazonosítást elősegítő informatikai rendszer alkalmazásával végzett adatkezelés jogoszerűségének tárgyában. A Körtv. vonatkozó szabályai lényegében azt írják elő, hogy az NBSZ jogosult a körözési adatbázis arckép adatait átvenni, és ha a személyazonosítást elősegítő informatikai rendszere üzemeltetése során olyan találatot észlel, amely olyan körözött személy azonosítását segíti elő, akinek az adatai közérdekből nyilvánosak és a találat jelzése az NBSZ feladatai ellátását nem sérti, úgy a rendszer értesíti a körözési eljárást lefolytató szervet a találatról. A vázolt jogi szabályozás csak utal az NBSZ személyazonosítást elősegítő informatikai rendszerére, de sem a Körtv., sem más törvény nem tisztázza annak rendeltetését és alkalmazásának szabályait, ezért a Hatóság megkereste az NBSZ főigazgatóját a tényállás tisztázása érdekében.

Az NBSZ főigazgatója válaszának értelmében az arcképfelismerő rendszer adatkezelője az NBSZ. A rendszer alapvető célja és rendeltetése az NBSZ nemzetbiztonsági szolgálatokról szóló 1995. évi CXXV. törvény (a továbbiakban: Nbtv.) 8. § (1) bekezdés a) pontjában meghatározott szolgáltatói tevékenységének elősegítése. A rendszer azon személyek azonosítását segíti elő, akiket illetően az NBSZ a titkos információgyűjtésre feljogosított szervek megkeresésének teljesítése érdekében figyelési feladatot hajt végre. Emellett a figyelési feladatok végrehajtásának elősegítésére kiépített rendszer a Körtv. szabályai szerint alkalmazható a körözött személy azonosítására és tartózkodási helyének meghatározására is. (A Körtv. alapján önálló eszközalkalmazás nem történik.) A rendszernek az arcképfelismerésen túl nem célja az érintettek személyazonosságának meghatározása, és erre irányuló technikai megoldás nem is része a rendszernek.

A rendszer működéséhez (az arckép felismeréshez) szükséges arckép referenciaadatok az NBSZ szolgáltatásának igénybevételére jogosult szervektől érkezhetnek, illetve a körözési eljárás esetében a körözési nyilvántartást vezető

szervtől. A körözési eljárás elősegítése érdekében az NBSZ jogosult közvetlen hozzáféréssel átvenni a körözési nyilvántartás közérdekből nyilvános adatait. Ha az NBSZ a rendszer működtetése során körözött személyre vonatkozó találatot észlel, akkor értesíti a körözési eljárást folytató szervet a további intézkedések megtétele érdekében.

A rendszer állandó helyszíneken, valamint mobil adatgyűjtő pontok alkalmazásával is szerez mozgókép adatokat. Az adatgyűjtési helyszíneket az Nbtv. által feljogosított szervek megrendeléseiben szereplő helyadatok határozzák meg, az adatgyűjtés időtartamával együtt. Egy-egy adott helyszín mérete és elhelyezkedése szabja meg az adatgyűjtési pontok számát, amelyek elhelyezése során az adott helyszín megközelítési útvonalai teljes lefedettsége elsődleges szempont. Az NBSZ a megkeresésekben szereplő időintervallum, valamint a megrendelő szervvel végzett előzetes egyeztetés alapján dönt arról, hogy állandó kiépítésre vagy mobil adatgyűjtésre kerüljön sor.

A rendszerben az Nbtv. által feljogosított szervek írásbeli megrendeléseihez csatolt arcképek egyedi jellemzőinek algoritmikus elemzésével hozzák létre azt a biometrikus arckép referencia-adatbázist, amelyhez a rendszer működése során az adatgyűjtési pontokról származó képadatokat automatizáltan, emberi közreműködéssel hasonlítják. Az NBSZ az Nbtv. alapján a titkos információgyűjtésre jogosult szervek megkereséseinek teljesítése érdekében kezelt arcképadatokat a megkeresés érvényességi idejére (teljesítésének időtartamára) rendezи be a rendszer biometrikus arckép referencia-adatbázisába. A körözések kapcsán kezelt adatokat folyamatos adatkapsolattal szinkronizálják a körözési nyilvántartáshoz.

Ha az NBSZ a rendszer üzemeltetése során körözött személy azonosítását elősegítő találatot észlel, akkor értesíti a körözési eljárást lefolytató szervet. A rendszer működtetése során a reagáló képesség érdekében egy adott helyszínen az NBSZ állományának személyes jelenléte mellett az intézkedést foganatosító szerv állományának is jelen kell lennie ahhoz, hogy a körözött személlyel szemben intézkedést lehessen foganatosítani. A rendszer működtetése során közreműködő NBSZ munkatársak csak az arcképet, az ahhoz rendelt egyedi azonosító számot, valamint a megrendelő szerv megnevezését látják. Az adatgyűjtési pontokon nem helyeznek el az NBSZ által végzett képfelvételre utaló figyelmezhető táblát, vagy egyéb jelzést.

A rendszer 2018-ban mintegy 6000 arckép-azonosságot jelzett, amely alapján a nyílt intézkedést folytató szervek a helyszíneken összesen 209 igazoltatást hajtottak végre és 4 fő előállítására került sor.

A Hatóság a megismert információk alapján megállapította, hogy az NBSZ által üzemeltetett rendszer elsődleges rendeltetése a figyelési feladatok végrehajtásának elősegítése titkos információgyűjtés keretében, ami választ ad arra, hogy miért nincsenek végrehajtási rendeletben szabályozva a rendszer működtetésének részletei, és miért nem helyez el az NBSZ a figyelési helyszíneken a képfelvétel készítésére figyelmeztető jelzést. Mindazonáltal az adatkezelő szerv fentebb ismertetett válaszai alapján megállapítható, hogy bár az NBSZ vizsgált rendszerének működése rejttet, részben automatizált és az adatfelvételi ponton rögzített képallokányokban felismert személyek esetében az aktuális (figyelési és körözési) referencia-adatbázissal összefüzetve a cél a keresett személyek kiszűrése, ám megállapítható, hogy az adatkezelés nem lépi túl a nemzetbiztonsági szolgálatok Nbtv.-ben meghatározott titkos információgyűjtési és adatkezelési felhatalmazását, különös tekintettel a következőkre:

1. Az adatkezelő szerv azzal válaszolt a Hatóság adatgyűjtési pontok számára, az adatgyűjtés helyszíneire (a települések megnevezésére), valamint az adatgyűjtő pontok elhelyezésére vonatkozó kérdésére, hogy a helyszíneket az Nbtv. által feljogosított szervek megrendeléseiben meghatározott helyadatok határoz zák meg, az adatgyűjtés időtartamával együtt. A Hatóság ebből arra következtetett, hogy az NBSZ által működtetett rendszer nem nagy földrajzi területen kiépített, állandóan működő megfigyelőrendszer, hanem egyes konkrét megfigyelési feladatok által meghatározott helyszínekre lokalizáltan, az adott feladat határidejéhez igazodva működtetik azt.
2. Az NBSZ által működtetett rendszer nem alkalmas arra, hogy az adatgyűjtési pontokon a kamera látóterében megjelenő személyeket automatizáltan azonosítva tömeges, készletező személyazonosítással járó adatgyűjtést végezzen, hanem kizárolag csak a referencia-adatbázis aktuális adattartalma alapján végez arckép összehasonlítást. A referencia-adatbázis figyelési feladatokkal kapcsolatos adattartalmának megőrzési ideje az adott feladat időtartamára korlátozott. A referencia-adatbázis körözéssel kapcsolatban tárolt arcképadatait a körözési nyilvántartáshoz szinkronizálják.
3. A gépi rendszerrel segített arckép összehasonlítás, valamint a reagálás emberi munkát igényel. Az élőmunka igény olyan szűk keresztmetszetet hoz létre

az adatok felhasználásának folyamatában, amely kizárja a tömeges, készletező jellegű biometrikus adatgyűjtést.

A vizsgálat során nem jutott a Hatóság birtokába olyan információ, amely arra utalna, hogy az NBSZ a megfigyelési feladatok végrehajtását segítő és emellett a Körty.-ben foglaltak szerint is használt rejtegett megfigyelő rendszere a személyes adatok védelméhez való jog tömeges sérelmét okozó, nagy földrajzi területen folyamatosan működő, automatizált, szűrő-kutató jellegű, tömeges titkos megfigyelést végző infrastruktúraként működne. A Hatóság ezért az ügyben folytatott vizsgálatot lezárta.

VI.2. A rendőrségi informátorok adatainak megismerhetősége

Egy állampolgár amiatt fordult a Hatósághoz, mert az Országos Rendőrfőkapitányság (ORFK) nem teljesítette az arra vonatkozó adatkérését, hogy az általa megjelölt személyek a rendőrség személyi állományába tartoznak-e, illetve rendőrségi informátorok-e. A Hatóság a bejelentés alapján vizsgálatot indított az ügyben és az ORFK Hivatalához fordult a tényállás tisztázása érdekében. A megismert adatok alapján megállapítható volt, hogy az ORFK Hivatala a tényleges jogi helyzettel lényegében összhangban álló írásbeli tájékoztatást adott az adatkérőnek arról, hogy a rendőrséggel titokban együttműködő személyek (az adatkérő megfogalmazása szerint „informátorok”) kihagyása és a rendőrséggel való együttműködésük ténye nem tartozik a közérdekké vagy közérdekből nyilvános adatok körébe, hanem védendő személyes adatok, amelyek nem ismerhetők meg közérdekké adatigény alapján. A Hatóság szerint az ORFK álláspontját az is alátámasztja, hogy ha kitudónak a rendőrséggel együttműködő személyek adatai, akkor az érintetteknek tartaniuk kellene azoknak a bűnözői köröknek a bosszújától, akikkel szemben a bűnfelderítés munkáját segítették. Ilyen körülmenyek között senki sem vállalná a rendőrséggel való együttműködést, ami súlyosan veszélyeztetné a rendőrség bűnfelderítő tevékenységének hatékonyságát. Továbbá a rendőrséggel titokban együttműködő személyek nem tartoznak az Infotv. 26. § (2) bekezdésében foglaltak³⁰ hatálya alá, ugyanis a rendőrséggel titokban együttműködő személy nem tartozik a közzeladatot ellátó szerv fel-

30 „Közérdekké vagy közérdekből nyilvános adat a közzeladatot ellátó szerv feladat- és hatáskörében eljáró személy neve, feladata, munkaköre, vezetői megbízása, a közzeladat ellátásával összefüggő egyéb személyes adata, valamint azok a személyes adatai, amelyek megismerhetőségét törvény előírja. A közérdekből nyilvános személyes adatok a célhoz kötött adatkezelés elvének tiszteletben tartásával terjeszthetők. [...]”

dat- és hatáskörében eljáró személyek körébe. Ennek alapján a Hatóság arra a következtetésre jutott, hogy panaszos adatkérésében megjelölt személyek rendőri informátori minőségére vonatkozó kérdés megválaszolásának elutasítása miatti panasz nyilvánvalóan alaptalan, ezért ebben a kérdésben a vizsgálatot megszüntette és erről a panaszost tájékoztatta.

A másik kérdés esetében az ORFK Hivatala azzal indokolta a panaszos levelében megjelölt személyek rendőrségi személyi állományhoz tartozására vonatkozó kérdés megválaszolásának elutasítását, hogy Infotv. 26. § (2) bekezdésében foglaltak alapján önmagában az a tény, hogy meghatározott természetes személy a Rendőrség személyi állományába tartozik-e vagy sem, csak abban az esetben minősül közérdekből nyilvános adatnak, ha a közérdekű adatigénylés a megjelölt személy valamelyen tevékenységével kapcsolatos, ami a Rendőrség közfeladatának ellátásával vagy a közhatalmi jogosítványainak gyakorlásával összefügg. Továbbá a közérdekből nyilvános adatok csak a célhoz kötött adatkezelés elvének tiszteletben tartásával terjeszthetők és az ORFK Hivatala szerint „*a jelen esetben az adatigénylés nem jelölt meg semmiféle olyan célt, indokot, ami alapján mérlegelni lehetne, hogy amennyiben a megjelölt személyek a Rendőrség valamely szervének állományába tartoznának, úgy ez az adatigénylés vonatkozásában közérdekből nyilvános információnak minősülne, és ezzel korlátozható lenne az érintettek személyes adataihoz fűződő joga*”.

A Hatóság rámutatott arra, hogy az ismertetett gondolatmenet nem teljes, mert nem veszi figyelembe a rendvédelmi feladatokat ellátó szervek hivatásos állományának szolgálati viszonyáról szóló 2015. évi XLII. törvény (a továbbiakban: Hszt.) 276. § (2) bekezdését, amely szerint az Infotv. 26. § (2) bekezdésében foglalt adatokon túl közérdekből nyilvános adat a hivatásos állomány tagjának rendfokozata, állampolgársága, szolgálati helye, valamint a részére adományozott kitüntető cím és a kitüntető cím adományozásának időpontja is. A hivatkozott Hszt. szabály nem tartalmaz olyan megkötést, hogy a felsorolt adatok csak valamely a szolgálati viszonytal kapcsolatos tevékenységgel vagy eseménnyel (például kitüntető cím adományozása) összefüggésben lennének megismerhetők. Bár a felsorolás a Rendőrség személyi állományához tartozás tényét nem nevesíti a közérdekből nyilvános adatok között, ám a normaszövegben meghatározott adatkör – például a rendfokozat és a szolgálati hely adatok – implikálják ezen információ nyilvánosságát is. Ezért a Hszt 276. § (2) bekezdésében meghatározott, közérdekből nyilvános adatok tekintetében az adatkérés nem tagadható meg. A Hatóság ezt azzal egészítette ki, hogy az Infotv. 26. § (2) bekezdése, illetve a Hszt. 276. § (2) bekezdése szerinti adatok közül nem kell kiadni

azokat, amelyek – például a fedett nyomozók esetében – nemzeti minősített adatot képeznek.

Ami pedig a közérdekből nyilvános személyes adatok terjesztésének célhoz kötött voltát illeti, a Hatóság szerint azt is figyelembe kell venni, hogy a közérdekből nyilvános adatot kezelő szerv nem jogosult arra, hogy az adatigénylő tervezett adatfelhasználási céljának közlésétől, illetve az adatfelhasználási célra vonatkozó nyilatkozat tartalmától tegye függvé a kért, közérdekből nyilvános adatok megismerhetővé tételeit. Annak azonban nincs akadálya, hogy a közérdekből nyilvános adatok megismerhetővé tételevel egyidejűleg felhívja az adatigénylő figyelmét arra, hogy az adatkérés eredményeként megkapott közérdekből nyilvános személyes adatok jogoszerű felhasználásáért és a célhoz kötött adatkezelés követelményének megfelelő terjesztéséért a törvényben meghatározottak szerint felelősséggel tartozi.

Végül a Hatóság arra kérte az adatkezelő szervet, hogy ha a jövőben olyan adatkérést, vagy adatkéréseket észlel, amelyek a Rendőrség személyi állományának alapvető jogokat sértő szisztematikus feltérképezésére, listázására irányuló akció részeként lennének értelmezhetők, úgy erről értesítse a Hatóságot, hiszen a Rendőrség állományába tartozó személyek adataival történő tömeges visszaélés éppúgy elfogadhatatlan, mint bármely más állampolgár esetében.

