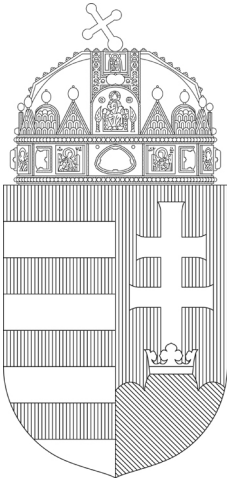
A Nemzeti Adatvédelmi és Információszabadság Hatóság

Beszámolója

a 2016. évi tevékenységéről

B/13846

Nemzeti Adatvédelmi és Információszabadság Hatóság
Budapest, 2017



Bevezető

Köszöntöm az Olvasót!

2016 mérföldkő az európai és hazai adatvédelem történetében, hiszen több éves előkészítés után április végén elfogadták az uniós adatvédelmi reformcsomagba tartozó általános adatvédelmi rendeletet és a bűnügyi irányelvet is. Ezzel új időszámítás kezdődik az uniós adatvédelmi hatóságok számára, megkezdődik a kétéves felkészülés azokra az új eljárási és anyagi jogi mechanizmusokra, melyek a személyes adatok kezelésének folyamatát gyorsabbá, hatékonyabbá, de reményeink szerint a polgárok számára biztonságosabbá is teszik. Jelen beszámoló ezért kiemelt figyelmet fordít ezen újítások, változások bemutatására, hangsúlyozva, hogy még csupán elméleti ismertetésről lehet szó, hiszen a gyakorlati részletek időigényes kimunkálása több szinten is nagy intenzitással folyik.

A magánszféra mellett a transzparencia védelme is kiemelt feladatunk annak érdekében, hogy az állam működése és gazdálkodása a polgárok számára átlátható legyen. A vizsgálati ügyek mellett képzéseken, konferenciákon ismertettük az aktuális jogszabály-változásokkal kapcsolatos tudnivalókat, gyakorlati tapasztalatainkat a közfeladatot ellátó szervek munkatársaival, törekedve arra, hogy praktikus megoldások ajánlásával megkönnyítsük a közzététellel és a közérdekű adatigénylések teljesítésével kapcsolatos kötelezettségeik teljesítését.

A NAIH nemzetközi szerepvállalásainak körében kiemelkedik az Európai Adatvédelmi Biztosok Éves Tavaszi Konferenciája, melynek először 2006-ban adatvédelmi biztosként, majd 2016-ban adatvédelmi hatóságként voltunk Budapesten házigazdái. A 2016-os Tavaszi Konferencia két fő témája a nemzetközi együttműködés erősítése és a nemzetbiztonsági szolgálatok működésének alkotmányos keretek közötti ellenőrzése volt. Ez utóbbi téma fontosságát számos tragikus, Európában történt terrorcselekmény támasztja alá, hiszen ’9/11’ után először az USA-ban, 2016-ban pedig Európában merült fel komoly dilemmaként a *„biztonság versus szabadság”* kérdése. A mi válaszunk erre az, hogy az emberek biztonságáért felelős szerveket hagyni kell dolgozni, de működésük nem maradhat alkotmányos kontroll nélkül. Meggyőződésünk, hogy erre léteznek olyan jogállami keretek, módszerek és gyakorlatok, melyek megakadályozzák, hogy feladni kényszerüljünk európai alkotmányos értékeinket, köztük a magánélet védelméhez való jogot is.

Mivel a Tisztelt Olvasó jelen beszámolót 2017-ben veszi kezébe, mindenképpen szeretnék ezen az oldalon megemlékezni két jeles évfordulóról.

Az 1989-es, majd 1990-es alkotmánymódosítás alapjogi szintre emelte az információs jogok magyarországi védelmét. Ezt követően 1992-ben, 25 évvel ezelőtt megszületett az első adatvédelmi és információszabadság törvényünk, a kelet-európai poszt-szocialista térségben először, de három évvel megelőzve az uniós Adatvédelmi Irányelvet és egyébként több nyugat-európai ország jogalkotását is. A magyar szabályozás kezdettől fogva a két információs alapjog együttes, egymásra ható szabályozási modelljét követi, mely modell napjainkban Európa nagy részén láthatóan egyre inkább teret hódít.

A magyar adatvédelmi és információszabadság parlamenti biztosának hivatala a gyakorlatban 1995-ben, az első adatvédelmi ombudsman megválasztásával kezdte meg működését. Az állampolgárok bizalmát igen hamar elnyerte, emellett pedig a közéletben is nagy jelentőségre tett szert, hiszen szava és érintettsége – talán megengedik nekem, hogy második adatvédelmi biztosként így fogalmazzak: szavunk és súlyunk volt sok fontos ügyben.

2011-től azonban az alkotmányos reform magával hozta az ombudsmani rendszer átalakítását és mivel az uniós jog megköveteli a teljes függetlenséget, az információs jogok felügyeletéért felelős szervezet 2012-től, pontosan 5 éve az új Info. törvény alapján hatósági keretek között állt fel és folytatta a munkát.

Az új Hatóság létrejöttét követően öt évvel ismét nagy változások következnek, az új adatvédelmi szabályok alkalmazása jelentős feladatokat ró minden szereplőre, nem csupán az adatkezelőkre, hanem az adatvédelmi hatóságokra is. A Hatóság számára elsődleges feladat a következő időszakban, hogy az adatvédelmi rendelet alkalmazása zökkenőmentes legyen, és az érintettek jogai maradéktalanul érvényesüljenek a mindennapok során.

Budapest, 2017. március 6.

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


NAIH

I. A Hatóság működésének statisztikai adatai

I.1. Ügyeink statisztikai jellemzői

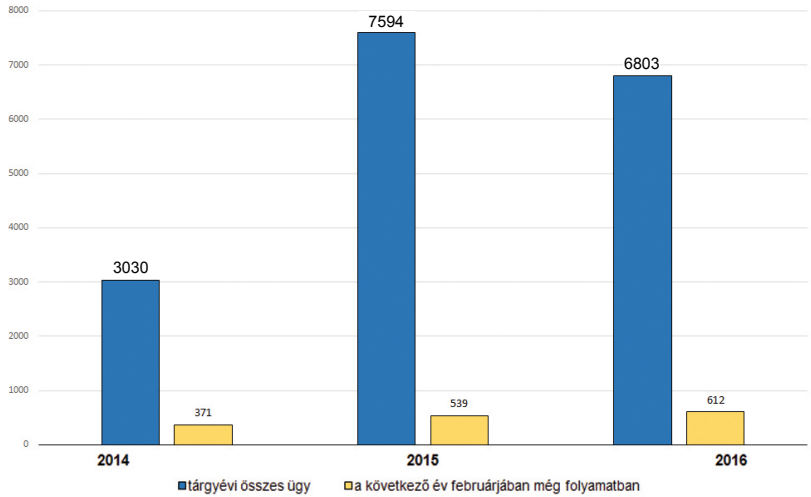
A Nemzeti Adatvédelmi és Információszabadság Hatóság 2012. január 1-jei megalapítása óta 2016 volt az ötödik év. Ebben az évben az elektronikus iktatókönyvben összesen 6803 ügy szerepelt, ez közel 800 üggyel kisebb szám az előző évi adatnál, ugyanakkor az adatvédelmi nyilvántartásba elektronikus úton 17091 nyilvántartási bejelentés érkezett, ami több mint 7000-rel haladta meg az előző év 9965 darab elektronikus bejelentését. Az ügyszámcsökkenés egyik tényezője, hogy míg 2015-ben 350 gazdálkodási ügyet iktattunk, ezek száma 2016-ban 135-re csökkent (-215), ezen kívül az adatvédelmi nyilvántartást érintő iktatott ügyek száma 3680-ról 3251-re csökkent (-429-ügy) tekintettel arra is, hogy a Hatóság visszaállította az adatvédelmi nyilvántartási bejelentésekkel kapcsolatos telefonos ügyfélszolgálati és konzultációs lehetőséget. A fenti adatokból megállapítható, hogy a NAIH további érdemi feladatait érintő ügyekben nem következett be számottevő számbeli változás.

Az iktatott ügyiratok közül 2016 során 113 ügyben folyt hatósági eljárás. A nyilvántartott 6803 ügyünkből 2759 bejelentést vizsgálati ügyként kezeltünk. A vizsgálati ügyeink száma az előző évi 2655-ről tehát 104 üggyel nőtt 2016 során, így a két évvel korábbi adathoz képest (2026 ügy) is jelentős növekedés nem torpant meg.

A többi ügyirat a NAIH Infotv.-ben szereplő további feladatköreit érintette, melyek jellemzően az adatvédelmi nyilvántartás vezetésével összefüggő ügyek, konzultációk és tájékoztatás kérések, a jogalkotással kapcsolatos tevékenységeink, jogszabály-véleményezés, a nemzetközi ügyek, belső adatvédelmi felelősök konferenciája, adatvédelmi audit és BCR ügyek, és a Hatóság belső ügyei, üzemeltetési, informatikai és ügyviteli iratok voltak. A hatósági eljárások részletes adatait, eredményeit az Adatvédelmi illetve a Titokfelügyeleti fejezetben ismertetjük.

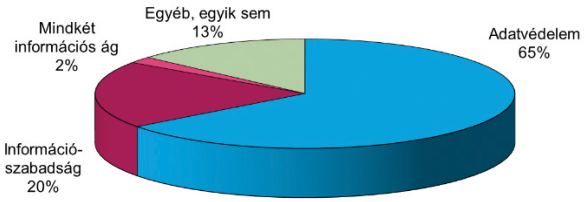
A 2016 során érkezett ügyek közül 2017. február 1-jén 612 ügy volt folyamatban, ez az összes ügy 9 %-a, az előző 2015-ös évből összesen 644 ügy átiktatására került sor 2016-ban.

A NAIH iktatott és folyamatban lévő ügyei 2014-2016



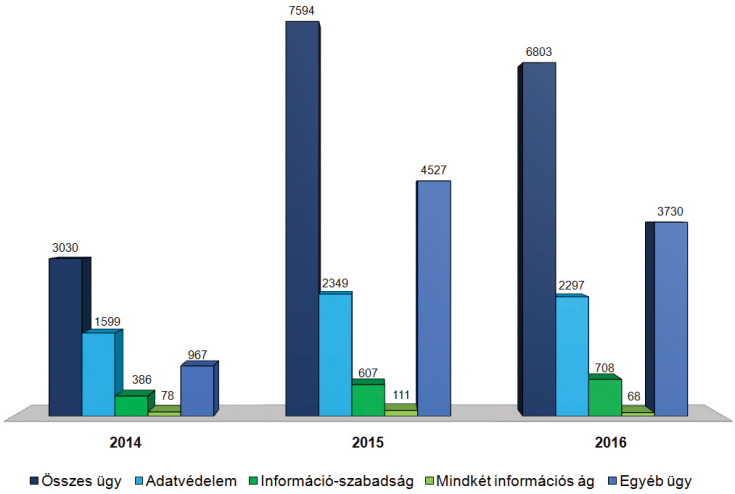
Az Infotv. rendelkezései alapján a NAIH alapfeladata – a további, törvényben felsorolt feladatai mellett – a személyes adatok védelméhez, valamint a közérdekű és a közérdekből nyilvános adatok megismeréséhez való jog érvényesülésének ellenőrzése és elősegítése. A következő ábra ennek megfelelően az ügyek információs ágak szerinti megoszlását szemlélteti úgy, hogy az egyébként nagyszámú, a statisztikát jelentősen módosító adatvédelmi nyilvántartási bejelentéseket és az ahhoz kapcsolódó konzultációs ügyeket az információs ág szerint ezúttal nem veszi figyelembe.

A NAIH ügyeinek megoszlása információs ágak szerint 2016
(az adatvédelmi nyilvántartási ügyek nélkül)



Az ügyeink információs jogok szerinti megoszlása a következő: adatvédelmet érint 2297 (65%), információszabadságot érint: 708 (20%), mindkét alapjogot érintette: 68 (2%), egyéb, a Hatóság más feladatkörébe tartozó ügy: 479 (13%) és az itt figyelembe nem vett, iktatott adatvédelmi nyilvántartási ügyek száma 3251 volt. A közérdekű, illetve közérdekből nyilvános adatok megismeréséhez való alapjogot tehát valamilyen formában a beérkezett ügyek összesen 22%-a, összesen mintegy 776 ügy érintette. Ez összességében azt jelenti, hogy az adatvédelmet érintő ügyiratok száma kismértékben csökkent, az információ-szabadságot érintő ügyeké kismértékben nőtt.

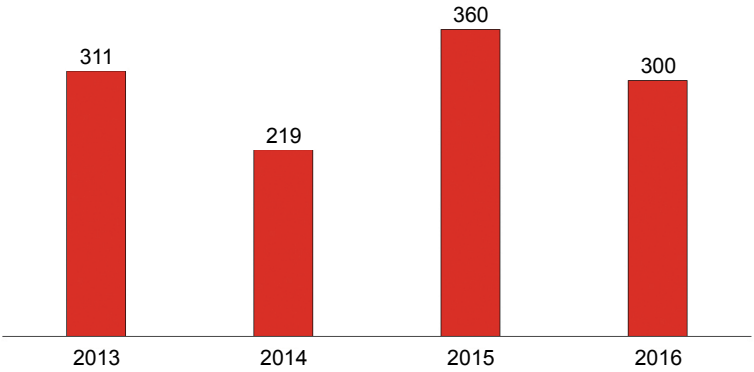
A beérkezett ügyiratok információs ágak szerinti száma 2014-2016
(az adatvédelmi nyilvántartási ügyek itt az egyéb kategóriában)



2016 során 300 jogszabály-véleményezést érintő ügyünk volt, amely az előző évi kiugróan magas ügyszámhoz (360) képest valamelyest (közel 7%-kal) csökkent.

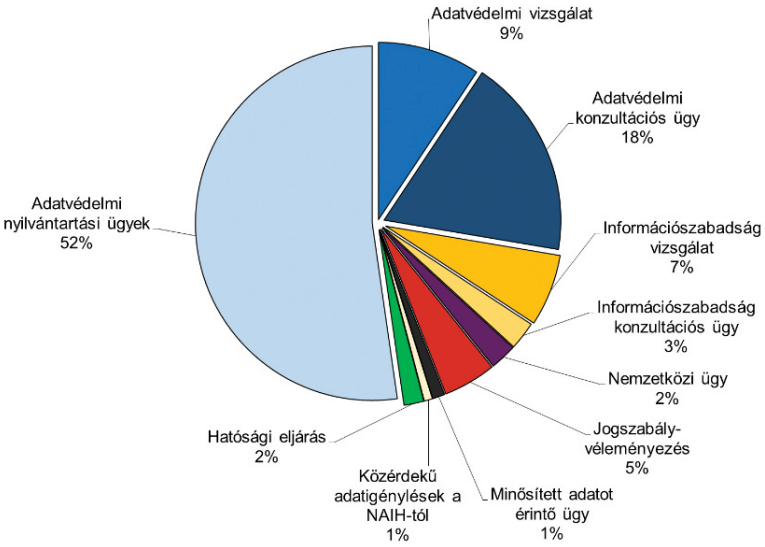
A Hatóság jogalkotási monitoring rendszert működtet, és hivatalból figyelemmel kíséri az információs jogokat érintő kodifikációs tevékenységet, és amennyiben az szükséges, véleményezi a hozzánk el nem küldött előterjesztéseket, vagy a parlamenti szakaszban benyújtott módosító javaslatokat.

Az iktatott jogszabály-véleményezések száma 2013-2016



A 2016-ban folyamatban lévő ügyeinkben összesen 40 jogszabály módosítást kezdeményeztünk, ezek közül 32 az adatvédelmet, 8 a közérdekű adatok nyilvánosságát érintette. A beérkezett ügyiratok közül 14 bejelentést más szervekhez tettünk át. A vizsgálati eljárást kezdeményező ügyeink közül 215 adatvédelmi tárgyú és 69 a közadatok nyilvánosságát érintő bejelentés vizsgálatát utasítottuk el. Az elutasított ügyek száma összességében csökkent az előző évhez képest.

Az érdemi ügyiratok megoszlása 2016



Tényleges vizsgálati eljárás alá összesen 990 ügyet vontunk, ami 80 üggyel több, mint 2015-ben. Ezek közül 582 (59%) adatvédelmi, és 408 (41%) információszabadság tárgyú volt. Bár mindkét információs ágat érintő vizsgálati eljárásaink száma nőtt, kiemelendő tendencia, hogy az információszabadságot érintő bejelentések és vizsgálatok száma és aránya évek óta növekedést mutat.

A 990 vizsgálat alá vont ügyben – e fejezet megírásáig – összesen 482 vizsgálatban állapítottunk meg részben vagy egészben valamilyen jogellenes adatkezelési gyakorlatot. A megállapított jogsértések száma összességében csökkent, mivel az előző évben 513 jogsértést regisztrálhattunk.

A sérelmet megállapító ügyek közül 249 a személyes adatok kezeléséhez és 233 a közadatok nyilvánosságához volt köthető. Fontos adat, hogy a megállapított jogsértések száma az adatvédelmi ügyek esetében csökkent (-39) míg az információszabadságot érintőkében ismét – bár kismértében, de – nőtt 225-ről 233-ra (+8). Így a megállapított jogsértések 52 %-a az információs önrendelkezési jog, 48 %-a pedig az információszabadság jogának sérelmét jelezte.

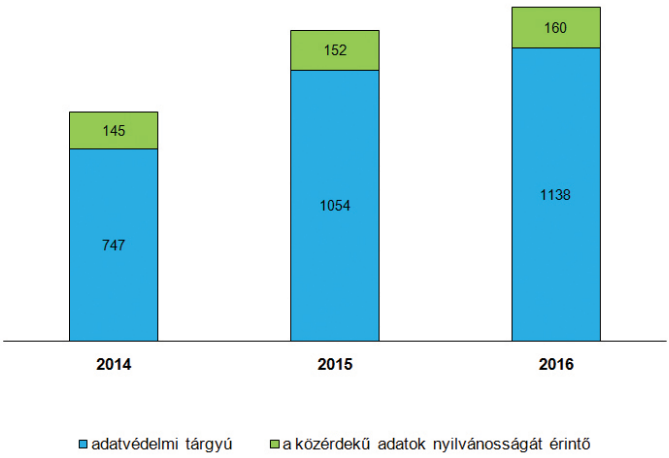
A Hatóság vizsgálati tevékenysége mellett fontos kiemelni az érdemi jogi állásfoglalást tartalmazó ügyeink között az összesen 1298 konzultációs ügyiratot is. Az ilyen típusú beadványainak száma 2016-ban is tovább emelkedett (+92 ügy) ami azt jelenti, hogy az elmúlt két év során 406-tal több ilyen ügyünk volt, mint 2014-ben.

Ezen ügyeink nagyban hozzájárulnak ahhoz, hogy az Infotv. 38. § (2) bekezdésében meghatározott, az információs jogok érvényesülésének elősegítésére irányuló tevékenységünk eredményei a gyakorlatban is megvalósulhassanak. Konzultációs ügyeinkre általában jellemző, hogy a konzultációt kezdeményező *„kérdező”* – akár valamely állampolgár, akár egy adatkezelő, vagy közfeladatot ellátó szervezet – meghatározott ügyben tanácsot, tájékoztatást, iránymutatást, megerősítést kér egy általa ismertetett, az információs jogokat érintő esetről, esetleg a leírtak jogszerűségéről, szakszerűségéről szeretne hivatalos állásfoglalást kapni. A konzultációs ügyek egy jelentős része állami-, önkormányzati szervektől, illetve magán adatkezelőktől, társadalmi- illetve gazdálkodó szervezetektől érkezik, a másik része az adatkezeléssel érintett magánszemélyektől, akik jellemzően nem kérnek vizsgálatot, vagy az ügyükben nem állnak fenn a vizsgálat megindításának feltételei. A Hatóság által kibocsátott tájékoztatásoknak, állásfoglalásoknak nehezen túlbecsülhető szerepe van abban, hogy a jogkövető magatartást támogassa, és ezáltal eredményesen és hatékonyan hozzájárul a jogsértések megelőzéséhez, megszüntetéséhez, a jó gyakorlatok kialakításához, továbbá az

érintettek figyelmét ráirányítja a jogtudatos és felelős magatartás fontosságára, és a törvényben biztosított egyéni jogérvényesítési lehetőségeikre.

A konzultációs tárgyú beadványok közül 1138 az adatvédelemre, 160 pedig a közérdekű vagy közérdekből nyilvános adatok megismerhetőségére vonatkozott. A konzultációs tárgyú ügyeink esetében egyértelmű tendencia, hogy az adatvédelmet érintő megkeresések száma ismételten emelkedett, két év alatt összesen közel 400-zal több ilyen ügyet küldtek a NAIH-nak. Az adatnyilvánosságot érintő konzultációs ügyeink száma nem emelkedett jelentősen. Egyes esetekben a konzultációs ügyek vizsgálata során is megállapíthatóvá vált, hogy valamely adatkezelő gyakorlata nem felel meg a törvények rendelkezéseinek, illetve az állásfoglalással jogsértő helyzet kialakulását, vagy annak közvetlen veszélyét előztük meg. 2016-ban 63 adatvédelmi, illetve 13 információszabadság ügyben állapítottunk, illetve előztünk meg jogsértést.

Az információs jogokat érintő konzultációs beadványok száma 2014-2016



2016-ban összesen 117 nemzetközi ügyünk volt, ezen felül 34 vizsgálati, illetve hatósági ügynek külföldi vonatkozása is volt (például európai uniós, vagy harmadik országbeli adatkezelőt, adatfeldolgozót érintett a bejelentés).

A minősített személyes vagy közérdekű adatok kezelését összesen 70 vizsgálat érintette, ami azt jelenti, hogy a titokvédelmi ügyeink száma az előző évhez ké-

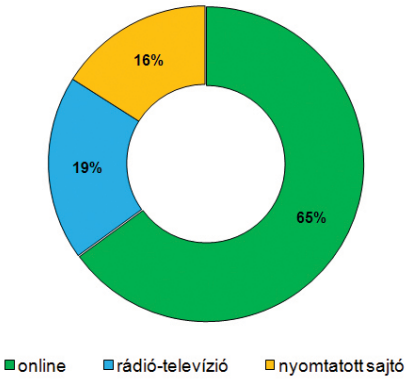
pest megháromszorozódott. A nemzetközi ügyeket, illetve a titokfelügyeleti vizsgálatokat a beszámoló külön fejezeteiben ismertetjük.

Az adatvédelmi audit ügyek száma 13 volt, a BCR-eket, a kötelező szervezeti szabályozások (Binding Corporate Rules) Hatóság általi jóváhagyását érintő ügyeink száma 54 volt. A NAIH-hoz 2016-ban 47 közérdekű adatigénylés érkezett, melyek mindegyikét megválaszoltuk. Az adatigénylések száma az előző évhez képest nem változott.

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

Jelen fejezetrész a Hatóság 2016. évi média megjelenéseit összegzi. 2016. január 1. és december 31. között összesen 6435 hírt közöltek a médiumok a Nemzeti Adatvédelmi és Információszabadság Hatóságról, ez közel 1600-zal több, mint az előző évben volt. A médiatípusok közül legtöbbször továbbra is az online médiában találkozhattunk a Hatóság tevékenységéről szóló híradásokkal, szám szerint 4183 alkalommal (65%), a nyomtatott sajtóban 1007-szer (16%), az elektronikus médiában pedig 1244-szer (19%). Érdekes tendencia, hogy a nyomtatott sajtóban és a rádió-televízió adásokban megjelenő hírek száma mellett az arányuk is nőtt az összes megjelenések arányán belül a tavalyi évhez képest, előzőnél +299, 2%, utóbbinál +632, 6% volt a hírek számának növekedése.

A NAIH megjelenéseinek aránya a különböző médiumokban 2016-ban



Forrás: Observer Budapest Médiafigyelő Kft.

II. Az európai adatvédelmi rendelet, GDPR

II.1. Bevezető

A 95/46/EK irányelv tapasztalatai egyértelművé tették, új adatvédelmi szabályozásra van szükség, ugyanis az Irányelv nem akadályozta meg, hogy az Unió tagállamaiban az adatvédelem végrehajtása széttagolt módon valósuljon meg, illetve jogbizonytalanság alakuljon ki. Széles körben alakult ki az a benyomás, hogy a természetes személyek jelentős kockázatnak vannak kitéve az online környezetben, az eltérő védelmi szinteket eredményező tagállami átültetés az adatok szabad áramlásának útjában állhat, ezek az eltérések a gazdasági tevékenységek akadályát jelenthetik, amelyek torzíthatják a versenyt és a hatóságokat is hátráltatják feladataik ellátásában.

Az Európai Parlament és a Tanács 2016. április 27. napján négyéves előkészületet követően fogadta el az új adatvédelmi csomagot:

- Az Európai Parlament és a Tanács 2016/679 rendelete a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK rendelet hatályon kívül helyezéséről (általános adatvédelmi rendelet, GDPR)
- Az Európai Parlament és a Tanács (EU) 2016/680 irányelve (2016. április 27.) a személyes adatoknak az illetékes hatóságok által a bűncselekmények megelőzése, nyomozása, felderítése, a vádeljárás lefolytatása vagy büntetőjogi szankciók végrehajtása céljából végzett kezelése tekintetében a természetes személyek védelméről és az ilyen adatok szabad áramlásáról, valamint a 2008/977/IB tanácsi kerethatározat hatályon kívül helyezéséről.

A Rendelet teljes egészében kötelező és közvetlenül alkalmazandó, nem igényel tagállami átültetést. A Rendelet 2016. május 24. napjától hatályos, azonban 2018. május 25. napjától lesz alkalmazandó. A (171) preambulum bekezdés alapján a Rendelet alkalmazásának időpontja előtt megkezdett adatkezelést összhangba kell hozni a rendelettel, ami nagy felkészülést igényel, mind az adatkezelőktől, mind a hatóságoktól.

Nem tartoznak a rendelet hatálya alá:

- az olyan iratok, illetve iratok csoportjai, amelyek nem rendszerezettek;

- az uniós jog hatályán kívül eső tevékenységek (pl. nemzetbiztonság)
- a természetes személy által kizárólag személyes vagy otthoni tevékenység keretében végzett adatkezelések; személyes vagy otthoni tevékenységnek minősül például a levelezés, a címtárolás, valamint az említett személyes és otthoni tevékenységek keretében végzett, közösségi hálózatokon történő kapcsolattartás és online tevékenységek;
- az elhunyt személyekkel kapcsolatos személyes adatok sem; ugyanakkor a tagállamok számára lehetővé kell tenni, hogy az elhunyt személyek személyes adatainak kezelését szabályozzák.

II.2. Alapfogalmak az általános adatvédelmi rendeletben

Az adatvédelemnek az Infotv. alapján megismert alapfogalmait érdemben nem módosítja az általános adatvédelmi rendelet[1], nagyrészt megegyeznek azokkal a definíciókkal, amelyeket az Infotv. 3. §-a tartalmaz. Így például a rendeletben lényegét tekintve nem változik sem az érintett, sem pedig a személyes adat fogalma[2]. Az általános adatvédelmi rendelet alkalmazásában változatlanul mind a közvetlenül, mind a közvetetten azonosítható személy érintettnek minősül, és a vele összefüggésbe hozott bármely információ személyes adatnak tekintendő. Fontos azonban kiemelni, hogy a rendelet kimondja, hogy személyes adatnak minősül az érintett által használt készülékek, alkalmazások, eszközök és protokollok által rendelkezésre bocsátott online azonosítókkal, (például: IP-cím, cookie), valamint egyéb azonosítókkal (például: rádiófrekvenciás azonosító: RFID) összefüggő adat, minthogy ezen azonosítók felhasználhatóak a természetes személyes profiljának létrehozására és az adott személy azonosítására.[3]

Az Infotv.-ben különleges adatként ismert személyes adatok köre két új adattal bővült a rendeletben: biometrikus adattal és a genetikai adattal[4]. A magyar adatvédelemben ez utóbbi kategória eddig is különleges adatnak számított, hiszen rendszerint ezen adatot, mint egészségügyi adatot kezelték az arra feljogosított adatkezelők.

1 Általános adatvédelmi rendelet 4. cikk
2 Általános adatvédelmi rendelet 4. cikk 1. pont
3 Általános adatvédelmi rendelet (30) preambulum bekezdés
4 Általános adatvédelmi rendelet 4. cikk 13-14. pont, illetve 9. cikk (1) bekezdés

Az adatkezelés fogalma hasonló módon épül fel mind az Infotv.-ben, mind az általános adatvédelmi rendeletben[5]. Egyrészt előbb az uniós jogalkotó főszabályként határozza meg, hogy adatkezelésnek minősül a személyes adatokon végzett bármely művelet vagy műveletek összessége, majd aztán példálózó felsorolásban kiemeli a legfontosabb adatkezelési műveleteket. Ezzel kapcsolatban érdemes kiemelni azt, hogy az általános adatvédelmi rendelet nevesített adatkezelési műveletként tartalmazza a „*betekintést*" is, amely nem szerepelt az Infotv. hasonló felsorolásában.

Az adatkezelő meghatározásában[6] nincs számottevő változás, az általános adatvédelmi rendelet definíciója lényegében ugyanazokra a fogalmi ismérvekre épül, mint az Infotv. értelmező rendelkezése. Azonban az adatfeldolgozó fogalma[7] jelentősen egyszerűbb lesz az uniós jogszabályban, mint a magyarban, mivel a rendelet alapján minden egyes olyan szervezet adatfeldolgozónak tekinthető, amely „*az adatkezelő nevében személyes adatokat kezel*".

Habár a hozzájárulás definícióját[8] másként fogalmazza meg az általános adatvédelmi rendelet, mint az Infotv., azonban megvizsgálva az uniós jogi rendelkezést, látható, hogy nincs érdemi különbség a két értelmező rendelkezés között. A hozzájárulásnak változatlanul önkéntesnek, megfelelő tájékoztatáson alapulónak, egyértelműnek és félreérthetetlennek kell lennie. A hozzájárulás, mint jogalappal összefüggésben azonban számos új követelményt fogalmaz meg az általános adatvédelmi rendelet, de erről később még részletesen szó lesz.

Az általános adatvédelmi rendeletben az adatkezelők több új, a magyar adatvédelmi jogban eddig ismeretlen fogalommal találkozhatnak. Így például a rendelet külön alapfogalomként határozza meg egy automatizált adatkezelés egyik elterjedt formáját: a profilalkotást[9]. A rendelet alapján a profilalkotás azt a tevékenységet jelenti, amikor az adatkezelők bizonyos személyes adatokat, a munkahelyi teljesítmény, gazdasági helyzethez, egészségi állapothoz, személyes preferenciákhoz, érdeklődéshez, megbízhatósághoz, viselkedéshez, tartózkodási helyhez vagy mozgáshoz kapcsolódó jellemzők elemzésére vagy előrejelzésére használják. A profilalkotás jellemzően marketingterületen fordul elő, mint a reklámozás hatékonyságát növelő adatkezelés.

5 Általános adatvédelmi rendelet 4. cikk 2. pont
6 Általános adatvédelmi rendelet 4. cikk 7. pont
7 Általános adatvédelmi rendelet 4. cikk 8. pont
8 Általános adatvédelmi rendelet 4. cikk 11. pont
9 Általános adatvédelmi rendelet 4. cikk 4. pont

Új fogalom továbbá az álnevesítés[10] is. Az általános adatvédelmi rendelet alapján álnevesítés útján további információk felhasználása nélkül többé már nem állapítható meg, hogy a személyes adat mely konkrét természetes személyre vonatkozik, mivel az ilyen további információt külön tárolják. Az álnevesített személyes adatok, amelyeket további információ felhasználásával valamely természetes személlyel kapcsolatba lehet hozni, azonosítható természetes személyre vonatkozó adatnak kell tekinteni.[11] Azonban az álnevesítés csökkentheti az érintettek számára a kockázatokat, valamint segíthet az adatkezelőknek és az adatfeldolgozóknak abban, hogy az adatvédelmi kötelezettségeiknek megfeleljenek.[12] Az álnevesítés például egy adatbiztonsági intézkedésként alkalmazhatja az adatkezelő, amely mérsékelheti egy adatvédelmi incidens következményét azáltal, hogy például a jogellenesen nyilvánosságra hozott, de álnevesített adatokból az érintettek kiléte nem állapítható meg.

Emellett még számos, az általános adatvédelmi rendelet újításaihoz kapcsolódó fogalom található a rendeletben, mint például a személyes adatok határokon átnyúló kezelésének a definíciója[13]. Ilyen adatkezelésnek tekinthető például az, ha egynél több tagállamban tevékenységi hellyel rendelkező adatkezelő több tagállamra kiterjedő adatkezelést végez, vagy az adatkezelés jelentős mértékben egynél több tagállamban jelentős mértékben kihat az érintettekre. Az ilyen adatkezelésekre több speciális rendelkezést tartalmaz a rendelet, például az illetékes fő felügyelő hatóság meghatározása vonatkozásában.