A levélváltás eredményeként az ORFK Hivatala a közérdekből nyilvános adatok tekintetében megválaszolta a panaszos adatkérését. (NAIH/2019/6373)

VI.3. A Hatóság adatmegismerési jogosultságának korláta

A Hatóság Alaptörvényben konstituált információs alapjogvédelmi ellenőrző rendeltetéséből eredő követelmény, hogy megismerhesse mindenkorat az adatokat, amelyek a feladatainak ellátásához szükségesek. Az adatok megismerésére vonatkozó jogosítványokat (például az adatkezelés helyszínére történő belépés, írásbeli felvilágosítás kérés stb.) az egyes eljárástípusokra (például vizsgálati eljárás, adatvédelmi hatósági eljárás, titokfelügyeleti hatósági eljárás) vonatkozó törvényi normaanyag tartalmazza, a megismerhető adatköröket pedig az Infotv. 71. §-a szabályozza. E rendelkezés értelmében a Hatóság eljárása során – az annak lefolytatásához szükséges mértékben és ideig – főszabály szerint kezelheti mindenkorat személyes adatokat, valamint törvény által védett titoknak és hi-

vatás gyakorlásához kötött titoknak minősülő adatokat, amelyek az eljárással összefüggnek, illetve amelyek kezelése az eljárás eredményes lefolytatása érdekében szükséges. A Hatóság az eljárásai során jogoszerűen megszerzett iratot, adatot vagy egyéb bizonyítási eszközt más eljárásában felhasználhatja. A minősített adatot érintő adatkezeléssel kapcsolatos eljárása során a Hatóság elnökhelyettese, vezetői munkakört betöltő közisztviselője és vizsgálója – ha megfelelő szintű személyi biztonsági tanúsítvánnyal rendelkezik – a minősített adatot a minősített adat védelméről szóló törvényben meghatározott felhasználói engedély nélkül is megismerheti. (A Hatóság elnökének minősített adatokkal kapcsolatos jogosítványai a minősített adatok védelméről szóló törvényben szerepelnek.)

Azonban az Infotv. a főszabály alóli kivételként előír olyan korlátozásokat, amelyek számos adatkör tekintetében lényegében kizárták az adatok Hatóság általi megismerését. E korlátozások mindenkor nem akadályozták a Hatóság feladatainak ellátását, azonban 2019. folyamán több olyan titokfelügyeleti hatósági eljárás is indult, amelyekben az ügy érdemére jelentősen kiható körülményként jelentek meg, mert az ügy tárgyát képező minősített adatok e korlátozás alá esnek. Érdemes ezért erről bővebben is szót ejteni.

Az Infotv. 71. § (3) bekezdése értelmében a Hatóság az Infotv.-ben meghatározott eljárásai során az alapvető jogok biztosáról szóló 2011. évi CXI. törvényben (a továbbiakban: Ajbtv.) felsorolt egyes adatkörök esetében az adatokat az Ajbtv.-ben meghatározottak szerint ismerheti meg. Az Ajbtv. Infotv. által hivatkozott szabályai azokat az iratfajtákat és dokumentumokat sorolják fel, amelyekbe az alapvető jogok biztosa a Magyar Honvédséget, nemzetbiztonsági szolgálatokat, rendőrséget, Nemzeti Adó- és Vármegyei vármegyei feladatokat ellátó szerveit és bűnügyi főigazgatóságát, valamint az ügyészség nyomozást végző szervét érintő vizsgálata során nem tekinthet be. Az Infotv. szerint az Ajbtv.-ben felsoroltak közül mintegy huszonöt iratfélés megismerése a Hatóság számára is tilos. Például a Hatóság a Magyar Honvédséget érintő eljárása esetében a következő iratokat nem ismerheti meg:

- a) a Magyarország védelmét szolgáló, honvédelmi szempontból kiemelkedő fontosságú találományra, gyártmányra, védelmi beruházásra, valamint a védelmi képesség fejlesztésére vonatkozó olyan irat, amelyből azok lényege megismerhető,
- b) a Magyar Honvédség hadrendje hadrendi kivonatát seregtetszintig bezárólag tartalmazó, valamint a hadászati anyagi készletek megalakítására, fenntartására és szételepítésére vonatkozó összesített adatokat tartalmazó irat,

- c) a Magyar Honvédség különleges jogrend időszakában történő alkalmazására vonatkozó terveket tartalmazó irat,
- d) az állami és a katonai felsővezetés védett vezetési rendszerére vonatkozó irat,
- e) a Magyar Honvédség harckészültségi, riasztási és értékesítési rendszerével kapcsolatos irat, a mozgósítási készségről, a hadrafoghatóság szintjéről szóló összesített irat, valamint a katonai területek, a velük azonos vagy magasabb szintű katonai szervezetek összesített harckészültségi tervei és az ehhez kapcsolódó, az egész szervezetre vonatkozó irat,
- f) a honvédelemről felelős miniszter által vezetett minisztérium és a Magyar Honvédség híradása megszervezésének összesített terve, a rendszerezített vagy alkalmazott különleges információvédelmi eszközök kulcs- és egyéb dokumentációi,
- i) a hadászati felderítés eszközeire, azok működésére vonatkozó irat, valamint a Magyar Honvédség felderítés elleni védelmére vonatkozó összesített adatokat tartalmazó irat.

Az Infotv. szerint a Hatóság a felsorolt „[...] adatokat az Ajbtv. 23. § (7) bekezdésében meghatározottak szerint ismerheti meg”³¹. Az Ajbtv. 23. § (7) bekezdése ezen adatok esetében úgy rendelkezik, hogy ha az alapvető jogok biztosa az ügy teljes körű feltárása érdekében a felsorolt iratok megvizsgálását is szükségesnek tartja, a feladatkörrel rendelkező minisztertől kérheti azok megvizsgálását. A feladatkörrel rendelkező miniszter köteles az alapvető jogok biztosa által megkívánt vizsgálatot elvégezni vagy elvégeztetni, és a vizsgálat eredményéről az alapvető jogok biztosát az általa megállapított határidőn belül tájékoztatni. A határidő nem lehet rövidebb harminc napnál.

A Hatóság jogalkalmazó szervként a hatályos törvényben foglaltak szerint jár el, ám véleményünk szerint az előbbiekből felvázolt rendelkezések több olyan jogi problémát is felvetnek, amelyek összességükben kérdéssé válnak a szabályok alkotmányosságát és alkalmazhatóságát. A fő problémák a következők:

1. Az ismertetett jogi konstrukció az Ajbtv.-ben felsorolt iratok, illetve adatok esetében nem teszi lehetővé az adatkezelés jogszervségeinek független, külső ellenőrzését, hiszen a független külső ellenőrző szerv meg sem ismerheti azok tartalmát, hanem kizárolag a feladatkörrel rendelkező miniszter, vagyis olyasvalaki véleményére kell hagyatkoznia, aki közvetlenül érdekkelt lehet a minősítés fenntartásában.

³¹ Az Infotv. 71. § (3a) – (3c) bekezdései néhány részletet illetően enyhítik az adatok megismerésének korlátozását, de lényegében nem változtatnak a szabályozási konstrukción, ezért tárgunk szempontjában nem szükséges az ismertetésük.

2. Arról nem is szólva, hogy ha a Hatóságnak a miniszter által minősített, a fentebb ismertetett korlátozás alá eső adat minősítésének jogoszerűségét kellene ellenőriznie, úgy e szabályozási konstrukció alapján végső soron a miniszter saját maga döntené el, hogy jogoszerűen minősítette-e az adatot, és ebbe a Hatóságnak érdemben nem lehetne beleszólása.
3. Az előző pontokban vázolt problémák súlyát növeli, hogy amiatt került sor a titokfelügyeleti hatósági eljárás bíróság általi kezdeményezésének Infotv.-ben történő szabályozására, mert a 4/2015. (II. 13.) AB határozat azt állapította meg, hogy mulasztásban megnyilvánuló alaptörvény-ellenesség állt fenn annak következetében, hogy a közérdekű, illetve közérdekből nyilvános adat minősítése esetén a jogalkotó nem biztosította, hogy e nyilvánosságkorlátozással szemben a közérdekű adatok megismeréséhez való alapvető jogot közvetlenül, az adatminősítés tartalmi felülvizsgálatát jelentő eljárás útján érvényesíteni lehessen. Az AB határozat indoklása szerint az Alkotmánybíróság megállapította, hogy az adatminősítés feletti érdemi kontroll nélkül a közérdekű adatok megismeréséhez való jog korlátozásának szükségessége és arányossága nem biztosítható. Amennyiben a jogrendben nincs olyan hatékony eljárás, amely alkalmas a minősítő nyilvánosságot korlátozó döntését érdemben felülvizsgálni és felülbírálni, úgy nem garantálható, hogy az adatminősítés a közérdekű és a közérdekből nyilvános adatok közül csak azokra vonatkozzon, amelyek esetében az valóban elkerülhetetlen. Nem garantálható továbbá az sem, hogy a minősítő indokolási kötelezettségének megfelelően eleget tegyen, s mérlegelése során kellő súllyal vegye figyelembe a nyilvánossághoz fűződő közérdeket. A közérdekű adatok megismeréséhez való jog alapján tehát az adatminősítés felett olyan közvetlenül kezdeményezhető érdemi kontrollt kell biztosítani, amely alkalmas arra, hogy annak során ne csupán a minősítés formai és eljárási követelményeinek megtartását ellenőrizzék, hanem arra is, hogy a minősítés tartalmi indokoltságát, meg-alapozottságát, a nyilvánosság-korlátozás szükségességét és arányosságát érdemben felülvizsgálják. Az Alkotmánybíróság felhívta az Országgyűlést, hogy jogalkotói feladatának 2015. május hó 31. napjáig tegyen eleget. Ennek nyomán került sor az Infotv. kiegészítésére azzal, hogy ha a közérdekű adat megismerése iránti igény teljesítését az adatkezelő az adatok minősített volta miatt tagadja meg, és az adatot igénylő a közérdekű adat megismerésére vonatkozó igény elutasítása felülvizsgálatának érdekében a bírósághoz fordul, a bíróság köteles a Hatóság titokfelügyeleti hatósági eljárását kezdeményezni, egyidejűleg a peres eljárást felfüggeszti. Vagyis az ismertetett AB határozat és törvényszöveg értelmében a Hatóság titokfelügyeleti hatósági eljárásának kell betöltenie az adatminősítés tartalmi felülvizsgálatát jelentő érdemi kontroll szerepét. E köve-

telménnyel nem egyeztethető össze az, ha a törvény úgy szabályozza a Hatóság eljárásának rendjét, hogy bizonyos adatkörök esetében ténylegesen egy miniszter mondhatja ki a végső szót arról, hogy jogosít-e az adat minősítése.

4. A kifogásolt jogi konstrukció keretei között a Hatóságnak a titokfelügyeleti hatósági eljárásban egyetlen eszköze van a tényállás tisztázására, mégpedig az, hogy a minisztertől kérje az olyan iratoknak a megvizsgálását, amelyek tartalmát nem ismerheti meg. A bizonyítás ezen eszközének kizárolagossá tétele nincs összhangban az általános közigazgatási rendtartás szabad bizonyítási rendszerével.

5. Ha egy adatigénylő jogorvoslatot keres a bíróság előtt amiatt, mert az adatkezelő megtagadta a közérdekű adat megismerésére vonatkozó kérésének teljesítését és a bíróság az emiatt indult perben az Infotv. 31. § (6a) bekezdésének megfelelően a Hatóság titokfelügyeleti eljárását kezdeményezi, majd a titokfelügyeleti hatósági eljárásban a Hatóságnak kizárolag az adat tekintetében feladatkörrel rendelkező miniszter (aki adott esetben lehet maga a minősítő, vagy a minősítő felettese, vagy egyébként a minősítés fenntartásban érdekkelt személy) véleményére hagyatkozva kell a határozatában megállapítania azt, hogy az adat minősítése jogosít volt az megalapozottan vetheti fel az adatigénylő tisztességes eljáráshoz való jogának szükségtelen és aránytalan korlátozását is.

VII. Nemzetközi ügyek és társadalmi kapcsolatok

Az Európai Adatvédelmi Testületet (a továbbiakban: Testület) az EU általános adatvédelmi rendelete hozta létre 2018. május 25-én. A 2019-es év volt az első teljes naptári év a Testület működésében. A Hatóság a Testület tevékenységében aktívan részt vesz, az alábbiakban részletesen is beszámolunk a szakértői alcsoportokban zajló munkáról. A Hatóság valamennyi szakértői alcsoportban képviselteti magát, sőt, azon túl is részt vállal olyan feladatokban, amelyek ki-emelkedő nemzetközi jelentőségűek. Ilyen az Amerikai Egyesült Államok és az EU kapcsolatában jelentős szerepet betöltő Adatvédelmi Pajzs mechanizmus (Privacy Shield) éves felülvizsgálata, amelyben magyar szakértő is rendszeren részt vesz.

VII.1. Az Európai Adatvédelmi Testület tevékenysége, jogértelmezési munkája

A Testület tevékenysége sokrétű, azonban vannak olyan hatáskörei, amelyeket mindezeitig nem gyakorolt még. Így például a hatóságok közötti vitarendezésre sem került sor. A Testület a jogértelmezés területén aktívabb, így iránymutatásokat, ajánlásokat, véleményeket fogalmaz meg és tesz közzé.

VII.1.1. A Testület jogértelmezési munkája

1. A Testület iránymutatásai

A Testület 2019-ben öt iránymutatást fogadott el. A magatartási kódex és az ellenőrző szerv működésére vonatkozó iránymutatás a GDPR 40-41. cikkének megfelelő alkalmazását segíti elő. A Testület egy másik iránymutatásban a szerződéses jogalap [6. cikk (1) bekezdés b) pont] online közegben nyújtott szolgáltatásokhoz kapcsolódó helyes alkalmazására irányuló álláspontját tette közzé.³²

³² https://edpb.europa.eu/our-work-tools/our-documents/smernice/guidelines-22019-processing-personal-data-under-article-61b_hu

A kép- és hangfelvételre alkalmas eszközök révén megvalósuló adatkezelésekkel összefüggő iránymutatás az egyik legnagyobb várakozással övezett dokumentum.³³ A Testület ezt az iránymutatást is nyilvános konzultációt követően véglegesítette. Szintén technológiai vonatkozású volt az a két irányutatás, amelyet a Testület még 2019-ben elfogadott: az egyik a beépített és az alapértelmezett adatvédelem témaörében³⁴ született meg, míg a másik az elfelejtéshez való jog kérdéseit³⁵ foglalta össze. Ez utóbbi a következő időszakban ki fog egészülni egy második részzel, minden esetre a Testület már közzétette azokat az ajánlásait, amelyekben konszenzusra jutott.

2. A Testület véleményei

A Testület által nyilvánosságra hozott vélemények legnagyobb része az egységességi mechanizmus körében született. Az egységességi eljárások során a tagállami hatóságok tagállami szinten gyakorolt hatásköre testületi jóváhagyás mellett történik. A GDPR ezen eljárások révén kívánta biztosítani, hogy a rendelet egységesen kerül alkalmazásra az Unió tagállamaiban. Az adatvédelmi felügyeleti hatóságok az adatvédelmi hatásvizsgálat alá vonandó adatkezelések listáját a GDPR 35. cikk (4) bekezdése alapján fogadták el, amelyek minden egyike egységességi eljárásban keresztül nyerte el végső formáját³⁶. E döntések egy része 2019-ben született, így a Testület véleményeinek egy része e listákat érintette.

Ugyanilyen eljárás keretében határozzák meg a hatóságok azokat az adatkezeléseket, amelyek nem tartoznak adatvédelmi kötelezettség hatálya alá. 2019-ben három ilyen vélemény, és ehhez kapcsolódó tagállami döntés született.

Fontos jogértelmezési kérdésekben is egységességi eljárásra került sor, így ennek keretében fogadott el véleményt a Testület a GDPR és az elektronikus hírközlési adatkezeléseket szabályozó, ún. *e-Privacy irányelv egymásra tekintettel történő alkalmazásáról*³⁷, továbbá arról, hogy melyik adatvédelmi felügyeleti ha-

33 https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-32019-processing-personal-data-through-video_hu

34 https://edpb.europa.eu/our-work-tools/public-consultations-art-704/2019/guidelines-42019-article-25-data-protection-design_en

35 https://edpb.europa.eu/our-work-tools/public-consultations-art-704/2019/guidelines-52019-criteria-right-be-forgotten-search_en

36 https://edpb.europa.eu/our-work-tools/consistency-findings/register-for-decisions_en

37 https://edpb.europa.eu/our-work-tools/our-documents/stanovisko-vyboru-cl-64/opinion-52019-interplay-between-eprivacy_hu

tóság illetékes eljárni abban az esetben, ha a vizsgálat alá vont adatkezelő fő, vagy egyetlen tevékenységi helye az eljárás során változik meg az EU-ban³⁸.

Az egységességi mechanizmus keretében hagyja jóvá a Testület a kötelező erejű vállalati szabályokat (BCR). 2019-ben két ilyen vélemény született, ám ezek száma a jövőben várhatóan jelentősen emelkedni fog. A Testület a felsoroltakon túl is gyakorol hatásköröket a harmadik országba irányuló adattovábbítások szabályozását illetően, amely nélkülözhetetlen a GDPR egységes alkalmazásának előmozdításában, ehhez kapcsolódóan pedig az egységes védelmi szint megőrzésében.

3. A Testület egyéb dokumentumai

A Testület az Európai Adatvédelmi Biztossal közös véleményt bocsátott ki az elektronikus egészségügyi szolgáltatások ügyfeleinek adatkezelését érintő kérdésekben³⁹.

A Testület emellett meghatározta az európai adatvédelmi békelyegző létrehozására irányuló jóváhagyási eljárás szabályait is⁴⁰. A tanúsítás terén kevés fejlemény tapasztalható az Európai Unióban, kívánatos lenne, hogy az adatkezelő szervezetek éljenek a megfelelést biztosító önkéntes eszközökkel, így a tanúsítással is. Ennek a dokumentumnak az elfogadása értelemszerűen ebbe az irányba mutat.

VII.1.2. Szakértői alcsoportok

Az előbbiekben a Testület plenáris ülésén elfogadott dokumentumokat mutattuk be. A testületi munka döntéshozatali fóruma a plenáris ülés, azonban a munka legnagyobb része az ún. szakértői alcsoportokban zajlik. Ezt a munkát részletesen mutatjuk be a következőkben, alcsoporti bontásban.

38 https://edpb.europa.eu/our-work-tools/our-documents/parere-del-comitato-articolo-64/opinion-82019-competence-supervisory_hu

39 https://edpb.europa.eu/our-work-tools/our-documents/edpb-edps-joint-opinion/edpb-edps-joint-opinion-12019-processing_hu

40 https://edpb.europa.eu/our-work-tools/our-documents/procedure/edpb-document-procedure-approval-certification-criteria-edpb_hu

1. A GDPR kulcsfontosságú rendelkezéseivel foglalkozó szakértői alcsoport (Key provisions Expert Subgroup - KPESG)

A korábbi 95/46/EK irányelv 29. cikke alapján létrehozott Adatvédelmi Munkacsoport „Key Provisions” alcsoportja folytatta munkáját az Európai Adatvédelmi Testület felállítását követően is, „Key Provisions” szakértői alcsoport néven (a továbbiakban: KPESG). A szakértői alcsoportban az EU tagállamainak nemzeti szakértői képviselik az egyes tagállami felügyeleti hatóságokat. A KPESG kiemelt feladata általános útmutatások kidolgozása az európai adatvédelmi jogszabályok, különösen pedig a GDPR és a bűnfügyi adatvédelmi irányelv egységes értelmezésének és alkalmazásának előmozdítása érdekében. Munkájába bevonja a jogalkalmazókat és más szakértőket is nyilvános konzultációk formájában.

Kiemelendő a KPESG vezetésével kidolgozott, a személyes adatoknak a GDPR 6. cikk (1) bekezdésének b) pontja alapján történő kezeléséről az online szolgáltatások nyújtása során címmel elfogadott 2/2019. számú EDPB iránymutatás. A dokumentum tárgya a GDPR szerződéses jogalappal kapcsolatos rendelkezéseinak értelmezése, gyakorlati útmutatás az annak alkalmazása során felmerülő kérdésekkel kapcsolatban. Az iránymutatás, amelyet szintén nyilvános konzultációra bocsátottak, megtalálható a Testület honlapján⁴¹.

2. IT Felhasználói szakértő csoport (IT User Expert Subgroup)

Az IT User szakértői alcsoport a Testület egyik legfiatalabb alcsoportja. Feladata a Testület által üzemeltetett információs rendszerekkel kapcsolatos egységes felhasználói gyakorlat kialakításának elősegítése, illetve a rendszerek fejlesztéseinének és bővítésének felügyelete, különös tekintettel a Belső Piaci Információs Rendszerre (Internal Market Information System; IMI rendszer).

A szakértői alcsoport elsősorban az IMI rendszer fejlesztésével és a rendszer fennálló problémáinak felszámolásával foglalkozik. A csoport ülésein a tagok visszajelzéseket és javaslatokat fogalmaznak meg a rendszert fejlesztő csapat felé, valamint nyomon követik a fejlesztések ütemezését.

⁴¹ https://edpb.europa.eu/our-work-tools/our-documents/smernice/guidelines-22019-processing-personal-data-under-article-61b_hu

A szakértői alcsoport ülései alkalmával megtárgyalja a legfrissebb rendszerfejlesztéseket, számba veszi a hatóságoktól érkezett fejlesztési javaslatokat, illetve dönt a rendszert érintő jelentősebb változtatásokkal kapcsolatos kérdésekben.

Emellett az üléseken lehetőség nyílik arra, hogy a tagállami szakértők megosszák egymással belső ügykezelési gyakorlatuk részleteit, illetve a Testület Titkársága is intézhet felhívásokat a tagok felé a helyes és egységes felhasználói gyakorlat kialakulásának érdekében.

Habár fókuszában az IMI rendszer áll, ez a szakértői alcsoport foglalkozik a Testület működését segítő egyéb informatikai rendszerekkel is. Ilyen például az EDPB videokonferencia rendszer, valamint a tagállami hatóságok közötti belső együttműködést segítő tudásbázis és dokumentum megosztó rendszer, az EDPB Confluence.

3. Pénzügyi szakértői alcsoport (*Financial Matters Expert Subgroup*)

A pénzügyi szakértői alcsoport feladata az adatvédelmi rendelkezések alkalmazásával összefüggő kérdések vizsgálata a pénzügyi szektorban. A 2019-es évben az alcsoport feladatai közé tartozott többek között az USA külföldön élő polgárainak adózási kötelezettségeit nyomon követni hivatott megállapodás (FATCA) vizsgálata, vélemény kidolgozása az Európai Értékpapír-piaci Hatósággal (ESMA) kötendő közigazgatási megállapodáshoz, valamint egy OECD egységes jelentési rendszerhez (CRS) kapcsolódó kérdőív elkészítése.

A szakértői csoport kiemelt feladata ebben az évben a belső piaci pénzforgalmi szolgáltatásról szóló 2015/2366/EU irányelv (PSD2 irányelv) és a GDPR kapcsolatról szóló iránymutatás előkészítése, tekintve, hogy a PSD2 tagállami jogba való áltültetését követően számos adatvédelmi vonatkozású kérdés felmerült. Az alcsoport 2019. februárban PSD2 workshopot szervezett a piac szereplőivel, annak érdekében, hogy valamennyi érdemi kérdést beazonosítson, amelyre az iránymutatásnak ki kell térnie. Az iránymutatás szövegezése folyamatban van, a nyilvános közzétételre annak a Testület általi elfogadása után kerülhet sor, amely 2020. második félévében várható.

A fentiekben túl a szakértői alcsoport egy ajánlás előkészítésén dolgozik a hitelkártya adatok online kezelése és megőrzése vonatkozásában, továbbá együttműködik a technológiai szakértői alcsoporttal a blockchain és kriptovaluták téma körében készülő átfogó iránymutatás kidolgozásában.

4. Együttműködési szakértői alcsoport (Cooperation Expert Subgroup)

A szakértői alcsoport tevékenysége kevéssé követhető a külülvilág számára, hiszen olyan ügyekkel foglalkozik, amelyek a hatóságok egymás közötti együttműködésével állnak összefüggésben. A Cooperation szakértői alcsoport által előkészített dokumentumok címzettje nem az érintett polgár vagy az adatkezelő, hanem maguk az adatvédelmi hatóságok. Az alcsoportnak fontos szerepe van abban, hogy a GDPR alkalmazása a hatóságok között gördülékenyen, az eljárási szabályok közös megközelítése alapján folyhasson.

5. Közösségi oldalakkal foglalkozó szakértői alcsoport (Social Media Expert Subgroup)

A 2018-ban létrehozott szakértői alcsoport 2019-ben négy alkalommal ült össze. A kialakult gyakorlatnak megfelelően – az átláthatóság, a kölcsönös tájékoztatás és a releváns információk megosztása céljából – az ülések elején az alcsoportba delegált tagok röviden beszámolhatnak a közösségi médiával kapcsolatos, nemzeti szinten folyó tevékenységeikről, így az esetlegesen kiadott iránymutatásokról, ajánlásokról, a fontosabb vizsgálatok állásáról.

Tekintettel arra, hogy 2019-ben európai parlamenti, illetve számos tagállamban nemzeti választások is voltak, az ülések visszatérő eleme volt a személyes adatok választások során történő kezelésével és felhasználásával, illetve a politikai pártok közösségi média használatával kapcsolatos tapasztalat- és információcsere is.

Az ülések állandó eleme volt a közösségi média felhasználónak céltzott megkeresésével kapcsolatos iránymutatás megszövegezése, a dokumentum vélegesítésére azonban az ülések korlátozott száma, illetve az iránymutatás egyes részeivel kapcsolatos nem egységes álláspont miatt egyelőre nem került sor.

A szakértői alcsoport készített a felügyeleti hatóságok részére szóló, a felügyelet közös stratégiai prioritásaival kapcsolatos javaslatokat tartalmazó dokumentumot, melyet a Testület is jóváhagyott.

A szakértői alcsoport a Testülettől mandátumot kapott a közösségi hálózatok működésével kapcsolatos dokumentum elkészítésére. A tervezet szerint a dokumentum csak a felhasználói felülethez kapcsolódó (front-end) adatkezelésre fog fókusználni, és ezzel kapcsolatos ajánlásokat és legjobb gyakorlatokat fog tartal-

mazni, a háttérben futó folyamatokat (back-end) viszont nem elemezné. A dokumentum összeállítása és az érdemi munka 2020-ban folytatódik.

6. *Technológiai Szakértői Csoport (Technology Expert Subgroup)*

A Testület Technológiai Szakértői Csoportja a korábbi évekhez hasonlóan 2019-ben is több fontos iránymutatás előkészítésében, szövegezésében vett részt. A 2019-es év folyamán befejeződött a kamerás megfigyelésről szóló irányutatás szövegezése, a csoport emellett irányutatást készített a beépített és alapértelmezett adatvédelem kérdéséről⁴².

A szakértői csoport elkészítette az összekapcsolt járművekről szóló irányutatás tervezetét⁴³, továbbá az e-Privacy Irányelv és a GDPR közös alkalmazásának kérdéseiről szóló vélemény tervezetét⁴⁴ is.

A tavalyi évhez hasonlóan a szakértői csoport másik jelentős feladata a felügyeleti hatóságok által a GDPR 35. cikkének (4) bekezdése alapján benyújtott adatkezelési műveletek listájának egységességi elemzése volt. A 2019-es évre valamennyi tagállami lista elkészült és minden benyújtott lista után követését lefolytatta a szakértői alcsoport. 2019-ben több hatóság a 35. cikk (5) bekezdése alapján benyújtott olyan adatkezelési műveletek típusainak a jegyzékét, amelyekre vonatkozóan nem kell adatvédelmi hatásvizsgálatot végezni. A szakértői alcsoport ezeknek a listáknak az elemzését is elvégezte a döntéstervezeteket a plenáris ülés elé terjesztette.

Az előzőekben említettek mellett tovább folyt a munka számos ajánlás és irányutatás szövegezésével kapcsolatosan, amelyek közül kiemelendő az adatvédelmi incidensek kockázatelemzéséről és a blokkláncról szóló tervezetek szövegezése.

42 https://edpb.europa.eu/our-work-tools/public-consultations-art-704/2019/guidelines-42019-article-25-data-protection-design_en

43 https://edpb.europa.eu/our-work-tools/public-consultations-art-704/2020/guidelines-12020-processing-personal-data-context_hu

44 https://edpb.europa.eu/our-work-tools/our-documents/stanovisko-vyboru-cl-64/opinion-52019-interplay-between-eprivacy_hu

7. *Megfelelőséggel, on-line közigazgatással és egészségügyi adatkezeléssel foglalkozó szakértői alcsoport (Compliance, eGovernment and Health Expert Subgroup)*

A Testület Compliance, eGovernment and Health szakértői csoportjának hatás-körébe a GDPR szerinti magatartási kódexek, tanúsítás, adatvédelmi hatásvizsgálat, beépített és az alapértelmezett adatvédelem elvének való jogi megfelelés tartozik, ezek mellett az elektronikus közigazgatással összefüggő és az egészségügyi adatkezelések problémái is a csoport hatáskörébe tartoznak. A 2019-es évben a szakértői csoport összesen tizenegy ülést tartott.