A rendelet ehhez kapcsolódóan természetesen meghatározza a tevékenységi központ fogalmát[14] is: a tevékenységi központ főszabályként az adatkezelőnek Unión belüli központi ügyvitelének helye, kivéve, ha az adatkezelést érintően érdemi döntés(eke)t más tevékenységi helyen hozták, amely ezért felelősséggel is tartozik. A tevékenységi központot objektív szempontok alapján kell meghatározni, így különösen, hogy az adatkezelésre vonatkozó fő döntéseket meghatározó ügyvezetési tevékenységet tényleges, valós és tartós jelleggel hol gyakorolják. Ugyanakkor a tevékenységi központ meghatározásában nincs jelentősége annak, hogy egy adott tevékenységi helyen találhatók a személyes adatok kezelésére szolgáló műszaki eszközök, illetve ott használják, ez önmagában nem jár együtt tevékenységi központként való minősítéssel. A tevékenységi központ egyben kijelöli azt is, hogy melyik az illetékes fő felügyeleti hatóság.

10 Általános adatvédelmi rendelet 4. cikk 5. pont
11 Általános adatvédelmi rendelet (26) preambulum bekezdés
12 Általános adatvédelmi rendelet (28) preambulum bekezdés
13 Általános adatvédelmi rendelet 4. cikk 23. pont
14 Általános adatvédelmi rendelet 4. cikk 16. pont

II.3. Az alapelvek az általános adatvédelmi rendeletben

Az Infotv. alapelvei mind-mind megtalálhatóak az általános adatvédelmi rendeletben[15], sőt az uniós jogszabály egyes, az Infotv. más rendelkezései között nevesített adatkezelői kötelezettségeket alapelvi szintre emel.

A tisztességes és törvényes adatkezelés elve egy újabb követelménnyel egészül ki az Infotv.-ben megismert tartalomhoz képest. Az uniós jogalkotó az alapelv fókuszába állítja azt is, hogy az adatkezelést az érintett számára átlátható módon kell végezni. Ez utóbbi követelmény hangsúlyos szerepet kap például az érintettek előzetes tájékoztatásánál: *„tájékoztatást tömör, átlátható, érthető és könnyen hozzáférhető formában, világosan és közérthetően megfogalmazva nyújtsa."*[16]

A célhoz kötött adatkezelés elve tartalmilag megegyezik az Infotv.-ben szereplő változatával, ugyanakkor az uniós jogalkotó a rendelet szövegébe beemelte a céltól eltérő adatkezelés tilalmát. Ez alól két kivételt nevesít a rendelet. Egyfelől a közérdekű archiválási, tudományos és történelmi kutatási, illetve statisztikai célú adatkezelést a rendelet az eredeti adatkezelési céllal összeegyeztethető további adatkezelésnek tartja. Másfelől az általános adatvédelmi rendelet egy komplex szempontrendszert határozott meg[17], amelynek segítségével az adatkezelők felmérhetik azt, hogy a tervezett adatkezelés összeegyeztethető-e azzal a céllal, amelyből a személyes adatokat eredetileg gyűjtötték.

Az adatminimalizálás (adattakarékosság) elve szintén lényegében megegyezik az Infotv.-ben szereplő alapelvvel. Az általános adatvédelmi rendelet szerint a személyes adatok kezelésének az adatkezelés céljai szempontjából megfelelőek és relevánsak kell, hogy legyenek, és az adatkezelésnek az elengedhetetlenül szükségesre kell korlátozódniuk.

Az általános adatvédelmi rendelet elválasztja egymástól a célhoz kötött adatkezelés elvét, illetve azt az alapvető kötelezettséget, hogy a személyes adat csak a cél megvalósulásához szükséges ideig kezelhető. A rendelet ezt az elvet *„korlátozott tárolhatóság"* alapelveként ismeri el. A rendelet kimondja, hogy a személyes adatok tárolásának olyan formában kell történnie, amely az érintettek azonosítását csak a személyes adatok kezelése céljainak eléréséhez szükséges ideig teszi

15 Általános adatvédelmi rendelet 5. cikk
16 Általános adatvédelmi rendelet 12. cikk (1) bekezdés, illetve (58) és (60) preambulum bekezdés
17 Általános adatvédelmi rendelet 6. cikk (4) bekezdése

lehetővé. Ezen főszabály alól a közérdekű archiválási, tudományos és történelmi kutatási, illetve statisztikai célú adatkezelések jelenthetnek kivételt, feltéve, hogy az adatkezelők megfelelő technikai és szervezési intézkedésekkel biztosítják az érintettek személyes adatok védelméhez fűződő jogát. Ilyen intézkedés lehet az adatkezelők részéről a már korábban említett álnevesítés, amely alkalmas lehet arra, hogy például az érintett személyes adataira is kiterjedő tudományos kutatás úgy valósuljon meg, hogy a kutató előtt az érintett kiléte nem lesz ismert, minthogy az azonosításához szükséges adatokat külön tárolják.

Mind az Infotv, mind az általános adatvédelmi rendelet tartalmazza a pontos, naprakész adatkezelés elvét. Az uniós jogalkotó ezt az alapelvet kiegészítette még azzal az általános kötelezettséggel is, hogy minden ésszerű intézkedést meg kell tenni annak érdekében, hogy az adatkezelés céljai szempontjából pontatlan személyes adatokat haladéktalanul töröljék vagy helyesbítsék.

Az általános adatvédelmi rendelet egyik újítása az integritás és bizalmas jelleg alapelvének beemelése a jogszabályba. A rendelet által megfogalmazott kötelezettség az Infotv.-ben adatbiztonsági intézkedésként szerepelt. A Hatóság álláspontja szerint e rendelkezés alapelvi szintre emelésével az uniós jogalkotó azt kívánta kifejezni, hogy az adatkezelők teljes tevékenységét átható alapelv legyen az adatbiztonság megteremtése, hiszen az elmúlt években egyre gyakoribbá váltak az olyan jogellenes cselekmények, amelyek nyomán illetéktelenek többszázezer személyes adatot hoztak nyilvánosságra.[18]

II.3.1. Az elszámoltathatóság

Az Adatvédelmi Irányelv alapján kialakított tagállami adatvédelmi jogszabályok alkalmazásának egyik fontos tapasztalata volt, hogy az adatvédelmi elvek és kötelezettségek gyakran nem jelennek meg kellőképpen az adatkezelő konkrét belső intézkedéseiben és gyakorlataiban. Az Általános Adatvédelmi Rendelet megalkotása során ezért kiemelt prioritássá lépett elő, hogy az adatkezelőknek eszközöket biztosítson az adatvédelemnek a szervezeten belüli gyakorlati előmozdításához. Ennek sikeres alkalmazásához, illetve kikényszeríthetőségéhez azonban szükséges volt egy általános szabályozás bevezetésére, amely az adatkezelőtől az adatvédelmi tudatosságot megköveteli.

18 A sajtó is egyre gyakrabban beszámol különféle hackertámadásokról, amelyek nyomán olykor „*csak*" több ezer, de egyes esetekben milliós nagyságrendben kerülnek nyilvánosságra személyes adatok, így leggyakrabban felhasználónevek, jelszavak.

Az Általános Adatvédelmi Rendeletnek ennek megfelelően az egyik leghangsúlyosabb újítása, hogy alapelvi szintre emelte az elszámoltathatóság koncepcióját. Az adatkezelőknek 2018 májusától sokkal nagyobb tudatosság mellett kell az adatkezeléseiket végezni. Az adatkezelés megtervezésétől kezdve az adatkezelés megkezdésén át egészen a kezelt személyes adatok törléséig valamennyi adatkezelési műveletet úgy kell megvalósítaniuk, hogy bármelyik pillanatban bizonyítani tudják, hogy miként feleltek meg az adatvédelmi előírásoknak.

Az elszámoltathatóság nem új jelenség sem a vállalati kultúrában, sem az adatvédelemben. A nagyvállalati környezetben jól ismert compliance-hez hasonló intézményről beszélhetünk. Az Infotv. 22. §-a pedig eddig is tartalmazott az elszámoltathatósághoz hasonló kötelezettséget, bár ez csak a bírósági jogérvényesítéshez volt köthető.

Az Általános Adatvédelmi Rendelet jelentős újítása, hogy alapelvi szintre helyezi az elszámoltathatóságot. A Rendelet 5. cikk (2) bekezdése értelmében ugyanis az adatkezelő felelős az adatvédelmi alapelveknek való megfelelésért, továbbá képesnek kell lennie e megfelelés igazolására (*„elszámoltathatóság”*). A Rendelet 24. cikke tovább részletezi az elszámoltathatóság kötelezettségét az adatkezelő feladatainál. Ennek megfelelően az adatkezelő az adatkezelés jellege, hatóköre, körülményei és céljai, valamint a természetes személyek jogaira és szabadságaira jelentett, változó valószínűségű és súlyosságú kockázat figyelembevételével megfelelő technikai és szervezési intézkedéseket hajt végre annak biztosítása és bizonyítása céljából, hogy a személyes adatok kezelése e rendelettel összhangban történik. Ezeket az intézkedéseket az adatkezelő felülvizsgálja és szükség esetén naprakésszé teszi. Ha az az adatkezelési tevékenység vonatkozásában arányos, ennek részeként az adatkezelő megfelelő belső adatvédelmi szabályokat is alkalmaz.

Az elszámoltathatóság elve a fenti megfogalmazásból adódóan mindenek felett álló alapelvvé vált az adatvédelemben. Ehhez az alapelvhez a Rendelet valamennyi rendelkezését hozzá lehet kapcsolni és ezt az alapelvet az adatkezelőknek mindig szem előtt kell tartaniuk.

Az elszámoltathatóság elve lényegében azt jelenti, hogy az adatkezelőknek mind a szervezeti kultúrájukat, mind valamennyi tevékenységüket az adatvédelemi megfontolásokra tekintettel kell kialakítaniuk, végezniük. Az adatkezelőknek minden egyes lépésüknél át kell gondolniuk, hogy az adatvédelmi előírásokat miként vették figyelembe.

Természetesen ezen az általános attitűdön túl az Általános Adatvédelmi Rendelet számos elvi és gyakorlati eszközzel is megpróbálja segíteni az elszámoltathatóság elvének érvényesülését. Ennek megfelelően az elszámoltathatóság követelményének teljesítését segíti elő többek között a beépített és alapértelmezett adatvédelem (25. cikk); az adatkezelési tevékenységek nyilvántartása (30. cikk); az adatvédelmi hatásvizsgálat (35. cikk); az adatvédelmi tisztviselő (37-39. cikk); a magatartási kódexek (40-41. cikk) és tanúsítás (42-43. cikk); illetve a kötelező erejű vállalati szabályok (47. cikk); stb.

Fontos emellett kiemelni, hogy az elszámoltathatóságnak nem csak az Általános Adatvédelmi Rendeletben szereplő eszközökkel lehet megfelelni. Számos olyan adatvédelmet elősegítő technika (Privacy Enhancing Tecnologies, PET) létezik, amely nincs nevesítve a Rendeletben, de segít az adatkezelőknek az adatvédelmi megfelelés kialakításában és igazolásában.

II.4. Jogalapok az általános adatvédelmi rendeletben

A leggyakrabban használt jogalapok változatlanul megmaradnak az általános adatvédelmi rendeletben[19] is, azonban néhány, az Infotv.-ben szereplő, ugyanakkor az adatkezelők által ritkán használt jogalap[20] már nem szerepel az uniós jogszabályban.

A rendelet első helyen említi az érintett hozzájárulását. Ezzel összefüggésben számos új adatvédelmi követelményt fogalmaz meg az uniós jogszabály az adatkezelők számára:

- Egyrészt az adatkezelőnek képesnek kell lennie annak igazolására, hogy az érintett személyes adatainak kezeléséhez hozzájárult.[21]
- Másrészt, ha az adatkezelő írásbeli nyilatkozaton keresztül szerzi be az érintett hozzájárulását, akkor a nyomtatványon a hozzájárulás iránti kérelmet egyértelműen és világosan el kell választani a szerződés többi részétől, valamint e kérelmet érthető és egyszerű nyelvezettel kell az adatkezelőnek megfogalmaznia.[22]

19 Általános adatvédelmi rendelet 6. cikk
20 Így például az Infotv. 6. § (6)-(7) bekezdésében szereplő jogalapokat az általános adatvédelmi rendelet nem tartalmazza.
21 Általános adatvédelmi rendelet 7. cikk (1) bekezdés
22 Általános adatvédelmi rendelet 7. cikk (2) bekezdés

– Harmadrészt az adatkezelőnek biztosítania kell azt, hogy az érintett a hozzájárulását bármikor visszavonhassa, és a hozzájárulás visszavonását ugyanolyan egyszerű módon kell lehetővé tennie, mint annak megadását.[23]

Az általános adatvédelmi rendelet emellett további olyan adatvédelmi követelményeket is előír, amelyek ismerősek lehetnek a magyar adatkezelők számára, hiszen e követelményekkel már találkozhattak a Hatóság egyes határozataiban:

– Az általános adatvédelmi rendelet kiemeli, hogy a hallgatás, az előre bejelölt négyzet vagy a nem cselekvés nem minősül hozzájárulásnak.[24]
– A rendelet – az Adatvédelmi Munkacsoport gyakorlatával összhangban – rögzíti azt is, hogy a hozzájárulás megadása nem tekinthető önkéntesnek, ha az érintett nem rendelkezik valós vagy szabad választási lehetőséggel, és nem áll módjában a hozzájárulás megtagadása vagy visszavonása, anélkül, hogy ez kárára válna.[25]
– Az uniós jogszabály szerint nem tekinthető önkéntesnek a hozzájárulás, ha a szerződés teljesítését (például: a szolgáltatás nyújtását) olyan adatkezeléshez való hozzájáruláshoz kötik, amely adatkezelés nem szükséges a szerződés teljesítéséhez.[26]
– A hozzájárulás továbbá nem tekinthető önkéntesnek akkor sem, ha nem tesz lehetővé külön-külön hozzájárulást a különböző személyes adatkezelési műveletekhez.[27]

A Hatóság azt javasolja az adatkezelők számára, hogy az általános adatvédelmi rendeletben szereplő követelmények áttekintésével vizsgálják felül, hogy az érintettek hozzájárulásán alapuló adatkezeléseik megfelelnek-e a rendeletnek. Amennyiben igen, akkor nem kell új hozzájárulást beszereznie az adatkezeléshez. Ha viszont a rendeletben megfogalmazott követelmények nem teljesülnek az általuk végzett adatkezeléssel kapcsolatban, akkor 2018. május 25-éig adatkezelésüket összhangba kell hozni az új követelményekkel.[28]

Az adatkezelés egy másik lehetséges jogalapja az, amikor „*az adatkezelés olyan szerződés teljesítéséhez szükséges, amelyben az érintett az egyik fél, vagy az a szerződés megkötését megelőzően az érintett kérésére történő lépések meg-*

23 Általános adatvédelmi rendelet 7. cikk (3) bekezdés
24 Általános adatvédelmi rendelet (32) preambulum bekezdés
25 Általános adatvédelmi rendelet (42) preambulum bekezdés
26 Általános adatvédelmi rendelet 7. cikk (4) bekezdés
27 Általános adatvédelmi rendelet (43) preambulum bekezdés
28 Általános adatvédelmi rendelet (171) preambulum bekezdés

tételéhez szükséges."[29] Hasonló jogalapot az Infotv. is tartalmazott[30], azonban azt – a Hatóság tapasztalatai szerint – ritkán alkalmazták az Infotv. hatálya alá adatkezelők. A Hatóság értelmezése szerint a rendelet e jogalapját megszorítóan kell értelmezni, és ennek alkalmazása nem vezethet ahhoz, hogy valamely, a szerződés végrehajtásához nem szükséges adatkezelés esetében a hozzájárulás helyett a rendelet e jogalapját alkalmazza az adatkezelő, és emiatt az adatkezelő nem szerzi be az érintett hozzájárulását. Egy ilyen gyakorlat ugyanis súlyosan csorbítaná az érintett információs önrendelkezési jogát. A Hatóság álláspontja szerint ez a jogalap alkalmazható például az érintettel kötött írásbeli szerződés esetében a természetes személyazonosító adatok (név, születési hely és idő, anyja neve) kezelésének jogalapjaként.

Az általános adatvédelmi rendelet két olyan jogalapot is tartalmaz, amelyek jogszabályon alapuló adatkezelésnek tekinthető. A rendelet szerint személyes adat kezelhető akkor is, ha az adatkezelés:

- „*az adatkezelőre vonatkozó jogi kötelezettség teljesítéséhez szükséges*"[31],
- „*közérdekű vagy az adatkezelőre ruházott közhatalmi jogosítvány gyakorlásának keretében végzett feladat végrehajtásához szükséges*"[32].

A rendelet mindkét jogalap vonatkozásában megköveteli, hogy az adatkezelésről uniós jog vagy tagállami jogszabály rendelkezzen.[33] Ezzel egyidejűleg a rendelet kifejezetten felhatalmazza a tagállamokat arra, hogy további, konkrét jogszabályi rendelkezéseket alkothatnak (hatályában tarthatnak) e jogalapok alapján végzett adatkezelésekre (például a kezelt adatok körére, az adatkezelő kijelölésére vagy az adatkezelés időtartamára vonatkozóan).[34] Mint látható, az adatvédelmi rendelet az Infotörvénnyel ellentétben nem követeli meg, hogy törvényben (vagy annak felhatalmazása alapján kiadott önkormányzati rendeletben) kell rendelkeznie a jogalkotónak az adatkezelés körülményeiről, hanem lehetőséget ad arra, hogy más, alacsonyabb szintű jogszabály tartalmazza az adatkezelési körülményeket.

Az általános adatvédelmi rendelet szintén nevesíti az érdekmérlegelés jogalapját.[35] Ezen jogalap az érintett hozzájárulása nélkül lehetőséget biztosít az

29 Általános adatvédelmi rendelet 6. cikk (1) bekezdés b) pont
30 Infotv. 6. § (4) bekezdés
31 Általános adatvédelmi rendelet 6. cikk (1) bekezdés c) pont
32 Általános adatvédelmi rendelet 6. cikk (1) bekezdés e) pont
33 Általános adatvédelmi rendelet 6. cikk (3) bekezdés
34 Általános adatvédelmi rendelet 6. cikk (2) bekezdés, illetve (45) preambulum bekezdés
35 Általános adatvédelmi rendelet 6. cikk (1) bekezdés f) pont

adatkezelésre, feltéve, hogy az adatkezelés szükséges az adatkezelő vagy egy harmadik fél jogos érdekeinek érvényesítéséhez, és az adatkezelés arányosan korlátozza az érintett személyes adatok védelméhez fűződő jogát. A jogos érdek fennállásának megállapításához az adatkezelőnek körültekintően meg kell vizsgálni többek között azt, hogy az érintett a személyes adatok gyűjtésének időpontjában és azzal összefüggésben számíthat-e ésszerűen arra, hogy adatkezelésre az adott célból kerülhet sor. Az érintett érdekei és alapvető jogai elsőbbséget élvezhetnek az adatkezelő érdekével szemben, ha a személyes adatokat olyan körülmények között kezelik, amelyek közepette az érintettek nem számítanak további adatkezelésre. Jogos érdekről lehet szó például olyankor, amikor releváns kapcsolat áll fenn az érintett és az adatkezelő között, például olyan esetekben, amikor az érintett az adatkezelő ügyfele vagy annak alkalmazásában áll.[36]

Emellett az uniós jogalkotó kimondja, hogy ha az érintett gyermek[37], akkor csak kivételesen, rendkívüli körültekintés mellett lehet alkalmazni ezt a jogalapot. Továbbá a rendelet kifejezett tilalmat is előír: az érdekmérlegelés jogalapja nem alkalmazható a közhatalmi szervek által feladataik ellátása során végzett adatkezelésre, tekintettel arra, hogy ilyenkor jogalkotónak kell jogszabályban rendelkeznie az adatkezelésről.[38]

Ezen túlmenően az általános adatvédelmi rendelet néhány példát is említ[39], hogy mely adatkezelések esetében is alkalmazható az érdekmérlegelés jogalapja:

- személyes adatoknak a csalások megelőzése céljából feltétlenül szükséges kezelésére,
- személyes adatok közvetlen üzletszerzési célú kezelésére,
- a vállalkozáscsoporton belül belső adminisztratív célból személyes adatok továbbítására,
- bűncselekményhez vagy közbiztonságot fenyegető veszélyhez kapcsolódó releváns személyes adatok az illetékes hatóságnak történő továbbítására.

Az általános adatvédelmi rendeletben a különleges adatok kezelésére vonatkozó rendelkezés arra a főszabályra épít, hogy a különleges adatok kezelése tilos.[40]

36 Általános adatvédelmi rendelet (47) preambulum bekezdés
37 Az általános adatvédelmi rendelet 8. cikk (1) bekezdése az Infotv.-hez hasonlóan a 16 éven aluli érintettet gyermeknek tekinti, az esetükben a 8. cikk külön szabályokat tartalmaz.
38 Általános adatvédelmi rendelet 6. cikk (1) bekezdés f) pont és (47) preambulum bekezdés
39 Általános adatvédelmi rendelet (47)-(50) preambulum bekezdés
40 Általános adatvédelmi rendelet 9. cikk (1) bekezdés

Ez alól a rendelet összesen 10 kivételt ismer el, amelyek nagy része a közérdekhez vagy a jogszabályban előírt adatkezeléshez kapcsolódik.

A kivételek közül érdemes kiemelni az érintett kifejezett hozzájárulása esetét[41], amely az Infotv. hasonló rendelkezésével szemben nem követeli meg azt, hogy írásban kerüljön sor a hozzájárulásra. Azonban a hozzájárulás jogalapjával összefüggésben korábban említett valamennyi követelményét e jogalap esetében is alkalmazni kell. A Hatóság ezzel kapcsolatban továbbá kiemeli azt is, hogy ebben az esetben az adatkezelő bizonyítási kötelezettsége arra is kiterjed, hogy igazolni tudja azt, hogy az érintettnek tudomása volt arról is, hogy különleges adatot ad meg, és ennek ismeretében kifejezetten hozzájárult ahhoz, hogy az adatkezelő a különleges adatait kezelhesse.

A rendelet a kivételek között külön több egy-egy élethelyzetre szűkíthető, speciális esetkört nevesít, így például politikai, világnézeti, vallási vagy szakszervezeti célú szervezet kezelheti a tagokra vonatkozó különleges adatokat vagy szintén jogszerű lehet az adatkezelés akkor is, ha az adatkezelés jogi igények előterjesztéséhez, érvényesítéséhez, illetve védelméhez szükséges.

II.5. Érintetti jogok

Az információs társadalom jelentette kihívások újszerű megoldásokat követelnek meg az érintetti jogok szabályozása terén is. A technológiai fejlődés hatására az adatalanyok egyre kevésbé képesek befolyásolni az online megosztott tartalmak, különösen a személyes adatok felhasználását, további sorsát. Az érintettek és az adatkezelők közötti egyensúly megbomlott az utóbbiak javára, amely egyrészt azzal a következménnyel jár, hogy az információs önrendelkezési jog számos esetben korlátozottan érvényesül csupán. Másrészt eddig soha nem látott mértékben van lehetőség a személyes adatokkal történő visszaélésekre.

A GDPR megalkotására – többek között – azért került sor, hogy tompítsák azt a széles körben kialakult benyomást, hogy a *„természetes személy védelme – különösen az online tevékenységek esetében – jelentős kockázatoknak van kitéve”*.[42] Ennek köszönhető, hogy a Rendelet az Adatvédelmi Irányelvben foglalt *„klasszikus”* érintetti jogok mellett olyan új rendelkezéseket is tartalmaz, amely az

41 Általános adatvédelmi rendelet 9. cikk (2) bekezdés a) pont
42 GDPR (9) preambulum bekezdés.

adatalanyokat további jogokkal vértezi fel az információs társadalom kihívásaira válaszul. Amíg ugyanis az előbbiek elsődlegesen egyfajta jogorvoslati funkciót töltenek be, addig az új jogosítványok már kifejezetten az érintett saját személyes adatai feletti önrendelkezésének megerősítését célozzák az online térben. Az említett új rendelkezések az elfeledtetéshez, valamint az adathordozhatósághoz való joghoz kapcsolódnak.

Az elfeledtetéshez való jog egyes elemeit [43] már az Adatvédelmi Irányelv is tartalmazza. A GDPR e jog kapcsán alapvetően három aspektust szabályoz: az érintett törléshez való jogát, e jog online környezetben történő alkalmazásának szabályait, valamint a jog gyakorlásának korlátait. A törléshez való jog kapcsán kiemelendő, hogy az uniós jogalkotó külön figyelmet fordított a gyermekek jogainak érvényesülésére. Amennyiben ugyanis a személyes adatok gyűjtésére közvetlenül gyermekeknek kínált, információs társadalommal összefüggő szolgáltatások vonatkozásában került sor, az adatalany jogosult arra, hogy kérésére az adatkezelő indokolatlan késedelem nélkül törölje a rá vonatkozó személyes adatokat.[44] E rendelkezés azokra az esetekre vonatkozik, amikor az érintett gyermekként adta meg hozzájárulását, de még nem volt teljesen tisztában az adatkezelés kockázataival, később pedig el akarja távolítani a szóban forgó személyes adatokat, különösen az internetről.

A törléshez való jog online környezetben történő megerősített szabályozása szintén azt célozza, hogy a felhasználók továbbra is fenntartsák az önrendelkezési jogukat a személyes adataik felett abban az esetben is, amennyiben azokat közzétették az interneten. Eszerint, ha az adatkezelő nyilvánosságra hozta a személyes adatot, és azt a Rendelet értelmében törölni kellene, az elérhető technológia és a megvalósítás költségeinek figyelembevételével megteszi az ésszerűen elvárható lépéseket, hogy *„tájékoztassa az adatokat kezelő adatkezelőket, hogy az érintett kérelmezte tőlük a szóban forgó személyes adatokra mutató linkek vagy e személyes adatok másolatának, illetve másodpéldányának törlését”*.[45] A tájékoztatás során az adatkezelőnek figyelembe kell vennie a rendelkezésre álló technológiai lehetőségeket és a végrehajtás költségeit is annak érdekében, hogy a személyes adatokat kezelő adatkezelők értesüljenek az érintett kéréséről.

A GDPR meghatározza azokat a kivételeket, amelyek esetében nem érvényesülhet a törléshez való jog. A korlátozásokat alapvetően három csoportra lehet bontani. Az elsőbe tartoznak azok az esetek, amikor az adatkezelés a véleménynyilvánítás szabadságához, valamint a tájékozódáshoz való jog (a tágan értelmezett infor-

43 Adatvédelmi Irányelv 12. cikk b)-c) pont.
44 GDPR 17. cikk (1) bekezdés f) pont.
45 GDPR 17. cikk (2) bekezdés.

mációszabadság) gyakorlása céljából szükséges.[46] A második csoportot azok az esetek alkotják, amelyeknél közérdek indokolja az adatkezelés szükségességét.[47] A harmadik csoportba pedig a védendő magánérdekek szerepelnek, azaz nem alkalmazandó az elfeledtetéshez való jog, amennyiben az adatkezelés jogi igények előterjesztéséhez, érvényesítéséhez, illetve védelméhez szükséges.[48]

II.5.1. Az adathordozhatóság

A GDPR egyik jelentős újítása az adathordozhatósághoz való jog elismerése. Ennek célja, hogy az adatalanyok ténylegesen birtokába jussanak korábban rendelkezésre bocsátott adataiknak és felhasználhassák azokat. (20. cikk)

E jog szerint az érintett jogosult arra, hogy azokat az adatokat, amit ő bocsátott az adatkezelő rendelkezésére, tagolt, széles körben használt, géppel olvasható és interoperábilis formátumban megkapja, használja, valamint jogosult azokat egy másik adatkezelőnek továbbítani, vagy azt kérni, hogy egy másik adatkezelőnek továbbítsák.

A jog gyakorlásának feltétele, hogy az adatokat maga az érintett bocsássa az adatkezelő rendelkezésére, méghozzá a hozzájárulása alapján, vagy szerződés teljesítése érdekében. Abban az esetben tehát nem gyakorolható a jogosultság, ha az adatkezelés jogalapja a hozzájárulástól vagy a szerződéstől eltérő egyéb jogalap. Fontos még, hogy csak automatizált adatkezelés esetében hivatkozhat az érintett e jogosultságára.

Az adatkezelőknek nem kötelességük az adathordozhatóságot lehetővé tevő formátumok kifejlesztése, ugyanakkor a Rendelet szerint ösztönözni kell rá őket, valamint nem kötelesek egymással műszakilag kompatibilis adatkezelő rendszereket bevezetni vagy fenntartani. Az érintett akkor jogosult arra, hogy az adatokat az adatkezelők egymás között közvetlenül továbbítsák, ha ez technikailag megvalósítható.

A jog gyakorlásának korlátja továbbá, hogy az nem sértheti az egyéb érintettek jogait, ha az adott személyes adatállomány egynél több érintettre vonatkozik. Az adathordozhatóság nem érinti továbbá az adatalanynak a Rendelet 17. cikkében rögzített, adatai törléséhez való jogát.

46 GDPR 17. cikk (3) bekezdés a) pont.
47 GDPR 17. cikk (3) bekezdés b)-d) pont.
48 GDPR 17. cikk (3) bekezdés e) pont.

II.5.2. Az előzetes tájékoztatás

Az Infotv. 20. § (2) bekezdésében foglalt példálózó felsoroláshoz képest a GDPR többletkövetelményként az alábbi információk előzetes megadását támasztja az adatkezelők számára, amelyeket az érintettek tudomására kell hozniuk:

- az adatkezelő illetve képviselője, és az adatvédelmi tisztviselő kiléte, elérhetősége;
- a 6. cikk (1) bekezdésének f) pontján [49] alapuló adatkezelés esetén az adatkezelő vagy harmadik fél jogos érdekei;
- azon címzettek kategóriái, akik megismerhetik az adatokat;
- az adatkezelő harmadik országba vagy nemzetközi szervezet részére továbbítja-e a személyes adatokat, továbbá
- a Bizottság megfelelőségi határozatának léte vagy annak hiánya, vagy a GDPR-ben rögzített adattovábbítást érintő esetekben a megfelelő és alkalmas garanciák megjelölése, valamint az azok másolatának megszerzési módjaira vagy elérhetőségükre való hivatkozás;
- az adatkezelés időtartama meghatározásának szempontjai, ha a tárolás ideje egyértelműen nem meghatározható;
- az érintett adathordozhatóságának joga;
- a hozzájárulás bármely időpontban történő visszavonásához való jog, amely nem érinti a visszavonás előtt az érintett tájékozott beleegyezése alapján végrehajtott adatkezelés jogszerűségét;
- a személyes adat szolgáltatása jogszabályon vagy szerződéses kötelezettségen alapul vagy szerződés kötésének előfeltétele-e, valamint hogy az érintett köteles-e a személyes adatokat megadni, továbbá hogy milyen lehetséges következményekkel járhat annak elmaradása;
- az automatizált döntéshozatal ténye, ideértve a profilalkotást is, valamint, hogy az ilyen adatkezelés milyen jelentőséggel, és az érintettre nézve milyen várható következményekkel bír.

Amennyiben a személyes adatokat nem az érintettektől veszik fel, a fentieken túlmenően a tájékoztatónak az adatok kategóriáit, (nyilvánosan hozzáférhető) forrását is tartalmaznia kell. Ez esetben az adatkezelő a tájékoztatást ésszerű határidő alatt, de legkésőbb egy hónapon belül adja meg; amennyiben az érintettel történő kapcsolattartás céljából használják személyes adatait, akkor az első

49 *„f) az adatkezelés az adatkezelő vagy egy harmadik fél jogos érdekeinek érvényesítéséhez szükséges, kivéve, ha ezen érdekekkel szemben elsőbbséget élveznek az érintett olyan érdekei vagy alapvető jogai és szabadságai, amelyek személyes adatok védelmét teszik szükségessé, különösen, ha az érintett gyermek."*

kapcsolatfelvétel alkalmával; ha pedig harmadik személy rendelkezésére is bocsátják az adatokat, azok első alkalommal történő közlésekor.

Amennyiben a személyes adatokat nem az érintettek bocsátják az adatkezelő rendelkezésére, úgy az adatkezelőknek nem kell megadniuk a tájékoztatást, ha:

- az érintett már tudomással bír személyes adatainak kezelésével kapcsolatos tudnivalókról;
- az információnyújtás lehetetlen vagy az adatkezelő számára nagy erőfeszítést igényel, viszont ez esetben is mindent meg kell tenni az érintettek jogának, jogos érdekének védelme érdekében;
- az adat megszerzését vagy közlését Uniós vagy tagállami jogszabály írja elő.