A 2019-as év első ülésein a szakértői csoport véglegesítette a magatartási kódexekre és az elfogadott magatartási kódexnek való megfelelést ellenőrző szervezetekre vonatkozó iránymutatás szövegét. Az iránymutatást a Testület is jóváhagyta, majd a nyilvános konzultációt követően véglegesített szövegét 1/2019-es számon nyilvánosságra hozta, amely azóta magyar nyelven is elérhető, mind a Testület, mind a NAIH honlapján.⁴⁵

A szakértői alcsoport egyik fő feladata az egyes tagállami felügyeleti hatóságok által kibocsátandó, a magatartási kódexek ellenőrzését végző szerv akkreditációjára vonatkozó szempontrendszerék véleményezése. A GDPR 64. cikk (1) bekezdés c) pontja alapján ugyanis az ilyen döntéstervezetet egységességi mechanizmusban kell elfogadni. 2019-ben összesen két tagállam (Ausztria, Egyesült Királyság) nemzeti felügyeleti hatósága által összeállított szempontrendszeret véleményezett a Testület, valamint további három másik tagállam (Spanyolország, Franciaország, Belgium) kezdeményezte a Testületnél az eljárást, amelyek 2020. év elején még folyamatban voltak. A NAIH a 2020-as év első felében tervezte beadni szempontrendszerét véleményezésre a Testületnek.

A szakértői alcsoport másik fő feladata a tanúsító szervezetek akkreditációjára vonatkozó kiegészítő szempontrendszerék véleményezése, amelyről szóló döntést szintén egységességi mechanizmusban kell elfogadni. 2019-ben összesen két tagállam (Egyesült Királyság, Luxemburg) kezdeményezte a Testületnél az eljárást, amelyek még 2020. év elején folyamatban voltak. A NAIH a 2020-as év első felében tervezte beadni szempontrendszerét véleményezésre a Testületnek.

45 https://edpb.europa.eu/our-work-tools/our-documents/wytyczne/guidelines-12019-codes-conduct-and-monitoring-bodies-under_hu

8. Jogalkalmazással foglalkozó szakértői alcsoport (Enforcement Expert Subgroup)

A Testület jogalkalmazással foglalkozó alcsoportjának hatáskörébe tartozik minden olyan anyagi és eljárási jogi kérdéssel kapcsolatos téma, ügy, amely nem tartozik valamely más alcsoport feladatkörébe. Az alcsoportban jellemzően több a hatósági jogalkalmazással kapcsolatos egyeztetés, azonban, mivel a jogalkalmazás is jogértelmezést feltételez, az adatkezelői-adatfeldolgozói oldalt, valamint magukat az adatainak érintő kérdések is napirendre kerülhetnek.

A 2018. év gyakorlatával egyezően az alcsoport kéthavonta ülésezik. Az alcsoporti ülések visszatérő napirendi pontja az egyes tagállamok felügyeleti hatóságai által megvitatni javasolt anyagi és eljárási jogkérdések, gyakorlati problémák megtárgyalása, rendszerint egy-egy, a kezdeményező hatóság gyakorlatában felmerült jogeseten keresztül. A 2019. évben szó esett például a nagy állami nyilvántartásokkal kapcsolatos jogkérdésekről, a cookie-használatról, a postai szolgáltatókról, a GDPR 15. cikk (3) bekezdésének értelmezéséről, a GDPR 57. cikk (4) bekezdésének alkalmazásáról, a hatóságok vizsgálati hatásköreivel kapcsolatos tapasztalatok megosztásáról, a panaszok együttes kezelésének lehetőségeiről, az ún. érintett hatóságok azonosításával kapcsolatos feladatokról, valamint személyes adatok határon átnyúló kezelése esetében az ún. fő felügyeleti hatóság által meghozott végleges döntés megosztásáról.

A fentiek mellett az alcsoportnak továbbra is feladata az egységes jogalkalmazást segítő irányutatások kidolgozása, valamint – amennyiben szükségessé válik – a már kibocsátott dokumentumok felülvizsgálata. Az alcsoport 2019-ben bocsátotta a plenáris ülés elé a felejtés jogára vonatkozó irányutatás-tervezet első részét, amelyet a plenáris ülés 5/2019-es számon el is fogadott, és társadalmi konzultációra bocsátott.⁴⁶

⁴⁶ https://edpb.europa.eu/our-work-tools/public-consultations-art-704/2019/guidelines-52019-criteria-right-be-forgotten-search_en

9. Bírságkiszabással foglalkozó alcsoport (Fining Taskforce)

Ez a szakértői csoport az EDPB jogalkalmazással foglalkozó alcsoportjából (Enforcement Expert Subgroup) vált ki, feladata annak elősegítése, hogy a tagállami felügyeleti hatóságok bírságkiszabási gyakorlata minél inkább közeledjen egymáshoz.

A fenti cél elérése érdekében a csoport a 2019. évben is több kérdőívben mérte fel az egyes tagállamok bírságkiszabási gyakorlatát, így például a csekély súlyú, az ismétlődő és folyamatos, a természetes személyek által megvalósított adatvédelmi jogszertések körében. A kérdőívek révén a bírságkiszabással kapcsolatban nyert információk kiindulópontként szolgálhatnak egy vagy több, az összehangolt bírságkiszabást elősegítő iránymutatás kidolgozásához.

A 2019. év egyik kiemelt feladata volt az alcsoportban a „vállalkozás” GDPR (150) preambulumbekezdése, valamint GDPR 83. cikk (4)-(6) bekezdéseiben foglalt fogalmának értelmezése.

10. Nemzetközi adattovábbítás alcsoport (International Transfers Expert Subgroup - ITS)

Az Európai Adatvédelmi Testület nemzetközi adattovábbítás alcsoportja (ITS) a 2019-es évben hat alkalommal tartott ülést. A 2019-es évet a GDPR V. fejezetében található, személyes adatok harmadik országba vagy nemzetközi szervezetek részére történő továbbítására vonatkozó rendelkezések értelmezésével kapcsolatos munka határozta meg.

Az év elején fogadta el a Testület a személyes adatoknak az EGT-n kívül működő pénzügyi felügyeleti hatóságai közötti továbbításáról szóló közigazgatási megállapodás tervezetéről szóló 4/2019. számú véleményét. Ebben a Testület véleményt alkotott egy, a GDPR 46. cikk (3) bekezdés b) pontja szerinti, közhatalmi vagy egyéb, közzeladatot ellátó szervek között létrejött, közigazgatási megállapodásba beillesztendő rendelkezésekrol. A megállapodás vizsgálata, illetve a Testület véleményének előkészítése az ITS keretein belül zajlott. A vélemény kiindulópontja emellett az alcsoport szakértői által készített, a közhatalmi és közzeladatot ellátó szervek közötti adattovábbításra szolgáló eszközökről szóló iránymutatásnak, melynek szövegezése 2019. végére még nem fejeződött be. Ez az iránymutatás arra szolgálta, hogy összefoglalja a GDPR 46. cikk (2) bekezdés a) pontjában, illetve 46. cikk (3) bekezdés b) pontjában rögzített eszközökkel szemben támasztott minimális követelményeket.

Az alcsoport emellett megkezdte egy, a magatartási kódex és tanúsítás mint adattovábbítás eszközeivel kapcsolatos iránymutatás kidolgozását is, melyben a Testület összefoglalná, hogy ez a két – a GDPR által bevezetett – új eszköz milyen módon és követelmények teljesítése mellett nyújt megfelelő garanciákat személyes adatok harmadik országba történő továbbítása során.

Az ITS szakértői a 2019-es év során számos, kötelező erejű vállalati szabályok (Binding Corporate Rules, 'BCR') jóváhagyásával, és egyéb adattovábbítással kapcsolatos konkrét kérdésről is folytattak szakmai egyeztetést és tapasztalatcserét. Két esetben a Testület véleményt bocsátott ki az illetékes felügyeleti hatóság BCR jóváhagyására irányuló döntéstervezetéről is (15/2019. és 16/2019. számú vélemények), melyeknek előkészítésére szintén az ITS keretein belül került sor.

Szintén az alcsoport keretében került sor, a norvég felügyeleti hatóság szervezésében 2019. június 11-12-én Osloban egy BCR workshopra, melynek során a témaival kapcsolatban nagy tapasztalattal bíró szakértők tartottak előadásokat, illetve BCR véleményezésével kapcsolatos gyakorlati feladatok megoldására is sor került.

VII.2. A Privacy Shield határozat harmadik éves felülvizsgálata

A 2016-ban az Európai Bizottság által elfogadott megfelelőségi határozat (amely alapján az EU-USA Adatvédelmi Pajzs, ún. „Privacy Shield”, alá tartozó szervezetek megfelelő védelmi szintet biztosítanak a személyes adatoknak) harmadik éves közös felülvizsgálata 2019. szeptember 11-13. között került megrendezésre Washingtonban, melyen a NAIH egy munkatársa is részt vett. A felülvizsgálat során az Európai Bizottság munkatársainak és az Európai Adatvédelmi Testület által delegált szakértőkből álló közös uniós vizsgálócsoporthoz és az Amerikai Egyesült Államok delegációja találkozott, hogy a határozat második éves felülvizsgálata óta eltelt időben történt fejleményekről tárgyaljanak és megvitassák a Privacy Shield keretegyezményben vállalt kötelezettségekkel kapcsolatban felmerülő kérdéseket.

A felülvizsgálat során a megfelelőségi határozat hatálya alá tartozó gazdasági és kereskedelmi adatkezelésekkel kapcsolatos prezentációkra és egyeztetésre

került sor, illetve a nemzetbiztonsági és bűnüldözési célú adatkezelésekkel kapcsolatos témákat vitatták meg a felek.

A felülvizsgálatot követően az Európai Bizottság és a Testület külön jelentést készített és tett közzé annak eredményéről. A Testület jelentésének főbb megállapításai az alábbiak:

1. *Gazdasági és kereskedelmi adatkezeléssel összefüggő megállapítások*
 - A Testület üdvözölte, hogy mind a Kereskedelmi Minisztérium (Department of Commerce, 'DoC'), mind a Szövetségi Kereskedelmi Bizottság (Federal Trade Commission, 'FTC') új hivatalból eljárásokat folytatott le, melyek során ellenőzte, hogy a tanúsítással rendelkező szervezetek megfelelnek-e a Privacy Shield elveknek.
 - Általános problémaként azonosította a Testület – hasonlóan a korábbi évekhez – azt, hogy továbbra sem terjednek ki az ilyen eljárások a Privacy Shield elveknek való tényleges, tartalmi jellegű megfelelés vizsgálatára. Ennek egyik kiemelt pontjaként azonosította a jelentés az újból továbbítások („onward transfer”) esetén alkalmazott szerződéses rendelkezések vizsgálatának hiányát.
 - A Testület a jelentésében javasolta az újratanúsítási eljárásra vonatkozó határidők szigorítását, annak érdekében, hogy az eljárás elhúzódása ne eredményezzen bizonytalanságot az adatot továbbító Uniós szervezetek, illetve az érintettek számára.
2. *Nemzetbiztonsági és bűnüldözési célú adatkezelésekkel kapcsolatos megállapítások*
 - A jelentés üdvözölte az ombudsman kinevezését, illetve az adatvédelmi és polgári szabadságjogi felügyelő tanács (Privacy and Civil Liberties Oversight Board, 'PCLOB') hiányzó tagjainak kinevezését. Ez utóbbi ezáltal hosszú idő után újra képes lesz véleményeket és jelentéseket elfogadni a nemzetbiztonsági adatgyűjtésekkel kapcsolatban.
 - A jelentés fenntartotta a nemzetbiztonsági és bűnüldözési célú adatkezelésekkel kapcsolatban a korábbi években megfogalmazott aggályok egy részét, így például a jogorvoslat hiányát a külföldi hírszerzői tevékenység megfigyeléséről szóló törvény ('FISA') 702-es pontja, illetve a 12333. számú elnöki rendelet alapján történő adatgyűjtések esetén.

- A Testület ismételten megfogalmazta azon aggályát, hogy a nemzetbiztonsági célú adatgyűjtésekkel kapcsolatban nagyon kevés információt oszt meg az Amerikai Egyesült Államok delegációja a felülvizsgálat során, amely megnehezíti a megfelelő védelmi szint meglétének elemzését.

VII.3. A Hatóság nemzetközi kapcsolatai

A Hatóság kiemelten fontosnak tartja mind az európai uniós, mind az EU-n kívüli országok adatvédelemmel és információszabadsággal foglalkozó szervezeteivel való tapasztalatcserét, valamint nyitott a külföldről érkező delegációk, szakemberek és egyetemi hallgatók fogadására. Jó példa erre egyrészt az a több éves együttműködés, melynek keretében az Ukrán Tudományos Akadémia Kijevi Jogi Egyetemének hallgatói rendszeresen vesznek részt a Hatóság által kiírt pályázatokon. Másrészt kiemelendő a 2019 novemberében aláírt együttműködési megállapodás az Ukrán Parlament Emberi Jogi Biztosa és a NAIH között. A megállapodás célja a magyar és az ukrán félnek „az emberi jogok és alapvető szabadságjogok, a jogállamiság és a demokratikus fejlődés terén, különös tekintettel a személyes adatok védelmére, a nemzetközi normák kidolgozásának és hatékony végrehajtásának elősegítését célzó erőfeszítéseinek a megerősítése”.

1. A Hatósághoz érkező külföldi delegációk 2019-ben

2019. március 7-8. között bosnyák adatvédelmi szakemberek tettek látogatást Hatóságunknál. A munkatársaink által tartott előadásokon keresztül – a bosnyák kollégák előzetesen megküldött érdeklődési körének megfelelően – megismertették a GDPR és a bűnügyi adatvédelmi irányelv alkalmazásának, implementációjának magyarországi vonatkozásait.

2019. április 26-án egy Törökországot képviselő delegáció látogatott el a NAIH-hoz. A látogatás célja az volt, hogy a 2016-ban alakult török hatóság munkatársai megismerjék a NAIH működését, szervezeti felépítését, az egyes szervezetek egységek hatásköreit, feladatait, hogy az ezekből nyert ismeretekkel hatékonyabbá tegyék saját működésüket.

2019. szeptember 16-18. között a Hatóság az Ukrán Tudományos Akadémia Kijevi Jogi Egyetemének hallgatóit fogadta. Az Egyetem és a NAIH közötti együttműködés keretében 2019-ben immár harmadik alkalommal került kiírás-

ra adatvédelem téma körben pályázat. A legjobb pályaművek írói utazhattak el Magyarországra és Hatóságunk mellett megismerhették az Alapvető Jogok Biztosának Hivatala, valamint az Alkotmánybíróság működését is.

2019. szeptember 19-én egy 14 fős japán küldöttség érkezett a Hatósághoz, akik egy tanulmányúton vettek részt, amelynek célja az volt, hogy bepillantást kapjanak a magyarországi, illetve az európai gyakorlati tapasztalatokba a GDPR kapcsán. A Hatóság munkatársainak előadásait követően folytatott konzultáció során a résztvevő jogalkalmazási kérdéseket vitattak meg.