Függetlenül attól, hogy mi az adatok forrása, az eltérő célú adatkezelés esetén az érintettet erről, valamint az ahhoz kapcsolódó minden jelentőséggel bíró információról tájékoztatni kell. Az előzetes tájékoztatás egyébként mellőzhető, amennyiben az érintett már rendelkezik a szükséges információkkal.

II.6. Adatkezelők, adatfeldolgozók kötelezettségei

II.6.1. Beépített és alapértelmezett adatvédelem

A *„beépített és alapértelmezett adatvédelem”* elvei új, nevesített alapelvekként jelennek meg a Rendeletben, funkciójuk az, hogy a természetes személyek magánszférájának és kapcsolódó jogainak védelme érdekében a Rendelet követelményeinek megfelelő technikai és szervezési intézkedések meghozatalára kötelezik az adatkezelőt.

Az említett intézkedések magukban foglalhatják a személyes adatok kezelésének minimálisra csökkentését, a személyes adatok mihamarabbi álnevesítését (azaz olyan módon történő kezelését, hogy további információk hiányában már nem állapítható meg, hogy a személyes adat mely konkrét személyre vonatkozik), a személyes adatok funkcióinak és kezelésének átláthatóságát, valamint azt, hogy az érintett nyomon követhesse az adatkezelést, az adatkezelő pedig biztonsági elemeket hozhasson létre és továbbfejleszthesse azokat.

A beépített adatvédelem (*privacy by design*) és az alapértelmezett adatvédelem (*privacy by default*) elvei lényegüket tekintve arra kívánják ösztönözni a személyes adatok kezelésével járó szolgáltatások és termékek kifejlesztőit, tervezőit, kiválasztóit és felhasználóit, hogy már a termékek, szolgáltatások és alkalmazások kifejlesztésekor és tervezésekor szem előtt tartsák a személyes adatok védelméhez való jogot, valamint a tudomány és technológia állását kellően figyelembe véve gondoskodjanak arról, hogy az adatkezelők és az adatfeldolgozók adatvédelmi kötelezettségeiknek eleget tegyenek.

II.6.2. Az adatkezelőkre és az adatfeldolgozókra telepített új, illetve szigorúbb kötelezettségek

Az átlátható tájékoztatás érdekében a Rendelet kötelezi az adatkezelőket, hogy az adatkezeléssel kapcsolatban az érintett rendelkezésére bocsátandó minden tájékoztatást tömör, átlátható, érthető és könnyen hozzáférhető formában, világosan és közérthetően nyújtsák, különösen akkor, ha a tájékoztatás címzettje gyermek. Mindemellett a Rendelet az adatkezelők kifejezett kötelességévé teszi, hogy segítsék elő az érintettek joggyakorlását. A jelenleg hatályos magyar szabályozáshoz képest változik az érintetti jogok gyakorlása tekintetében az adatkezelő intézkedésére nyitva álló határidő, ez a Rendelet alkalmazását követően 25 nap helyett egy hónap lesz.

Az Infotv. eddigi szabályozási módszerétől eltérően a Rendelet eltérő tartalmú tájékoztatási kötelezettséget határoz meg az adatkezelők részére az érintettek rendelkezésére bocsátandó információk tekintetében akkor, ha a személyes adatokat az érintettől gyűjtik, és arra az esetre, ha a személyes adatokat nem az érintettől szerezték meg.

A Rendelet – kibontva az Irányelv és az Infotv. még csak utalás szintjén meghatározott fogalmait – részletes szabályokat határoz meg az úgynevezett közös adatkezelői minőség esetére, tehát amikor az adatkezelés célját és eszközeit két vagy több adatkezelő közösen határozza meg. A jövőben a közös adatkezelők átlátható módon, a közöttük létrejött megállapodásban határozzák meg az érintett rendelkezésére bocsátandó információkért való felelősség megoszlását. A megállapodásban – melyet az érintett rendelkezésére kell bocsátani – rendelkezni kell a közös adatkezelők érintettekkel szembeni szerepéről és a velük való kapcsolat rendjéről. Lényeges, hogy a megállapodás tartalmától függetlenül az adatkezelő bármelyik adatkezelőhöz fordulhat érintetti jogainak gyakorlása érdekében.

Szintén a Rendelet újdonságai közé tartozik, hogy részletesen kifejti az adatkezelő és az adatfeldolgozó között megkötendő írásbeli szerződés tartalmi elmeit, emellett szigorítja az adatfeldolgozóra telepített felelősséget abban az esetben, ha az adatfeldolgozó al-adatfeldolgozót vesz igénybe, valamint ha az adatfeldolgozó – a Rendelet sérelmével – maga határozza meg az adatkezelés célját és eszközeit, tehát kvázi-adatkezelőként jár el.

Az Unióban tevékenységi hellyel nem rendelkező adatkezelők vagy adatfeldolgozók képviselői vonatkozásában a Rendelet fontos újdonságokat tartalmaz, az ilyen adatkezelőknek és adatfeldolgozóknak ugyanis írásban uniós képviselőt kell kijelölniük. A képviselőnek tevékenységi hellyel kell rendelkeznie az egyik olyan tagállamban, ahol:

a) azon érintettek tartózkodnak, akiknek személyes adatait áruknak, vagy
b) szolgáltatásoknak a részükre történő nyújtása során kezelik,
c) vagy akiknek a magatartását megfigyelik.

Az adatkezelő vagy az adatfeldolgozó által a képviselő számára adott megbízásnak ki kell terjednie arra, hogy az adatkezelő vagy az adatfeldolgozó helyett vagy mellett a képviselő járjon el az adatkezeléssel összefüggő minden ügyben, így különösen a felügyeleti hatóságok és az érintettek megkeresése tekintetében.

Lényeges, hogy önmagában az a tény, hogy az adatkezelő vagy az adatfeldolgozó képviselőt jelöl ki, nem érinti az adatkezelővel vagy az adatfeldolgozóval szembeni keresetindításhoz való jogot.

Az Unióban tevékenységi hellyel nem rendelkező adatkezelők vagy adatfeldolgozók esetében sem kell alkalmazni azonban a fenti rendelkezéseket,

a) az alkalmi jellegű adatkezelésre (ha az nem terjed ki sem a személyes adatok különleges kategóriáira, sem büntetőjogi felelősség megállapítására vonatkozó határozatokra és bűncselekményekre vonatkozó személyes adatok nagy számban történő kezelésére, és amely – figyelembe véve az adatkezelés jellegét, körülményeit, hatókörét és céljait – valószínűsíthetően nem jelent kockázatot a természetes személyek jogaira és szabadságaira nézve); vagy
b) ha az adatkezelő/adatfeldolgozó közhatalmi vagy egyéb, közfeladatot ellátó szerv.

A Rendelet adminisztratív szempontból egyik fontos újítása, hogy az adatkezelési tevékenységek nyilvántartását 2018. május 25. napjától már nem a felügyeleti hatóságok, hanem az adatkezelők és az adatfeldolgozók végzik, a Rendeletben részletesen meghatározott tartalommal.

III.6.3. Az adatvédelmi tisztviselő

Az Infotv. 24. §-a jelenleg a belső adatvédelmi felelős tisztségéről rendelkezik, amelynek funkcióját a Rendelet rendszerében az adatvédelmi tisztviselő látja majd el.

A Rendelet 37. cikke szerint az adatkezelő és az adatfeldolgozó adatvédelmi tisztviselőt jelöl ki minden olyan esetben, amikor:

a) az adatkezelést közhatalmi szervek vagy egyéb, közfeladatot ellátó szervek végzik, kivéve az igazságszolgáltatási feladatkörükben eljáró bíróságokat;
b) az adatkezelő vagy az adatfeldolgozó fő tevékenységei olyan adatkezelési műveleteket foglalnak magukban, amelyek jellegüknél, hatókörüknél és/vagy céljaiknál fogva az érintettek rendszeres és szisztematikus, nagymértékű megfigyelését teszik szükségessé;
c) az adatkezelő vagy az adatfeldolgozó fő tevékenységei a személyes adatok különleges kategóriáinak és büntetőjogi felelősség megállapítására vonatkozó határozatokra és bűncselekményekre vonatkozó adatok nagy számban történő kezelését foglalják magukban.

Látható tehát, hogy a Rendelet szabályai alapján a jelenleg alkalmazandó szabályokban meghatározottaknál szélesebb körben válik kötelezővé adatvédelmi tisztviselő kijelölése. A Rendeletben kifejezetten nem nevesített esetekben is gondoskodhat adatvédelmi tisztviselő kijelöléséről az adatkezelő vagy az adatfeldolgozó, illetve az előbbieket képviselő szervezetek, valamint az uniós és a tagállami jogalkotó is előírhatja azt.

Lényeges eltérés az Infotv. jelenleg hatályos szabályaitól, – mely szerint belső adatvédelmi felelősnek csak jogi, közigazgatási, informatikai vagy ezeknek megfelelő, felsőfokú végzettséggel rendelkező személy nevezhető ki, illetve bízható meg – hogy az adatvédelmi tisztviselőt szakmai rátermettség, és különösen az adatvédelmi jog és gyakorlat szakértői szintű ismerete, valamint a Rendelet 39. cikkében említett feladatok ellátására való alkalmasság alapján kell kijelölni. A szakértői ismeretek szükséges szintjét különösen az adatkezelő vagy az adat-

feldolgozó által végzett adatkezelés, valamint az általuk kezelt személyes adatok tekintetében megkövetelt védelem alapján kell meghatározni.

Az adatvédelmi tisztviselővel történő kapcsolatfelvétel megkönnyítése érdekében a Rendelet kötelezi az adatkezelőket, illetve az adatfeldolgozókat, hogy tegyék közzé az adatvédelmi tisztviselő nevét, valamint azt a felügyeleti hatósággal is közöljék.

A Rendelet 37. cikke alapján az adatvédelmi tisztviselő az adatkezelő vagy az adatfeldolgozó alkalmazottja lehet, vagy szolgáltatási szerződés keretében láthatja el a feladatait. Függetlenségének biztosítása érdekében a Rendelet előírja, hogy az adatkezelőnek és az adatfeldolgozónak biztosítania kell, hogy az adatvédelmi tisztviselő a feladatai ellátásával kapcsolatban utasításokat senkitől ne fogadjon el, az adatvédelmi tisztviselő feladatai ellátásával összefüggésben nem bocsátható el és szankcióval sem sújtható – ebbe a körben természetesen nem tartoznak a hanyag, illetőleg munkaköri kötelezettségek megszegésével járó magatartások. Az adatvédelmi tisztviselő közvetlenül az adatkezelő vagy az adatfeldolgozó legfelső vezetésének tartozik felelősséggel, feladatainak ellátásával kapcsolatban titoktartási kötelezettség terheli.

Megállapítható, hogy az adatvédelmi tisztviselő jogállása a jelenleg hatályos szabályozáshoz képest jelentős garanciális szabályokkal vált védettebbé, feladatainak ellátása során függetlenebbé.

Az Infotv. és a Rendelet vonatkozó rendelkezéseit összevetve megállapítható, hogy a belső adatvédelmi felelős helyébe lépő adatvédelmi tisztviselő feladatai elsősorban a Rendelet által bevezetett új jogintézményekre, illetve az adatkezelőkre vonatkozó új szabályokra tekintettel változnak, pontosabban bővülnek.

II.6.4. Az adatvédelmi hatásvizsgálat (Privacy Impact Assessment, PIA)

A GDPR egyik jelentős újítása az adatvédelmi hatásvizsgálat kötelezettségének bevezetése. Az adatvédelmi hatásvizsgálat a Rendelet két előtérbe kerülő koncepciójába illeszkedik, ugyanis egyfelől az elszámoltathatóság elvéhez, másrészről a Rendeletnek a kockázat alapú megközelítéséhez kapcsolódik. Hiszen a hatásvizsgálat egyrészről segítséget nyújt az adatkezelőnek abban, hogy a Rendelet rendelkezéseinek történő megfelelést elérje és bizonyítsa, másrészről akkor sikeres, ha jól mérhető kockázatokat tud azonosítani és azokat megfelelő

intézkedésekkel csökkenteni. A fenti célokat a Rendelet 24. cikke, az adatkezelő feladatainak általános meghatározásánál is megerősíti. Az adatkezelő az adatkezelés jellege, hatóköre, körülményei és céljai, valamint a természetes személyek jogaira és szabadságaira jelentett, változó valószínűségű és súlyosságú kockázat figyelembevételével megfelelő technikai és szervezési intézkedéseket hajt végre annak biztosítása és bizonyítása céljából, hogy a személyes adatok kezelése e rendelettel összhangban történik. Ezeket az intézkedéseket az adatkezelő felülvizsgálja és szükség esetén naprakésszé teszi.[50] Sem az elszámoltathatóság koncepciója, sem a kockázat alapú adatvédelmi megközelítés nem újdonság, de eddig a szabályozásban nem foglaltak el ilyen központi szerepet.

Az adatvédelmi hatásvizsgálatnak a Rendelet nem adja meg a tételes definícióját, csak leírja annak tartalmi elemeit. Egy általános fogalom akként definiálható, miszerint az adatvédelmi hatásvizsgálat egy adatkezelési folyamatra irányuló szisztematikus vizsgálat, amely célja annak felderítése és értékelése, hogy az adott adatkezelés milyen kockázatokat hordoz az érintettek magánszférájára nézve, illetve ezek a kockázatok milyen intézkedésekkel csökkenthetőek és szüntethetőek meg a minél magasabb szintű adatvédelmi megfelelés érdekében. Ennek megfelelően a hatásvizsgálat kiterjed a tervezett adatkezelési műveletek módszeres leírására és az adatkezelés céljainak ismertetésére, beleértve adott esetben az adatkezelő által érvényesíteni kívánt jogos érdeket. A hatásvizsgálat továbbá az adatkezelés céljaira figyelemmel magába foglalja az adatkezelési műveletek szükségességi és arányossági vizsgálatát; illetve figyelemmel az adatkezelés jellegére, hatókörére, körülményére és céljaira az érintett jogait és szabadságait érintő kockázatok vizsgálatát. A hatásvizsgálat emellett kiterjed a kockázatok kezelését célzó intézkedések bemutatására, ideértve a személyes adatok védelmét és a rendelettel való összhang igazolását szolgáló, az érintettek és más személyek jogait és jogos érdekeit figyelembe vevő garanciákat, biztonsági intézkedéseket és mechanizmusokat.[51]

Az adatvédelmi hatásvizsgálatot adatkezelésenként, adatkezelési műveletenként kell elvégezni, de olyan egymáshoz hasonló típusú adatkezelési műveletek, amelyek egymáshoz hasonló magas kockázatokat jelentenek, egyetlen hatásvizsgálat keretei között is értékelhetőek.[52] Bizonyos körülmények között ésszerűnek és gazdaságosnak bizonyulhat az adatvédelmi hatásvizsgálat nem egyetlen projekt tekintetében történő lefolytatása, például ha közhatalmi szervek vagy egyéb, közfeladatot ellátó szervek közös alkalmazást vagy adatkezelési felületet kívánnak

50 GDPR 24. cikk
51 GDPR 35. cikk (7) bekezdés
52 GDPR 35. cikk (1) bekezdés

létrehozni, vagy ha több adatkezelő közös alkalmazást vagy adatkezelési környezetet kíván bevezetni valamely ágazat vagy szegmens, vagy valamely széles körben végzett horizontális tevékenység tekintetében.[53]

Az adatvédelmi hatásvizsgálat a Rendeletnek történő megfelelést elősegítő eszköz, amely növeli az adatkezelő adatvédelmi tudatosságát, ennek megfelelően a lehető legszélesebb körben célszerű alkalmazni. A Rendelet azonban meghatározza, mely esetekben kötelező adatvédelmi hatásvizsgálatot végezni. A kritériumrendszer több egymást segítő részből épül fel. Egyrészről generálklauzula jelleggel, egy általános kritériumként jelenik meg, hogy kötelező hatásvizsgálatot végezni, ha az adatkezelés valamely – különösen új technológiákat alkalmazó – típusa, figyelemmel annak jellegére, hatókörére, körülményére és céljaira, valószínűsíthetően magas kockázattal jár a természetes személyek jogaira és szabadságaira nézve.[54] Ezt az általános szempontot pontosítja egy példálózó felsorolás, amely alapján adatvédelmi hatásvizsgálatot különösen az alábbi esetekben kell elvégezni. Egyrészről a természetes személyekre vonatkozó egyes személyes jellemzők olyan módszeres és kiterjedt értékelése esetén, amely automatizált adatkezelésen alapul – ideértve a profilalkotást is –, és amelyre a természetes személy tekintetében joghatással bíró vagy a természetes személyt hasonlóképpen jelentős mértékben érintő döntések épülnek.[55] Másrészről, ha a Rendelet 9. cikk (1) bekezdésében említett személyes adatok különleges kategóriái, vagy a 10. cikkben említett, büntetőjogi felelősség megállapítására vonatkozó határozatokra és bűncselekményekre vonatkozó személyes adatok nagy számban történő kezelése történik. Harmadrészről nyilvános helyek nagymértékű, módszeres megfigyelése esetén.[56] [57]

A fenti kritériumrendszert tovább pontosítja az a rendelkezés, amely alapján a felügyeleti hatóságnak össze kell állítania és nyilvánosságra kell hoznia az olyan adatkezelési műveletek típusainak a jegyzékét, amelyekre vonatkozóan adatvédelmi hatásvizsgálatot kell végezni.[58] Itt természetesen nem egy tételes felsorolásra kell gondolni, hanem inkább egy kritériumrendszert felsoroló listára, amely lista segítségével egy adatkezelő azonosíthatja, hogy az adatkezelése a kötelező hatásvizsgálatot igénylő körbe esik vagy sem.

53 GDPR (92) preambulum bekezdés
54 GDPR 35. cikk (1) bekezdés
55 Scoring rendszerű vagy profilalkotáson alapuló automatizált döntések
56 A megfigyelés nem csak kamerarendszereket jelenthet, ide sorolható például az érintettek helyzetének vagy viselkedésének megfigyelése nyilvános helyeken (pl. plázákban) wifi vagy bluetooth kapcsolatok felhasználásával.
57 GDPR 35. cikk (3) bekezdés
58 GDPR 35. cikk (4) bekezdés

Emellett az adatvédelmi hatóság a fenti lista inverzét is kibocsáthatja, amely az olyan adatkezelési műveletek típusainak a jegyzéke, amelyekre vonatkozóan nem kell adatvédelmi hatásvizsgálatot végezni.[59]

A hatásvizsgálat készítési kötelezettség természetesen a Rendelet hatálybalépését követő adatkezelésekre vonatkozik, tehát alapjában véve 2016 májusát követően megkezdett adatkezelések esetén kell elvégezni, és természetesen a GDPR alkalmazhatósága, azaz 2018 májusa után kötelező magát a hatásvizsgálatot lefolytatni. Az adatvédelmi hatásvizsgálatot (újra) el kell végezni, ha az első adatkezelés óta eltelt időre tekintettel ez szükségessé vált,[60] vagy ha az adatkezelés körülményeiben, vagy az adatkezelés során alkalmazott technikai környezetben jelentős változás történt. Mindenesetre kijelenthető, hogy jó gyakorlatnak tekinthető, ha legalább három évenként az adatkezelő új hatásvizsgálat keretében felülvizsgálja a valószínűsíthetően magas kockázattal járó adatkezeléseit.

Az adatvédelmi hatásvizsgálatot az adatkezelés megkezdése előtt kell elvégezni, amely a célszerűségi megfontolásokon túl illeszkedik a beépített és alapértelmezett adatvédelem elveihez is.[61] Az adatvédelmi hatásvizsgálatot és az elvégzéséhez szükséges információgyűjtést már az adatkezelés megtervezésének legelső fázisában érdemes megkezdeni, így érvényesülhetnek a fent említett alapelvek és előírások a leghatékonyabban. Ez természetesen magában hordozza annak a lehetőségét, hogy az egyes fejlesztési fázisokban a hatásvizsgálat egyes lépéseit újra el kell végezni, vagy frissíteni, módosítani kell, de hatékonyabban megtalálhatóak a kockázatokat csökkentő mechanizmusok, ha már az adatkezelés tervezésekor is szisztematikusan elemzik az adatkezelést adatvédelmi szempontból.

Az adatvédelmi hatásvizsgálatot az adatkezelőnek kötelezettsége naprakészen tartani, és szükség szerint, de legalább az adatkezelési műveletek által jelentett kockázat változása esetén ellenőrzést lefolytatni annak értékelése céljából, hogy a személyes adatok kezelése az adatvédelmi hatásvizsgálatnak megfelelően történik-e.[62] Az adatvédelmi kockázatok változhatnak, ha valamely tényezőjük (a kezelt személyes adatok köre, az adatkezelést kiszolgáló informatikai környezet, a kockázatok forrásai, a kockázatok hatásai, a veszélyforrások) megváltozik vagy az adatkezelés környezete jelentős mértékben átalakul.

59 GDPR 35. cikk (5) bekezdés
60 GDPR (89) preambulum bekezdés
61 GDPR 35. cikk (1) és (10) bekezdés, 25. cikk, illetve a (78) (90) és (93) preambulum bekezdések
62 GDPR 35. cikk (11) bekezdés

Az adatvédelmi hatásvizsgálatot az adatkezelőnek kell elvégeznie.[63] Természetesen a gyakorlatban ez jelentheti azt, hogy az adatvédelmi hatásvizsgálatot az adatkezelő megbízásából harmadik személy vagy szervezet végzi el, de az elszámoltathatóság alapelvére is tekintettel az adatkezelő felelős a hatásvizsgálat elkészítéséért és tartalmáért. Ha van kijelölt adatvédelmi tisztviselő, az adatkezelő az adatvédelmi hatásvizsgálat elvégzésekor az adatvédelmi tisztviselő szakmai tanácsát köteles kikérni.[64]

Az adatkezelő adott esetben – a kereskedelmi érdekek vagy a közérdek védelmének vagy az adatkezelési műveletek biztonságának sérelme nélkül – kikéri az érintettek vagy képviselőik véleményét a tervezett adatkezelésről.[65]

Az adatvédelmi hatásvizsgálattal kapcsolatos legfontosabb kérdéskör, hogy hogyan kell az adatvédelmi hatásvizsgálatot elvégezni. A hatásvizsgálatban egyrészről részletesen be kell mutatni a vizsgált adatkezelést. Ennek ki kell terjednie az adatkezelés környezetének az ismertetésére is. Ennek megfelelően be kell mutatni a kezelt személyes adatok körét, az adatkezelés célját, jogalapját, az adatfelvétel módját, kik férhetnek hozzá a kezelt személyes adatokhoz, a megőrzési határidőket, az adatkezelést támogató informatikai rendszereket; el kell készíteni az adatkezelés funkcionális leírását, esetlegesen az adatkezelés tervezése során alkalmazott magatartási kódexeket, stb.

Emellett a hatásvizsgálatnak ki kell terjedni annak a bemutatására is, hogy az adatkezelés miként felel meg a jogszabályi előírásoknak, különös tekintettel a Rendelet II. fejezetében leírtaknak. Ugyancsak meg kell vizsgálni, hogy az adatkezelés során az adatkezelő hogyan biztosítja a Rendelet III. fejezetében részletezett érintetti jogok gyakorlásának feltételeit.

Az adatvédelmi hatásvizsgálatnak talán a legfontosabb és legösszetettebb része a természetes személyek jogaira és szabadságaira nézve magas kockázatok elemzése. Ezzel kapcsolatban az adatkezelőnek meg kell vizsgálnia a kockázatok forrását, természetét, sajátosságait és súlyosságát. Minden kockázat tekintetében elemezni kell, miként fordulhat elő a nem kívánt hatás, ennek általános körülmények között mennyi a valószínűsége, ha a kockázat realizálódik, milyen következményekkel jár az érintett magánszférájára.

63 GDPR 35. cikk (1) (2) és (9) bekezdés
64 GDPR 35. cikk (2) bekezdés
65 GDPR 35. cikk (9) bekezdés

A természetes személyek jogait és szabadságait érintő kockázatok vezethetnek fizikai, vagyoni vagy nem vagyoni károkhoz. Ilyen kockázatok lehetnek különösen, ha az adatkezelésből hátrányos megkülönböztetés, személyazonosság-lopás vagy személyazonossággal való visszaélés, pénzügyi veszteség, a jó hírnév sérelme, a szakmai titoktartási kötelezettség által védett személyes adatok bizalmas jellegének sérülése, az álnevesítés engedély nélkül történő feloldása, vagy bármilyen egyéb jelentős gazdasági vagy szociális hátrány fakadhat. Ugyancsak jelentős kockázatként azonosítható, ha az adatkezelés miatt az érintettek nem gyakorolhatják jogaikat és szabadságaikat, vagy nem rendelkezhetnek saját személyes adataik felett. Vagy ha olyan személyes adatok kezelése történik, amelyek faji vagy etnikai származásra, vagy politikai véleményre, vallási vagy világnézeti meggyőződésre vagy szakszervezeti tagságra utalnak, valamint ha a kezelt adatok genetikai adatok, egészségügyi adatok vagy a szexuális életre, büntetőjogi felelősség megállapítására, illetve bűncselekményekre, vagy ezekhez kapcsolódó intézkedésekre vonatkoznak. Ugyancsak kockázatként értékelendő egy adatkezelésben, ha személyes jellemzők értékelésére, így különösen munkahelyi teljesítménnyel kapcsolatos jellemzők, gazdasági helyzet, egészségi állapot, személyes preferenciák vagy érdeklődési körök, megbízhatóság vagy viselkedés, tartózkodási hely vagy mozgás elemzésére vagy előrejelzésére kerül sor személyes profil létrehozása vagy felhasználása céljából. Ha kiszolgáltatott személyek – különösen, ha gyermekek – személyes adatainak a kezelésére kerül sor; vagy ha az adatkezelés nagy mennyiségű személyes adat alapján zajlik, és nagyszámú érintettre terjed ki.[66]

Az adatvédelmi hatásvizsgálatban részletezni kell azokat az intézkedéseket is, amelyek az előbb említett kockázatok csökkentésére vagy megszüntetésére irányulnak. Itt ki kell térni arra, hogy az adott intézkedés hogyan és milyen mértékben csökkenti a kockázatot, ki a felelős az intézkedés végrehajtásáért és az adott intézkedés mennyire általános megoldása az adott kockázat csökkentésének.

Az adatvédelmi hatásvizsgálatban természetesen rögzíteni kell az adatvédelmi tisztviselő észrevételeit, illetve amennyiben kikérték az érintettek véleményét, ezt is be kell mutatni. Ha a hatásvizsgálat alá vont adatkezelésben több adatkezelő is azonosítható, akkor rögzíteni kell az egyes adatkezelők felelősségét a megtett intézkedésekért. Ugyanígy kell eljárni, ha a hatásvizsgálatban azonosított kockázatok az adatfeldolgozók tevékenységét érintik.

Ha az adatvédelmi hatásvizsgálat azt jelzi, hogy a kockázat mérséklését célzó garanciák, biztonsági intézkedések és mechanizmusok hiányában az adatkeze-

66 GDPR (75) preambulum bekezdés

lés magas kockázattal járna a természetes személyek jogaira és szabadságaira nézve, és az adatkezelő véleménye alapján a kockázat nem mérsékelhető a rendelkezésre álló technológiák és a végrehajtási költségek szempontjából ésszerű módon, akkor az adatkezelési tevékenység megkezdése előtt a felügyeleti hatósággal konzultálni kell. E konzultációs eljárás során a szóban forgó adatkezelés tekintetében végzett adatvédelmi hatásvizsgálat eredményét, és különösen a természetes személyek jogait és szabadságait veszélyeztető kockázat mérséklésére szolgáló intézkedések tervezetét be kell nyújtani a felügyeleti hatóságnak.[67]

II.7. Magatartási kódexek és tanúsítási mechanizmusok

II.7.1. Magatartási kódexek

A tagállamok, a felügyeleti hatóságok, az Európai Adatvédelmi Testület (a továbbiakban: Testület) és a Bizottság ösztönzik olyan magatartási kódexek kidolgozását, amelyek – a különböző adatkezelő ágazatok egyedi jellemzőinek, valamint a mikro-, kis- és középvállalkozások sajátos igényeinek figyelembevételével – segítik a Rendelet helyes alkalmazását.

Az adatkezelők vagy az adatfeldolgozók kategóriáit képviselő egyesületek és egyéb szervezetek magatartási kódexeket dolgozhatnak ki, illetve a már meglévő magatartási kódexeket módosíthatják vagy bővíthetik abból a célból, hogy pontosítsák a Rendelet alkalmazását. Ilyen kódexek például a következő területekkel kapcsolatban alkothatók: tisztességes és átlátható adatkezelés; az adatkezelők jogos érdekei meghatározott körülmények között; az adatgyűjtés; személyes adatok álnevesítése; a nyilvánosság és az érintettek tájékoztatása; az érintettek jogainak gyakorlása; a gyermekek tájékoztatása és védelme, valamint a szülői felügyelet gyakorlójától származó hozzájárulás kikérésének módja; az adatkezelő feladatai, valamint a beépített és alapértelmezett adatvédelemre vonatkozó intézkedések és eljárások; valamint az adatkezelés biztonságát szolgáló intézkedések; a felügyeleti hatóságok értesítése, továbbá az érintettek tájékoztatása az adatvédelmi incidensekről; a személyes adatok harmadik országok vagy nemzetközi szervezetek részére történő továbbítása; az adatkezelők és érintettek közötti viták rendezése; az érintettek panasztételi joga a felügyeleti hatóságnál.

67 GDPR 36. cikk (1) bekezdés, illetve (84) és (94) preambulum bekezdés

A Rendelet hatálya alá nem tartozó adatkezelők vagy adatfeldolgozók is betarthatják a felügyeleti hatóság által jóváhagyott, vagy – amennyiben a magatartási kódex több tagállamot is érintő tevékenységekre vonatkozik – a Bizottság határozata alapján általános érvénnyel rendelkező magatartási kódexeket.

II.7.2. A jóváhagyott magatartási kódexeknek való megfelelés ellenőrzése

A magatartási kódexnek való megfelelés ellenőrzését olyan szervezet végezheti, amely a kódex tárgya tekintetében megfelelő szakértelemmel rendelkezik, és amelyet az illetékes felügyeleti hatóság erre akkreditál. Az akkreditáció általános feltételeit a Rendelet 63. cikke tartalmazza.

Az akkreditált szervezet a kódex valamely adatkezelő vagy adatfeldolgozó általi megsértése esetén – megfelelő garanciák mellett – megfelelő intézkedéseket tesz, beleértve az érintett adatkezelő vagy adatfeldolgozó felfüggesztését vagy kizárását a kódex alkalmazásából. Ezekről az intézkedésekről és azok indokairól az illetékes felügyeleti hatóságot tájékoztatja.

Lényeges, hogy a jóváhagyott magatartási kódexeknek való megfelelésre vonatkozó rendelkezések nem alkalmazandók a közhatalmi szervek és közfeladatot ellátó egyéb szervek által végzett adatkezelésre.

A magatartási kódexhez történő csatlakozás, illetve az annak való megfelelés több előnnyel jár az adatkezelők és adatfeldolgozók számára:

a. felhasználható annak bizonyítása részeként, hogy az adatkezelő teljesíti egyes, a Rendelet által meghatározott kötelezettségeit, az adatfeldolgozó pedig felhasználhatja annak bizonyítására, hogy megfelel egyes, a Rendelet által az adatfeldolgozókkal szemben előírt garanciális követelményeinek.
b. a jóváhagyott magatartási kódexekhez való csatlakozást mind az adatkezelő, mind az adatfeldolgozó felhasználhatja annak bizonyítása részeként, hogy a kockázatoknak megfelelő adatbiztonságot garantálja.
c. személyes adatok harmadik országba vagy nemzetközi szervezetek részére történő továbbítása esetén a jóváhagyott magatartási kódex, valamint a harmadik országbeli adatkezelő vagy adatfeldolgozó arra vonatkozó, kötelező erejű és kikényszeríthető kötelezettségvállalása együtt,

hogy alkalmazza a megfelelő – ideértve az érintettek jogaira vonatkozó – garanciákat, jogszerűvé teheti az adattovábbítást.

Végül annak eldöntésekor, hogy szükség van-e közigazgatási bírság kiszabására, illetve a közigazgatási bírság összegének megállapításakor minden egyes esetben kellőképpen figyelembe kell venni egyebek mellett azt is, hogy az adatkezelő vagy az adatfeldolgozó tartotta-e magát a jóváhagyott magatartási kódexekhez.

II.7.3. Tanúsítási mechanizmusok

A tagállamok, a felügyeleti hatóságok, a Testület, valamint a Bizottság – különösen uniós szinten – ösztönzik olyan adatvédelmi tanúsítási mechanizmusok, valamint adatvédelmi bélyegzők, illetve jelölések létrehozását, amelyek bizonyítják, hogy az adatkezelő vagy adatfeldolgozó által végrehajtott adatkezelési műveletek megfelelnek e rendelet előírásainak.

A tanúsítási folyamatnak, önkéntesnek, a tanúsítási eljárásnak pedig átláthatónak kell lennie.