2. *A Hatóság elnökének részvételle hazai és nemzetközi szakmai konferenciákon, rendezvényeken 2019-ben*

2019. február 5. – Budapest – Adatvédelmi Reggeli az ARB Privacy Consulting Kft. szervezésében – **A GDPR alkalmazásának tapasztalatai – kerekasztal beszélgetés**

2019. február 8. – Budapest – Első Magyar Döntéshozói Think Tank (Kihívás) szakmai- módszertani konferencia az OPH-csoport szervezésében – **A GDPR kihívásai, bevezetésének tapasztalatai, különös tekintettel az alkalmazás kritikus kérdéseire**

2019. február 11. – Budapest – „GDPR a gyakorlat oldaláról – értékes válaszok első kézből” konferencia az Adatvedelmi.hu szervezésében – **A GDPR alkalmazásának tapasztalatai a NAIH szemével**

2019. február 20. – Budapest – „FRAUD 2019, Nagyító alatt a PSD2 és IT biztonsági kihívásai” konferencia az IIR Magyarország szervezésében – **A GDPR Fraud vonatkozásai**

2019. február 26. – Budapest – Biztonságpiac 2018-2019 konferencia a GTTSZ, az MRTT és a Biztonságpiac Média és Kiadó Kft. szervezésében – **IT-innovációk, adatvédelem, információbiztonsági trendek Magyarországon** – pódiumbeszélgetés

2019. március 4. – Balatonakarattyva – Magyar Honvédség Adatvédelmi Konferencia – **2018. a Hatóság szemszögéből, a GDPR eddigi tapasztalatai**

2019. március 7. – Zamárdi – A Magyar Közigazgatási Ösztöndíjprogramban részt vevő hallgatók számára előadás tartása a Miniszterelnökség Közigazgatási Ösztöndíjprogramok és Kormányhivatali Képzési Osztály szervezésében – ***Információbiztonsági és adatvédelmi alapismeretek***

2019. március 10-13. – Johannesburg – ICIC 2019, International Conference of Information Commissioners – ***Right of access to information and the impact on vulnerable groups – panel moderator***

2019. március 20. – Budapest – Képzés önkormányzati vezetők és társasházkezelők részére a Nemzeti Adatvédelmi Szövetség szervezésében – ***Magyarázat a GDPR-ról című könyv bemutatása***

2019. március 21. – Szekszárd – Tolna Megyei Kormányhivatal évi első rendes ülése – ***GDPR alkalmazásának első tapasztalatai***

2019. március 25. – Budapest – „GDPR Salátatörvény 2019., Milyen változások várhatók az ágazati törvények GDPR szabályaihoz igazítása során?” című konferencia az Infoszféra szervezésében – ***A GDPR hazai alkalmazása***

2019. április 1. – Budapest – Nemzeti Közsolgálati Egyetem Acta Humana – Emberi Jogi Közlemény periodika Közigazgatási bíráskodás téma körében rendezett kötetbemutató konferencia – *megnyitó*

2019. április 25. – Budapest – „GDPR Salátatörvény 2019., A GDPR-ral kapcsolatos tavaszi törvénymódosítások” című konferencia az Infoszféra szervezésében – ***A GDPR hazai alkalmazása, salátatörvény, statisztikák***

2019. április 29. – Budapest – Magyar Döntéshozói Think Tank (Kihívás) konferencia sorozat az OPH-csoport szervezésében – ***Az EU adatvédelmi reform-jának hatása a magyar jogalkotásban***

2019. május 14. – Balatonszemes – GDPR adatgazdai értekezlet az OTP szervezésében – ***A GDPR Magyarországon***

2019. május 15. – Budapest – 1 éves a GDPR – fókuszban a friss ágazati jogszabályok és az elmúlt év gyakorlata – tematikus képzés a NAIH és adatvédelmi szakértők előadásában az Adatvedelmi.hu szervezésében – ***Az ágazati jogszabályok változásai, avagy mostantól élesedik a helyzet?***

2019. május 23. – Budapest – Bűnügyi Szakmai Nap a Nemzeti Adó- és Vármegyei Szolgálat szervezésében – **Az adatvédelem kérdései a bűnügyi személyes adatok specialitására figyelemmel a NAIH szemszögéből**

2019. május 24. – Lillafüred – Magyar Jogászegylet Negyvenkettedik Jogász Vándorgyűlés – **A módosított Infotv. és a GDPR alkalmazásának első tapasztalatai**

2019. május 28. – Budapest – ISACA Budapest Chapter Konferencia – 2019 – **Kínpadon a GDPR 2.0**

2019. június 3. – Budapest – Magyar Bankszövetség Elnökségi Ülés – **Bankszektorral összefüggő aktuális adatvédelmi kérdések**

2019. június 4. – Budapest – IT Biztonság Szakmai Nap 2019. a Nádor Rendszerház szervezésében – **A módosított Infotv. és a GDPR alkalmazásának első tapasztalatai**

2019. június 14. – Budapest – GDPR továbbképzés és tapasztalatcsere című rendezvény a Magyar Könyvvizsgálói Kamara Oktatási Központ szervezésében – **A módosított Infotv. és a GDPR alkalmazásának első tapasztalatai**

2019. június 14. – Debrecen – Hajdú-Bihar Megyei Jogásznapi Magyar Jogász Egylet Hajdú-Bihar Megyei Szervezete szervezésében – **Az uniós adatvédelmi rendelet gyakorlati alkalmazása**

2019. július 11. – Budapest – Bírságelkerülési útmutató – hatósági ellenőrzési konferencia a Menedzser Praxis Kft. szervezésében – **NAIH bírságok a GDPR alapján**

2019. szeptember 26. – Budapest – A GDPR elmúlt 1 éve – hazai és nemzetközi gyakorlat, bírságolási tapasztalatok a KLART szervezésében – **Bírság kiszabása a gyakorlatban és érdekmérlegelés**

2019. szeptember 27. – Budapest – Kutatók éjszakája a Nemzeti Köszolgálati Egyetem szervezésében – **A GDPR alkalmazásának tapasztalatai**

2019. szeptember 30. – Madrid – Global Technology Governance for the Fourth Industrial Revolution konferencia a Digital Future Society szervezésében

2019. október 2. – Budapest – Az adatvédelem időszerű kérdései konferencia az NKE RTK Kiberbúnözés Elleni Tanszék szervezésében – **A GDPR alkalmazásának tapasztalatai**

2019. október 3. – Budapest – Jogtanácsosi konferencia a Budapesti Ügyvédi Kamara Jogtanácsosi Tagozata szervezésében – **A módosított Infotv. és a GDPR alkalmazásának tapasztalatai**

2019. október 8-9. – London – Intelligence Oversight Forum az Office of the High Commissioner for Human Rights szervezésében

2019. október 15. – Budapest – Adatvédelmi Reggeli az ARB Privacy Consulting Kft. szervezésében – **A GDPR alkalmazásának tapasztalatai – kerekasztal beszélgetés**

2019. október 16. – Balatonfüred – X. Infotér Konferencia – **MI Személyünk! – Az egyén és adatai az MI korában**

2019. október 17. – Budapest – Belügyminisztérium Probono továbbképzés – **A GDPR és az Infotv. alkalmazásának tapasztalatai – Az adatvédelem és a mesterséges intelligencia összefüggései**

2019. október 29. – Budapest – GDPR: Gyakorlati Tapasztalatok című workshop a Budapesti Kereskedelmi és Iparkamara és a NAIH szervezésében – **Gyakorlati tapasztalatok a GDPR-ral összefüggésben (hatósági ellenőrzések, bírságok)**

2019. november 6-7. – Moszkva – 10th International Personal Data Security Conference – **GDPR effects on the Hungarian legislation and data protection**

2019. november 8. – Esztergom – Jogász konferencia a katolikus egyházmezőknek dolgozó jogászok részére – **Gyakorlati tapasztalatok a GDPR-ral összefüggésben**

2019. november 14. – Debrecen – I. Egyetemi adatvédelmi tisztviselői konferencia – **GDPR – Hatósági tapasztalatok**

2019. november 25. – Balatonföldvár – Rendvédelmi adatvédelmi szakmai napok a Belügyminisztérium Országos Katasztrófavédelmi Főigazgatóság szervezésében – **Az új adatvédelmi rendelet szabályozásai**

2019. november 26. – Budapest – Éves adatvédelmi konferencia (Országos Rendőr-Főkapitányság) – **Az új adatvédelmi rendelet szabályozásai**

2019. december 3-4. – Gibraltár – 2nd Case Handling Workshop on Freedom of Information and Access to Information

2019. december 5. – Budapest – Emberi jogi konferencia, Párbeszéd, vagy monológ: Az Európai Unió jövője címmel – **Az új európai adatvédelmi szabályozás és a nemzeti szuverenitás**

2019. december 11. – Budapest – Infoszféra Konferencia: Adatvédelem 2019-2020, A GDPR alkalmazásának gyakorlata – **A NAIH tapasztalatai, határozatai, tervei**

2019. december 12. – Budapest – „Legújabb fejlemények az adatvédelmi jogban” konferencia Giovanni Buttarelli emlékére KRE-ÁJK Infokommunikációs Jogi Tanszék VII. konferenciája közös szervezésben a NAIH-hal – **A NAIH joggyakorlatának legutóbbi fejleményei**

VII.4. Pályázat az Európai Adatvédelmi Biztos pozíciójáért

Az Európai Adatvédelmi Biztos intézménye 2004-ben jött létre, amely az Európai Unió intézményeinek és egyéb szerveinek adatkezelését hivatott ellenőrizni, a tagállami adatvédelmi hatóságokhoz hasonló hatáskörrel. A biztos mandátuma öt évre szól. A mandátum lejárta előtt nyilvános pályázatot hirdetnek, amelyen a megállapított szakmai feltételeknek megfelelő jelöltek indulhatnak.

A 2019-24-es biztosi mandátumot magyar szakértő is megpályázta. A NAIH elnökhelyettese az Európai Adatvédelmi Biztos történetében első magyarként került az Európai Bizottság által a posztra javasolt szakértők rövidített listájára egy lengyel és egy francia jelölt mellett. A pályázat utolsó körébe jutott három jelöltet az Európai Unió Tanácsának állandó képviselet-vezetői (Coreper), majd pedig az Európai Parlament szakbizottsága, a LIBE is meghallgatta.

A biztosi pozíciót a pályázati eljárás végén a lengyel jelölt, Wojciech Wiewiórowski nyerte el, mindenkorral Szabó Endre Győző jelöltére a hazai adatvédelem sikereként könyvelhető el. A jelölt a Magyar Távirati Irodának elmondta, a magyarországi adatvédelmi kultúra erejét és a magyar hatóság aktív uniós szerepét is jelzi, hogy egy magyar jelölt is állva maradt az Európai Bizottság szokásos, felső vezetői kiválasztásra irányuló eljárásában. A jelölt nélkül nem utolsósorban olyan intézményi tapasztalatot is jelent, amely a jövőben hasonló pozícióra pályázó magyar jelöltek számára is hasznos.



Kép: Az Európai Adatvédelmi Biztos pozíciójára pályázó három szakértő (balról: Wojciech Wiewiórowski (PL), Yann Padova (FR), Szabó Endre Győző) az Európai Parlamentben, Strasbourgban, 2019. november 25-én, a LIBE szakbizottság előtti meghallgatás után.

VIII. A NAIH projektjei

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

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

VIII.1.1. A STAR projekt

A STAR projekt („Supporting Training Activities on the data protection Reform”) projekt az Európai Unió társfinanszírozásában, a Jogok, Egyenlőség és Polgárság 2014-2020 (REC-RDAT-TRAI-AG-2016) program égisze alatt 769138 sz. futott 2017. november 1- 2019. október 31. között.

A STAR projekt az adatvédelmi hatóságok, valamint egyéb érintettek részére, kifejezetten az adott szektor igényeinek és kihívásainak megfelelő, illetve ehhez könnyen adaptálható módon új képzési anyagokat állított össze az általános adatvédelmi rendelet megfelelő alkalmazásának elősegítése érdekében. A STAR Konzorcium 2019. október 17-én adatvédelmi tisztviselők részére rendezett konferenciát Brüsszelben, valamint részt vett az Adatvédelmi Biztosok 41. Nemzetközi Konferenciája (ICDPPC) eseményei közé felvett, adatvédelmi hatóságok részére rendezett panelen 2019. október 22-én.

Az alábbi 11 témaörben, bárki által felhasználható és az igényekhez könnyen alakítható PowerPoint prezentációs formában készült oktatási anyagok (és a kézikönyv) szabadon elérhetők és letölthetők a projekt honlapjáról angolul <http://www.project-star.eu/training-materials>, illetve a NAIH honlapjáról magyarul is⁴⁷.

- *Bevezetés az uniós adatvédelmi rendszerbe*
- *A személyes adatak kezelésének céljai és jogalapjai*
- *Az érintett jogok és azok gyakorlása*
- *Az adatkezelők és adatfeldolgozók felelőssége*
- *Az adatvédelmi tisztviselő szerepe*
- *Az adatvédelmi hatóság szerepe*

47 <https://www.naih.hu/eredmenyek.html>

- *Technikai és szervezési intézkedések*
- *Az adatvédelem kockázatalapú megközelítése*
- *Adatvédelmi hatásvizsgálat*
- *Kommunikáció az adatvédelem területén*
- *Nem csak a GDPR – a GDPR kapcsolódó jogszabályok és rendelkezések*

Az egyes képzési modulok az oktató számára útmutatást adnak az alkalmazandó pedagógiai megközelítésről, hivatkozásokat tartalmaznak a további kiegészítő anyagokhoz és forrásokhoz, valamint segítenek a diasorok adott hallgatóság igényeihez való igazításához. A képzési anyagok mellett kidolgozásra került egy kézikönyv is, amely útmutatást tartalmaz az oktatók számára a STAR képzési anyagainak használatához, valamint tartalmaz egy listát a többi GDPR képzés minőségének és átfogóságának értékeléséhez.

VIII.1.2. A STAR II projekt

A STAR II projekt („SupporT small And medium enterprises on the data protection Reform II”) az Európai Unió társfinanszírozásában, a Jogok, Egyenlőség és Polgárság 2014-2020 (REC-RDAT-TRAI-AG-2017) program keretei között, 814775 sz. fut 2018. augusztus 1.-2020. július 31. között.

A projekt a kis- és középvállalkozások struktúráját és igényeit figyelembe véve nyújt támogatást a szóban forgó vállalkozásoknak a megfelelő adatvédelmi gyakorlat kialakításában, továbbá elősegíti a GDPR egységes alkalmazását, a határokon átnyúló együttműködést, a legjobb gyakorlat terjesztését a tagállamok között.

A projekt során a Partnerek felmérik, hogy az EU-s adatvédelmi hatóságok minden módon támogatják a kis- és középvállalkozásokat (továbbiakban: KKV) a GDPR-nak való megfelelés érdekében, valamint kidolgoznak egy útmutatót az adatvédelmi hatóságok számára, amely segíti a kis- és középvállalkozásokkal való kapcsolattartásukat.

A NAIH a projekt keretében egy kimondottan erre a célra létrehozott, 2019. március 15. és 2020. március 15. között működő hotline keretében e-mail címen (kkvhotline@naih.hu) fogadja az EU-ban működő KKV-k kérdéseit. A KKV-k konzultációs jellegű kérdéseire a Hatóság munkatársai gyorsan és természetesen ingyen válaszolnak – ezzel is (az EU-ban egyedülálló módon) segítve a KKV szektor működését. A projekt során a hotline tapasztalatait is feldolgozva

kidolgozásra kerül egy kézikönyv, amely széles körben elérhető és felhasználható lesz EU-szerte.