A tanúsítványt az erre akkreditált tanúsító szervezetek vagy az illetékes felügyeleti hatóságok állítják ki, az illetékes felügyeleti hatóság vagy a Testület által jóváhagyott szempontok alapján. Ha a szempontokat a Testület hagyja jóvá, ennek eredményeként közös tanúsítvány, az európai adatvédelmi bélyegző állítható ki. Az adatkezelési tevékenységét a tanúsítási mechanizmusnak alávető adatkezelő vagy adatfeldolgozó a tanúsító szervezet vagy adott esetben az illetékes felügyeleti hatóság részére minden olyan információt megad és minden olyan adatkezelési tevékenységéhez hozzáférést biztosít, amely a tanúsítási eljárás lefolytatásához szükséges.

Az adatkezelő vagy adatfeldolgozó részére legfeljebb hároméves időtartamra lehet kiállítani a tanúsítványt, amely megújítható, feltéve, hogy a vonatkozó követelmények továbbra is teljesülnek. Abban az esetben azonban, ha a tanúsításra vonatkozó követelmények már nem teljesülnek, az erre akkreditált tanúsító szervezet vagy az illetékes felügyeleti hatóság a tanúsítványt visszavonja.

Lényeges, hogy a tanúsítás nem csökkenti az adatkezelő vagy adatfeldolgozó Rendelet betartásáért való felelősségét, és nem sérti az illetékes felügyeleti hatóságok feladat- és hatáskörét.

A Testület valamennyi tanúsítási mechanizmust és adatvédelmi bélyegzőt, illetve jelölést egy nyilvántartásban állítja össze, és megfelelő módon nyilvánosan elérhetővé teszi őket.

Az illetékes felügyeleti hatóság feladat- és hatásköreinek sérelme nélkül a tanúsítvány kiállítását és megújítását olyan tanúsító szervezet végzi, amely az adatvédelem terén megfelelő szakértelemmel rendelkezik. A tanúsító szervezet akkreditációját az illetékes felügyeleti hatóság, illetve az erre a feladatra megnevezett nemzeti akkreditáló testület végzi el.

A tanúsító szervezetek akkreditációjának általános feltételeit a Rendelet meghatározza (például: kielégítő bizonyíték a szervezet függetlenségére és szakértemére nézve stb.), az akkreditáció öt éves időtartamra adható meg, és megújítható. A tanúsítás vagy annak visszavonása alapjául szolgáló megfelelő vizsgálat lefolytatásáért az akkreditált tanúsító szervezet felelős, ez azonban nem érinti az adatkezelő vagy adatfeldolgozó felelősségét.

Az adatkezelők vagy adatfeldolgozók számára a tanúsítási mechanizmusok jelentősége abból a szempontból is kiemelt, hogy személyes adatok harmadik országba vagy nemzetközi szervezet részére történő továbbítása esetén a megfelelő garanciákat jelentheti – egyebek mellett – a jóváhagyott tanúsítási mechanizmus a harmadik országbeli adatkezelő vagy adatfeldolgozó arra vonatkozó, kötelező erejű és kikényszeríthető kötelezettségvállalásával együtt, hogy alkalmazza a megfelelő garanciákat, ideértve az érintettek jogait illetően is. A Testület valamennyi tanúsítási mechanizmust és adatvédelmi bélyegzőt egy nyilvántartásban állítja össze, és azokat megfelelő módon nyilvánosan elérhetővé teszi.

Annak eldöntésekor, hogy szükség van-e közigazgatási bírság kiszabására, illetve a közigazgatási bírság összegének megállapításakor minden egyes esetben kellőképpen figyelembe kell venni egyebek mellett azt is, hogy az adatkezelő vagy az adatfeldolgozó tartotta-e magát a jóváhagyott tanúsítási mechanizmusokhoz.

II.8. Az adatvédelmi incidensek

Összefoglalva a főbb változásokat elmondható, hogy a Rendelet alapján az adatkezelőket és az adatfeldolgozókat is egy általános adatvédelmi incidens bejelentési kötelezettség terheli. Az adatfeldolgozónak is be kell jelentenie ugyanis

az adatvédelmi incidenseket az adatkezelő részére, az adatkezelőknek pedig az incidenseket be kell jelenteniük a felügyeleti hatóságnak, illetve bizonyos esetekben az érintetteket is tájékoztatniuk kell, illetve az adatvédelmi incidensekről továbbra is nyilvántartást kell vezetniük.

A Rendelet 4. cikk 12. pontja szerint adatvédelmi incidens: *„a biztonság olyan sérülése, amely a továbbított, tárolt vagy más módon kezelt személyes adatok véletlen vagy jogellenes megsemmisítését, elvesztését, megváltoztatását, jogosulatlan közlését vagy az azokhoz való jogosulatlan hozzáférést eredményezi”.*

Az új definíció az incidenseket egyértelműen a biztonság sérülésén keresztül határozza meg. A Rendelet 32. cikk (2) bekezdésének megfogalmazása alapján a biztonság megfelelő szintjének meghatározásakor kifejezetten figyelembe kell venni az adatkezelésből eredő olyan kockázatokat, amelyek különösen a továbbított, tárolt vagy más módon kezelt személyes adatok véletlen vagy jogellenes megsemmisítéséből, elvesztéséből, megváltoztatásából, jogosulatlan nyilvánosságra hozatalából vagy az azokhoz való jogosulatlan hozzáférésből erednek. A Rendelet megfogalmazása gyakorlatilag egybeesik az adatvédelmi incidens fogalmával, azaz már a biztonság megfelelő szintjének meghatározásakor kifejezetten figyelembe kell venni az adatkezelésből eredő olyan kockázatokat, melyek adatvédelmi incidensekből származhatnak.

A Rendelet 33. cikk (1) bekezdése alapján az adatvédelmi incidenst az adatkezelő indokolatlan késedelem nélkül, és ha lehetséges, legkésőbb 72 órával azután, hogy az adatvédelmi incidens a tudomására jutott, köteles bejelenteni az illetékes felügyeleti hatóságnak.

Fontos szabály, hogy az adatfeldolgozót is bejelentési kötelezettség terheli az adatkezelő felé, így az adatvédelmi incidenst, az arról való tudomásszerzését követően indokolatlan késedelem nélkül az adatfeldolgozónak is be kell jelentenie az adatkezelőnek.

A bejelentés módjára, tartalmára nézve a Rendelet 33. cikk (3) bekezdése részletes szabályokat állapít meg.

Ha az adatkezelő az elszámoltathatóság elvével összhangban bizonyítani tudja, hogy az adatvédelmi incidens valószínűsíthetően nem jár kockázattal a természetes személyek jogaira és szabadságaira nézve, úgy nem terheli bejelentési kötelezettség a felügyeleti hatóság felé.

A Rendelet szabályozásának további újdonsága az adatkezelőkre nézve, hogy ha az adatvédelmi incidens valószínűsíthetően magas kockázattal jár a természetes személyek jogaira és szabadságaira nézve, az adatkezelő indokolatlan késedelem nélkül tájékoztatja az érintettet az adatvédelmi incidensről. A fenti rendelkezés célja elsősorban az, hogy az érintett megtehesse a szükséges óvintézkedéseket.

A tájékoztatásban világosan és közérthetően ismertetni kell az adatvédelmi incidens jellegét, valamint az érintettel is közölni kell alapvetően ugyanazokat az információkat és intézkedéseket, melyeket a felügyeleti hatóságnak küldött bejelentés is tartalmaz.

A tájékoztatásnak tartalmaznia kell tehát annak leírását, hogy milyen jellegű az adatvédelmi incidens, valamint az érintett a természetes személynek szóló, a lehetséges hátrányos hatások enyhítését célzó javaslatokat. Az érintettek tájékoztatásáról az észszerűség keretei között a lehető leghamarabb gondoskodni kell, szorosan együttműködve a felügyeleti hatósággal, és betartva az általa vagy más érintett hatóságok, például bűnüldöző hatóságok által adott útmutatást.

Amennyiben 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, vagy megállapíthatja azon feltételek valamelyikének teljesülését, melyek esetén nem kell tájékoztatni az érintetteket. A Rendelet meghatározza azokat az eseteket is, melyekben az érintettek értesítése mellőzhető.

A Rendelet 33. cikk (5) bekezdése alapján az adatkezelő nyilvántartja az adatvédelmi incidenseket, feltüntetve az adatvédelmi incidenshez kapcsolódó tényeket, annak hatásait és az orvoslására tett intézkedéseket. E nyilvántartás lehetővé teszi, hogy a felügyeleti hatóság ellenőrizze az e cikk követelményeinek való megfelelést, azaz hogy megfelelően bejelentette-e az adatkezelő az incidenst a felügyeleti hatóságnak.

II.9. Személyes adatok harmadik országba történő továbbítása az adatvédelmi rendeletben

Az adatvédelmi rendelet nagy hangsúlyt fektet a személyes adatok Unión kívülre történő továbbítására, és az adatvédelmi irányelvhez, csakúgy, mint az Infotv.-hez

képest lényegesen részletesebben szabályozza ezt a területet. A rendelet (101) preambulum bekezdésében emlékeztet rá, hogy a nemzetközi kereskedelem és együttműködés bővítéséhez szükség van személyes adatok Európai Unión kívülre történő továbbítására, amely során – tekintettel az ezzel kapcsolatos egyedi kihívásokra és problémákra – azon adatkezelő vagy adatfeldolgozó, aki személyes adatok kíván továbbítani harmadik országba, köteles teljesíteni a rendelet V. fejezetében támasztott feltételeket.

Az Infotv. nem követi teljes mértékben az irányelv IV. fejezetében foglaltakat, a külföldi adattovábbításra vonatkozó 8. § nem ugyanazon struktúrában – alapelv és kivételek – rendezi a jogalapokat, sőt, voltak olyan eszközök is, amelyek hiányoznak az Infotv.-ből. A rendelet tehát jelentős újítást fog jelenteni a külföldi adattovábbítás vonatkozásában a Magyarországon letelepedett adatkezelők, adatfeldolgozók számára, hiszen létrehoz egy minden tagállamra kötelezően alkalmazandó egységes feltételrendszert.

A rendelet feltételrendszerének lényege, hogy megállapít egy alapelvet (*„az adattovábbításra vonatkozó általános elv”*), és ezt követően – hierarchikus sorrendben – megállapítja azon jogalapokat, eszközöket, amelyek alapján sor kerülhet Unión kívülre történő adattovábbításra. Az adattovábbítás általános elvének kiindulópontja az, hogy személyes adatok harmadik országbeli adatkezelőknek, adatfeldolgozóknak történő továbbítása esetén nem sérülhet a természetes személyeknek az Unióban biztosított védelem szintje. A rendelet kiemeli emellett azt is, ami újításként is értékelhető az irányelvhez képest, hogy ennek a védelemnek nem csak a harmadik ország irányába, hanem az onnan további vagy újbóli továbbítására is ki kell terjednie. A rendeletbeli alapelv szerint csak akkor kerülhet sor adattovábbításra, ha az adatot továbbító szervezet a rendeletet teljes mértékben betartja, és teljesíti az V. fejezetben előírtakat.

Az adattovábbítás rendeletbeli feltételrendszere egyben hierarchikus sorrendet is meghatároz, tehát az adatot továbbító szervezetnek meg kell vizsgálnia a megállapított sorrendben, hogy melyik jogalap, illetve eszköz alkalmazható az adott továbbítás vonatkozásában.

II.9.1. Adattovábbítás megfelelőségi határozat alapján

Az első, amit meg kell vizsgálni egy adattovábbítás kapcsán az az, hogy az adott célország vonatkozásában fogadott-e el a Bizottság olyan határozatot, amelyben

ezen ország vonatkozásában megállapította, hogy biztosítja a személyes adatok megfelelő szintű védelmét. A rendelet – ellentétben az irányelvvel – viszonylag részletes szabályokat állapít meg a megfelelőségi határozatok elfogadására, amelyben arra is kitér, hogy mely körülményeket kell figyelembe venni és elemezni. A rendelet arról is rendelkezik, hogy a korábban elfogadott ilyen határozatok – mint például a legutóbbi, a Privacy Shield-del kapcsolatos döntés – hatályban maradnak (45. cikk (9) bekezdés).

II.9.2. Megfelelő garanciák alapján történő adattovábbítás

Amennyiben a célország vonatkozásában nem fogadott el a Bizottság megfelelőségi határozatot, az adattovábbításra akkor kerülhet sor, ha a továbbító szervezet megfelelő garanciákat nyújt, és az érintettek számára érvényesíthető jogok és hatékony jogorvoslati lehetőségek állnak rendelkezésre.

A megfelelő garanciák alapján történő adattovábbítások egy részére a felügyeleti hatóságok külön engedélye nélkül kerülhet sor, ezek:

a) közhatalmi, vagy egyéb, közfeladatot ellátó szervek közötti, jogilag kötelező erejű, kikényszeríthető jogi eszköz;
b) kötelező vállalati szabályok (BCR);
c) a Bizottság által elfogadott általános adatvédelmi kikötések („modellszerződések”);
d) a felügyeleti hatóság által elfogadott, és a Bizottság által jóváhagyott általános adatvédelmi kikötések;
e) jóváhagyott magatartási kódex, a harmadik országbeli adatkezelő vagy adatfeldolgozó kötelezettségvállalásával, hogy alkalmazza a megfelelő garanciákat;
f) jóváhagyott tanúsítási mechanizmus a harmadik országbeli adatkezelő vagy adatfeldolgozó kötelezettségvállalásával, hogy alkalmazza a megfelelő garanciákat.

Egyes esetekben a rendelet szerint csak a felügyeleti hatóság külön engedélye mellett kerülhet sor a továbbításra, ezek:

a) az adatot továbbító és a harmadik országbeli adatkezelő vagy adatfeldolgozó, vagy a személyes adatok címzettje között létrejött szerződéses rendelkezések;

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

Felügyeleti hatóság külön engedélye nélkül	**Felügyeleti hatóság engedélyével**
Közfeladatot ellátó szervek közötti kikényszeríthető jogi eszköz	Harmadik országbeli adatkezelővel, adatfeldolgozóval kötött szerződéses rendelkezések
BCR	
Bizottság vagy felügyeleti hatóságok által elfogadott általános adatvédelmi kikötések	Közfeladatot ellátó szervek közötti közigazgatási megállapodások
Magatartási kódex	
Tanúsítási mechanizmus	

A rendelet kiemeli, hogy az engedélyezési eljárás során a hatóságoknak alkalmazni kell az egységességi mechanizmust.

A megfelelő garanciákat nyújtó eszközök közül kiemelten, részletesen tartalmaz a rendelet rendelkezéseket a BCR-ról. Ez azért fontos előrelépés, mert ezt az eszközt a 29-es Munkacsoport dolgozta ki, és a rendeletet megelőzően e globális eszköz egységességét az általa elfogadott számos munkadokumentum biztosította. A rendelet, a munkadokumentumokban foglaltakat átvéve, definiálja a BCR-t, és részletes, pontos meghatározást ad a BCR kötelező tartalmi elemeire vonatkozóan. Emellett a jóváhagyási eljárás vonatkozásában szintén az egységességi mechanizmus alkalmazásáról rendelkezik, felváltva a korábbi informális együttműködési eljárást.

Ahogy a felsorolásból is látszik, a rendelet megteremti annak a lehetőségét, hogy az újonnan bevezetett eszközök – a magatartási kódex és a tanúsítási mechanizmust – is alkalmazhatóak legyenek a harmadik országba történő adattovábbítás esetén. Ezeknek a részletes szabályait a IV. fejezet tartalmazza, azonban a har-

madik országban található szervezet kötelezettségvállalása esetén az adattovábbítás garanciáinak megteremtése céljából is alkalmazhatóak.

II.9.3. Különös helyzetekben biztosított eltérések

A rendelet, az irányelvhez hasonlóan megteremti annak a lehetőségét, hogy amennyiben a célországra vonatkozóan nincs megfelelőségi határozat, illetve az adatot továbbító adatkezelő vagy adatfeldolgozó nem biztosít megfelelő garanciákat, akkor is sor kerülhessen kivételes esetekben az adattovábbításra.

Az irányelvvel ellentétben a rendelet már elnevezésében is egyértelműen utal arra, hogy ezeket a jogalapokat csak kivételes esetekben lehet alkalmazni, és szűken értelmezve kell alkalmazni, továbbá rendszeres vagy tömeges adattovábbítás esetén – összhangban a 29-es Munkacsoport WP 12-es véleményében foglaltakkal – nem lehet ezeket alkalmazni. Ilyen kivételes jogalap lehet például az érintett kifejezett hozzájárulása, vagy ha szerződés teljesítéséhez, fontos közérdek, vagy az érintett vagy más személy létfontosságú érdekeinek védelme érdekében szükséges a továbbítás.

A fentieken kívül a rendelet tartalmaz még egy speciális kivételt, amely nagyon szűk körben alkalmazható. A 49. cikk (1) bekezdés utolsó fordulata alapján, ha az adattovábbítás nem alapulhat sem megfelelőségi határozaton, sem megfelelő garanciákon, és az egyedi helyzetekre vonatkozó eltérések egyike sem alkalmazandó, az alábbi feltételek mellet sor kerülhet harmadik országba történő adattovábbításra:

- a továbbítás nem ismétlődő;
- csak korlátozott számú érintettre vonatkozik;
- az adatkezelő olyan kényszerítő erejű jogos érdekében szükséges, amely érdekhez képest nem élveznek elsőbbséget az érintett érdekei, jogai és szabadságai;
- és az adatkezelő az adattovábbítás minden körülményét megvizsgálta, és ez alapján megfelelő garanciákat nyújtott.

Az ilyen kivételes adattovábbításról az adatkezelőnek tájékoztatnia kell a felügyeleti hatóságot, és az érintettet is. Ebben a kivételes helyzetben tehát az érdekmérlegelés alkalmazandó.

A harmadik országba történő adattovábbításokkal kapcsolatban a rendelet az V. fejezeten kívül is rendez fontos kérdéseket. Így a 13. cikk f) pontjában kü-

lön nevesíti, hogy az előzetes tájékoztatás keretében a harmadik országokba történő adattovábbítással kapcsolatban mely körülményekről kell tájékoztatni az érintetteket. Ez alapján tájékoztatni kell például az érintetteket az adattovábbítás tényén kívül arról is, hogy az adott célországra vonatkozóan van-e hatályos megfelelőségi határozat, illetve hogy annak hiányában hogyan biztosítják a megfelelő garanciákat.

A személyes adatok továbbításakor megnövekedhet annak a kockázata, hogy az érintettek nem képesek gyakorolni információs önrendelkezési jogukat. Az adattovábbítással kapcsolatos kérdések emellett a tagállami hatóságok számára is összetett feladatot jelentenek, hiszen sokszor bonyolult, több országon és szervezeten átívelő komplex adatáramlásokat kell egy-egy eljárás során megvizsgálni. A harmadik országba történő adattovábbítások területén tehát kiemelt fontossággal bír a rendelet, amely megerősíti a tagállami felügyeleti hatóságok közötti együttműködést, információcserét, egységesíti a hatásköröket, eljárásokat és nem utolsó sorban az alkalmazandó jogszabályokat.

II.10. A szankcionálás szabályai a Rendeletben

1) A Rendelet a felügyeleti hatóságok korrekciós hatáskörében hozandó döntések keretében intézkedések elrendelését, megrovás alkalmazását, illetve bírság kiszabását írja elő. Intézkedések tekintetében a hatályos szabályozáshoz hasonló intézkedések lesznek alkalmazhatóak, míg bírság tekintetében az adatkezelés típusa alapján differenciált és jelentősen nagyobb összegű bírságok kiszabását teszi lehetővé.

2) Intézkedésként a Hatóság elmarasztalhatja az adatkezelőt a Rendelet rendelkezéseinek megsértéséért, utasíthatja az érintett jogainak gyakorlására vonatkozó kérelem teljesítésére, továbbá ezzel összefüggésben elrendelheti az érintett személyes adatainak helyesbítését, törlését. Kötelezheti az adatkezelőt arra is, hogy alakítsa át adatkezelési gyakorlatát a Rendelet szabályainak megfelelően, valamint átmenetileg, vagy véglegesen korlátozhatja, illetve meg is tilthatja az adatkezelést. Elrendelheti továbbá személyes adatok harmadik országba továbbításának a felfüggesztését is.

3) A Hatóság az eset körülményeitől függően megrovást alkalmazhat, illetve közigazgatási bírságot szabhat ki. A bírság kiszabására sor kerülhet intézkedés alkalmazása mellett vagy helyett is. A Hatóságnak biztosítania kell, hogy a kisza-

bott közigazgatási bírság minden esetben hatékony, arányos és visszatartó erejű legyen. A bírság kiszabásának szükségessége, valamint mértékének megállapítása során a Rendelet alapján figyelembe kell venni

a) a jogsértés jellegét, súlyosságát, időtartamát, az adatkezelés jellegét, körét, célját, az érintettek számát és az elszenvedett kár mértékét,
b) a jogsértés szándékos vagy gondatlan jellegét,
c) az adatkezelőnek vagy az adatfeldolgozónak az érintettek által elszenvedett kár enyhítése érdekében tett intézkedéseit,
d) az adatkezelő vagy adatfeldolgozó felelősségének mértékét (különös tekintettel az általuk alkalmazott adatbiztonsági, valamint beépített és alapértelmezett adatvédelmet),
e) korábban elkövetett jogsértéseket, korábbi, ugyanabban a tárgyban elrendelt intézkedések végrehajtását,
f) a Hatósággal a jogsértés megszüntetése érdekében történő együttműködés mértékét,
g) a jogsértéssel érintett személyes adatok kategóriáit,
h) megfelelt-e a jóváhagyott magatartási kódexnek,
i) valamint az eset körülményei szempontjából releváns egyéb súlyosbító vagy enyhítő körülményeket.

A bírság maximális összege 10.000.000 EUR, illetve vállalkozások esetében az előző pénzügyi év teljes éves világpiaci forgalmának legfeljebb 2%-át kitevő összeg lehet, amennyiben a jogsértés például gyermekek információs társadalommal összefüggő adatkezelését, a beépített és alapértelmezett jogvédelem követelményét érinti, illetve amennyiben adatfeldolgozás, az adatkezelési tevékenységek nyilvántartása, adatbiztonság, adatvédelmi incidensek, az adatvédelmi hatásvizsgálat követelményeinek a megsértése körében történik.

A bírság kiszabható legmagasabb összege 20.000.000 EUR, illetve vállalkozások esetén az előző pénzügyi év teljes éves világpiaci forgalmának legfeljebb 4 %-át kitevő összeg, az alábbi jogsértési kategóriák esetében: az adatkezelés elvei, ideértve a hozzájárulás feltételeit is, az érintettek jogai, személyes adatok harmadik országba való továbbítása, speciális tagállami szabályok megsértése, valamint abban az esetben, ha az a Hatóság előző pontban bemutatott intézkedéseinek be nem tartása, illetve a Hatóság eljárása során az adatkezelés vizsgálata körében a hozzáférés biztosításának elmulasztása miatt volt szükséges.

II.11. A panasztételhez és a jogorvoslathoz való jog

Minden érintett személy jogosult arra, hogy panaszt tegyen egy tagállam adatvédelmi hatóságánál, ha megítélése szerint a személyes adatai védelméhez való jogát megsértették. Az adatvédelmi hatóság köteles tájékoztatni a panaszost az eljárási fejleményekről és annak eredményéről.

Az Infotv.-ben jelenleg szabályozott vizsgálati eljárással szemben újdonság az, hogy amennyiben az adatvédelmi hatóság nem jár el valamely panasz alapján, illetve részben vagy egészben elutasítja, vagy megalapozatlannak tekinti azt, vagy három hónapon belül nem tájékoztatja az érintettet a panasszal kapcsolatos eljárása eredményéről, az érintett az adatvédelmi hatósággal szemben bírósági jogorvoslatra jogosult.

A Rendelet által bevezetett újdonság az is, hogy az érintettnek jogában áll megbízni egy, a személyes adatok védelmével foglalkozó nonprofit szervet, szervezetet vagy egyesületet, hogy a nevében eljárva nyújtson be panaszt az adatvédelmi hatóságnál, vagy gyakorolja a bírósági jogorvoslathoz való jogot. Egy adott tagállam rendelkezhet arról is, hogy az adott tagállamban ilyen nonprofit szerv, szervezet, egyesület az érintett megbízásától függetlenül, önállóan is jogosult legyen az adatvédelmi hatósághoz panaszt és bírósági jogorvoslati kérelmet benyújtani, ha az érintett jogainak védelmében szükségesnek tartja azt.

II.12. A kártérítéshez való jog és a felelősség

A Rendelet nem csak az adatkezelők, hanem az adatfeldolgozók kártérítési felelősségét is rögzíti. A Rendelet[68] szerint minden olyan személy, aki a Rendelet megsértésének eredményeként vagyoni vagy nem vagyoni kárt szenved, az elszenvedett kárért az adatkezelőtől vagy az adatfeldolgozótól kártérítésre jogosult. Az adatfeldolgozó csak abban az esetben tartozik felelősséggel az adatkezelés által okozott kárért, ha nem tartott be valamely, kifejezetten az adatfeldolgozókat terhelő kötelezettséget, vagy ha az adatkezelő jogszerű utasításait figyelmen kívül hagyta vagy azokkal ellentétesen járt el.

Ha egy adatkezelésben több adatkezelő, illetve adatfeldolgozó vesz részt, akkor minden egyes adatkezelő vagy adatfeldolgozó egyetemleges felelősség-

68 GDPR 82. cikk

gel tartozik a teljes kárért. A kártérítési kötelezettség megosztható az eljárásba bevont egyes adatkezelők és adatfeldolgozók között a kár arányában, feltéve hogy így is biztosított marad, hogy az érintettet ért kárt teljes mértékben és ténylegesen megtérítik. Az az adatkezelő vagy adatfeldolgozó, aki teljes kártérítést fizetett, viszonkeresetet indíthat a többiekkel szemben, hogy visszaigényelje a kártérítésnek azt a részét, mely megfelel a károkozásért való felelősségük mértékének.

A kártérítéshez való jog érvényesítését célzó bírósági eljárást az adatkezelő vagy adatfeldolgozó tevékenységi helye szerinti tagállam bírósága előtt kell megindítani. Az érintett a bírósági eljárást megindíthatja a saját tartózkodási helye szerinti tagállam bírósága előtt is, kivéve akkor, ha az adatkezelő vagy adatfeldolgozó valamely tagállamnak a közhatalmi jogkörben eljáró közhatalmi szerve.

II.13. A szervezetrendszer

A Rendelet alapján az látható, hogy az adatvédelmi hatóságok megerősítésre kerülnek, új feladat- és hatáskörökkel. A felügyeleti hatóságok annak érdekében, hogy védjék a természetes személyek személyes adatainak kezelését, valamint biztosítsák a személyes adatok belső piacon belüli szabad áramlását, figyelemmel kísérik az e rendelet szerinti rendelkezések alkalmazását, és hozzájárulnak azoknak az Unió egész területén történő egységes alkalmazásához. E célból a felügyeleti hatóságok együttműködnek egymással és a Bizottsággal.

Az e rendelettel összhangban rá ruházott hatáskörökkel élve, az intézkedésekre vonatkozó kötelező erejű döntések elfogadására a fő hatóság illetékes. A fő hatóságként eljáró felügyeleti hatóság a döntéshozatali folyamatban együttműködik az érintett felügyeleti hatóságokkal és koordinálja az eljárást.

A fő felügyeleti hatóságra az együttműködésre és az egységességi mechanizmusra vonatkozó szabályokat nem lehet alkalmazni abban az esetben, ha az adatkezelést közhatalmi szervek vagy közérdekből eljáró magánfél szervezetek végzik. Ilyen esetben kizárólag az a felügyeleti hatóság lehet illetékes az e rendelettel összhangban rá ruházott hatáskörök gyakorlására, amely annak a tagállamnak a felügyeleti hatósága, ahol az adott közhatalmi szerv vagy magánfél szerv székhelye található.

A Rendelet minden tagállamban való egységes alkalmazásának biztosítása érdekében a felügyeleti hatóságok közötti együttműködést szolgáló egységességi mechanizmusnak kell érvényesülnie. (GDPR 63. cikk)

A GDPR 58. cikke alapján új hatásköri szabályozás lép érvénybe az alábbiak szerint:

- vizsgálati hatáskör
- korrekciós hatáskör
- engedélyezési és tanácsadási hatáskör.

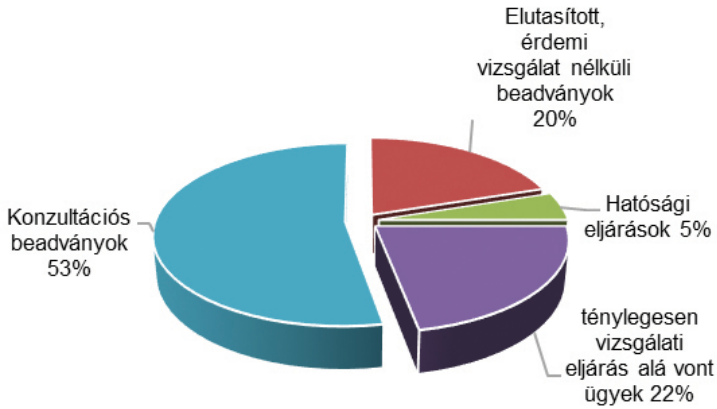
Az intézményrendszer új szereplője az Európai Adatvédelmi Testület, amelynek nem csupán koordinatív, tanácsadó szerepe lesz, hanem kikényszeríthető döntéseket is fog hozni. E Testület lép az eddigi 29-es munkacsoport helyébe. Nagy szerepe lesz a vitarendezési mechanizmusnak, amelynek keretében a hatóságok közti egyet nem értés esetén a Testület hozza meg a kötelező erejű döntést.

III. Adatvédelem

III.1. Statisztikai adatok

A 2016-os évben az adatvédelmi ügyek intézése az eddig kialakított eljárási rend szerint, de már az új általános adatvédelmi rendeletre való felkészülés szellemében folyt.

Adatvédelmi ügyek 2016



Az adatvédelmi ügyek fele konzultációs típusú vizsgálati ügy. Az ügyek 20%-ában a Hatóság eljárást, vizsgálatot nem indított. A ténylegesen vizsgálati eljárás alá vont ügyek a teljes ügyszám egynegyedét teszik ki, és ezek közel felében állapított meg jogsértést a Hatóság.

A 2016-os évre is elmondható, hogy a vizsgálati eljárások száma nagyobb, mint a hatósági eljárások száma. A hatósági ügyek általában nagyobb súlyú, összetett ügyek, melyek részletes tényállás tisztázáson alapulnak, formalizáltabb eljárásban zajlanak, és hosszabb ideig tartanak.

Az adatvédelmi hatósági eljárások száma, az összes ügy számához viszonyított aránya ebben az évben növekedett az előző évekhez viszonyítva. 2016-ban 63 hatósági eljárás indult, az előző évről áthúzódó ügyekkel együtt pedig összesen 77 hatósági ügy volt folyamatban.

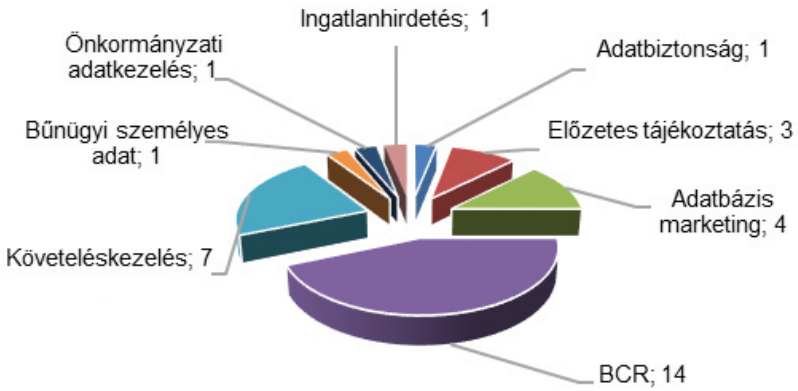
Évek	Eljárások száma	A Hatóság döntései			A kiszabott bírság összege
		Végzés eljárás megszüntetéséről	Bírságot is megállapító határozat	Bírságot nem tartalmazó határozat	
áthúzódó ügyek, 2016-ban született döntés	14	6 [69]	5	4	6.900.000 Ft
2016-ban indult ügyek	63	4	5	12	13.300.000 Ft

A Hatóság 2016-ban összesen 36 hatósági eljárást zárt le, amelyből 26 esetben állapított meg jogsértést és 10 esetben szabott ki bírságot.

Látható, hogy a Hatóság a korábbi évekhez képest jóval kevesebb esetben szabott ki bírságot a jogellenes adatkezelések miatt. Ennek oka, hogy a Kúria 2016-ban született jogerős ítélete szerint – az elsőfokú bíróság ítélete és a Hatóság korábbi szakmai álláspontjától eltérően – a Hatóságnak is alkalmaznia kell a kis- és középvállalkozásokról, fejlődésük támogatásáról szóló 2004. évi XXXIV. törvényt (Kkv. tv.), mely szerint a kis- és középvállalkozások tekintetében első alkalommal elkövetett jogsértés esetén bírság kiszabása helyett figyelmeztetést kell alkalmazni. Tehát amennyiben az adott ügyben a Hatóság megállapítja, hogy az eljárás során vizsgált adatkezelő kis- és középvállalkozásnak minősül, és az adatkezelővel szemben korábban nem állapított meg jogsértést, (valamint a Kkv. tv.-ben meghatározott kivételek sem állnak fenn), akkor a jogsértés megállapítása mellett adatvédelmi bírságot nem szabhat ki a Hatóság. Ilyen esetekben a jogsértő adatkezelővel szemben a Hatóság a Kúria döntésének megfelelően, a Kkv. tv.-t alapul véve figyelmeztetést alkalmaz.

69 Az egyik ügyben két végzés született

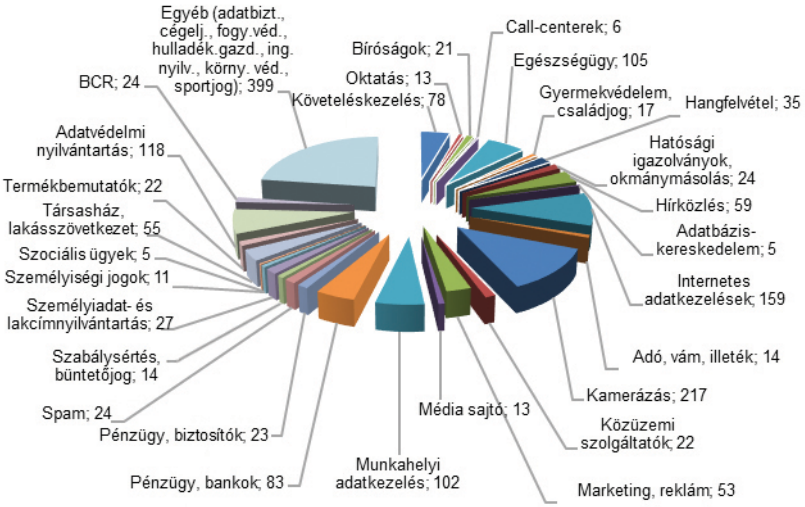
Határozatok és lezáró végzések megoszlása az ügy tárgya szerint 2016



Peres ügyek						
	2012	**2013**	**2014**	**2015**	**2016**	**Összesen**
Hatósági ügy	33	40	30	30	63	**196**
Felülvizsgálat iránti per	11	11	8	2	4	**36**
Folyamatban lévő per	0	0	2	1	4	**7**
Pernyertesség	8	8	2	1	0	**19**
Részbeni pernyertesség	0	2	1	0	0	**3**
Perveszteség	3	1	3	0	0	**7**
Összes bírósági döntés	**11**	**11**	**6**	**1**	**0**	**29**

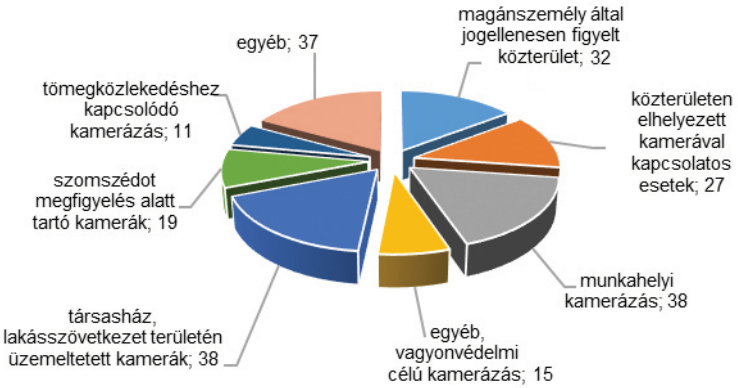
Az adatvédelmi tárgyú beadványok jelentős számában, több területet is érintő adatkezeléssel összefüggően állapított meg jogsértéseket eljárásai során a Hatóság. Az alábbi ügytípus diagram tehát nem a ténylegesen, adott területen előforduló ügyek számát, hanem egy adott ügyben érintett szakterületek számát szemlélteti (egy ügyben több panasz/témakör is szerepelhet).

Az adatvédelmi ügyek ügytípus szerinti gyakorisága 2016



A Hatósághoz a 2016. év során is jelentős mennyiségű olyan vizsgálati bejelentés és konzultációs beadvány érkezett, amely az elektronikus megfigyelőrendszerekhez, kamerarendszerekhez kapcsolódó adatkezelésre vonatkozott. A *„kamerás ügyek”* jelentik ez évben is a leggyakoribb ügytípust, arányában a legtöbb beadvány e tárgyban érkezik.

Kamerás ügyek típusai 2016



Ahogy a fenti ábrából is látható, a kamerás megfigyeléssel kapcsolatban küldött beadványok sokszínűek, több kategóriába sorolhatóak. Az ügytípusok között számos esetben átfedés van, rendszeresen előfordul például, hogy egy olyan ügyben indít vizsgálatot a Hatóság, melyben a beadvánnyal érintett adatkezelő egyszerre tart megfigyelés alatt közterületet és szomszédos magánterületet is.

Elmondható, hogy az ilyen ügyek kivizsgálása során az Infotv. mellett számos, az egyes konkrét adatkezelésekre irányadó rendelkezéseket tartalmazó ágazati jogszabálynak való megfelelést is részletesen vizsgálnia kell a Hatóságnak, emellett figyelemmel kell lenni a tárgyban releváns, az Európai Unió Bíróságának ítéleteiben[70] megjelenő joggyakorlatra is.

III.2. Eljárási tapasztalatok

III.2.1. Előzetes tájékoztatás követelményének vizsgálata

A Hatóság a korábbi évek adatvédelmi eljárásainak tapasztalatai alapján, valamint arra tekintettel, hogy évről évre jelentős számú panasz érkezik a Hatósághoz az adatalanyok nem megfelelő tájékoztatása miatt, a 2016-os évben folytatott eljárásaiban kiemelt figyelmet fordított az előzetes tájékoztatás követelményének való megfelelés vizsgálatára.

Az adatkezelések leggyakrabban alkalmazott jogalapja a hozzájárulás. A törvényi definíció szerint akkor tekinthető jogszerűnek a hozzájárulás, ha az megfelelő tájékoztatáson alapul. Amennyiben tehát nem kap az érintett az adatkezelés megkezdése előtt az Infotv. 20. § (2) bekezdésében – illetve a Hatóság értelmezése szerint az Infotv. 15. § (1) bekezdésében – foglaltak szerint megfelelő tájékoztatást az adatkezelés lényeges körülményeiről, nem tekinthető megadottnak a hozzájárulás. Ezen jogszabályi követelményeknek való megfelelés elősegítése érdekében a Hatóság ajánlást bocsátott ki 2015-ben[71], majd pedig 2016-os vizsgálati tervének részévé téve vizsgálta az adatkezelők gyakorlatát mind a vizsgálati előzménnyel, más tárgyban indult, mind a kifejezetten az előzetes tájékoztatás követelményének való megfelelést vizsgáló hatósági eljárásaiban.

70 Például az Európai Unió Bíróságának a C-212/13. számú, egy magánházon elhelyezett kamerákat érintő ügyben hozott ítélete.

71 http://naih.hu/files/tajekoztato-ajanlas-v-2015-10-09.pdf

A Hatóság a következő, jellemző hibákat tapasztalta:

- adatkezelő(k) személyéről és elérhetőségéről való hiányos tájékoztatás;
- az adatkezelési célokat legtöbbször elnagyoltan, nem kellően pontosan jelölik meg, vagy a megjelölt cél megfogalmazása nem közérthető, olyan kifejezést alkalmaznak, aminek nincs egyértelmű, mindenki számára nyilvánvaló jelentése;
- jellemzően nem egyértelmű, hogy mely adatkezelési célhoz, pontosan milyen személyes adatukat is használják fel és ennek következtében nem állapítható meg, hogy az adatkezelő eleget tesz-e a célhoz kötött adatkezelés követelményének;
- nem különítik el a kötelezően és önkéntesen megadandó adatok körét;
- az adatkezelés időtartamának megjelölésénél nincs abszolút határidő megjelölve, vagy olyan, az érintett számára nem kellő információt biztosító tájékoztatást alkalmaznak, mint, hogy az adatkezelés céljának megszűnésig, vagy a szerződéses jogviszonnyal kapcsolatos jogszabályban meghatározott elévülési idő végéig kezelik az adatokat;
- adatfeldolgozóról való tájékoztatás is hiányos volt a legtöbb esetben, itt az arról való tájékoztatást mulasztották el az adatkezelők, hogy mely adatfeldolgozók, milyen személyes adataikhoz, milyen időtartamig férhetnek hozzá, illetve mire használják fel az adott személyes adatot (milyen tevékenységet végeznek az adatkezelő részére);
- gyakori hiányosság, hogy elmulasztják az adatok felvételének helyén elérhetővé tenni a tájékoztatót (pl. honlapon gyűjtött adatok esetében az űrlapon közvetlenül kattintható linken);
- tájékoztató közérthetősége továbbra is komoly probléma a jogszabályok szövegének – így pl. az Infotv. értelmező rendelkezéseinek – szószerinti megismétlése valamint különböző szakzsargonban alkalmazott kifejezések használata miatt
- komplex adatkezelések bemutatásánál nem fektetnek kellő hangsúlyt az adatkezelők az érintettek megfelelő, érthető és áttekinthető tájékoztatására, amely jelentős mértékben rontja egy adatkezelési tájékoztató minőségét, hiszen kibogozhatatlanná válik az állampolgárok számára és nem tudja betölteni a funkcióját;
- érintettek személyes adatainak kezelését szabályozó hatályos jogszabályról való hibás tájékoztatás (még 4 évvel az Infotv. hatályba lépése után is előfordul, hogy a korábbi jogszabály, az Avtv. szerint tájékoztatják az érintetteket).

Mind a vizsgálati, mind a hatósági ügyekben szerzett tapasztalatok alapján elmondható, hogy ugyan fokozatosan javul a tájékoztatók minősége és egyre nagyobb figyelmet fordítanak az adatkezelők a megfelelő tájékoztatásra, azonban még mindig gyakran találkozik a Hatóság átgondolatlan, kellően ki nem dolgozott adatkezelési folyamatokkal és továbbra sem biztosítanak minden esetben közérthető és világos tájékoztatást az adatkezelők az érintettek számára.

III.2.2. Az érintetti jogok érvényesülése

A Hatósághoz folyamatosan érkeznek olyan bejelentések, amelyekben az állampolgárok azt kifogásolták, hogy az adatkezelők a személyes adataik kezeléséről kért tájékoztatást nem vagy nem megfelelően teljesítették, illetve az érintetti jogaik gyakorlását nem biztosították. A 2016-os év eljárási tapasztalatai azt igazolták, hogy a bejelentők panaszai az esetek túlnyomó többségében megalapozottak.

Egyes eljárások tapasztalatai szerint a leggyakoribb hibák az alábbiak szerint foglalhatóak össze:

1) Az esetek többségében az adatkezelők az érintettek kérelmeit szolgáltatási panaszként, reklamációként kezelik, ezért a panaszkezelési szabályzataik alapján bírálják el, melyben az Infotv. 15. §-ának előírásai nem játszanak szerepet. A válaszadás során csak a tevékenységüket szabályozó ágazati előírásokról adnak számot, az adatkezelési kérdések megválaszolását gyakran mellőzik az adatkezelők.

2) A tájékoztatás megadása nem tehető feltételtől függővé. Az Infotv. nem tartalmaz olyan korlátozó rendelkezést, amely e jog gyakorlását az érintett személyes megjelenéséhez kötné, ezért az adatkezelő sem jogosult a tájékoztatás teljesítési módjának korlátozására.

Akadt olyan adatkezelő, aki az adatalany írásbeli kérelmére csupán azt a választ adta, hogy *„bármikor az irodában rendelkezésre állunk minden felvilágosítással”.* A Hatóság vizsgálati eljárása során az írásbeli tájékoztatás mellőzését az egyik adatkezelő azzal indokolta, hogy ezzel a tájékoztatás egyszerűbb és praktikusabb formáját választotta.

3) Vannak olyan adatkezelők, akik az adatkezelési tájékoztatóikhoz vagy a belső adatvédelmi szabályzataikhoz formanyomtatványokat mellékelnek. Az érintetteknek a kérelmeiket ezeken kell benyújtani, sőt indokolással is el kell látni.

Az adatalanyok tájékoztatásához való joga az információs önrendelkezési jog egyik konstitutív eleme, és mint ilyen, a személyes adatok védelméhez fűződő alkotmányos alapjog egyik aspektusa. Ebből következően az érintettnek a saját személyes adataival kapcsolatos tájékoztatás iránti kérelmét nem kell indokolnia, hiszen azok megismerésének, információs önrendelkezési joga gyakorlásának semmilyen érintettség vagy érdek nem lehet feltétele: a puszta kíváncsiság éppúgy megfelelő motiváció, mint az, ha valaki a kapott információk nyomán egyéb jogi lépéseket foganatosít.

Az Infotv. nem tartalmaz olyan korlátozó rendelkezést sem, amely e jogot célhoz kötötté tenné, vagy az előterjesztését formakényszerhez kötné, ezért az adatkezelő sem jogosult a tájékoztatás céljának vizsgálatára, sem az alaki követelmények előírására. Az adatkezelő alkalmazhat formanyomtatványokat, azonban a nem ezen benyújtott kérelmeket is be kell fogadnia és meg kell válaszolnia.

4) Közigazgatási szervek esetében a leggyakoribb adatkezelői hiba az, hogy a kérelmezőt ügyfélnek tekintik, és a Ket. szabályaira hivatkozással különböző hiánypótlásokat küldenek ki. Az Infotv.-ben szabályozott tájékoztatáshoz való jog gyakorlása azonban nem hatósági ügy, az adatalany érintett és nem ügyfél, ezért a tájékoztatás megadása nem tartozik a Ket. hatálya alá.

5) Az is gyakori, hogy az adatkezelők a kérelem megválaszolását elmulasztják, holott a tájékoztatás esetleges megtagadását kötelesek lennének megindokolni. A mulasztás okaként rendszerint ügyintézői hibára hivatkoznak az adatkezelők. A Hatóság álláspontja szerint azonban ez az érvelés nem mentesíti a munkáltatókat (cégeket, egyéb intézményeket) az adatkezelői felelősség alól, tekintettel arra, hogy az Infotv. 3. § 9. pontja értelmében a munkáltató minősül adatkezelőnek és nem a munkavállalói. A munkáltató az, aki megszervezi az adatkezelés folyamatát és meghozza az adatkezelésre vonatkozó döntéseket, nem pedig az ügyintézői.

6) Sűrűn előfordul, hogy az adatkezelők az érintetti kérelmeknek csak részben tesznek eleget, a kérelmek egyes kérdéseiről hallgatnak. A gyakorlatban, sok esetben csak az adatkezelésük jogalapjáról adnak írásbeli tájékoztatást a kérelmet előterjesztő érintettnek, az adatkezelés egyéb lényeges körülményeiről (a kezelt személyes adatai köréről, azok forrásáról, az adatfeldolgozó nevéről, címéről, adattovábbítás esetén az adattovábbítás céljáról és jogalapjáról) azonban kifejezetten erre is irányuló kérdése ellenére nem adnak tájékoztatást.

A Hatóság szakmai álláspontja szerint azonban az adatfeldolgozó igénybevételének vagy az adattovábbítás esetleges hiánya sem mentesíti az adatkezelőt tájé-

koztatási kötelezettségének teljesítése alól. A tájékoztatásnak nem az esetleges adatkezelési, adattovábbítási lehetőségekről kell szólnia, hanem arról, hogy az érintett ügyében erre konkrétan sor került-e vagy sem, ha igen kinek, milyen célból és jogalappal.

Arra is akadt példa, hogy az adatkezelő arról tájékoztatta az adatalanyt, hogy minden kezelt adatát törölte, holott a Hatóság eljárása során megállapítást nyert, hogy ennél több személyes adatot kezelt az érintettről. Ezzel a megtévesztő tájékoztatással a tisztességes adatkezelés elve sérült.

Általánosságban azonban elmondható, hogy a tájékoztatáshoz való jog a személyes adatokon végzett műveletek transzparenciáját szolgálja, ily módon pedig elősegíti a tisztességes adatkezelés elvének érvényesülését. Az adatalany továbbá az Infotv. 14-15. §-ában foglalt jog révén érvényesítheti minden más – az adatkezelés tekintetében őt megillető – jogot.

A tájékoztatáshoz való jog egyik szükséges előfeltétele annak, hogy az érintett a személyes adatok feldolgozása vonatkozásában az egyének védelméről és az ilyen adatok szabad áramlásáról szóló 95/46/EK irányelv (a továbbiakban: Irányelv) 12. cikk b) és c) pontjában szereplő jogait gyakorolja, vagyis hogy kérelmére az adatkezelő helyesbítse, törölje vagy zárolja az olyan adatokat, amelyek feldolgozása nem felel meg az irányelv rendelkezéseinek. Az érintett kérelmére továbbá az adatkezelőnek értesítenie kell az adatokról tudomást szerző harmadik feleket ezek helyesbítésről, törlésről vagy zárolásról, kivéve, ha ez lehetetlennek bizonyul, vagy aránytalanul nagy erőfeszítést igényel [51. bekezdés]. E jog nélkülözhetetlen továbbá az Irányelv 14. cikkében szereplő tiltakozáshoz való jog gyakorlásához, illetőleg 22. és 23. cikkben biztosított kártérítési igény érvényesítéséhez is [52. bekezdés]. Könnyen belátható ugyanis, hogy a tájékoztatás hiányában az adatalany nem ismeri az adatkezelés körülményeit, annak jogszerű vagy jogellenes voltát, sőt adott esetben magáról az adatkezelésről sem értesül.

III.2.3. Külföldi adattovábbítások

A külföldi adattovábbítás 2016-os aktualitásai – így például az EU-USA adatvédelmi pajzs megalkotása, valamint az Infotv. kötelező szervezeti szabályozással (a továbbiakban: BCR) kapcsolatos 2015-ös módosítása – hatására a Hatóság, az EU-s adatvédelmi hatóságokhoz hasonlóan, nagy hangsúlyt fektetett a külföldi adattovábbítással kapcsolatos kérdésekre.

Ennek keretében a Hatóság 2016-ban 24 hatósági ügyet indított a külföldi adattovábbítás Infotv. 8. §-a szerinti követelményeinek teljesítése tárgyában. Az eljárások tárgya tehát annak vizsgálata volt, hogy az adatkezelők az Infotv. 8. §-a szerinti mely jogalapokat és hogyan alkalmazzák a harmadik országba történő adattovábbítások során. A 24 eljárásból 10 zárult határozattal, 4 esetben az eljárást a Hatóság végzéssel szüntette meg, 10 pedig folyamatban van.

Összegezve a Hatóság tapasztalatait, elmondható, hogy az adatkezelők sok esetben helytelenül jelölték meg az adattovábbítás jogalapját az egyes adatkategóriák vonatkozásában. A vizsgálatok eredményeként emellett a Hatóság számos alkalommal a BCR, mint jogalap alkalmazásával kapcsolatos jogsértést állapított meg, a Hatóság álláspontja szerint ugyanis az Infotv. vonatkozó rendelkezései (3. § 25. pont, illetve a 64/A-64/C. §-ok) értelmében az erre való hivatkozás csak abban az esetben jogszerű, ha az alkalmazott BCR-t a Hatóság az Infotv. 64/A-64/C. §-ai szerinti eljárás eredményeként jóváhagyta.

III.2.4. A szakvéleményekkel kapcsolatos adatkezelések

A Hatósághoz több alkalommal is érkeztek bejelentések egy adott magánszemélyre vonatkozó pszichológiai, pszichiátriai szakvélemények más személyek általi felhasználásával, valamint azzal kapcsolatban, hogy a polgári, valamint büntetőeljárások során keletkezett és a résztvevők által megismerhető iratokon olyan nagyobb mennyiségű személyes adat szerepelt, amelyek nyilvánosságra kerülése, megismerése a szükségesség és arányosság elvének figyelembevételével nem volt indokolt. Az adott ügyben beszerzett, de később az eljárás szempontjából irrelevánssá vált személyes adatok korlátlan megismerhetővé tétele nem feleltethető meg az Infotv. alapelveinek. Különösen igaz ez abban az esetben, amikor igazságügyi szakértő, elmeorvos szakértő által a peres félről elkészített – különleges adatokat tartalmazó – szakvélemény teljes tartalmát az ellenérdekű fél is megismerheti. A Hatóság álláspontja szerint a teljes szakvéleménynek az ellenérdekű fél és képviselője általi megismerése a szükségesség és a célhoz kötött adatkezelés elvével ellentétes. Erre tekintettel a különleges, érzékeny adatok magasabb szintű védelme érdekében a Hatóság szabályozási javaslatot tett és az új büntetőeljárásról szóló törvénnyel kapcsolatban javasolta a fentiek figyelembe vételét.

Egy esetben a bejelentő azt kifogásolta, hogy volt házastársa a bejelentő hozzájárulása nélkül használta fel a könnyű testi sértés vétsége miatt indult bírósági eljárás során a pszichológus szakértő rá vonatkozó szakvéleményét. A bírói

függetlenség elvére is tekintettel a Hatóság nem rendelkezik olyan hatáskörrel, amely alapján egy bírósági eljárásban bizonyítékok felhasználásának jogszerűségét vizsgálhatja, illetve a bizonyítékok közül bármelyiket kizárathatná. A pszichológus, pszichiáter szakértők szakvéleményeinek felhasználásával kapcsolatban ellenérveit, aggályait a bejelentő az eljáró bíróságnál terjesztheti elő. Azzal a körülménnyel kapcsolatban, hogy a volt házastárs a bejelentő beleegyezése nélkül használta fel az iratanyagot, a Hatóság álláspontja az, hogy a magánszemélyek közötti, ún. *„háztartási"* adatkezelési problémákat nem vizsgálja az Infotv. 2. § (4) bekezdésében foglaltakra tekintettel[72], mivel erre az Infotv. hatálya nem terjed ki. *[NAIH/2016/5120/V]*

III.2.5. A tudakozó szolgáltatással kapcsolatos panaszok

A NAIH-hoz 2016-ban sok olyan panaszbeadvány érkezett, melyek egy online elérhető, tudakozó szolgáltatást nyújtó weboldal adatkezeléséhez kapcsolódtak (a továbbiakban: Weboldal).

A panaszok elsősorban arra irányultak, hogy a Weboldalon található adatbázisban az érintettek engedélye nélkül szerepelnek a személyes adataik (név, lakcím, telefonszám, egyéb személyes információk), melyek megjelentetéséhez nem járultak hozzá, így a Weboldalt üzemeltető társaság jogtalanul tette azokat közzé illetve továbbította közzétételre egy másik szolgáltatónak.

A Hatóság a beadványok alapján indított vizsgálati eljárásaiban részletesen megvizsgálta az adatkezelés és adattovábbítás jogi hátterét.

Az elektronikus hírközlésről szóló 2003. évi C. törvény (továbbiakban: Eht.) alapján a szolgáltató valamennyi helyhez kötött telefonszolgáltatást igénybe vevő előfizetőjéről évente nyomtatott (telefonkönyv) vagy elektronikus formában előfizetői névjegyzéket *köteles készíteni.*[73]

Az Eht. alapján minden, az előfizetőkhöz telefonszámokat rendelő szolgáltató, köteles teljesíteni minden olyan ésszerű kérést, amely a nyilvánosan elérhető tudakozószolgálatok és telefonkönyvek szolgáltatása céljából a megfelelő infor-

72 Az Infotv. 2. § (4) bekezdés: *„Nem kell alkalmazni e törvény rendelkezéseit a természetes személynek a kizárólag saját személyes céljait szolgáló adatkezelésre."*

73 Eht. 160. § (2) bekezdés

mációk egyeztetett formában, tisztességes, tárgyilagos, költségalapú és megkülönböztetéstől mentes rendelkezésre bocsátására irányul.[74]

A fenti adattovábbítással kapcsolatosan megállapítottuk, hogy az Európai Unió Bírósága (a továbbiakban: Bíróság) a C-543/09. számú[75] ügyben hozott döntése alapján egy elektronikus hírközlési szolgáltató jogosult – sőt, amennyiben a tagállami jog azt előírja, köteles – az előfizetők személyes adatait újabb hozzájárulásuk nélkül továbbítani valamely nyilvános telefonkönyvet megjelentetni szándékozó másik vállalkozáshoz.

Összefoglalva a Bíróság ítéletét elmondható, hogy amennyiben a szolgáltató az előfizetőt megfelelően tájékoztatja arról, hogy a személyes adatait – nyilvános telefonkönyvben való megjelentetés céljából – valamely harmadik vállalkozás számára is továbbíthatja, és az előfizető egyébként hozzájárult ahhoz, hogy az említett adatok megjelenjenek a telefonkönyvben, úgy ugyanezen személyes adatoknak egy másik vállalkozás számára való továbbításához nem szükséges az előfizető újabb hozzájárulása, amennyiben a személyes adatok felhasználásának célja azok nyomtatott vagy elektronikus telefonkönyvben való megjelentetése, vagy e telefonkönyveknek tudakozószolgálaton keresztül való hozzáférhetővé tétele.

A fentieket összefoglalva a Hatóság a vizsgálata során megállapította, hogy a hatályos magyar és EU jogszabályok alapján az alábbiak szerint kezelheti egy elektronikus hírközlési szolgáltató az érintettek adatait az előfizetői névjegyzékkel és a tudakozó szolgáltatásokkal összefüggésben:

- Amennyiben az érintett hozzájárult ahhoz, hogy telefonszámát a szolgáltató feltüntesse az előfizetői névjegyzékben, úgy az ott található személyes adatait – név, lakcím, telefonszám – a szolgáltató jogosult, illetőleg erre irányuló igény esetén köteles is továbbítani olyan vállalkozások – így a társaság – részére, melyek tevékenysége tudakozó szolgáltatás nyújtására irányul.
- Amennyiben azonban az érintett az Eht. által biztosított[76] jogával élve korábban úgy nyilatkozott, hogy nem kíván szerepelni a nyomtatott vagy elektronikus névjegyzékben, úgy a szolgáltató – a Hatóság álláspontja szerint – az adattovábbítással jogellenes adatkezelést valósít meg, a

74 Eht. 146. § (1)-(2) bekezdése
75 http://eur-lex.europa.eu/legal-content/HU/TXT/?uri=CELEX:62009CJ0543 (2016.08.02.)
76 Eht. 160. § (4) bekezdés a) pontja

fentiek alapján ugyanis ebben az esetben a szolgáltató sem arra nem rendelkezett megfelelő jogalappal, hogy az érintett adatait feltüntesse az előfizetői névjegyzékben, sem pedig arra, hogy azokat továbbítsa a társaság részére.

A Hatóság a vizsgálat során az érintettek részére az alábbi intézkedések megtételét javasolja abból a célból, hogy a fentiek szerint jogszerűen továbbított és közzétett személyes adataikat a Weboldalról el tudják távolíttatni:

- Az érintett az Eht. 160. § (4) a) pontjára hivatkozással jelezze a szolgáltatójának, hogy ki kíván maradni a nyomtatott és elektronikus névjegyzékből, így telefonszámát kezeljék titkosan, az ne jelenjen meg semmilyen tudakozóban. A Hatóság javasolja továbbá, hogy az érintett jelezze a szolgáltató részére azt is, hogy járjon el az általa a társaságnak továbbított adatok ügyében is, így töröltesse azokat a társaság adatbázisából, valamint gondoskodjon arról is, hogy a jövőben ne küldjék meg az érintett személyes adatait a társaság részére.
- Amennyiben a szolgáltató a fenti kérést nem teljesíti, úgy az érintett a Hatóságnál bejelentéssel vizsgálatot kezdeményezhet arra hivatkozással, hogy személyes adatok kezelésével kapcsolatban jogsérelem következett be, vagy annak közvetlen veszélye fennáll.
- Az érintett a társaságtól is kérheti személyes adatainak eltávolítását, továbbá kérheti, hogy a Google távolítsa el a személyes adatait a kereső találatai közül.

III.2.6. Egészségügyi adatok kezelésével kapcsolatos ügyek

Az egészségügyi adatok kezelését érintő beadványok változatos képet mutattak. Rendszeresen előfordulnak egészségügyi dokumentáció kiadására vonatkozó ügyek. Az egyik beadvány szerint például egy édesanya a terhesgondozás során keletkezett és a gyermek születésére vonatkozó iratokat kívánta másolatban megkapni, mely másolás ellenszolgáltatásának díját az egészségügyi intézmény több mint százezer forintban határozta meg.

A Hatóság 2015 végén ajánlást bocsátott ki az adat-megismerési/dokumentáció másolási jognak a gyakorlati alkalmazását érintően, az egészségügyi dokumentáció másolási díjának jogszabályban történő meghatározásának érdekében. 2016-ban e kérdés még nem rendeződött, a megfelelő jogalkotási lépések még nem történtek meg.

Kirívó jogsértést tartalmazott egy beadvány, egy multinacionális vállalat táppénzen lévő munkavállalóira vonatkozó adatkezeléssel kapcsolatban. A bejelentés szerint a munkáltató a táppénzen lévő munkatársakról, a táppénz alapjául szolgáló betegségekről táblázatot vezetett, melyet a vezetők reggelente áttekintettek. Az adatkezelő válasza szerint céljuk a munka hatékony szervezése, a kieső munkavállalók helyettesítésének optimális biztosítása volt. A munkáltató azonban a kifogásolható adatkezelést megszüntette, az adatkezelésről való tudomásszerzés után azonnal intézkedett, minden vonatkozó állományt törölt, valamint a vezetők részére adatvédelmi képzéseket szervezett.

Több beadvány érkezett a munkavállalók vagy álláskeresők egészségügyi alkalmassági vizsgálatával kapcsolatban. Kérdésként merült fel, hogy a vizsgálatról, egészségi problémákról tájékoztatást kap-e a munkáltató vagy a foglalkoztatási szerv.

A munkavédelemről szóló 1993. évi XCIII. törvény (Mvt.) 50. §-a szerint **„***a munkavállaló csak olyan munkával bízható meg, amelynek ellátására egészségileg alkalmas, rendelkezik az egészséget nem veszélyeztető és biztonságos munkavégzéshez szükséges ismeretekkel, készséggel és jártassággal.*” Jogszabályban rögzítetten a munkavállaló együttműködési kötelezettsége körében rendszeres orvosi alkalmassági vizsgálaton köteles részt venni. A munkáltató vagy a foglalkoztató szerv csak arra vonatkozó véleményt kezel, hogy az érintett az adott munkára alkalmas, illetve nem alkalmas. Egészségügyi adat a munkáltató részére nem továbbítható, azt az egészségügyi szolgáltató kezeli.

Egy háziorvos beadványában előadta, hogy hallásszűréssel foglalkozó cég egy-egy körzet betegeinek szűrésre invitáló nyomtatványt küld. A vizsgálat során megállapítottuk, hogy a háziorvosok nem adták át a körzetükhöz tartozó személyek adatait, ugyanakkor a cég részéről az adatkezelésről adott tájékoztatás több helyen is hiányos volt.

Számos egyéb egészségügyi tárgyú beadvány érkezett, ezek egy része az adatvédelmi nyilvántartásba történő bejelentkezést érintette, de volt például lemondott védőnői szolgáltatást követő adatmegőrzési kötelezettségre, vagy az orvossal, a vizit alkalmával folytatott beszélgetés hangrögzítésére vonatkozó kérdés is.

Az Országos Mentőszolgálat egyrészt arról kérte a Hatóság állásfoglalását, hogy a mentőszolgálat diszpécsere az általuk végzett ellátási eseményről a telefonon érdeklődők közül kinek és milyen tartalmú felvilágosítást adhat, másrészről, hogy televíziós műsor készítői vonulhatnak-e a mentőkkel a riasztások helyszínére, dokumentálni a munkájukat, vagyis kép- és hangfelvételt készíteni.

A Hatóság álláspontja az ügyben az volt, hogy – törvényi felhatalmazás hiányában – az érintett ellátott írásbeli hozzájárulását igényelné a személyes és különleges adatairól harmadik személy számára történő tájékoztatás az OMSZ részéről. Ugyanakkor a Hatóság elismerte az érdeklődő, aggódó rokonok, hozzátartozók méltányolható igényét, hogy szerettük hollétéről információt szerezzenek, és sürgős ellátási esetben nem életszerű az, hogy a mentőegység a beteg ellátása közben az érintett írásbeli hozzájárulását is beszerezze az adattovábbításhoz. Így a Hatóság álláspontja szerint amennyiben valószínűsíthető, hogy az érdeklődő valóban hozzátartozó – az érintett nevét, életkorát pontosan tudja – úgy a szállítás ténye és az átvevő intézmény neve közölhető az Infotv. 6. § (2) bekezdése alapján[77].