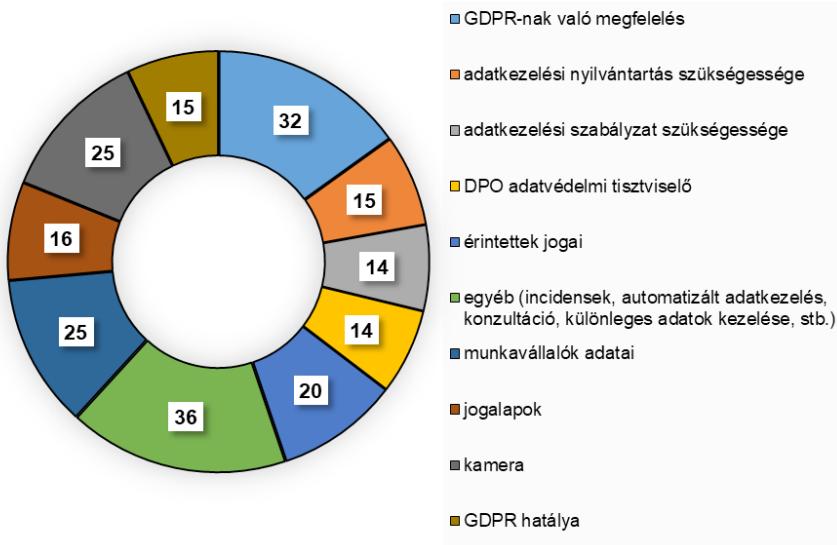
A KKV-hotline működésének első tíz hónapjában 212 kérdés érkezett a Hatósághoz. A beérkező kérdések közül 186 a GDPR konkrét esetben történő alkalmazásával, 18 a GDPR értelmezésével kapcsolatos, 8 kérdés pedig nem a hotline hatáskörébe tartozik.

A KKV-hotline-ra beérkező kérdések téma kör szerinti megoszlása



Tárgy szerint a kérdések legnagyobb része egy konkrét adatkezelés GDPR-nak való megfelelésére vonatkozott, ezt követik a kép- és hangrögzítés szabályaira, a munkavállalók személyes adatainak kezelésére, az érintett jogok gyakorlására, az adatkezelés jogalapjára valamint az adatkezelési nyilvántartás, adatkezelési szabályzat szükségességére és a GDPR hatályára vonatkozó kérdések.

A beérkező kérdések megoszlása



A hotline tapasztalatait az adatvédelmi tisztviselők (és a nyilvánosság) számára szervezett elektronikus konferencián is bemutattuk:

10. A kis- és középvállalkozásuktól a Hatósághoz beérkező kérdések bemutatása

Megtekintés

VIII.2. A KÖFOP projekt

A „Jogszabályban rögzített közzétételi kötelezettségek alá eső adatok körének felülvizsgálata” című projekt a Közigazgatás- és Közszolgáltatás-fejlesztés Operatív Program éves fejlesztési keretének megállapításáról szóló 1004/2016. (I. 18.) Korm. határozat módosításával került nevezésre 2018. november végén. A NAIH a Kormány határozatban nevezített kedvezményezettként 2019 augusztusában támogatási kérelmet nyújtott be „Az információszabadság hazai gyakorlatának feltérképezése és hatékonyságának növelése” című kiemelt projekt megvalósítására. A támogatási kérelem elbírálása folyamatban van.

VIII.3. IJR Projekt a NAIH általános adatvédelmi rendelet alkalmazására történő felkészülését és szakfeladatainak végrehajtását támogató projektje

Az 1004/2016. (I.18.) Korm. határozat alapján a KÖFOP 1.0.0. – VEKOP-15 kiemelt kormányzati projekt keretében a költségvetési szervek adminisztratív terheinek csökkentését célzó projektek között jött létre az Integrált Jogalkotási Rendszer (a továbbiakban: IJR).

A projekt keretében valósult meg 2019-ben a NAIH európai uniós kötelezettségeiből adódó jogszabály-változáshoz igazodó eljárásrendi, ügyviteli, információtechnológiai és információbiztonsági fejlesztése.

2017 áprilisában aláírásra került a 1585/2016. (X. 25.) Korm. határozat alapján az IJR projekt Támogatási Szerződés 1. számú módosítása, amely a konzorciumi partnerek között nevesít a Hatóságot, illetve a projekt által támogatott és a GDPR-ból is fakadó támogatott feladatokat.

A GDPR-ban foglalt követelmények teljesítése a NAIH jogi szakmai területeinek teljes optimalizálását, áttervezését és ezek megvalósítását igényelte 2019-ben, továbbá szükségessé vált az újratervezett folyamatokat támogató IT Környezet kialakítása és üzemben tartásának biztosítása, a rugalmas áttervezhetőség biztosítása mellett.

A NAIH szervezeti keretei is sokkal inkább a hatósági eljárásokhoz szükséges működési követelmények irányába mozdultak el, amely hangsúlyozottan egy fejesebb és kontrollálhatóbb működési megközelítést igényelt 2019-ben.

A projekt keretében végrehajtásra került jogi- szakmai és IT-fejlesztés eredménytermékéhez a támogatásnak (support) és az üzemeltetésnek is igazodnia kellett úgy, hogy közben a jogi szakmai szervezetfejlesztés során kialakított új szervezeti struktúrát is létre kellett hozni.

Az IJR projekt keretében 2018-ban létrejött az adatvédelmi incidensek adatkezelők általi bejelentésére szolgáló rendszer (DBN), és a feldolgozást biztosító (DBP) rendszer, mely a 2019-es évben több mint 500 adatvédelmi incidenst jelentést kezelt.

2019-ben az IJR projekt keretében folytatódott a NAIH számára egy integrált, intelligens ügyintéző és határozat-előkészítő modul fejlesztése, valamint sor került, a rendszerek informatikai, IT biztonsági és szervezeti implementációjára is.

Az IJR projekt 2019-es eredménytermékei az ügyintézői és határozatszerkesztő modul, melynek bevezetése és szervezeti implementációja folyamatban van. A Konzorcium vezető (Igazságügyi Minisztérium) kezdeményezte a KÖFOP IH felé a projekt végrehajtási időszakának 2020.12.31-ig meghosszabbítását.

IX. Mellékletek

IX.1. Elutasított közérdekűadat-igénylések és tájékoztatási kérelmek

IX.1.1. Az elutasított közérdekűadat-igényléskről és azok indokairól szóló 2019. évi tájékoztatási kötelezettség teljesítésének statisztikai adatai

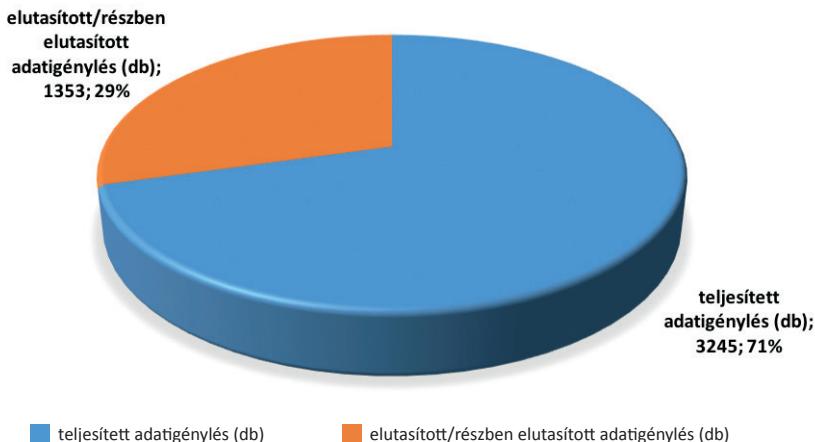
Az Infotv. 30. § (3) bekezdés második fordulata alapján a közzeladatot ellátó szerveknek a tárgyévet követő év január 31-éig tájékoztatniuk kell a Hatóságot a közérdekű és a közérdekből nyilvános adat megismerése iránt tárgyévben benyújtott, elutasított kérelmekről, illetve az elutasítások indokairól. A Hatóság az adatszolgáltatás teljesítésének és feldolgozásának egyszerűsítése érdekében adatlapot készített és tett közzé a honlapján (www.naih.hu, https://naih.hu/files/adatlap_honlapra_INFSZ_eves_-jelenteshez_2019.pdf).

A Hatósághoz **2020. február közepéig 403 adatkezelői** jelentés érkezett, ezek minősége azonban eltérő. Optimális esetben az erre a célra létrehozott adatlapon a Hatóság teljes tájékoztatást vár el az adott évben benyújtott közérdekű adatok megismerésére irányuló kérelmek és a teljesített adatigénylések számáról is.

A közérdekű és a közérdekből nyilvános adatok megismerése iránt benyújtott adatigénylések teljesítése/elutasítása a Hatósághoz beérkezett tájékoztatások alapján, 2019-ben			
adatkezelők száma	összes adatigénylés (db)	ebből teljesített (db)	elutasított/részben elutasított (db)
403	4520	3231	1353

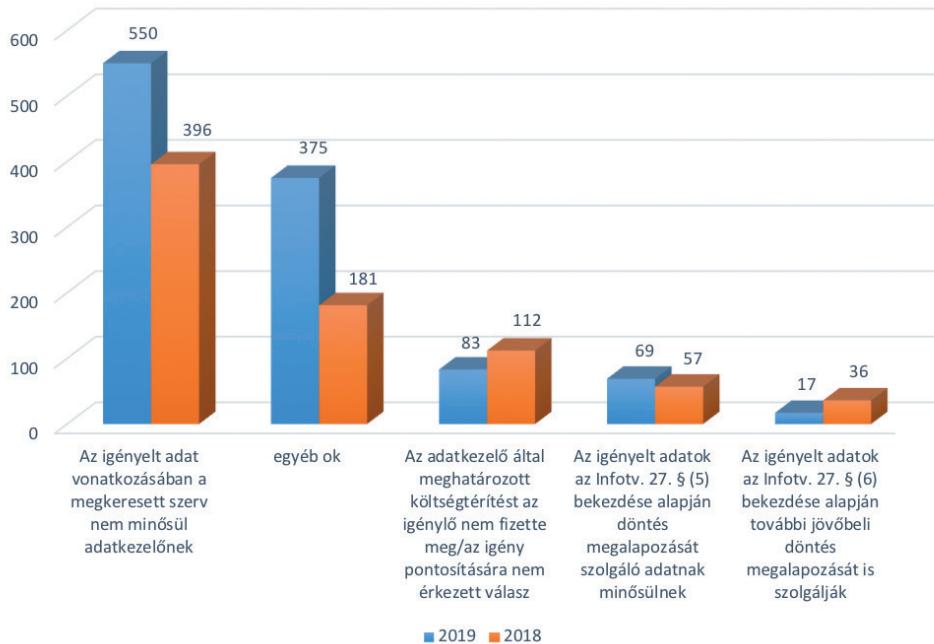
IX.1.2. Az adatmegismérés megtagadási okai

A közérdekű és a közérdekből nyilvános adatok megismerése iránti igények teljesítésének és elutasításának aránya 2019. évben

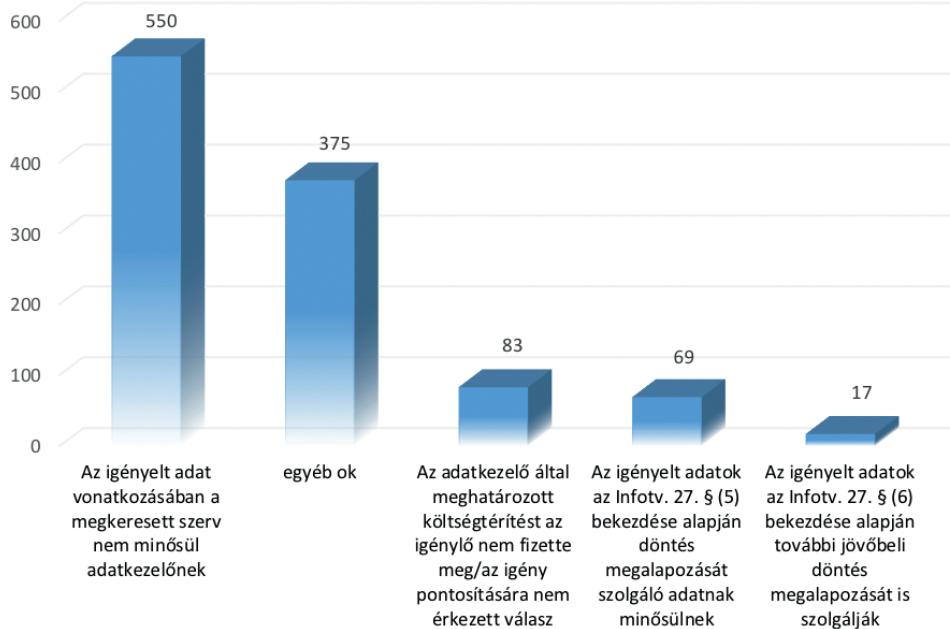


Az adatigénylések jogoszerű megtagadási okai sokfélék lehetnek, melyeket alkalmasnak is a közfeladatot ellátó szervek eljárásuk során. Az áttekinthetőség érdekében a második grafikonon a leggyakrabban hivatkozott megtagadási okokat és azok gyakoriságát jelenítettük meg.

*Leggyakrabban alkalmazott megtagadási okok aránya
2018-2019. évek vonatkozásában*



A közfeladatot ellátó szervek által legtöbbször alkalmazott megtagadási okok



IX.1.3. Az „egyéb” elutasítási okok részletezése

A Hatósághoz beküldött jelentésekben szerepeltek megtagadási okok között 375 esetben hivatkozott a közzeladatot ellátó szerv ún. „egyéb” okra az adatigénylés elutasításakor. A Hatóság felé adatszolgáltatást teljesítő közzeladatot ellátó szervek közül 99 szerv tagadta meg az „egyéb” kategóriába sorolt indokkal az adatigénylés teljesítését.

Hivatkozott „egyéb” megtagadási okok:

- az adatigénylés címzettje nem minősül közzeladatot ellátó szervnek, nem alanya az Infotv. 26. § (1) bekezdés szerinti kötelezettségnek;
- az igényelt adat nem közérdekű adat;
- az adatigénylés időpontjában az igényelt adat nem állt rendelkezésre;
- a kért formában nem áll rendelkezésre a kért adat;
- az adatok nem állnak rendelkezésre, és a közzeladatot ellátó szerv nem köteles annak előállítására a NAIH-4205-2/2012/V. számú állásfoglalás, valamint a 2003/98/EK irányelv alapján;
- a törvény céljával nem összeegyeztethető az adatigénylés.

Több közzeladatot ellátó szerv jelölt meg konkrét törvényi rendelkezéseket, melyek véleménye szerint korlátozzák az adat megismerését, ilyenek például:

- a gyermek védelméről és a gyámügyi igazgatásról szóló 1997. évi XXXI. törvény 27. § (4) bekezdése,
- az általános közigazgatási rendtartásról szóló 2016. évi CL. törvény 33. § (3) bekezdése,
- az Infotv. 3. § 9 pontja;
- az Infotv. 30. § (7) bekezdése, illetve
- a minősített adatot, az ország alapvető biztonsági, nemzetbiztonsági érdekeit érintő vagy a különleges biztonsági intézkedést igénylő beszerzések sajátos szabályairól szóló 218/2011. (X.19.) Korm. rendelet 7. § (5) bekezdése⁴⁸.