A hozzátartozó további tájékoztatása a beteg állapotáról már az adott intézmény hatásköre, így a Hatóság álláspontja szerint a beteg állapotáról való tájékoztatás, a mentőszolgálat által biztosított ellátás részletes leírása már nem tartozhat bele a telefonon közölhető információk körébe. Amennyiben a hozzátartozói kapcsolat nem valószínűsíthető, úgy a Hatóság álláspontja szerint nem adható az átvevő intézményről sem tájékoztatás, így egyéb érdeklődők, újságírók részére sem.

A riasztások dokumentálásával kapcsolatban a Hatóság kifejtette, hogy egy ember képmása és hangja az Infotv. 3. § 2. pontja értelmében személyes adatnak minősül, amelyeknek egy televíziós műsorban történő kezeléséhez (Infotv. 3. § 10. pont), különösen a felvétel készítéséhez, nyilvánosságra hozatalához – törvényi felhatalmazás hiányában – az érintett hozzájárulása szükséges, és amennyiben egy műsorban a betegek különleges adatainak – mint például betegségének – közlésére is sor kerül, akkor ahhoz az Infotv. 5. § (2) bekezdés c) pontja szerint, a beteg által megadott írásbeli hozzájárulás szükséges. A felvételen szereplő környék, az ellátás helyszíne, a beteg ruházata és beszéde is különleges adatnak minősülhet adott esetben, hiszen a beteg faji eredetére, nemzetiséghez tartozására, akár kóros szenvedélyére is engedhetnek következtetni, még akkor is, ha a beteg arca ki van takarva, hiszen a beteg ismerősei még ilyen intézkedés mellett is felismerhetik őt.

A további törvényi feltételek – célhoz kötöttség, hozzájárulás önkéntessége, előzetes tájékoztatás – ismertetése után a Hatóság úgy összegezte álláspontját,

77 Infotv. 6. § (2) bekezdés: ha az érintett cselekvőképtelensége folytán vagy más elháríthatatlan okból nem képes hozzájárulását megadni, akkor a saját vagy más személy létfontosságú érdekeinek védelméhez, valamint a személyek életét, testi épségét vagy javait fenyegető közvetlen veszély elhárításához vagy megelőzéséhez szükséges mértékben a hozzájárulás akadályainak fennállása alatt az érintett személyes adatai kezelhetőek.

hogy kizárólag az érintett, beteg írásbeli hozzájárulásával lehetne az adott televízióműsor készítőinek az egészségügyi személyzettel együtt vonulni a riasztások helyszínére, és azt dokumentálni, azaz film és hangfelvételeket készíteni, azt nyilvánosságra hozni, különösen a betegről. Azonban egy sürgős ellátási esetben nem életszerű az, hogy a mentőegység a beteg ellátása közben az érintett írásbeli hozzájárulását is beszerezzék az adatkezeléshez, ezért a Hatóság egyetért az OMSZ álláspontjával, mely szerint a felvételek készítése ily módon nem valósulhat meg.

Visszatérő panasz, hogy a biztosítók kárigény elbírálásához széles körben kérnek egészségügyi adatot az érintettől. A biztosítókról és a biztosítási tevékenységről szóló 2014. évi LXXXVIII. törvény (Bit.) 136. §-a szerint *„az ügyfél egészségi állapotával összefüggő adatait a biztosító a Bit. 135. § (1) bekezdésében meghatározott célokból, kizárólag az érintett írásbeli hozzájárulásával kezelheti”.* A Bit. 135. § (1)-(3) bekezdései szerint a biztosító vagy a viszontbiztosító jogosult kezelni ügyfeleinek azon biztosítási titoknak minősülő adatait, amelyek a biztosítási szerződéssel, annak létrejöttével, nyilvántartásával, a szolgáltatással összefüggnek. Az adatkezelés célja csak a biztosítási szerződés megkötéséhez, módosításához, állományban tartásához, a biztosítási szerződésből származó követelések megítéléséhez szükséges, vagy az e törvény által meghatározott egyéb cél lehet.

Általánosságban kijelenthető, hogy minden olyan esetben, amikor az adatkérés nem korlátozódik a biztosítási szerződésből származó követelések megítélésével közvetlenül összefüggő adatkörre, túl széleskörű az adatkezelés. Esetenként vizsgálandó, hogy az igényelt egészségügyi adatokra a törvényi mentesülések, valamint a biztosítási szerződésben meghatározott kizárások megítéléséhez esetleg szükség lehet egészségügyi adatok megadására.

III.2.7. Szcientológia

A Hatósághoz több bejelentés érkezett a korábbi Magyarországi Szcientológia Egyház, illetve a jelenlegi Magyarországi Szcientológia Vallási Egyesület (a továbbiakban: Vallási Egyesület) adatkezelése miatt. A panaszok szerint az adatalanyokat megillető jogok sérültek a szervezetek adatkezelései során. A bejelentésekre, és a jogsértések valószínűsítésére tekintettel a Hatóság úgy döntött, hogy hatósági eljárást indít. Ennek keretén belül két helyszínen (a szervezet központi, budapesti irodájában, valamint a szervezet nyíregyházi missziójánál), helyszíni szemlét tartott, amelyek során elektronikus és papír alapú adathordozó-

kat foglalt le. A hatósági eljárás célja annak megállapítása, hogy a Vallási Egyesület adatkezelése összhangban áll-e a magyar adatvédelmi szabályozással. A hatósági eljárás 2017-ben folytatódik.

III. 3. Ajánlások, tájékoztatók

A Hatóság az Infotv. 38. § (4) bekezdés c) pontjában biztosított lehetőséggel élve ajánlásokat bocsát ki, illetve tájékoztatókat és állásfoglalásokat tesz közzé annak érdekében, hogy egyes, sokakat érintő adatvédelmi kérdésekben mind az adatkezelőknek, mind az érintetteknek útmutatóval szolgáljon a jogszerű adatkezelés kialakításában.

A 2016. évben tette közzé a Hatóság a hangfelvételek készítéséről, megismerhetőségéről és a másolat kiadásához való jogról szóló ajánlást.

A Hatóság 2016-ban három adatvédelmi tárgyú tájékoztatót bocsátott ki: a hangfelvétel készítéséről, felhasználásáról; a munkahelyi adatkezelések alapvető követelményeiről; valamint a webáruházakra vonatkozó adatvédelmi követelményekről szóló tájékoztatókat.

III.3.1. Hangfelvételek

A Hatósághoz rendszeresen érkeznek beadványok a hangfelvételek készítésének, valamint felhasználásának jogszerűségével kapcsolatban. Ebből adódóan a Hatóság fontosnak tartotta, hogy az érintettek tájékozódása végett tájékoztatót (elérési linkje: https://www.naih.hu/files/2016_05_09_tajekoztato_hangfelvetelekrol.pdf) bocsásson ki a kérdésben.

E dokumentum tartalmazza az ágazati jogszabályok által előírt, tehát a kötelező adatkezelés körébe eső szabályokat, továbbá azt az esetkört, amikor az adatkezelő dönt akként, hogy – az Infotv. rendelkezéseinek betartása mellett, de az érintett hozzájárulása alapján – hangfelvételt készít a beszélgetésről.

A Hatóság számára a beérkező esetek tükrében, valamint a jogszabályok áttekintését követően azonban nyilvánvalóvá vált, hogy a joggyakorlat e téren nem következetes, így – az egyes ágazati jogszabályok egységesítésére történő figyelemfelhívás, valamint az adatkezelők jogkövető magatartásának elősegítése

okán – ajánlást tett közzé a kérdésben (elérési linkje: https://www.naih.hu/files/ajanlas_hangfelvetel_NAIH-2016-4718-V.pdf).

III.3.1.1. Hangfelvételek megismerhetősége és a másolat kiadásához való jog

Az érintettek tájékoztatást az Infotv. 14. §-ának a) pontja alapján kérhetnek személyes adataik kezeléséről, mely részletszabályait az Infotv. 15. §-a rögzíti. Az adatkezelők gyakorlata azonban eltérő azon esetekben, amikor az adatalany a hangfelvételről másolatot kér. Az elektronikus hírközlési szolgáltatók kötelesek rendelkezésre bocsátani a hangfelvételt, míg a pénzintézetek számára a szektoriális törvények más tájékoztatási módot határoznak meg (visszahallgatás, hitelesített jegyzőkönyv rendelkezésre bocsátása). A fogyasztóvédelemről szóló 1997. évi CLV. törvény (a továbbiakban: Fgytv.) és az Infotv. nem határoz meg tájékoztatási módot, e két jogszabály nem írja elő kötelezően a másolat kiadását.

Az információs alapjogok minél teljesebb érvényesülése érdekében a Hatóság az alábbi szempontokra kívánja felhívni az adatkezelők figyelmét:

- A hangfelvételek rögzítésével együtt járó adatkezelés esetén az biztosítja a legmagasabb szinten a tájékoztatás teljességét és közérthetőségét, ha az érintettnek lehetősége van a hangfelvételt visszahallgatni, amely megvalósulhat az adatkezelő székhelyén vagy telephelyén, az adatkezelés helyén történő meghallgatásával, de megvalósulhat azáltal is, hogy az adatkezelő a hangfelvételről készített másolatot az érintettnek átadja.
- Az információs önrendelkezési jogból következő tájékoztatási jogosultságon kívül az érintettnek jogos érdeke fűződhet ahhoz, hogy a hangfelvétel a birtokába kerüljön. Ilyen lehet például az, ha kérdésessé és bizonyítandóvá válik, hogy a hangfelvételről készített jegyzőkönyv szöveghű-e, vagy esetleg elhallást tartalmaz, de előfordulhat az is, hogy a beszélgetés hangnemét kell bizonyítania. Bizonyos esetekben az érintett jogorvoslati jogának minél teljesebb érvényesülése is szükségessé teheti, hogy számára a hangfelvételek másolatát kiadják.
- A Hatóság álláspontja, hogy nem az ügyfélszolgálatot működtető társaság hivatott megítélni, hogy indokolt-e a hangfelvételnek az érintett általi felhasználása.
- Erre irányuló kérelem esetén a személyes adatok kezeléséről való tájékoztatás, illetve a hangfelvétel másolatának kiadása nem köthető egyéb feltétel meglétéhez vagy teljesítéséhez, csak amelyeket jogszabály

(Infotv. és szektoriális jogszabályok) előír. Mindezért az érintett tájékoztatását az adatkezelő az Infotv. 9. § (1) bekezdésében, valamint a 19. §-ban meghatározott esetekben tagadhatja meg, vagyis akkor, ha törvény, nemzetközi szerződés vagy az Európai Unió kötelező jogi aktusa alapján az adatkezelő a hozzá továbbított személyes adatot akként veszi át, hogy az adattovábbítással egyidejűleg jelezték számára az adatkezelés korlátait, vagy az érintetti jogok érvényesülését törvény korlátozza.

A hangfelvételt készítő cégek indokolatlanul korlátozzák az érintetti jogok érvényesülését, például amikor a hangfelvételek másolatának kiadását a cég székhelyén vagy telephelyén történő személyes megjelenéséhez vagy eljárásához kötik, a kiadás költségeként irreálisan magas összeget állapítanak meg, a felvétel személyes visszahallgatásán történő közreműködés címén ügyvédi díjat is felszámítanak az érintett terhére. A másolat kiadásához való jog ajánlás szerinti értelmezését erősíti meg a már hatályos, de csak 2018. május 25-től alkalmazandó az Európai Parlament és a Tanács 2016/679/EU rendelete[78] (továbbiakban: általános adatvédelmi rendelet) is, amely kifejezetten nevesíti a másolat kiadásához való jogot.

III.3.1.2. Hangrögzítés az érintett/fogyasztó által

Az érintett, illetve a fogyasztó által történő hangfelvétel rögzítésére jogszabályi kötelezettség nem áll fenn, ugyanakkor jogosnak tekinthető elvárás, hogy amennyiben a szolgáltatók, illetve a vállalkozások rögzíthetik a telefonbeszélgetést, ugyanezt megtehesse a másik fél is. Ennek során figyelembe veendő szempontok:

- Az érintett tevékenysége nem terjeszkedhet túl azon a célon, amely cél elérése érdekében az adatkezelő is rögzíti a beszélgetést. Ennek megfelelően az érintett is kizárólag az adatkezelővel folytatott jogviták rendezése

78 Az Európai Parlament és a Tanács 2016/679 rendelete a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK rendelet hatályon kívül helyezéséről (általános adatvédelmi rendelet) 15. cikk (3) bekezdés. *„Az adatkezelő az adatkezelés tárgyát képező személyes adatok másolatát az érintett rendelkezésére bocsátja. Az érintett által kért további másolatokért az adatkezelő az adminisztratív költségeken alapuló, ésszerű mértékű díjat számíthat fel. Ha az érintett elektronikus úton nyújtotta be a kérelmet, az információkat széles körben használt elektronikus formátumban kell rendelkezésre bocsátani, kivéve, ha az érintett másként kéri."* 15. cikk (4) bekezdés: *„A (3) bekezdésben említett, másolat igénylésére vonatkozó jog nem érintheti hátrányosan mások jogait és szabadságait."*

során használhatja fel a rögzített beszélgetést, azonban például a beszélgetést nem hozhatja nyilvánosságra. Abban az esetben, ha az érintett jogszerűtlenül túllépi az Infotv. szerinti saját céljait szolgáló adatkezelést[79], úgy az Infotv. szerint adatkezelőnek minősül. Kiemelendő továbbá, hogy az érintetti hangrögzítés esetében is jogos elvárás, hogy a telefonhívás megkezdésekor tájékoztassák a másik felet a hangfelvétel rögzítéséről. A szolgáltatást nyújtó cég munkatársa a telefonos ügyfélszolgálat során a cég képviseletében, annak üzleti tevékenységével kapcsolatban jár el. A munkáltató feladata e körben az, hogy munkavállalóját megfelelően tájékoztassa az érintettek/fogyasztók felmerülő jogos igényeiről és az alkalmazottak munkakörének ellátásával kapcsolatba hozható adatkezelési kérdésekről.

- Az érintett hangrögzítéséhez történő hozzájárulás nem tagadható meg üzleti titokra hivatkozással. Az üzleti titok sérelme ugyanis, egyéb feltételek fennállása mellett, már bekövetkezik az üzleti titok illetéktelen személy tudomására jutásával is, függetlenül attól, hogy a beszélgetést az érintett rögzíti vagy sem. Másrészről üzleti titok csak olyan adat lehet, amelynek illetéktelen megismerése ténylegesen sérti a jogosult pénzügyi, gazdasági vagy piaci érdekeit, és amely adat titokban tartása végett a jogosult szükséges intézkedéseket tett. Az üzleti titok jogosultjának a felelőssége az is, hogy alkalmazottja üzleti titkot ne közöljön a telefonbeszélgetés során.

III.3.1.3. Az ajánlás eredménye

Az ajánlás kibocsátását követően az Országgyűlés – a nemzeti fejlesztési miniszter javaslatára – elfogadta az elektronikus hírközléssel és a fogyasztóvédelemmel összefüggő egyes törvények módosításáról szóló 2016. évi CLXVIII. törvényt. E törvény szabályai eleget tesznek az ajánlásban foglaltaknak.

III.3.2. Tájékoztató a munkahelyi adatkezelések alapvető követelményeiről

A Hatósághoz minden évben jelentős számban érkeznek munkahelyi adatkezeléseket érintő panaszok, konzultációs jellegű beadványok. Erre tekintettel a Hatóság indokoltnak tartotta – részben hiánypótló jelleggel is – egy olyan tájékoztató

79 Az Infotv. 2. § (4) bekezdése értelmében: *„Nem kell alkalmazni e törvény rendelkezéseit a természetes személynek a kizárólag saját személyes céljait szolgáló adatkezeléseire”.*

közzétételét, amelyben összefoglalja álláspontját mind a munkavállalók, mind a munkáltatók számára, hogy a leggyakoribb munkahelyi adatkezelések során milyen adatvédelmi követelményeknek kell érvényesülniük.

A Hatóság tájékoztatója két fő részből épül fel. Az első, általános szabályokat tartalmazó rész ismerteti, hogy a munkahelyi adatkezelések során milyen adatvédelmi alapelveknek kell érvényesülniük, illetve mely jogalapok alkalmazhatók. A jogalapok közül fontos kiemelni a munkáltató jogos érdekén alapuló adatkezelést, hiszen a munkahelyi ellenőrzéssel együtt járó adatkezeléseknél minden esetben ez a jogalap alkalmazható.

A tájékoztató az általános szabályok között foglalkozik továbbá az előzetes tájékoztatás követelményével, a külföldre történő adattovábbítással, az adatvédelmi nyilvántartásba történő bejelentési kötelezettséggel, valamint a joghatósággal kapcsolatos kérdésekkel.

A tájékoztató második fő része az egyes speciális munkahelyi adatkezeléseket tartalmazza: álláspályázatra jelentkezés és magán-munkaközvetítés; alkalmassági vizsgálatok; a munkavállalók feddhetetlen előéletének igazolása; GPS navigációs rendszer alkalmazhatósága; biometrikus rendszerek alkalmazhatósága; a belső visszaélés-bejelentési rendszer (whistleblowing) adatvédelmi követelményei.

Ezek mellett kiemelt fejezetként szerepel a munkavállalók munkaviszonnyal összefüggő magatartásának ellenőrzése, tekintettel arra, hogy a Hatóság munkahelyi adatkezelésekkel kapcsolatos ügyeinek döntő része ezt a területet érinti. Az ellenőrzéssel összefüggő főbb adatkezelések a következők: munkahelyi kamerás megfigyelés; a munkáltató által a munkavállaló rendelkezésére bocsátott e-mail fiók, illetve laptop használatának ellenőrzése; az internethasználat ellenőrizhetősége; valamint a *„céges mobiltelefon”* használatának ellenőrizhetősége.

A Hatóság bízik abban, hogy a tájékoztatóban szereplő alapvető szempontok segítségül szolgálnak egyrészt a munkáltatók számára a jogszerű adatkezeléseik kialakításában, másrészt a munkavállalók számára, hogy tisztában legyenek azzal, milyen adatvédelmi követelményeknek kell érvényesülniük a munkahelyi adatkezelések során.

A Hatóság előzetes elemzése alapján a 2018. május 25. napjától Magyarországon is alkalmazandó új adatvédelmi rendelet jelentős változásokat nem fog eredményezni ezen ügyek tartalmi megítélésében.

A Hatóság munkahelyi adatkezelések alapvető követelményeiről szóló tájékoztatója az alábbi linkről érhető el: http://naih.hu/files/2016_11_15_Tajekoztato_munkahelyi_adatkezelesek.pdf

III.3.3. Tájékoztató a webáruházakra vonatkozó adatvédelmi követelményekről

A Hatósághoz rendszeresen érkeznek panaszok, beadványok a webáruházak adatkezelésével illetve annak jogszerűségével kapcsolatosan. Tekintettel e témakör iránt érdeklődők és az érintettek széles körére, a Hatóság tájékoztatót bocsátott ki a webáruházak adatkezelésével kapcsolatban. A tájékoztató célja, hogy útmutatóul szolgáljon mind a felületet üzemeltető adatkezelők, mind az adatkezelésben érintettek számára, hogy megismerjék, az internetes vásárlással összefüggő adatkezelések esetében milyen követelményeknek kell érvényesülniük.

A tájékoztató összefoglalja a webáruházakkal összefüggő adatkezelések jogszabályi hátterét, illetve az azokban foglalt kötelezettségeket. Ennek során kitér az internetes vásárlással összefüggő adatkezelés lehetséges jogalapjaira, az érintettek hozzájárulásának érvényességi feltételeire (különösen az érintettek előzetes hozzájárulására), az adatkezelés alapelveire és az érintettek jogaira. A tájékoztató rövid összefoglalást tartalmaz a webáruházakkal kapcsolatban alkalmazott sütik (cookie-k) jogi hátteréről, illetve csoportosításáról, továbbá a hírlevelek adatvédelmi vonatkozásairól.

A tájékoztató a Hatóság eljárási tapasztalatai alapján, példákon keresztül mutatja be, hogy milyen, a gyakorlatban előforduló megoldásokat tart a jogszabályi rendelkezéseknek megfelelőnek és melyek azok a gyakorlatok, amelyek a Hatóság álláspontja szerint módosítandók a jogszerű adatkezelés érdekében.

IV. Adatvédelmi Audit és BCR-ok

IV.1. Az adatvédelmi audit

Az adatvédelmi auditok tekintetében a 2016-os évben egyfajta trendforduló volt megfigyelhető, ugyanis a Hatóság adatvédelmi audit tevékenysége során többségbe kerültek az úgynevezett *„koncepció auditok”*, amikor a Hatóság a még meg nem kezdett, tervezett adatkezelések koncepcióját elemezte.

A Hatóság üdvözölte az adatkezelőknek ilyesfajta szemléletváltását, hiszen sokkal sikeresebb és hatékonyabb lehet egy adatvédelmi audit, ha még az adatkezelés megkezdése előtt értékelésen esik át valamennyi fontos adatvédelmi szempont. Az adatkezelő is szabadabban kommunikál az adatvédelmi audit során, hiszen könnyebben változtatható egy még meg sem kezdett folyamat, mint egy évek óta végzett adatkezelési tevékenység.

A fentieken túlmenően azért is örvendetes ez a megközelítés, mert ezzel az adatvédelmi auditban résztvevő adatkezelők az Általános Adatvédelmi Rendelet 35. cikkében leírt adatvédelmi hatásvizsgálathoz hasonló folyamatban vettek részt, ezzel is elősegítve a Rendeletre történő minél könnyebb átállást. A Hatóság adatvédelmi audit értékelése ugyanis hasonlít az adatvédelmi hatásvizsgálatra, hiszen mindkét dokumentum tartalmazza a tervezett adatkezelési műveletek módszeres leírását és az adatkezelés céljainak ismertetését, beleértve adott esetben az adatkezelő által érvényesíteni kívánt jogos érdeket; az adatkezelés céljaira figyelemmel az adatkezelési műveletek szükségességi és arányossági vizsgálatát; az érintett jogait és szabadságait érintő kockázatok vizsgálatát; és a kockázatok kezelését célzó intézkedésekre tett javaslatokat. Ennek megfelelően elmondható, hogy a Hatóság adatvédelmi audit gyakorlata egy önkéntes, kvázi adatvédelmi hatásvizsgálattá nőtte ki magát.

IV.2. A kötelező szervezeti szabályozás (binding corporate rules-BCR)

2016-ban 26 kérelem érkezett a Hatósághoz kötelező szervezeti szabályozás (BCR) jóváhagyása iránt. Ezek mindegyike olyan BCR jóváhagyására irányult, amelyet korábban más EU-s tagállam adatvédelmi hatósága, mint vezető hatóság

a 29-es Munkacsoport WP 107-es munkadokumentuma szerint együttműködési eljárás lefolytatását követően jóváhagyott.

A NAIH az alábbi adatkezelők (vagy adatkezelők csoportja) által alkalmazott BCR-okat hagyta jóvá 2016-ban, amelyeknek a megnevezését az érintettek tájékoztatásának elősegítése érdekében honlapunkon[80] is közzétettünk:

Jóváhagyás dátuma	Vállalatcsoport megnevezése	A BCR-t Magyarországon alkalmazó adatkezelők megnevezése
2016.12.15	Novartis	Novartis Hungária Kft.
2016.12.15	Novartis	Alcon Hungária Kft.
2016.12.15	Novartis	Sandoz Hungária Kft.
2016.12.15	Intel	Intel Corporation Hungary Kft.
2016.11.21	Amgen	Amgen Gyógyszerkereskedelmi Kft.
2016.11.21	Johnson Controls	Johnson Controls Mór Bt.
2016.11.21	Johnson Controls	Johnson Controls Management Mór Kft.
2016.11.21	Johnson Controls	Johnson Controls International Kft.
2016.11.21	Johnson Controls	Johnson Controls Autóakkumulátor Kft.
2016.11.21	Johnson Controls	Adient Mezőlak Kft.
2016.09.28	Flextronics	Flextronics International Kft.
2016.09.02	American Express	Global Business Travel Magyarország Kft.
2016.09.02	American Express	American Express Services Europe Limited Fióktelep, Magyarország
2016.08.26	Novo Nordisk	Novo Nordisk Hungária Gyógyszer Kereskedelmi és Szolgáltató Kft.
2016.08.23	Citigroup	Citibank International Limited Magyarországi Fióktelepe
2016.08.23	Citigroup	Citibank Europe plc. Magyarországi Fióktelepe
2016.08.11	LeasePlan	LeasePlan Hungária Zrt.
2016.07.29	ING	ING Bank N.V. Magyarországi Fióktelepe
2016.07.29	Ernst & Young	Ernst & Young Könyvvizsgáló Kft.
2016.07.29	Ernst & Young	Ernst & Young Tanácsadó Kft.
2016.07.29	Ernst & Young	EY Training Center Kft.
2016.07.29	Ernst & Young	NCOA Kereskedelmi és Szolgáltató Kft.
2016.07.29	Ernst & Young	Vámosi-Nagy Ernst & Young Ügyvédi Iroda
2016.07.28	Philips	Philips Magyarország Kereskedelmi Kft.
2016.07.28	Philips	Philips Lighting Hungary Kft.
2016.07.28	Philips	PHILIPS INDUSTRIES Magyarország Elektronikai Mechanikai Gyártó és Kereskedelmi Kft.

80 http://naih.hu/a-bcr-t-magyarorszagon-alkalmazo-adatkezel-k.html

2016.07.08	UCB	UCB Magyarország Kft.
2016.07.08	Cargill	Cargill Takarmány Zrt.
2016.07.08	Cargill	Cargill Magyarország Zrt.
2016.07.08	Shell	Shell Hungary Zrt.
2016.06.20	BP	BP Business Service Centre Kft.
2016.06.20	BP	BP Europa SE Magyarországi Fióktelepe
2016.06.20	BP	Castrol Hungária Kft.
2016.05.24	Capgemini	Capgemini Magyarország Kereskedelmi és Szolgáltató Kft.
2016.05.24	AstraZeneca	AstraZeneca Kereskedelmi és Szolgáltató Kft.
2016. 04.19	GE	GE Hungary Ipari és Kereskedelmi Kft.
2016. 04.19	GE	General Electric International, Inc. Magyarországi Fióktelepe
2016. 04.19	GE	GE Infrastructure Central & Eastern Europe Holding Kft.
2016. 04.19	GE	GE Infrastructure Hungary Holding Kft.
2016. 04.19	GE	GE Holdings Forint Hungary Kft.
2016. 04.19	GE	GE Közép-Európai Ellátó és Szolgáltató Kft.
2016. 04.19	GE	GE Water and Process Technologies Hungary Termelő és Szolgáltató Kft.
2016. 04.19	GE	Zenon Systems Termelő és Szolgáltató Kft.
2016. 04.19	GE	GE Energy Parts International, LLC Magyarországi Fióktelep, Granite Services International Inc. Magyarországi Fióktelepe
2016. 04.19	GE	Alstom Hungária Zrt.
2016.03.07	Corning	Corning Hungary Adatfeldolgozó Kft.
2016.03.07	GlaxoSmithKline plc	GlaxoSmithKline Kft.
2016.03.07	GlaxoSmithKline plc	GlaxoSmithKline Biologicals Kft.
2016.03.07	GlaxoSmithKline plc	GlaxoSmithKline-Consumer Kft.
2016.02.11	Continental Group	Continental Hungaria Kft.
2016.02.11	Continental Group	Contitech Magyarország Kft.
2016.02.11	Continental Group	Continental Automotive Hungary Kft.
2016.02.11	Continental Group	Contitech Rubber Industrial Kft.
2016.02.11	Continental Group	Continental Fluid Automotive Hungária Kft.
2016.02.09	HP Inc.	HP Inc Magyarország Kft.
2016.02.09	Hewlett Packard Enterprise	Hewlett-Packard Informatikai Kft.
2016.02.09	Hewlett Packard Enterprise	Hewlett-Packard Magyarország Kft.
2016.02.09	Hewlett Packard Enterprise	Hewlett-Packard Technológiai Licencek és Licencnyújtó Kft.

V. Információszabadság

A NAIH Alaptörvényből fakadó kötelezettsége nemcsak a személyes adatok védelme, de az állampolgárok azon alkotmányos jogának garantálása is, hogy az állam működését és gazdálkodását tényszerűen jellemző közérdekű, közérdekből nyilvános adatokhoz szabadon hozzáférjenek. A transzparencia érvényre juttatásáért 2016-ban is sok állami, önkormányzati szervvel, ezek többségi tulajdonában álló gazdasági társasággal szemben kellett vizsgálatot folytatni, felszólítással élni, illetve amennyiben a Hatóság intézkedéseinek nem volt foganatja, úgy jelentésben összegezni a mulasztásokat. Egyes szereplők továbbra is a közfeladatot ellátó szervi státuszukat vitatják, mások túl szélesen szeretnék értelmezni a döntés megalapozását szolgáló adatra való hivatkozást a nyilvánosság megkerülése érdekében.

V.1. Közfeladatot ellátó szervek

Az Infotv. nem tartalmaz felsorolást arra vonatkozóan, hogy mi minősül az állami vagy helyi önkormányzati, valamint jogszabályban meghatározott egyéb közfeladatnak. Ezt a tényt csak adott, egyedi ügy kapcsán, az eset körülményeinek figyelembe vételével lehet megállapítani. A közfeladat fogalma mindenesetre tágan értendő, így abba a tevékenységek széles köre beletartozik.

A közfeladatot ellátó szerv minőséget számos tényező megalapozhatja. Egyrészt ilyennek minősül az adott szerv, amennyiben állami vagy helyi önkormányzati feladatot, valamint jogszabályban meghatározott egyéb közfeladatot lát el. Másrészt a vonatkozó törvények rendelkezéseit figyelembe véve megállapítható, hogy a jelenlegi jogszabályi környezet nemcsak arra helyezi a hangsúlyt, hogy valamely szerv, személy jogszabályban meghatározott tényleges közfeladatot lát-e el, hanem a nemzeti vagyonnal való rendelkezés és gazdálkodás tényére is. Ezen rendelkezések és következtetések figyelembe vételével tehát irrelevánssá vált az állami, illetve önkormányzati tulajdonban álló gazdasági társaságok azon *„védekezése”* a közérdekű adatigénylések teljesítésének kötelezettségével szemben, amely szerint ők nem minősülnek közfeladatot ellátó szervnek, mert nincs jogszabályban meghatározott feladatkörük. Figyelembe kell továbbá venni azt is, hogy az Alkotmánybíróság a 6/2016. (III. 11.) AB határozatban kifejtette: az információszabadság szempontjából csak az számít, hogy az adott szerv közérdekű adatot kezel, s önmagában ennél fogva terheli – a közérdekű adatok megismeréséhez való jog érvényesülése érdekében – az adatigény teljesítésére

vonatkozó kötelezettség. Ez az általános érvényű kötelezettség nem korlátozható a címzettek körének szűkítésével, hogy az ne eredményezné egyúttal a közérdekű adatok megismeréséhez való jog korlátozását.

Az egyik ügyben a NAIH azt vizsgálta, hogy az Erzsébet Üzemeltető Kft. (a továbbiakban: Kft.) jogszerűen tagadta-e meg a hozzá érkezett adatigénylést azon az alapon, hogy a társaság nem kezel közérdekű és közérdekből nyilvános adatokat, illetve hogy nem tartozik az Infotv. hatálya alá. A Hatóság megállapította, hogy a cégnyilvántartás adatai alapján a Kft.-nek a HUNGUEST Vagyonkezelő Zrt. a tulajdonosa, mely esetében a szavazati jog több mint 50 %-át a Magyar Nemzeti Üdülési Alapítvány gyakorolja. A Kft. ráadásul azzal a céllal jött létre, hogy az Erzsébet programban résztvevő, elsősorban szociálisan rászorultak, gyermekek üdültetésének, táboroztatásának háttérbázisául szolgáló ingatlanegyüttest üzemeltesse, karbantartsa. A társaság tehát ténylegesen közfeladatot lát el, ezért az Infotv. szerinti közfeladatot ellátó szervnek minősül. Következésképpen köteles az Erzsébet-táborok üzemeltetésével kapcsolatos, 5 millió forintot meghaladó összegű szerződések megismerésére vonatkozó adatigénylés teljesítésére.

Egy másik ügyben a NAIH az Infotv. szerinti *„adatkezelő“* és *„adatfeldolgozó“* fogalmak alkalmazhatóságát vizsgálta az információszabadság vonatkozásában. A Miniszterelnökség (ME) ugyanis azon az alapon tagadta meg az egyébként kezelésében lévő, a humán közszolgáltatások differenciált szervezésének bevezetéséről szóló kormányhatározat 1. pontja szerint elfogadott koncepció elektronikus másolatának megismerésére irányuló adatigénylést, hogy annak kidolgozásával a jogszabály az emberi erőforrásokért felelős minisztert bízta meg, így az ME azzal összefüggésben nem minősül adatkezelőnek. A NAIH az Alkotmánybíróság 6/2016. (III. 11.) AB határozatában foglaltakra tekintettel megállapította, hogy az ME nem hivatkozhatott volna az Infotv. 3. § 9. pontja szerinti adatkezelői minőségének hiányára. Következésképpen köteles eleget tenni a kezelésében lévő koncepció megismerhetőségével kapcsolatos, Alaptörvényből és Infotv.-ből eredő kötelezettségeinek.

A NAIH megállapította a Magyar Bírósági Végrehajtói Kar (a továbbiakban: Kar) közfeladatot ellátó szerv minőségét is. A Kar ugyanis – többek között – amiatt tagadta meg az 5 millió forintot elérő szerződései listájának megismerésére vonatkozó adatigénylést, hogy a szervezet közpénzekkel nem gazdálkodik, így az igényelt adatok nem tartoznak sem a közérdekű, sem pedig a közérdekből nyilvános adatok körébe. Másrészt álláspontja szerint a Kar számára az igényelt adatok kiadása aránytalan nehézséget jelentene. A NAIH az ügyben hozott állásfoglalásában megállapította, hogy – a bírósági végrehajtásról szóló 1994. évi LIII. törvény

rendelkezéseire tekintettel – a Kar az Infotv. szerinti közfeladatot ellátó szervnek minősül, ezért a végrehajtáshoz kapcsolódó közfeladatok ellátásával összefüggő információk közérdekű adatoknak minősülnek. Azok megismerhetőségére tehát alkalmazni kell az Infotv. 26-30. §-aiban foglaltakat. A NAIH továbbá hangsúlyozta, hogy az Infotv. az aránytalan nehézség, vagy munkateher fogalmát nem elutasítási okként definiálja, hanem az adatigénylés teljesítésének módját, valamint a költségszámítást befolyásoló tényezőként. Következésképpen a Kar jogellenesen tagadta meg az adatigénylés teljesítését.

A NAIH a Magyar Állam kizárólagos tulajdonában álló Nemzeti Eszközgazdálkodási Zrt. (a továbbiakban: Zrt.) vonatkozásában is megállapította, hogy a társaság közfeladatot ellátó szervnek minősül, amelynek vagyonára és annak felhasználására vonatkozó minden információ közérdekű vagy közérdekből nyilvános adat. Ezen adatok megismerhetővé tétele tekintetében a társaság az Infotv.-ben foglaltak szerint köteles eljárni. Következésképpen bárki számára megismerhető a Zrt. által az Adriatiq Island Group átvilágítására kiírt közbeszerzés eredményeként megkötött szerződés tartalma, feltételezve, hogy az nem tartalmaz védett adatokat. A Zrt. ezért megsértette az adatigénylő közérdekű és közérdekből nyilvános adatok megismeréséhez fűződő jogát azáltal, hogy nem teljesítette az említett szerződéses adatok megismerésére irányuló igényét.

A NAIH hasonló álláspontot fogalmazott meg egy önkormányzat 100 %-os tulajdonát képező társaság által kötött szerződés rendelkezésre bocsátásával kapcsolatban is. Az ügyben folytatott vizsgálat során a NAIH kimondta, hogy a társaság az Alaptörvény, az Infotv., illetőleg az állami vagyonról szóló 2007. évi CVI. törvény és a nemzeti vagyonról szóló 2011. évi CXCVI. törvény szerinti közfeladatot ellátó szervnek minősül. Ebben a vonatkozásban – a közpénzek felhasználására vonatkozóan – köteles a részére benyújtott közérdekű adatigénylés érdemi elbírálására.

2016-ban is számos beadvány érkezett, amelynek kapcsán a Hatóságnak a Hallgatói Önkormányzatok különböző üléseinek nyilvánosságáról, a jegyzőkönyvek kiadhatóságáról, az egyetemek szenátusi üléseinek jegyzőkönyveiről, valamint a tisztségviselők bizonyos adatainak közérdekből nyilvános voltáról kellett állást foglalnia.

Az egyik ügyben a NAIH-nak abban a kérdésben kellett állást foglalnia, hogy a Hallgatói Önkormányzatok Országos Konferenciája (a továbbiakban: HÖOK) Választmányának jegyzőkönyvei megismerhetőek-e közérdekű adatigénylés keretében. Ezzel kapcsolatban a NAIH – a korábbi gyakorlatát is figyelembe véve –

megállapította, hogy a nemzeti felsőoktatásról szóló 2011. évi CCIV. törvény értelmében a HÖOK látja el a hallgatók országos képviseletét. A HÖOK a hallgatói önkormányzatok képviselőiből álló testület által elfogadott alapszabállyal rendelkező jogi személy, székhelye Budapest, képviseletére az elnök jogosult. A szervezet felett az ügyészség gyakorol törvényességi ellenőrzést. A HÖOK beszámolási és könyvvezetési kötelezettségére pedig az egyéb szervezetekre vonatkozó szabályokat kell alkalmazni. Következésképpen a HÖOK – az országos hallgatói érdekképviseleti szerepe révén – olyan jelentős, a felsőoktatási intézményrendszer demokratikus működésével együtt járó feladatokat lát el, amelyek közvetlenül és elválaszthatatlanul kapcsolódnak a felsőoktatás, mint állami közfeladat elvégzéséhez. E jelleget tovább erősíti az a tény, hogy a tagszervezetei sui generis közfeladatot ellátó szerveknek minősülnek. Ezek aktív részvétele a szervezet működésében tovább erősíti annak közfeladat ellátó jellegét. A fentiekre figyelemmel a Hatóság ezért kimondta, hogy a HÖOK a vonatkozó jogszabályok értelmében közfeladatot ellátó szervnek minősül, amely így köteles eleget tenni a tevékenységével összefüggésben álló információk tekintetében az Infotv.-ből eredő kötelezettségeknek.

V.2. Közérdekből nyilvános személyes adatok

A NAIH 2016-ban is számos olyan ügyet kapott, amelyben azt kellett vizsgálnia, hogy a közfeladatot ellátó személyek bizonyos személyes adatai mennyiben ismerhetőek meg. A beadványokban leggyakrabban az említett személyi kör részére adott egyedi, vagy rendszeres juttatások, illetőleg a vagyonnyilatkozatok nyilvánosságának kérdésköre merült fel.

Az egyik ügyben a bejelentő azért fordult a NAIH-hoz, mert a Miniszterelnökség (a továbbiakban: ME) megtagadta az ott foglalkoztatott közigazgatási államtitkároknak és helyettes államtitkároknak 2010 óta kifizetett jutalmakkal és célprémiumokkal, továbbá ezek odaítélésének feltételeivel, eljárásával, és a döntést meghozó személyekkel kapcsolatos adatok rendelkezésre bocsátását.

A NAIH az ügyben folytatott vizsgálat folyamán hangsúlyozta, hogy mivel közpénzek felhasználásáról van szó, az átláthatóság és ellenőrizhetőség – mint közérdek – kiemelt fontosságú. Ugyanakkor az információszabadságnak és az információs önrendelkezési jognak egymásra tekintettel kell érvényesülnie, így a közfeladat ellátásával összefüggő egyéb személyes adatok körének meghatározásánál figyelembe kell venni, hogy azok nyilvánossága nem sérti-e aránytalanul

a magánszférához való jogot. Tipikusan a vezetőknek kifizetett rendszeres, eseti, pénzbeli és természetbeni juttatások, így például a szabadságmegváltás, jutalom, helyettesítési díj, kereset-kiegészítés, céljuttatás összege a közfeladat ellátásával összefüggésben keletkezett személyes adatnak minősülnek, azokat bárki megismerheti. Azonban a szociális vagy rászorultsági alapon kapott juttatásokat – lakhatási, lakásépítési- és vásárlási támogatás, albérleti díj hozzájárulás, családalapítási támogatás, szociális támogatás – a NAIH tipikusan úgy értelmezte, hogy azokat a közfeladatot ellátó szerv a magánszférához köthető eseményekre, élethelyzetekre tekintettel folyósítja a kormánytisztviselőnek. Ezért azokat név szerinti bontásban csak az érintettek hozzájárulásával lehet nyilvánosságra hozni. Hozzájárulás hiányában ezek az információk kizárólag összesített formában – mint a közfeladatot ellátó szerv gazdálkodásával összefüggő közérdekű adatok – adhatók ki.

A NAIH végezetül megállapította, hogy az Infotv. 26. § (2) bekezdése nyilvánosnak rendel el minden olyan személyes adatot, amely a közfeladatot ellátó személy közfeladatával összefügg, mind a közigazgatási államtitkárok és a helyettes államtitkárok jutalmainak, célprémiumainak pontos összege, mind a döntést meghozó személy neve, az odaítélés eljárásának menete, a döntést orientáló szempontok olyan közérdekből nyilvános adatok, amelyek a közfeladatot ellátó állami vezetők feladatának ellátásával szorosan összefüggnek, hiszen azok jutalmazására irányul. Az ME ezért megsértette a bejelentő közérdekű adatok megismeréséhez fűződő alkotmányos jogát.

A NAIH hasonló álláspontra helyezkedett abban az ügyben is, amelynek tárgya egy város jegyzője részére juttatott utazási költségtérítés és bérlettámogatás összegének rendelkezésre bocsátása volt.

A vizsgálat nyomán hozott állásfoglalásában a NAIH kimondta: állandó gyakorlata értelmében az illetményre vonatkozó adatok körét tágan kell értelmezni, abba beletartoznak a közszolgálati jogviszonyra tekintettel, illetve azzal összefüggésben szerzett egyéb járandóságok, juttatások is. Ezen adatok nyilvánossága segítheti – egyebek mellett – az illetményre és egyéb pénzbeli, természetbeni juttatásokra vonatkozó egyenlő bánásmód követelményének érvényesülését is.

A fenti gyakorlatából következően a jegyző részére bármilyen jogcímen az önkormányzat által juttatott kifizetésekre, így többek között a költségtérítés és bérlettámogatás összegére vonatkozó információk közérdekből nyilvános adatok. Ezeket az adatokat bárki megismerheti. Mivel az adott város polgármestere megtagadta

az igényelt adatok rendelkezésre bocsátását, ezért sérült a bejelentő közérdekű és közérdekből nyilvános adatok megismeréséhez fűződő alapjoga.

A vagyonnyilatkozatok nyilvánosságával kapcsolatban a NAIH az egyik ügyben megállapította, hogy ellentétes az Infotv. rendelkezéseivel az, hogy az adatigénylő csak írásban terjesztheti elő a közérdekű adat megismerése iránti igényét, illetve hogy csupán betekintés, vagyis csak személyes megjelenés útján ismerheti meg az információkat. Másrészt sérti az információszabadságot az, ha az önkormányzati képviselő vagyonnyilatkozatáról az állampolgár nem kaphat másolatot. A polgármester, illetve az önkormányzati képviselők vagyonnyilatkozata ugyanis közérdekből nyilvános, amelyet – a vonatkozó törvényi előírásoknak megfelelően kell bárki számára megismerhetővé tenni.

A NAIH egy másik ügyben ugyancsak kimondta, hogy a nemzetiségi önkormányzati képviselők vagyonnyilatkozataiban foglalt adatok tekintetében alkalmazandóak az Infotv. információszabadság érvényesülésére vonatkozó rendelkezései. A nemzetiségek jogairól szóló 2011. évi CLXXIX. törvény ugyanakkor csupán arról rendelkezik, hogy az említett dokumentumok nyilvánosak, nem írják elő azonban azok nyilvánosságra hozatalát. Következésképpen a nemzetiségi önkormányzati képviselők vagyonnyilatkozatainak közzétételét a helyi önkormányzat nem rendelheti el kötelező jelleggel.

V.3. Döntés-előkészítő adatok

Az információszabadság, mint alapjog, nem abszolút jellegű. Ez azt jelenti, hogy korlátozásnak vethető alá, illetve bizonyos esetekben akár ki is zárható a közérdekű vagy közérdekből nyilvános adatok megismerhetősége. A nyilvánosság korlátozásának eseteit az Infotv. 27. §-a tartalmazza, amelyek közül kiemelendő a döntés megalapozását szolgáló adatok nyilvánosságának korlátozása.

A közfeladatok illetéktelen befolyástól mentes ellátását szolgálja az, hogy a döntés megalapozását szolgáló adatok, illetve az azokat tartalmazó dokumentumok legfeljebb tíz évig elzárhatók a nyilvánosság elől. Erre azonban csak akkor van lehetőség, amennyiben a nyilvánosság kizárása nem vezet a döntési folyamat átláthatatlanná tételéhez, illetőleg ha erősebb közérdek fűződik az adatok titokban tartásához, mint azok nyilvánosságra hozatalához. Az Infotv. alapján döntést megalapozó adatként indokoltan zárhatók el a nyilvánosságtól azok az információk, amelyek ténylegesen a döntési folyamat részét képezik, és nyilvánosságra

hozataluk veszélyeztetné a végrehajtás sikerét, vagy például egyes piaci szereplőket indokolatlan előnyökhöz juttatna.

A védelem a döntés meghozatala után is megilleti azokat az adatokat, amelyeknek a megismerése veszélyeztetné az érintett szerv törvényes működési rendjét, vagy feladat- és hatáskörének illetéktelen külső befolyástól mentes ellátását. A döntés megalapozását szolgáló adat megismerésére irányuló igény a döntés meghozatalát követően akkor is elutasítható, ha az adat további jövőbeli döntés megalapozását is szolgálja. Amennyiben tehát a kérdéses információ olyan adatösszesség része, amelynek egyes elemei tekintetében már döntés született, de más elemei még további döntés tárgyai lesznek, ez utóbbi adatok tekintetében az első döntés meghozatala után nem érvényesül a nyilvánosság. Annak eldöntése, hogy melyik adat kapcsolódhat adott esetben egy további döntéshez, nem teljesen egyértelmű. Egy információ gyakorlatilag számtalan további tevékenység vagy döntés alapjául szolgálhat, az információszabadság korlátozásának ilyen tág értelmezése azonban alaptörvény-ellenes lenne.

A közfeladatot ellátó szerveknek mérlegelniük kell, hogy – a döntés meghozatalát követően – az egyes adatok tekintetében fennáll-e olyan közérdek, amely a nyilvánosság korlátozását indokolná. Amennyiben nem, például az adott döntés megszületett, további intézkedések már nem szükségesek, a döntés megalapozását szolgáló adatok megismerhetőségét biztosítani kell. Hasonló mérlegelésre van szükség a további döntések meghozatalához szükséges információk tekintetében: itt azt kell megvizsgálni, hogy van-e olyan döntés, amelynek részrehajlásmentes meghozatalát a korábban keletkezett döntés megalapozását szolgáló adatok veszélyeztethetnék. Ilyen indokok hiányában az információszabadság korlátozására nem kerülhet sor.

Az egyik ügyben a bejelentő azt kifogásolta, hogy a Nemzeti Választási Iroda (továbbiakban: NVI) megtagadta a népszavazási kezdeményezések során összegyűjtött aláírások ellenőrzésével kapcsolatos útmutató rendelkezésre bocsátását. Az NVI azon az alapon utasította el az adatigénylés teljesítését, hogy a megismerni kívánt dokumentum döntés megalapozását szolgáló adatokat tartalmaz.

A NAIH az ügyben folytatott vizsgálat során – az adatelv és az Alkotmánybíróság gyakorlata alapján – kimondta, hogy a döntés-előkészítő adatok nyilvánossága korlátozható ugyan, de nem diszkrecionális jelleggel, hanem kizárólag a vonatkozó döntésekben lefektetett szigorú követelmények figyelembevételével. Erre tekintettel megállapította, hogy az NVI eljárása nem felelt meg az Alaptörvény és az Infotv. előírásainak, következésképpen az adatigénylés teljesítésének el-

utasítása sértette a bejelentő közérdekű adatok megismeréséhez fűződő jogát. Egyrészt az NVI nem indokolta meg kellőképpen a bejelentő által megismerni kívánt dokumentum nyilvánosságának korlátozását. Önmagában ugyanis *„az aláírás-ellenőrzés befolyástól mentes elvégzése”* még nem minősül olyan indoknak, amely megalapozná a döntés megalapozását szolgáló adatok nyilvánosság elől való elzárását. Az NVI ugyanakkor – a rendelkezésre álló adatok alapján – nem vizsgálta azt, hogy a nyilvánosság milyen módon befolyásolná az érintett munkavállalók munkavégzését. E megállapítás különösen azon tény fényében állja meg a helyét, miszerint az NVI az adatigénylés elutasítását követően nyilvánosságra hozta az említett dokumentumot a sajtóban *„megjelent valótlan állításokra”* válaszul.

Másrészt az NVI az információszabadság korlátozása tekintetében nem jelölte meg konkrétan azt az adatkört, amelynek vonatkozásában a döntés megalapozását szolgáló adatok nyilvánosság előli elzárása megalapozott lenne. Ehelyett az egész dokumentumot tekintette olyannak, amely az Infotv. 27. § (5) bekezdésének hatálya alá tartozik. Az eljárás ily módon sértette az Alkotmánybíróság határozataiban foglalt alkotmányos követelményeket.

Egy másik ügyben a NAIH egy konzultációs beadvány nyomán vizsgálta az önkormányzati ASP[81] rendszerről szóló 257/2016. (VIII. 31.) Korm. rendelet (a továbbiakban: Rendelet) 9. § (1) bekezdését, amelynek értelmében *„[a]z önkormányzati adattárház adattartalma a kormányzati és önkormányzati döntések előkészítését szolgálja”.*

A NAIH az állásfoglalásában megállapította, hogy a vizsgált rendelkezés olyan értelmezése, amely szerint az önkormányzati adattárház teljes adattartalma döntés-előkészítőnek minősül, sértené mind az Infotv., mind pedig az Alaptörvény rendelkezéseit. Egyrészt az ilyen joggyakorlat ahhoz vezetne, hogy a kormányzati és önkormányzati döntések átláthatósága megszűnik az önkormányzati adattárház vonatkozásában. Másrészt a döntések megalapozását szolgáló adatok e minősége nem értelmezhető általánosan az említett nyilvántartásban szereplő adatok tekintetében. Az egyes információk ugyanis bármely jövőbeli döntés megalapozását szolgálhatják. Egy bizonytalan döntéssel való absztrakt viszony ugyanakkor nem szolgálhat az információszabadság korlátozásának indokaként. Ez ugyanis teljes mértékben kiüresítené a közérdekű és közérdekből nyilvános adatok megismeréséhez fűződő alapjogot.

81 Application Service Provider – alkalmazás szolgáltatási modell: egységes önkormányzati gazdálkodási és adó szakrendszer

Egy harmadik ügyben a NAIH azért indított vizsgálatot, mert a Nemzetgazdasági Minisztérium (NGM) megtagadta a Családi Otthonteremtési Kedvezménnyel (CSOK) kapcsolatos jogszabályokat előkészítő hatástanulmányok megismerésére irányuló adatigénylés teljesítését. Az NGM álláspontja szerint az említett dokumentumok nyilvánosságának korlátozását azok az információk indokolják, amelyek döntés megalapozását szolgáló adatoknak minősülnek.

A NAIH az állásfoglalásában kiemelte, hogy a vonatkozó jogszabályok – a jogalkotásról szóló 2010. évi CXXX. törvény, az előzetes és utólagos hatásvizsgálatról szóló 24/2011. (VIII. 9.) KIM rendelet, valamint a jogszabályok előkészítésében való társadalmi részvételről szóló 2010. évi CXXXI. törvény – alapján az NGM-nek közzé kellett tennie a társadalmi egyeztetésre bocsátott tervezettel kapcsolatos előzetes hatásvizsgálat összefoglalóját. A kötelezően közzéteendő adatok esetében azonban nem lehet azok döntés megalapozásául szolgáló jellegére hivatkozni, hiszen azok proaktív, internetes nyilvánosságát törvény rendeli el. A hatástanulmányok e részét – de legalább az azokat tartalmazó oldalakra mutató pontos elérési utat – tehát mindenképpen köteles lett volna az NGM megküldeni az adatigénylőnek.

A NAIH továbbá kimondta, hogy a döntés meghozatala, azaz a tanulmányok alapján született jogszabályok megalkotása szerint is különbséget kell tennünk a dokumentumok megismerhetőségében. Azáltal ugyanis, hogy a jogszabály megszületik, az azt megalapozó elemzések, tanulmányok eltitkolásához fűződő érdek is elenyészik. Ezekben az esetekben a dokumentumok azon részének nyilvánossá tétele lehet megfontolandó, amelyek ellentétesek az elkészült jogszabállyal, avagy amely részeket a jogszabály megalkotásához nem használtak fel a tanulmányokból. Összességében tehát a NAIH megállapította, hogy az NGM eljárása az adatigénylés megtagadását illetően több szempontból is ellentétes volt a döntés megalapozásául szolgáló nyilvánosság-korlátozás alkotmányos követelményeivel.

V.4 Az adatigénylés teljesítéséért megállapítható költségtérítés szabályai

A Kormány 2016 folyamán fogadta el a közérdekű adat iránti igény teljesítéséért megállapítható költségtérítés mértékéről szóló 301/2016. (IX. 30.) Korm. rendeletet (a továbbiakban: Rendelet), amely 2016. október 15-én lépett hatályba. A közfeladatot ellátó szerveknek az Infotv. módosítás hatályba lépésétől (2015. október

1-től) ugyanis lehetősége volt arra, hogy – meghatározott esetekben – költségtérítést állapítsanak meg a közérdekű adatigénylések teljesítéséért. A törvény azonban sem a felszámítható költségelemeket, sem pedig azok pontos mértékét nem határozta meg. A megfelelő szabályozás hiánya így számos esetben visszaélésre adott lehetőséget, amelynek kiküszöbölése a jogalkalmazói gyakorlat szinte állandó feladatává vált. A Rendelet hatályba lépése azonban – a NAIH reményei szerint – orvosolni fogja az esetleges problémákat, áttekinthető és világos szabályozást honosít meg a közérdekű adatigénylések teljesítése terén.

Az adatigénylések teljesítéséért felszámítható költségtérítés kapcsán mindenekelőtt hangsúlyozandó, hogy – az Infotv. rendelkezéseire tekintettel – annak megállapítása nem kötelező. Ezért minden esetben az adott közfeladatot ellátó szerv dönti el, hogy él-e e joggal vagy sem. Amennyiben a szerv költségtérítést kíván megállapítani, akkor arra a Rendelet hatályba lépése után benyújtott adatigénylések esetében az ott meghatározottak szerint van lehetősége. A jogszabály hatályba lépését megelőzően benyújtott adatigénylések teljesítésekor pedig a NAIH gyakorlatában kialakított elveknek és szabályoknak megfelelő költségek számíthatók fel. Amennyiben viszont a közfeladatot ellátó szerv úgy dönt, hogy nem él a törvényben biztosított lehetőséggel, akkor utólagos költség-megállapításra a továbbiakban nem kerülhet sor. Ugyanis sem az Infotv., sem pedig a Rendelet nem tartalmaz ilyen rendelkezést. Hasonlóan tilos az előzetesen kalkulált és kifizetett költségtérítés, valamint a ténylegesen felmerült költségek közötti különbözet követelése az adatigénylőtől.

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

A Rendelet az Infotv. vonatkozó rendelkezésének megfelelően háromfajta költségelem felszámolását teszi lehetővé. A teljesítés során kizárólag a felhasznált

adathordozó, a kézbesítés, valamint a munkaerőforrás ráfordítás költségeit lehet jogszerűen igényelni. Ezen túlmenően más költségelem nem vehető figyelembe, az ugyanis ellentétes lenne az Infotörvénnyel.

Az adathordozók tekintetében kiemelendő, hogy a Rendelet a másolás költségeinek alapját oldalanként, nem pedig laponként határozza meg. Ugyanakkor a másolatok esetében csak a 10 oldal feletti rész költsége téríttethető meg, azaz a rövid – közérdekű vagy közérdekből nyilvános adatokat tartalmazó – dokumentumok esetében másolási költségek nem számíthatók fel. A kézbesítési költségek tekintetében a Kormányrendelet nem fogalmaz meg külön előírást. Ebben a vonatkozásban ugyanis a – belföldre vagy külföldre – postai úton történő kézbesítés díjait kell figyelembe venni.

Az Infotv. 2015. évi módosításának egyik jelentős újítása volt az a rendelkezés, amelynek értelmében a közfeladatot ellátó szervek lehetőséget kaptak az adatigénylések teljesítéséhez szükséges munkaerőforrás-ráfordítás költségének megtérítésére. A Rendelet hatályba lépéséig azonban számos kérdés felmerült ezzel kapcsolatban. Ezek közé tartozott – többek között – az, hogy mi minősül munkaerőforrás-ráfordításnak, milyen költségek számíthatók fel e tekintetben, és hogy a közfeladatot ellátó szervek mely esetben állapíthatnak meg térítési kötelezettséget az említett költségelem vonatkozásában.

A Rendelet értelmében munkaerőforrás-ráfordításként vehető figyelembe az igényelt adat felkutatásához, összesítéséhez és rendszerezéséhez, az igényelt adat adathordozójáról másolat készítéséhez, valamint a másolaton a meg nem ismerhető adatok felismerhetetlenné tételéhez szükséges időtartam. Amennyiben ez az időtartam meghaladja a 4 munkaórát, akkor a költségelemet úgy kell számítani, hogy a közreműködő személy által teljesített munkaórák számát meg kell szorozni az egy munkaórára eső tényleges munkaerő költségével. Utóbbi az adott személyt megillető rendszeres személyi juttatások összegét, de – a Rendelet értelmében – legfeljebb 4400 Ft.-ot jelent. A járulékok, prémiumok, jutalmak és egyéb juttatások, például a béren kívüli juttatások, nem vehetőek figyelembe.

Lényeges azonban, hogy a munkaerőforrás-ráfordítás költsége nem a közérdekű adatigénylés teljesítésének *„ellenértéke”*. A közfeladatot ellátó szervek a közérdekű adatigénylések teljesítésekor nem szolgáltatást nyújtanak, hanem az Alaptörvényben meghatározott alapvető jogból eredő kötelezettségeiket teljesítik. E szervek továbbá nem gazdasági tevékenységük körében, üzletszerűen értékesítik a másolatokat, hanem lehetőségük van a felmerült anyagköltségek megtérítését kérni az adatigénylőtől. Az Infotv. ezért az említett költségelem felszámítását

kizárólag abban az esetben teszi lehetővé, amennyiben az (1) az alaptevékenység ellátásához szükséges munkaerőforrás (2) aránytalan mértékű igénybevételével jár. Példaként említhető, hogy *„kiszervezés”* esetén a külső cég munkája nem jár a közfeladatot ellátó szerv alaptevékenységének ellátásához szükséges munkaerőforrás aránytalan mértékű igénybevételével. Ilyen esetekben kizárólag a másolásért lehetne költségtérítést felszámolni, a munkaerő-ráfordításért nem.

Végezetül a NAIH hangsúlyozni kívánja, hogy az Infotv. értelmében a közfeladatot ellátó szervek tájékoztatni kötelesek az adatigénylőket a költségtérítés összegéről. Ez azonban nem jelenti azt, hogy e szervek kötelezettségei kimerülnek pusztán a költségelemek után elszámolt térítési díj közlésével. Az információszabadság, mint alapjog érvényesüléséhez ugyanis szükséges az is, hogy az adatigénylés teljesítéséért megállapított költségtérítésről szóló tájékoztatás kellően részletes legyen, abban a közfeladatot ellátó szervek kötelesek feltüntetni minden olyan indokot, illetőleg költségelemet, amelyek a megállapított összeg megalapozottságát támasztják alá. A megfelelő tájékoztatás ugyanis nagyban hozzájárul ahhoz, hogy az igénylő valóban tisztában legyen, és megértse azt, hogy miért, milyen költségtérítést kell megfizetnie ahhoz, hogy a megismerni kívánt adatok birtokába jusson. A tájékoztatás alapján továbbá képes lesz a megfelelő döntést meghozni az igénybe vehető jogorvoslati lehetőséggel kapcsolatban.

V.5. A NAIH korrupció megelőzésével kapcsolatos tevékenységei

A NAIH számos esetben hangsúlyozta, hogy az információszabadság kiemelt szerepet tölt be a korrupció megelőzésében és üldözésében. Az ebbe a körbe tartozó bűncselekmények elkövetéséért való felelősségre vonáshoz elengedhetetlenül szükséges a transzparencia követelményének érvényesülése. A nyilvánosság elrettentő hatása továbbá hatékonyan képes megelőzni az esetleges visszaéléseket. A NAIH ezért mindig is kiemelt figyelmet fordít a korrupció megelőzésével kapcsolatos feladatok ellátására, megvalósítására és támogatására.

A NAIH munkatársai a 2016-os év során is több antikorrupciós kezdeményezés megvalósításában működtek közre. Kiemelendők ebben a körben a Nyílt Kormányzati Együttműködés kezdeményezés keretében tett vállalások teljesítéséhez kötődő oktatási és szakmai-ismeretterjesztő tevékenységek, amelyek során szoros együttműködés alakult ki a NAIH, a Nemzeti Védelmi Szolgálat (NVSZ) és a Nemzeti Közszolgálati Egyetem (NKE) között.

A NAIH egyrészt közreműködött Magyarországnak a Nyílt Kormányzati Együttműködés kezdeményezés keretében a 2015–2017. évekre tett vállalásairól szóló második akciótervéről szóló 1460/2015. (VII. 8.) Korm. határozat 6. pontja szerinti vállalás teljesítését szolgáló e-learning képzés kialakításában. Másrészt tagja az NKE Integritás Fejlesztési Bizottságnak, amelynek célja az integritás tanácsadók egyetemi keretek között történő képzésének továbbfejlesztése, megújítása.

A NAIH emellett – az NVSZ-szel együttműködve – 2016. november 22. és december 12. között részt vett Magyarországnak a Nyílt Kormányzati Együttműködés kezdeményezés keretében a 2015–2017. évekre tett vállalásairól szóló második akciótervéről szóló 1460/2015. (VII. 8.) Korm. határozat 3. pontjában megfogalmazottak szerinti, a helyi önkormányzati döntéshozatal nyilvánosságának biztosításával, és az ehhez fűződő közzététellel kapcsolatos gyakorlat hatékonyabbá tétele céljából készült módszertani útmutató megismertetését célzó, önkormányzatok számára szervezett műhelymunka lebonyolításában is.

VI. A Hatóság jogalkotással kapcsolatos tevékenysége

Az utóbbi években kiadott állásfoglalások számait az alábbi táblázat mutatja jogforrási szint szerinti bontásban. Az egyes jogszabályok megalkotásának folyamata során több lépcsőben, illetve több alkalommal is sor kerülhet állásfoglalás, vélemény kibocsátására, ezért a jogszabály-véleményezések ügyszáma és az állásfoglalások száma kismértékben eltér.

A jogi szabályozással kapcsolatos állásfoglalásaink száma jogforrási szint szerinti bontásban

Jogforrás/év	**2014**	**2015**	**2016**
Törvény	33	79	85
Kormányrendelet	63	133	98
Miniszteri rendelet	85	126	83
Kormányhatározat	21	61	29
Egyéb (Ogy. Határozat, utasítás, stb.)	7	27	20
Összesen	**209**	**426**	**315**

A jogszabály-véleményezésekben tett érdemi észrevételek statisztikája

Észrevételek jellege/száma	**2015**	**2016**
Adatvédelemmel kapcsolatos	298	222
Információszabadsággal kapcsolatos	53	101
Egyéb	137	127
Összesen	**488**	**450**

A számsorokat áttekintve elsőként az tűnhet fel, hogy a véleményezett tervezetek száma 2015-höz képest mintegy negyedével csökkent. Azonban hasonló vagy nagyobb mértékű ügyszám ingadozásokra az elmúlt években is volt példa, ezért ez az egyetlen adat önmagában kevés ahhoz, hogy messzemenő következtetéseket lehessen levonni. A másik fontos mutatószám a jogszabály-előkészítési egyeztetések során tett érdemi észrevételek és javaslatok száma, amelyekről immár évek közötti összehasonlításra alkalmas összesített adatok állnak rendelkezésre. Amint látható, az észrevételek száma 2015-höz képest csak kis mértékben csökkent, ami azt jelzi, hogy a Hatóság az ügyszám csökkenése ellenére a korábbi évekhez hasonló figyelmet és munkát fordít az információs alapjogvédelem e területére.