A jelentések feldolgozásából megállapítható továbbá, hogy a közzeladatot ellátó szervek többsége a részben teljesített adatigénylések esetében nem jelölte meg az adatigénylés elutasított részének megtagadási okát.

⁴⁸ Hatályon kívül helyezte: 276/2014. (XI. 6.) Korm. rendelet 2. §. Hatálytalan: 2014. XI. 7-től. Lásd: 276/2014. (XI. 6.) Korm. rendelet 4. §.

IX.1.4. A Hatósághoz 2019. évben benyújtott közérdekű adatigénylések adatai

A Hatósághoz 2019. év folyamán 69 db közérdekűadat-igénylést nyújtottak be adatigénylők, melyekből 59 ügyben az igényt a Hatóság teljesítette, míg 10 esetben a következő indokokkal utasította el: adatkezelői minőség hiánya (7), Infotv. 27. § (2) bekezdés g) pontja (1), Infotv. 27. § (5) bekezdése (1), az adatigény nem közérdekből nyilvános személyes adatra irányult (1).

IX.2. A Hatóság 2019. évi gazdálkodása

A Nemzeti Adatvédelmi és Információszabadság Hatóság működésének és gazdálkodásának 8. évét is magunk mögött tudhatjuk 2019. december 31-ével. Ezen gazdálkodással összefüggő adatokról az alábbiakban adunk rövid tájékoztatást.

IX.2.1. A bevételi előirányzat és teljesítési adatai 2019. évben

A NAIH 2019. évi költségvetése, eredeti előirányzata 1 156 700 eFt volt, melyből a kiemelt személyi előirányzat 747 400 eFt, a munkáltatói járulék és szociális hozzájárulás előirányzat 128 400 eFt, a dologi kiadások kiemelt előirányzata 255 900 eFt, a felhalmozási célú előirányzat 25 000 eFt.

A 2019. év módosított előirányzata 1 476 792 eFt volt, mely tartalmazza az eredeti előirányzatot, a 252 799 eFt kötelezettségvállalással terhelt 2018. évi maradványt, valamint a STAR I és II EU-pályázatokból származó, 21 190 eFt egyéb bevételt, ezen kívül az egyéb működési célú 22 766 eFt bevételt. 2019-ben továbbá felhalmozási célú lakáskölcsön visszatérítéséből fakadó bevétel 336 eFt, míg közhatalmi bevétel (eljárási illeték) 498 eFt értékben keletkezett. A KÖFOP projekt második előlege 22 047 eFt-ban realizálódott. A garantált bérminimum összege 456 eFt-ot tett ki a központi, irányítószervi támogatásból. Az erre vonatkozó számokat a következő táblázat szemlélteti:

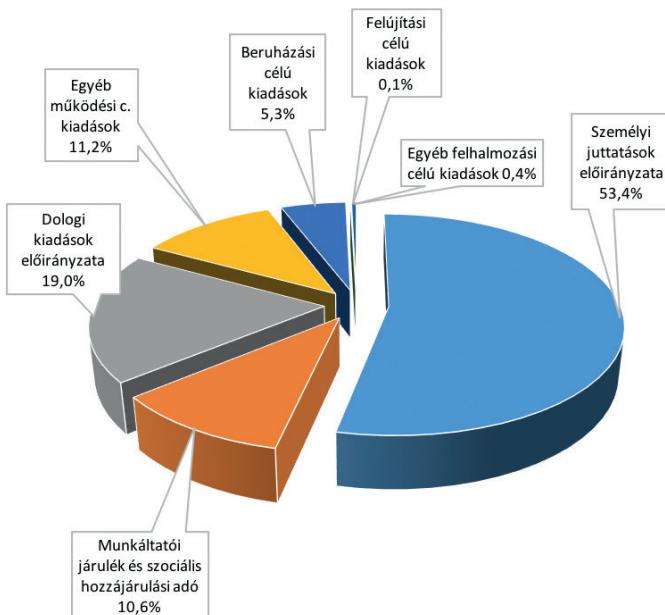
Megnevezés	Eredeti előirányzat	Módosított előirányzat	Teljesítés	Alaptevékenység 2019. évi maradványa
Eredeti előirányzat	1 156 700			
Működési c. egyéb támogatás fejezettről		22 047	22 047	
Közhatalmi bevételek		498	498	
Árfolyamnyereség		1 519	1 519	
Biztosító általi fizetett kárterítés		1 779	1 779	
Egyéb működési bevételek		19 468	19 468	
Egyéb működési c. átvett pénzeszköz (STAR I&II)		21 190	21 190	
Felhalmozás c. kölcsön megtérülése háztartástól		336	336	
2018. évi költségvetési maradvány		252 799	252 799	
Központi, irányító szervi támogatás	1 156 700	1 157 156	1 157 156	
ebből: garantált bérminimum		456	456	
Bevételi előirányzatok mindenkorábban	1 156 700	1 476 792	1 476 792	-
Személyi juttatások előirányzata	747 400	724 871	715 663	9 208
Munkáltatói járulék és szociális hozzájárulási adó	128 400	143 307	141 557	1 750
Dologi kiadások előirányzata	255 900	322 925	253 929	68 996
Egyéb működési c. kiadások	-	150 410	150 410	-
Beruházási célú kiadások	25 000	99 161	71 571	27 590
Felújítási célú kiadások		1 118	1 118	-
Egyéb felhalmozási célú kiadások		35 000	5 000	30 000
Kiadási előirányzatok mindenkorábban	1 156 700	1 476 792	1 339 248	137 544

IX.2.2. Kiadási előirányzatok és teljesítési adatai

A 2019. évi költségvetés eredeti előirányzata 1 156 700 eFt volt. A módosított kiadási előirányzat 1 476 792 eFt, melyből a teljesített személyi előirányzat kiadása 715 663 eFt. A munkáltatói járulék és szociális hozzájárulási adó kiadások teljesítése 141 557 eFt. A dologi kiadások összesen 253 929 eFt-ot tettek ki, az egyéb működési célú kiadások összege pedig 150 410 eFt volt. A felhalmozási kiadások 77 269 eFt.

A következő grafikon a módosított előirányzatok teljesült kiadásait mutatja %-os megoszlásban:

Teljesített kiadási előirányzatok megoszlása 2019

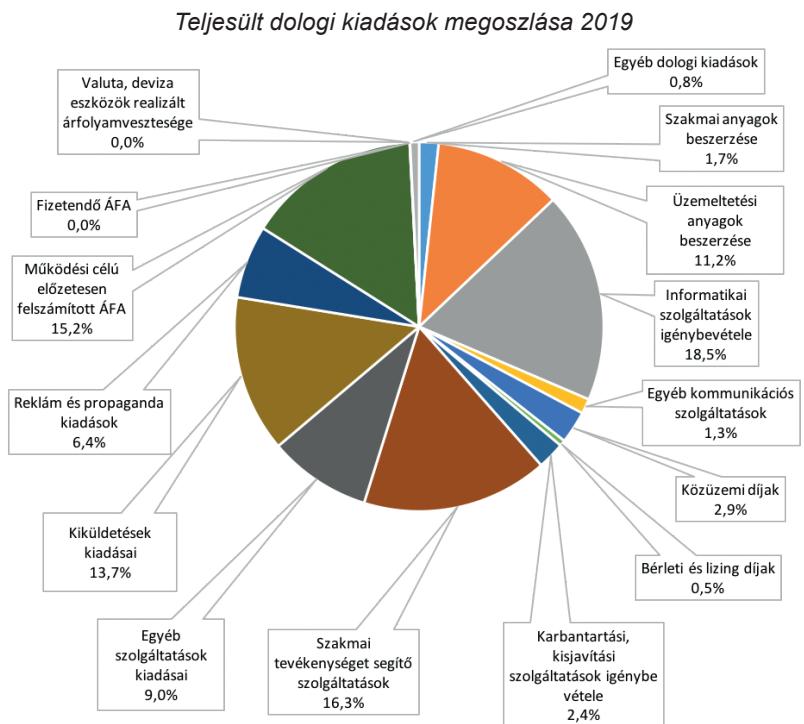


A 2019. évi módosított előirányzatok 53,4%-a a személyi juttatások kiadásaként teljesült. A munkáltatói járulék és szociális hozzájárulási adó 10,6% volt a teljes kiadáshoz mérten. A kiemelt dologi előirányzatok az összes módosított költségvetés 19%-át tettek ki. A felhalmozási célú kiadások a teljes költségvetés 5,5 %-a felett teljesült. Az egyéb működési célú kiadások értéke 11% felett volt.

A Hatóság alaptevékenységének 2019. évi maradványa 137 544 eFt lett, ebből 68 811 eFt kötelezettségvállalással terhelt maradványt keletkezett.

IX.2.3. A dologi kiadások megoszlása

A következő diagram a teljesült kiadási előirányzatok rovatrend szerinti %-os megoszlását mutatja.



A dologi kiadások legnagyobb részét a szakmai tevékenységet segítő szolgáltatás kiadásai teszik ki, mely 41 430 eFt, azaz 16%. A KÖFOP 2.2.6-VEKOP-18 projekthez kötött tanácsadói kiadások jelentős mértékben megemelték e kiadási kategória összegét.

A működési célú előzetesen felszámított Áfa - mivel Hatóságunk nincs visszaigénylő pozícióban - , 15 %-a teljes dologi kiadásnak, mely 38 648 eFt. A kiküldeti kiadások 2019-ben közel 35 000 eFt-ot tettek ki.

Az üzemeltetési anyagok értéke 28 510 eFt, valamint az informatikai szolgáltatások igénybe vételéért 47 005 eFt-ot fizetett ki a Hatóság.

A közüzemi díjakért Hatóságunk minden összesen 7 247 eFt-ot fizetett ki.

IX.2.4. A bírságbevételek alakulása

A Hatóság által kiszabott és befolyt bírság 112 734 eFt volt, mely teljes egészében a központi költségvetés bevétele.

IX.2.5. A Hatóság létszámának alakulása

A Hatóság 2019. december 31-i munkaügyi létszáma 105 fő volt. Hatóságunk olyan speciális ismertetékkal és jártasságokkal rendelkező szakembereket – jellemzően jogászokat és informatikusokat – foglalkoztat, akiknek a szaktudása és tapasztalata a GDPR 2018. évi bevezetésével (hasonlóan más tagállamokhoz) a munkaerőpiacon felértékelődött, ebből adódóan a megfelelő szintű, versenyképes illetmények biztosítása nélkül szinte lehetetlen a kvalifikált szakemberek megtartása. Fel kell hívni a figyelmet arra is, hogy a képzett, e területen kiemelkedő tapasztalattal rendelkező szakembereket érintően a munkaerő-piaci elszívó hatás nemcsak a versenyszféra felől jelentkezik, hanem a Hatóságénál kedvezőbb foglalkoztatási feltételek biztosítására képes, egyes, közszférába tartozó munkáltatók részéről is. Sajnos, a Hatóságunktól a közelmúltban – e tényezők miatt – megnőtt a munkaerő- elvándorlás mértéke. Ennek ellenére Hatóságunk – a lehetőségéhez képest – a munkaerő megtartására törekszik.

IX.3. A NAIH emlékérem kitüntetettjei

A „Nemzeti Adatvédelmi és Információszabadság Hatóság Emlékérem” adományozásáról szóló 19/2012. számú NAIH szabályzat alapján „Nemzeti Adatvédelmi és Információszabadság Hatóság Emlékérem” annak adományozható, aki az adatvédelem, illetve az információs önrendelkezési jog és információszabadság terén kiemelkedő, magas színvonalú, példaértékű eredményt ért el, vagy jelentősen hozzájárult ilyen eredmény eléréséhez. Az emlékérem ezüstből készül, Szabó Tamás ötvös mester alkotása. Átadására évente, az adatvédelem, illetve az információszabadság napja alkalmából kerül sor.

2019. január 25-én Dr. Péterfalvi Attila, a NAIH elnöke két elismerést adott át.

Az egyik ezüst emlékkérem kitüntetettje „*a személyes adatok védelméhez fűződő jogi ismeretek népszerűsítése, terjesztése érdekében végzett kiemelkedő tevékenységéért*” a Wolters Kluwer Hungary Kft volt.



Kézdi Katalin, a Wolters Kluwer Hungary Kft. ügyvezető igazgatója átveszi a Nemzeti Adatvédelmi és Információszabadság Hatóság Emlékérmet – Budapest, 2019. január 25.

A 2019-ben adományozott másik emlékérmet „*az uniós adatvédelmi reformcsoport elfogadásának folyamatában a magyar álláspont és a kapcsolódó hazai jogalkotási folyamat során a szakmai szempontok következetes képviseletében végzett kiemelkedő tevékenységéért*” Dr. Bendik Tamás, a NAIH elnöki főtanácsadója, korábban az Európai Unió intézményei (Tanács, Bizottság) által létrehozott formációk keretei között az adatvédelmi reformmal kapcsolatos tárgyalások során Magyarország álláspontját képviselő szakértő kapta.



Dr. Bendik Tamás átveszi a Nemzeti Adatvédelmi és Információszabadság Hatóság Emlékérmet – Budapest, 2019. január 25.

IX.4. Fényképek a Hatóság eseményeiről



*Információs Biztosok Nemzetközi Konferenciája - Johannesburg,
2019. március 10-13.*



IX. Nemzetközi Média Konferencia - Budapest, 2019. október 2.

IX.5. A beszámolóban említett jogszabályok és rövidítések jegyzéke

- Ajbtv., az alapvető jogok biztosáról szóló 2011. évi CXI. törvény
- Ákr. az általános közigazgatási rendtartásról szóló 2016. évi CL. törvény
- Alaptörvény, Magyarország Alaptörvénye (2011. április 25.)
- Általános adatvédelmi rendelet lásd: GDPR
- Art., az adózás rendjéről szóló 2003. évi XCII. törvény
- Bszi., a bíróságok szervezetéről és igazgatásáról szóló 2011. évi CLXI. törvény
- Bűnfüggelkívüli adatvédelmi irányelv, a bűnfüggelkívüli jogszabályokról szóló 2016. évi CLXII. törvény
- Bűnfüggelkívüli adatvédelmi irányelv, 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
- Bvtv., a büntetések, az intézkedések, egyes kényszerintézkedések és a szabálysértési elzárás végrehajtásáról szóló 2013. évi CCXL. törvény
- Ctv., a cégnyilvánosságról, a bírósági cégeljárásról és a végelszámolásról szóló 2006. évi V. törvény
- EESZT: Elektronikus Egészségügyi Szolgáltatási Tér
- 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
- Hszt., a rendvédelmi feladatakat ellátó szervek hivatásos állományának szolgálati viszonyáról szóló 2015. évi XLII. törvény
- ICO: az Egyesült Királyság Adatvédelmi Biztos Hivatala
- Infotv. Infotörvény, az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény
- Kijelölő rendelet, a Budapest közlekedésszervezési feladatainak ellátásáról szóló 20/2012. (III. 14.) Főv. Kgy. rendelet
- Kit., a kormányzati igazgatásról szóló 2018. évi CXXV. törvény

- Kkt., a kutatás és közvetlen üzletszerzés célját szolgáló név- és lakcímadatok kezeléséről szóló 1995. évi CXIX. törvény
- KNBSZ: Katonai Nemzetbiztonsági Szolgálat
- Körtv., a körözési nyilvántartási rendszerről és a személyek, dolgok felkutatásáról és azonosításáról szóló 2013. évi LXXXVIII. törvény
- Kttv., a közszolgálati tisztviselőkről szóló 2011. évi CXCIX. törvény
- Kvt., a környezet védelmének általános szabályairól szóló 1995. évi LIII. törvény
- MNB: Magyar Nemzeti Bank
- MOHOSZ: Magyar Országos Horgász Szövetség
- Mötv. a Magyarország helyi önkormányzatairól szóló 2011. évi CLXXXIX. törvény
- Mt., a munka törvénykönyvről szóló 2012. évi I. törvény
- NBSZ: Nemzetbiztonsági Szakszolgálat
- Nbtv., a nemzetbiztonsági szolgálatokról szóló 1995. évi CXXV. törvény
- Nvtv.: a nemzeti vagyonról szóló 2011. évi CXCVI. törvény
- OIF: Országos Idegenrendészeti Főigazgatóság
- Panasztörvény: a panaszokról és a közérdekű bejelentésekről szóló 2013. évi CLXV. törvény
- Ptk. új, a Polgári Törvénykönyvről szóló 2013. évi V. törvény
- Rtv., a rendőrségről szóló 1994. évi XXXIV. törvény
- SIS II, a Schengeni Információs Rendszer második generációjának létrehozásáról, működtetéséről és használatáról szóló 1987/2006/EK számú európai parlamenti és tanácsi rendelet
- SIS II tv., a 2012. évi CLXXXI. törvény a Schengeni Információs Rendszer második generációja keretében történő információcseréről, továbbá egyes rendészeti tárgyú törvények ezzel, valamint a Magyar Egyszerűsítési Programmal összefüggő módosításáról
- Szaztv., a személyazonosító jel helyébe lépő azonosítási módokról és az azonosító kódok használatáról szóló 1996. évi XX. törvény
- Számviteli törvény, a számvitelről szóló 2000. évi C. törvény
- Szjt., a szerzői jogról szóló 1999. évi LXXVI. törvény
- TAO törvény, a társasági adóról és osztalékadóról szóló 1996. évi LXXXI. törvény
- VIS rendelet, az Európai Parlament és a Tanács 767/2008/EK rendelete (2008. július 9.) a vízuminformációs rendszerről (VIS) és a rövid távú taratózkodásra jogosító vízumokra vonatkozó adatok tagállamok közötti cseréjéről

Egyéb jogszabályok:

- Aarhusi Egyezmény a környezeti ügyekben az információhoz való hozzáférésről, a nyilvánosságnak a döntéshozatalban történő részvételéről és az igazságszolgáltatáshoz való jog biztosításáról (kihirdette a 2001. évi LXXXI. törvény)
- a gyermekek védelméről és a gyámügyi igazgatásról szóló 1997. évi XXXI. törvény
- a jogalkotásról szóló 2010. évi CXXX. törvény
- a jogszabályok előkészítésében való társadalmi részvételről szóló 2010. évi CXXXI. törvény
- a kereskedelmi tevékenységek végzésének feltételeiről szóló 210/2009. (IX. 29.) Korm. rendelet
- a közérdekű adat iránti igény teljesítéséért megállapítható költségtérítés mértékéről szóló 301/2016. (IX. 30.) Korm. rendeletet
- a Közigazgatás- és Közszolgáltatás-fejlesztés Operatív Program éves fejlesztési keretének megállapításáról szóló 1004/2016. (I. 18.) Korm. határozat
- a közúti közlekedési nyilvántartásról szóló 1999. évi LXXXIV. törvény
- a mező- és erdőgazdasági földek forgalmáról szóló 2013. évi CXXII. törvény
- a minősített adatot, az ország alapvető biztonsági, nemzetbiztonsági érdekeit érintő vagy a különleges biztonsági intézkedést igénylő beszerzések sajátos szabályairól szóló 218/2011. (X.19.) Korm.rendelet
- a minősített adat védelméről szóló 2009. évi CLV. törvény
- a nyilvánosság környezeti információkhoz való hozzáférésének rendjéről szóló 311/2005. (XII.25.) Korm. rendelet
- a polgárok személyi adatainak és lakcímének nyilvántartásáról szóló 1992. évi LXVI. törvény
- a személyszállítási szolgáltatásokról szóló 2012. évi XLI. törvény
- a Tanács 2007. június 12-i 2007/533/IB Határozata a Schengeni Információs Rendszer második generációjának (SIS II) létrehozásáról, működéséről és használatáról
- a Tanács 1053/2013/EU rendelete (2013. október 7.) a schengeni vívmányok alkalmazását ellenőrző értékelési és monitoring-mechanizmus létrehozásáról és a végrehajtó bizottságnak a Schengent Értékelő és Végrehajtását Felügyelő Állandó Bizottság létrehozásáról szóló 1998. szeptember 16-i határozatának hatályon kívül helyezéséről
- az adózás rendjéről szóló 2017. évi CL. törvény

- az Elektronikus Egészségügyi Szolgáltatási Térrel kapcsolatos részletes szabályokat tartalmazó 39/2016. (XII.21.) EMMI rendelet
- az Európai Adatvédelmi Testület 3/2019. számú, a kamerás adatkezelési műveletekről szóló iránymutatása
- az Európai Parlament és a Tanács 603/2013/EU rendelete (2013. június 26.) a harmadik országbeli állampolgár vagy hontalan személy által a tagállamok egyikében benyújtott nemzetközi védelem iránti kérelem megvizsgálásáért felelős tagállam meghatározására vonatkozó feltételek és eljárási szabályok megállapításáról szóló 604/2013/EU rendelet hatékony alkalmazása érdekében az ujjlenyomatok összehasonlítását szolgáló Eurodac létrehozásáról, továbbá a tagállamok bűnöldöző hatóságai és az Europol által az Eurodac-adatokkal való, bűnöldözési célú összehasonlítások kérelmezéséről, valamint a szabadságon, a biztonságon és a jog érvényesülésén alapuló térség nagyméretű IT-rendszereinek üzemeltetési igazgatását végző ügynökség létrehozásáról szóló 1077/2011/EU rendelet módosításáról
- az Európai Parlament és a Tanács 95/46/EK irányelве (1995. október 24.) a személyes adatok feldolgozása vonatkozásában az egyének védelméről és az ilyen adatok szabad áramlásáról
- az Európai Parlament és a Tanács 2017/2226 rendelete (2017. november 30.) a tagállamok külső határait átlépő harmadik országbeli állampolgárok belépéseré és kilépéseré, valamint beléptetésének megtagadására vonatkozó adatok rögzítésére szolgáló határregisztrációs rendszer (EES) létrehozásáról és az EES-hez való bűnöldözési célú hozzáférés feltételeinek meghatározásáról, valamint a Schengeni Megállapodás végrehajtásáról szóló egyezmény, a 767/2008/EK rendelet és az 1077/2011/EU rendelet módosításáról
- az Európai Parlament és Tanács 2018. október 23-i (EU) 2018/1725 RENDELETE a természetes személyeknek a személyes adatok uniós intézmények, szervek, hivatalok, és ügynökségek általi kezelése tekintetében való védelméről és az ilyen adatok szabad áramlásáról, valamint a 45/2001/EK rendelet és a 1247/2002/EK határozat hatályon kívül helyezéséről
- az igazságügyi alkalmazottak szolgálati jogviszonyáról szóló 1997. évi LXVIII. törvény
- az ingyenes céginformációról szóló 47/2007. (X. 20.) IRM rendelet

Tartalomjegyzék

Bevezető	3
I. A Hatóság működésének statisztikai adatai.....	7
I.1. Ügyeink statisztikai jellemzői	7
I.2. Az adatvédelmi tiszviselők éves konferenciája	18
I.2.1. Az előzetes kérdőíves felmérés eredményei.....	18
I.2.2. Az adatvédelmi tiszviselők konferenciájának elektronikus oktatóanyagai.....	22
I.3. A Nemzeti Adatvédelmi és Információszabadság Hatóság megjelenése a médiában.....	24
II. Az általános adatvédelmi rendelet alkalmazása	25
II.1. Adatvédelmi ügyek.....	25
II.1.1. Munkahelyi adatkezelések	25
II.1.2. Egyes fontos, érdekes ügyek	31
II.1.3. Határon átnyúló ügyek	55
II.2. Az adatvédelmi incidensek bejelentése.....	57
II.3. Bíróság által felülvizsgált eljárások	65
III. A személyes adatok bűnuldözési, honvédelmi és nemzetbiztonsági célú kezelésével kapcsolatos eljárások.....	73
III.1. A személyes adatok Infotv. hatálya alá tartozó kezelésével kapcsolatos eljárások.....	73
III.1.1. A VÉDA rendszer.....	73
III.1.2. Az OIF arckép összehasonlítást elősegítő biometrikus alkalmazása..	75
III.1.3. A rendőri igazoltatás során kiállított RK lap adattartalma.....	76
III.1.4. A fogvatartottak levelezésének ellenőrzése.....	79
III.2. Az Infotv. hatálya alá tartozó adatkezeléseket érintő adatvédelmi inci- densekkel kapcsolatos eljárások.....	80
III.2.1. A bűnuldözési, honvédelmi és nemzetbiztonsági adatkezeléseket érintő adatvédelmi incidensekkel kapcsolatos eljárások sajátosságai....	80
III.2.2. A Hatóság bűnuldözési, honvédelmi és nemzetbiztonsági adatkezeléseket érintő adatvédelmi incidensekkel kapcsolatos eljárásainak tapasztalatai	82
III.3. A Schengeni Információs Rendszer magyarországi ellenőrzése	85
III.3.1. A Schengeni Információs Rendszer	85
III.3.2. Schengeni monitoring és értékelési mechanizmus	86
III.4. Részvétel az adatvédelmi hatóságok közös felügyeleti tevékenységében..	91
III.4.1. Határok, Utazás és Bűnuldözés Szakértői Csoport (Borders, Travel and Law Enforcement Expert Group – BTLE)	91

III.4.2. A Schengeni Információs Rendszer adatvédelmét felügyelő munkacsoport (SIS II SCG)	92
III.4.3. A Vízuminformációs Rendszer adatvédelmét felügyelő munkacsoport (VIS SCG)	93
III.4.4. Az Eurodac Rendszer adatvédelmét felügyelő munkacsoport (Eurodac SCG).....	94
III.4.5. Váminformációs Rendszer adatvédelmét felügyelő munkacsoport (Customs Information System – Supervision Coordination Group) és az Europol Cooperation Board	95
IV. Információszabadság.....	96
IV.1. Bevezetés.....	96
IV.2. Nemzetközi kitekintés.....	97
IV.3. Fontos alkotmánybírósági döntések	98
IV.4. Az adatigénylés teljesítéséért megállapítható költségtérítés szabályai – legújabb fejlemények.....	102
IV.5. Fontos bírósági döntések	106
IV.6. A közsolgálatban álló személyek közérdekből nyilvános adatai.....	108
IV.7. Helyi közügyek – az önkormányzati testületek működésének nyilvánossága.	110
IV.8. A közbeszerzési adatok nyilvánossága	113
IV.9. Döntés megalapozását szolgáló adat.....	114
IV.10. TAO támogatások	116
IV.11. Labdarúgó akadémiák	118
IV.12. Börtön-szabályzatok.....	119
IV.13. Környezeti információk	120
IV.14. Média- és internetes nyilvánosság	123
IV.15. Keresőmotorok.....	125
IV.16. Az adatigénylő személyének kérdése.....	127
V. A Hatóság jogalkotással kapcsolatos tevékenysége	128
V.1. A jogi szabályozással kapcsolatos ügyek statisztikai adatai	128
V.2. A jogszabályok társadalmi egyeztetésével kapcsolatos tapasztalatok	129
V.3. Az Európai Unió adatvédelmi reformjához kapcsolódó jogszabály módosítások.....	131
V.4. A nagy adatkezelők és adatkezelési rendszerek.....	133
V.5. Az információszabadsággal kapcsolatos jogi szabályozási tervezetek	137
VI. Titokfelügyelet, a minősített, illetve korlátozott nyilvánosságú közérdekű adatok	139
VI.1. A titkos megfigyelési feladatak ellátását és a személykörözést elősegítő informatikai rendszer.....	139
VI.2. A rendőrségi informátorok adatainak megismérhetősége.....	142
VI.3. A Hatóság adatmegismerési jogosultságának korlátai.....	144

VII. Nemzetközi ügyek és társadalmi kapcsolatok	149
VII.1. Az Európai Adatvédelmi Testület tevékenysége, jogértelmezési munkája ..	149
VII.1.1. A Testület jogértelmezési munkája	149
VII.1.2. Szakértői alcsoportok	151
VII.2. A Privacy Shield határozat harmadik éves felülvizsgálata	159
VII.3. A Hatóság nemzetközi kapcsolatai.....	161
VII.4. Pályázat az Európai Adatvédelmi Biztos pozíciójáért.....	166
VIII. A NAIH projektjei	168
VIII.1. A STAR I. és a STAR II. Projekt	168
VIII.1.1. A STAR projekt	168
VIII.1.2. A STAR II projekt	170
VIII.2. A KÖFOP projekt	172
VIII.3. IJR Projekt a NAIH általános adatvédelmi rendelet alkalmazására történő felkészülését és szakfeladatainak végrehajtását támogató projektje	173
IX. Mellékletek	175
IX.1. Elutasított közérdekű adat igénylések, és tájékoztatási kérelmek	175
IX.1.1. Az elutasított közérdekű adatigénylésekről és azok indokairól szóló 2019. évi tájékoztatási kötelezettség teljesítésének statisztikai adatai.....	175
IX.1.2. Az adatmegismérés megtagadási okai.....	176
IX.1.3. Az „egyéb” elutasítási okok részletezése.....	179
IX.1.4. A Hatósághoz 2019. évben benyújtott közérdekű adatigénylések adatai	180
IX.2. A Hatóság 2019. évi gazdálkodása	180
IX.2.1. A bevételi előirányzat és teljesítményi adatai 2019. évben	180
IX.2.2. Kiadási előirányzatok és teljesítményi adatai.....	182
IX.2.3. A dologi kiadások megoszlása	183
IX.2.4. A bírságbevételek alakulása	184
IX.2.5. A Hatóság létszámának alakulása	184
IX.3. A NAIH emlékkérem kitüntetettjei.....	184
IX.4. Fényképek a Hatóság eseményeiről	187
IX.5. A beszámolóban említett jogszabályok és rövidítések jegyzéke.....	188



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)



National Authority for Data Protection and Freedom of Information



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