A statisztikai adatokról a tartalmi elemzésre áttérve az egyik lehetséges osztályozás aszerint tesz különbséget a véleményezett jogszabálytervezetek között, hogy azok valamilyen hosszú távú stratégia alapján kidolgozott szakpolitikai koncepciót valósítanak meg, vagy egy váratlanul felmerült azonnali szabályozási igényre adnak választ. Megítélésünk szerint 2016-ban nőtt az utóbbi csoportba tartozó jogszabályok száma. Az okokat kutatva megállapítható, hogy az a kiterjedt és tömeges nemzetközi migráció, melynek hullámai az elmúlt években elérték Európát, a jelenkorban teljesen új és korábban nem tapasztalt jelenség, amit nem lehetett előre látni. Ezzel párhuzamosan az európai nagyvárosokban tömeggyilkos terrormerényleteket követtek el. Azt érzékeljük, hogy csökkent a stabilitás a világban és egyre gyakrabban következnek be olyan kedvezőtlen változások, amelyek próbára teszik az államok és a társadalmak alkalmazkodási képességét. E változások nyilvánvalóan erőteljes állami válaszokat provokálnak ki. Az új kihívásokra adandó válaszlépések közé tartozik az ország stabilitásának megőrzéséhez és a terrorellenes fellépéshez szükséges további jogszabályok megalkotása is. Nyilvánvaló, hogy e jogszabályi változások érintik és érinteni fogják az információs önrendelkezési jog és az információszabadság érvényesülésének jogi szabályozási feltételeit is, ám még nem világos, hogy hol fog létrejönni az új információs egyensúly az állam és az állampolgár között. Mennyit kell feláldoznunk az információs jogainkból azért, hogy a biztonságunkat megőrizhessük? A jogi szabályozással kapcsolatos ügyeink bemutatásakor elsősorban az ehhez kapcsolódó kérdéseket, dilemmákat és a válaszkeresés útjait szeretnénk bemutatni.

VI.1. A terrorizmus elleni fellépés: a terrorveszélyhelyzet szabályozása

2016 elején a sajtóból szereztünk tudomást arról, hogy a Honvédelmi Minisztérium a parlamenti pártok bevonásával egyeztetéseket folytat az Alaptörvény különleges jogrendre vonatkozó szabályainak terror veszélyhelyzettel kapcsolatos kiegészítéséről, valamint az ahhoz kapcsolódó törvénymódosító csomagról. Ez több alkotmányjogi kérdést is felvetett. A Hatóság számára az érdemi kérdés természetesen az volt, hogy miként fogják érinteni az információs alapjogokat a tervezett változtatások. Emellett azt is értékelnünk kellett, hogy összhangban van-e a közérdekű adatok megismeréséhez való joggal és a demokratikus jogállamiság alkotmányos értékeivel az, hogy az Alaptörvény módosításáról folyó politikai egyeztetés zárt ajtók mögött, egy minisztérium szervezésében zajlik. Azonban a legelső feladat annak tisztázása volt, hogy egyáltalán vizsgálhatja-e a Hatóság az Alaptörvény módosítására vonatkozó tervezet tartalmát?

A Hatóság abból indult ki, hogy az Alaptörvény az alkotmányozó hatalom, illetve – az Alaptörvény módosítása esetén – az alkotmánymódosító hatalom aktusa, amely létrehozza az állam jogi alaprendjét, az alapvető jogok rendszerét és az államcélokat. Ezért az Alaptörvény az annak keretei között létrejött állami szervek számára érinthetetlen közjogi vonatkoztatási rendszert képez. Az állami szervek feladata az, hogy az Alaptörvény alapján létrehozott jogszabályoknak megfelelően, a feladat és hatáskörük keretei között maximálisan érvényre juttassák a mindenkori Alaptörvényben testet öltött közakaratot. Ebből következően a Hatóság az alkotmányozó és az alkotmánymódosító hatalom autonómiáját tiszteletben tartva, az Alaptörvény VI. cikk (3) bekezdésében meghatározott feladatkörében eljárva sem az Alaptörvényhez, sem az Alaptörvény módosítására vonatkozó tervezethez nem tehet tartalmi észrevételt és javaslatot. Szerepe legfeljebb annyi lehet, hogy jelezze, ha azt észleli, hogy az Alaptörvény módosítására vonatkozó tervezet, – annak elfogadása esetén – nyilvánvaló belső kollíziót idézne elő az Alaptörvényben az információs alapjogokkal összefüggésben, vagy e téren nyilvánvalóan ellentétes lenne Magyarország valamely nemzetközi kötelezettségvállalásával.

Ugyanerre az eredményre vezet a Hatóság az Infotv.-ben meghatározott véleményezési jogkörének formális elemzése is. Ugyanis az Infotv. 38. § (4) bekezdés a) pontja szerint a Hatóság véleményezési jogköre a jogszabályok tervezetére vonatkozik. Az Alaptörvény T) cikk (2) bekezdése szerint jogszabály a törvény, a kormányrendelet, a miniszterelnöki rendelet, a miniszteri rendelet, a Magyar Nemzeti Bank elnökének rendelete, az önálló szabályozó szerv vezetőjének ren-

delete és az önkormányzati rendelet. Jogszabály, továbbá a Honvédelmi Tanács rendkívüli állapot idején és a köztársasági elnök szükségállapot idején kiadott rendelete. Az Alaptörvény módosítása nem tartozik a felsorolt jogforrások közé, ezért annak véleményezésére a Hatóság Infotv.-ben meghatározott feladatköre nem terjed ki.

Ugyanakkor a Hatóság feladatkörébe tartozik az Alaptörvény módosításával kapcsolatos jogszabályok tervezetének véleményezése, illetve szükség szerint javaslattétel e jogszabályok megalkotására, módosítására vagy hatályon kívül helyezésére.

Az Alaptörvény módosításával kapcsolatos törvénycsomag tervezetének elemzése alapján a Hatóság arra a következtetésre jutott, hogy a terrorveszélyhelyzet törvényi szabályozását nem célszerű önmagában, a jogszabályi környezetből kiragadva vizsgálni, ugyanis a különleges jogrend közös szabályai egy egységes szabályozási keretbe illesztik a terrorveszélyhelyzet szabályozását, amely egyébként is hasonlóságokat mutat a különleges jogrend más jogintézményeivel, így különösen a megelőző védelmi helyzet bevezetésével összefüggő egyes rendszabályokkal és intézkedésekkel. Ezért a Hatóság azt vizsgálta meg, hogy milyen alkotmányos keretek határozhatók meg a különleges jogrend egyes intézményeinek törvényi szabályozására információs alapjogi szempontból. E kérdések megválaszolása elsősorban az Alkotmánybíróság hatáskörébe tartozik. Azonban az Alkotmánybíróság csak akkor foglalhat állást valamely nyitott kérdésben, ha az Alkotmánybíróság eljárásának kezdeményezésére jogosult személy beadvánnyal fordul a testülethez.

A törvénycsomag tervezetében foglaltakat, valamint az információs alapjogi követelményrendszert áttekintve a Hatóság a következő megállapításokra jutott:

– A honvédelemről és a Magyar Honvédségről, valamint a különleges jogrendben bevezethető intézkedésekről szóló 2011. évi CXIII. törvényben (a továbbiakban: Hvt.) rögzíteni szükséges a terrorveszélyhelyzet lényegi meghatározását és ennek körében azt, hogy melyek azok a küszöbfeltételek, amelyek esetén a veszélyhelyzet elhárításához szükséges rendkívüli intézkedések hatályba léptethetők. Lényeges, hogy a terrorveszélyhelyzet kezdetének időpontja egyértelmű legyen, hiszen ettől kezdve vezethetők be a korlátozó intézkedések és ehhez igazodik a terrorveszélyhelyzet megszűnésének vagy meghosszabbításának határideje.
– Az Alaptörvény 54. cikk (4) bekezdésére tekintettel a Hvt.-ben egyértelművé szükséges tenni azt, hogy a terrorveszélyhelyzetben bevezethető

rendkívüli intézkedésekkel kapcsolatban mely állami szerv jogosult azok alkalmazására, mire terjed ki a hatásköre, mi az általa alkalmazható rendkívüli intézkedés lényege és milyen célból, kivel szemben, miként, milyen feltételekkel alkalmazható az.

– A Hatóság kezdeményezte azt, hogy megismerhesse a Hvt. 64. § (7) bekezdésében meghatározott tervezeteket, hogy az Alaptörvény VI. cikk (3) bekezdésében foglaltak érdekében elláthassa az Infotv. 38. § (4) bekezdés a) pontjában meghatározott véleményezési feladatát.
– A Hatóság megfontolásra javasolta az alapvető jogok biztosa számára, hogy kezdeményezze az Alkotmánybíróságnál az Alaptörvény 54. cikk (1) bekezdésében az I. cikk (3) bekezdésén túli jogkorlátozásra adott felhatalmazás értelmezését.
– A Hatóság felkérte a Magyar Honvédség vezérkari főnökét, hogy intézkedjen a *„NEM NYILVÁNOS!”* jelölés törlésére az Alaptörvény módosításának, valamint a kapcsolódó törvénymódosításoknak a tervezetét tartalmazó dokumentumról, ugyanis az Alaptörvény módosítása egy demokratikus jogállamban minden állampolgárt érintő közügy, melynek előkészítéséről a demokratikus közvéleménynek joga van tudomást szerezni. Ha a döntés-előkészítési folyamat már abba a szakaszba jutott, amikor a politikai pártok egyeztetnek a módosításról, akkor a megvitatandó tervezetet a nyilvánosság elé kell tárni.

VI.2. A terrorizmus elleni fellépés: a belügyi törvénycsomag

A Belügyminisztérium által előkészített terrorellenes törvénycsomag a közelmúlt történéseire, így különösen a nyugat-európai nagyvárosokban elkövetett terrortámadásokra és a migrációs nyomás erős növekedésére, valamint az ezzel összefüggő káros jelenségre reagálva olyan módosításokat irányzott elő, amelyek egy része az információs önrendelkezési jog korlátozására vonatkozott. A Hatóság a törvénytervezet közigazgatási egyeztetése során, majd ezt követően a törvényjavaslat országgyűlési vitája idején is közzétette az álláspontját. Ebben arra hívta fel a figyelmet, hogy az állam Alaptörvényben rögzített alapjogvédelmi kötelezettségéből következően a terrorellenes fellépéssel kapcsolatos információs jogkorlátozásnak nem szabad meghaladnia a szükséges és arányos mértéket, továbbá nem eredményezheti az állam információs túlhatalmát az állampolgárokkal szemben, ezért a törvényi szabályozásnak megfelelő adatvédelmi és magánszféra-védelmi garanciarendszert kell tartalmaznia.

A törvénycsomag olyan veszélyekkel szemben határoz meg megelőző és védelmi jellegű jogkorlátozó intézkedéseket, amelyekről még nem tudható, hogy átmenetiek-e, vagy hosszú időtávban számolni kell velük. A tervezett jogkorlátozó szabályok csak addig alkotmányosak és legitimek, ameddig azok oka, azaz a fokozott migrációs nyomás és a terrorveszély lehetősége fennáll. Ezért a Hatóság azt javasolta, hogy a törvényhozás időről időre vizsgálja felül a terrorveszéllyel kapcsolatos egyes jogkorlátozó szabályok további hatályban tartásának szükségességét.

A törvénycsomagban szereplő terrorellenes intézkedések lehetőséget biztosítanak a nemzetbiztonsági szolgálatok számára az automatizált adatgyűjtésre. Az automatizált adatátvétel kiiktatja az adatkezelő szerv közreműködését, ezért megnöveli annak a veszélyét, hogy a nemzetbiztonsági szolgálatok esetenként szükségtelen, indokolatlan, tömeges adatigényléssel éljenek. Ezért a Hatóság szerint az adatigénylések automatizálása a korábbinál erősebb adatvédelmi ellenőrzési rezsim kialakítását teszi szükségessé mind a nemzetbiztonsági szolgálatokon belül, mind a külső független ellenőrzést illetően. Ennek szükségességét az is alátámasztja, hogy az Európai Bíróság a Safe Harbor rendszer jogi alapjának megsemmisítéséről szóló határozatának indoklásában kitért arra, hogy az USA nemzetbiztonsági szolgálatai által végzett tömeges megfigyelés nincs összhangban az európai polgárok adatainak védelmére vonatkozó elvekkel. Az európai demokratikus jogállamoknak – így Magyarországnak is – maradéktalanul be kell tartani azokat az adatvédelmi és magánszféra-védelmi követelményeket, amelyeket más államokkal szemben joggal kérnek számon.

A Hatóság arra is felhívta a figyelmet, hogy a személyes adatoknak az illetékes hatóságok által a bűncselekmények megelőzése, nyomozása, felderítése, üldözése vagy büntetőjogi szankciók végrehajtása céljából végzett kezelése tekintetében a természetes személyek védelméről és az ilyen adatok szabad áramlásáról, valamint a 2008/977/JHA tanácsi kerethatározat hatályon kívül helyezéséről szóló európai parlamenti és tanácsi Irányelv (a továbbiakban: Irányelv) hatálybalépése szükségessé teszi a terrorellenes intézkedések felülvizsgálatát. Ugyanis az Irányelv IV. fejezete olyan újfajta kötelezettségeket ír elő, mint a beépített és alapértelmezett adatvédelem, adatvédelmi hatásvizsgálat és az előzetes konzultáció a felügyeleti hatósággal. Részletesebb és átfogóbb kötelezettséget ír elő az Irányelv az adatkezelési tevékenység nyilvántartására (24. cikk) és a naplózásra (25. cikk) is. A 26. cikk új jogintézményként szabályozza az adatvédelmi hatóság általi kötelező előzetes jóváhagyást, míg a 28. cikk az adatvédelmi incidens kötelező jelentését írja majd elő, amely rendelkezések az adatvédelmi hatósággal való még szorosabb együttműködésre és az általa java-

solt szempontrendszer még szélesebb körű érvényre juttatására kötelezi majd az adatkezelőt. Az Irányelv új szempontrendszert határoz meg a külföldre történő adattovábbításokat illetően is.

VI.3. A terrorellenes fellépés: az elektronikus kereskedelmi szolgáltatók együttműködésre kötelezése

Az infokommunikációs technika gyors fejlődése nem állt meg azzal, hogy a vezetékes telefonszolgáltatás mellett megjelent és széleskörűen elterjedt a mobiltelefon. Az új generációs elektronikus hírközlési hálózatokban mindinkább egységesül a hangkommunikációs és az elektronikus adattovábbítás. Az okoseszközök megjelenésével együtt számtalan, kommunikációval kapcsolatos alkalmazás és szolgáltatás jelent meg, amelyek számára az elektronikus hírközlési szolgáltatások biztosítják a kommunikációs infrastruktúrát. Ez számos, a nemzetbiztonsággal és a bűnüldözéssel kapcsolatos alapjogvédelmi kérdést vet fel, amelyek 2016-ban a közélet és a közvélemény érdeklődését is felkeltették. Például egy olyan alkalmazással, amely képes a kommunikáció végpontok közötti titkosítására, olyankor is megakadályozható a kommunikáció tartalmának megfigyelése, ha a megfigyelést végző állami szerv képes a hálózaton továbbított jelek megismerésére. Ezért a Belügyminisztérium egy olyan törvényt készített elő, amely arra kötelezte az elektronikus kereskedelmi szolgáltatások, valamint az információs társadalommal összefüggő szolgáltatások egyes kérdéseiről szóló 2001. évi CVIII. törvény (továbbiakban: Ekertv.) hatálya alá tartozó alkalmazásszolgáltatókat, hogy a külső engedélyhez kötött titkos információgyűjtésre jogosult szervezetek számára biztosítsanak hozzáférést a titkosított kommunikációt biztosító alkalmazás igénybevételével továbbított küldeményekhez, közlésekhez, valamint az azokkal kapcsolatban keletkező vagy kezelt adatokhoz. Emellett a módosítás értelmében az elektronikus kereskedelmi szolgáltatók kötelesek megőrizni az előfizetőre vagy felhasználóra vonatkozó adatokat, valamint a kommunikáció metaadatait.

Az alkalmazásszolgáltatások titkos információgyűjtés számára hozzáférhetővé tétele hasonló szabályozási kérdéseket vet fel, mint amelyek az elektronikus hírközlési szolgáltatások esetében felmerülnek. Kétségtelen, hogy a kommunikáció mind nagyobb hányada tevődik át a hagyományos hírközlési szolgáltatásoktól az alkalmazásszolgáltatások felé. Az újfajta eszközök, szolgáltatások és alkalmazások mind nagyobb szerepet kapnak az egyének magánéletében és kapcsolattartásában, ezért ezek állam általi megfigyelése és az ezekből történő titkos információgyűjtés a korábbi, hagyományos elektronikus hírközlési szolgáltatá-

sok (elsősorban a telefonbeszélgetések) titkos megfigyelésénél sokkal több és többféle információ megszerzésére alkalmas, következésképp az egyének magánéletének, kommunikációjának és kapcsolatrendszerének sokkal mélyebb és részletesebb megismerését teszi lehetővé az állam számára.

Az alkalmazásszolgáltatások egy részénél az is további adatvédelmi kockázatot jelent, hogy az adatkezelés és a kommunikáció megfigyelése és értelmezése a feldolgozás élőmunka-igényének csökkentésével vagy megszüntetésével a hagyományos elektronikus hírközlési szolgáltatásokhoz képest jobban automatizálható és tömegessé tehető.

Az alkalmazásszolgáltatásokból való titkos információgyűjtés erősebb beavatkozás és több kockázattal jár az egyén magánéletére és információs önrendelkezési jogának érvényesülésére, mint a hagyományos elektronikus hírközlési szolgáltatások megfigyelése, ezért a Hatóság szerint a szabályozásnak specifikus adatvédelmi többletgaranciákat kell tartalmaznia.

Ami az adatmegőrzési kötelezettséget illeti, a Hatóság szerint az elektronikus hírközlési szolgáltatók adatmegőrzésével kapcsolatos szempontokat szükséges alapul venni az elektronikus kereskedelmi szolgáltatók esetében is. Az Európai Unió Bírósága 2014-ben érvénytelennek nyilvánította a nyilvánosan elérhető elektronikus hírközlési szolgáltatások nyújtása, illetve a nyilvános hírközlő hálózatok szolgáltatása keretében előállított vagy feldolgozott adatok megőrzéséről és a 2002/58/EK irányelv módosításáról szóló 2006. március 15-i 2006/24/EK európai parlamenti és tanácsi irányelvet. A Hatóság az ítéletben foglaltak értelmében nem tartotta elfogadhatónak az általános, készletező jelleggel, egy éves időtartamra szóló adatmegőrzési kötelezettséget.

A Hatóság javasolta az adatmegőrzés céljának pontos meghatározását a törvényben. Míg a nyomós államérdekek – például a terrorizmus elleni harc vagy a nemzetbiztonsági szolgálatok elhárító tevékenysége – megfelelő jogi keretek között elégséges indok lehet az adatmegőrzési kötelezettség bevezetésére, addig például az otthoni számítógépen torrentezők állami ellenőrzése esetén a magánéletbe való beavatkozás az elérni kívánt célhoz képest aránytalanul nagy jogkorlátozás lenne, ezért az adatok hasonló célra történő felhasználása alkotmányos aggályokat vetne fel.

VI.4. A terrorellenes fellépés: a közlekedési infrastruktúra biztonságával kapcsolatos adatok védelme

Szintén a terrorcselekmények megelőzése volt a deklarált célja azoknak a törvénymódosításoknak, amelyek a vasúti közlekedési infrastruktúra és az állam, valamint a lakosság ellátása szempontjából kiemelten fontos létesítmények biztonságos működtetésével kapcsolatos adatok nyilvánosságának korlátozását teszik lehetővé. (Lásd: a közlekedéssel összefüggő egyes törvények módosításáról szóló 2016. évi CXLIV. törvény 30. §-át, valamint a Rendőrségről szóló 1994. évi XXXIV. törvény, valamint az elektronikus hírközlésről szóló 2003. évi C. törvény módosításáról szóló 2016. évi CXXVIII. törvény 1. §-át.). E szabályok nem a személyes adatok védelmét, hanem a közérdekű adatok megismeréséhez való jog érvényesülését érintik. A hivatkozott szabályok tervezetét elmulasztották véleményezésre megküldeni, azonban a törvényjavaslat benyújtását követően Dr. Tóth Bertalan országgyűlési képviselő részletes állásfoglalást kért a törvénymódosításokról, ami lehetőséget adott annak kifejtésére, hogy milyen információs alapjogvédelmi szempontok alapján vizsgálja a Hatóság e törvénymódosításokat, valamint a hasonló, a közérdekű adatok nyilvánosságát érintő törvényi korlátozásokat.

A Hatóság arra törekszik, hogy maradéktalanul beépítse a joggyakorlatába az Alkotmánybíróság által kimunkált, releváns alapjogvédelmi alkotmányossági követelményeket. Az elvi kiindulópontunk az, hogy a közérdekű és közérdekből nyilvános adatok megismeréséhez és terjesztéséhez való jogot az Alkotmánybíróság kezdettől információszabadságként fogta fel, melyet az Alaptörvény hatályba lépése utáni határozataiban is megerősített. Az információszabadság *„lehetővé teszi a választott népképviseleti testületek, a végrehajtó hatalom, a közigazgatás jogszerűségének és hatékonyságának ellenőrzését, serkenti azok demokratikus működését”* (32/1992. (V. 29.) AB határozat). Másrészt az információszabadság érvényesülése gyakran előkérdése és kiindulópontja a véleménynyilvánításhoz való jog gyakorlásának. Ezen alapjog kiemelt szerepet játszik az állam demokratikus működésének kialakításában (34/1994. (VI. 24.) AB határozat). Továbbá a közérdekű adatok megismeréséhez és terjesztéséhez való alapvető jog végeredményben a Nemzeti hitvallás azon pontja érvényre juttatását is szolgálja, mely szerint *„valljuk, hogy népuralom csak ott van, ahol az állam szolgálja polgárait, ügyeiket méltányosan, visszaélés és részrehajlás nélkül intézi”. „Ennél fogva a polgárait szolgáló demokratikus állam működésének egészével, általánosságban a közfeladatok ellátásával kapcsolatos alaptörvényi követelmény tehát az átláthatóság és a közélet tisztasága, valamint a közügyek méltányos, visszaélés és részrehajlás nélküli intézése (21/2013. (VII. 19.) AB határozat)”*.

Az Alkotmánybíróság határozatai mellett az Infotv. határozza meg az információs alapjogvédelmi keretrendszert a személyes adatok, illetve a közérdekű és a közérdekből nyilvános adatok kezelésére vonatkozó szektorális törvények számára, amint azt az Infotv. preambuluma, valamint a törvény célját meghatározó 1. § egyértelművé teszi. Az Infotv. az információs önrendelkezési jog és az információszabadság biztosítása érdekében, a személyes adatok védelmét, valamint a közérdekű és a közérdekből nyilvános adatok megismeréséhez és terjesztéséhez való jog érvényesülését szolgáló alapvető szabályokat határozza meg. Például azt, hogy legalább milyen tárgykörök szabályozására kell kitérnie egy kötelező adatkezelést előíró szektorális törvénynek. Azt is az Infotv. szabályozza, hogy a közérdekű adatok nyilvánossága milyen célból korlátozható valamely szektorális törvényben. E szabályok lerontása nem lehetséges olyan módon, hogy az adatkezelésre vonatkozó törvények az Infotv.-ben foglaltaktól eltérve az adott szektorális törvény hatálya alá tartozó területeken meggyengítik az információs alapjogvédelem garanciáit. A konkrét ügyben a Hatóság a következő megállapításokat tette:

A törvénymódosítások célja összhangban van az Infotv.-ben foglaltakkal. A terrorcselekmények megelőzése a bűnüldözési és a nemzetbiztonsági érdek érvényesítésének körébe tartozik. Az Infotv. 27. § (2) bekezdés b) és c) pontjaiban foglaltak szerint törvény bűnüldözési és nemzetbiztonsági érdekből korlátozhatja a közérdekű adatok megismeréséhez való jog érvényesülését.

A törvénymódosítások tartalmazzák azt, hogy a korlátozás milyen adatokra vonatkozik. Az adatkörök meghatározása a korlátozás tárgyának tartalmi meghatározásához elengedhetetlen. A magyar információs alapjogi szabályozás az Alkotmánybíróság határozatai által kibontott alkotmányossági követelménynek megfelelően az adatelvet érvényesíti.

Az elmúlt években a világ nagyvárosaiban végrehajtott terrortámadások több esetben a tömegközlekedési infrastruktúrát vagy a kormányzat működése, illetve a lakosság ellátása szempontjából kiemelten fontos objektumokat vették célba. A korlátozás csak azokra az adatokra vonatkozhat, amelyek terrorfenyegetettség szempontjából érzékenyek: csak biztonsági, védelmi, műszaki, üzemeltetési adatokról lehet szó. Más, az információszabadság érvényesülése szempontjából lényeges adatok, mint például a beruházások költségvetési forrásigénye vagy a létesítmények környezeti hatásaira vonatkozó adatok korlátozása nem tárgya a véleményezett törvénymódosításoknak.

Az információszabadság fontos garanciája, hogy a szóban forgó törvényjavaslatok nem *„ex lege”* nyilvánosságkorlátozást, hanem jogalkalmazói érdekmérle-

gelést írnak elő, azaz az adatkezelő szervnek minden esetben mérlegelnie kell, hogy az adott adatra nézve az adatigény benyújtásakor fennáll-e a nyilvánosság korlátozásának törvényben előírt feltétele, vagyis az, hogy az adat megismerése Magyarország nemzetbiztonsági érdekeit vagy a bűncselekmények megelőzéséhez fűződő érdekeit veszélyeztetné.

A törvénymódosítások 30 éves adatmegismerés korlátozási határidőt állapítanak meg. A határidő törvényi meghatározása azért lényeges, mert ha a szabályozás a közérdekű információt végérvényesen elvonná a megismerhetőség elől, az a közérdekű adatok megismeréséhez való jog lényeges tartalmát érintené, márpedig alapvető jog lényeges tartalmát törvény sem korlátozhatja. A 30 éves adatmegismerés korlátozási időtartam a nemzeti minősített adatok két legfelső minősítési szintjéhez, a „*Szigorúan titkos!*”-hoz és „*Titkos!*”-hoz rendelt maximális érvényességi idejével mérhető össze, ugyanakkor nagyjából összhangban van a védendő létesítmények tipikus élettartamával, ezért végső soron elfogadható.

VI.5. A titkos információgyűjtés külső engedélyezési rendszerének reformja

A nemzetbiztonsági célú titkos információgyűjtés külső engedélyezési rendszerének felülvizsgálatát elsősorban a strasbourgi Emberi Jogok Európai Bíróságának (EJEB) 2016. január 12-én meghozott ítélete (a továbbiakban: Ítélet) teszi szükségessé. Az Ítélet szerint Magyarország megsértette az Európai Emberi Jogi Egyezmény (továbbiakban: Egyezmény) magán- és családi élet tiszteletben tartásához való jogról szóló cikkét. Az Ítélet végső soron azért marasztalta el Magyarországot, mert a Terrorelhárítási Központ esetében a Rendőrségről szóló 1994. évi XXXIV. törvény (Rtv.) szabályai szerint a külső engedélyhez kötött titkos információgyűjtés igazságügyért felelős miniszter (IM) általi engedélyezése esetén hiányzik a független külső kontroll. Ugyanakkor a nemzetbiztonsági szolgálatokról szóló 1995. évi CXXV. törvényben (Nbtv.) foglaltak szerint a titkos információgyűjtés külső engedélyezése a nemzetbiztonsági szolgálatok esetében is tartozhat IM jogkörbe.

A per lényeges kérdése volt, hogy milyen független külső kontrollmechanizmusok révén ellenőrizhető Magyarországon a titkos információgyűjtés jogszerűsége. Sem az EJEB, sem a magyar államot képviselő minisztérium nem vonta be a Hatóságot a tényállás tisztázásába, illetve a vonatkozó magyar joganyag összegyűjtésébe, ezért nem volt mód arra, hogy a Hatóság a magyar álláspont

védelmében ismertesse a nemzetbiztonsági szolgálatok titkos információgyűjtő tevékenységének független külső ellenőrzése során nyert jogalkalmazási tapasztalatait. Sajnálatos módon elsikkadt az, hogy az Alaptörvény szerint a személyes adatok védelméhez és a közérdekű adatok megismeréséhez való jog érvényesülését ellenőrző, sarkalatos törvénnyel létrehozott, független hatóság a Nemzeti Adatvédelmi és Információszabadság Hatóság, amely az Infotv.-ben meghatározott keretek között jogosult a nemzetbiztonsági szolgálatok által Magyarország területén végzett valamennyi titkos információgyűjtő tevékenység ellenőrzésére.

Az Infotv. megfelelő eszközöket biztosít a Hatóság számára a jogsértő titkos információgyűjtés feltárására és a jogsértéssel szembeni fellépésre. A vizsgálati eljárás (Infotv. 52.-58. §-ai) szabályai az ombudsmani eljáráshoz hasonlóan erőteljes betekintési, másolatkérési, adat-megismerési, belépési, felvilágosítás-kérési és vizsgálat kezdeményezési jogosultságokat biztosítanak. Az Infotv. 71. § olyan szabályokat tartalmaz, amelyek kifejezetten a nemzetbiztonsági szolgálatokat érintő eljárások esetén is lehetővé teszik a Hatóság számára a szükséges adatok megismerését.

A Hatóság a vizsgálati eljárásban megismert adatokat – beleértve a nemzeti minősített adatokat is – felhasználhatja adatvédelmi hatósági eljárásban és például megtilthatja a személyes adatok jogellenes kezelését, elrendelheti a jogellenesen kezelt személyes adatok megsemmisítését, elrendelheti az érintett tájékoztatását, ha azt az adatkezelő jogellenesen tagadta meg, valamint bírságot szabhat ki.

A Hatóság a jogalkalmazási gyakorlatában abból indul ki, hogy a titkos megfigyelés jellegénél fogva megfosztja az adatalanyt a közvetlen jogorvoslat lehetőségétől, ezért e területen a független külső adatvédelmi ellenőrzés az információs magánszféra-védelem kulcseleme. Ennek megfelelően a Hatóság minden, az állampolgároktól érkező, titkos megfigyelésre vonatkozó panaszt, bejelentést kivizsgál, attól függetlenül, hogy a beadványban leírt körülmények utalnak-e titkos információgyűjtésre, illetve az érintett az eljárás eredményéről tájékoztatható-e.

A titkos információgyűjtés előzetes külső engedélyezési rendszerének átalakítása esetén többféle szabályozási modell érvényesülhet. A külső kontroll függetlensége és a közjogi-hatalommegosztási elvek szempontjából kifogástalan megoldást eredményezne, ha a jelenleg az IM-hez tartozó külső engedélyezési hatáskör a bírósághoz kerülne.

Az Ítélet megenged olyan értelmezést is, amely szerint a miniszter előzetes engedélyezési jogköre megmarad. Egy korábbi adatvédelmi vizsgálat eredményei arra

utaltak, hogy az IM külső engedélyezési eljárásai során az egyszemélyi döntési felhatalmazás ellentétbe kerülhet a megalapozott döntéshozatal követelményével. A nemzetbiztonsági szolgálatok főigazgatói évről évre olyan nagyszámú előterjesztést nyújtanak be, amelyeket egy személy – a miniszter – nem képes kellő mélységgel áttekinteni az engedélyről hozandó döntése előtt. Ezért ha a jogkör továbbra is miniszteriális keretek között marad, úgy célszerű lenne létrehozni egy olyan bizottságot, amelynek az lenne a feladata, hogy törvényességi és szükségességi szempontból szűrje az előterjesztéseket és javaslatot tegyen azok engedélyezhetőségéről. E bizottságban a titkos információgyűjtés törvényességében érdekelt kormányzati szervezetek (például: BM, nemzetbiztonsági szolgálatok) által delegált, a szükséges speciális nemzetbiztonsági ismeretekkel rendelkező szakértők vennének részt. E bizottság tehát nem független, külső kontrollt valósítana meg, hanem a döntések előkészítésében venne részt.

Az Ítéletben foglaltakra tekintettel a miniszteri külső engedélyezési jogkör fenntartása esetén elengedhetetlenül szükséges azt független külső kontroll alá helyezni. Közjogi szempontból nincs akadálya annak, hogy e szerepkört a Hatóság töltse be, amely az Alaptörvényben meghatározott független adatvédelmi ellenőrző hatóság, és amelynek feladatkörébe a titkos információgyűjtés jogszerűségének utólagos ellenőrzése egyébként is beletartozik.

VII. Titokfelügyelet, a minősített adatokat érintő eljárások

VII.1. A Nemzetbiztonsági Szakszolgálat adatvédelmi auditálása

A Nemzetbiztonsági Szakszolgálat (NBSZ) főigazgatója még 2015-ben kezdeményezte, hogy a Hatóság adatvédelmi audit keretében vizsgálja az NBSZ nemzetbiztonsági szolgálatokról szóló 1995. évi CXXV. törvény (Nbtv.) 8. § (1) bekezdés a) pontjában meghatározott szolgáltató tevékenységét és az ahhoz kapcsolódó adatkezelést. (Az Nbtv. 8. § (1) bekezdés a) pontja szerint az NBSZ „*a jogszabályok keretei között a titkos információgyűjtés, illetve a titkos adatszerzés eszközeivel és módszereivel – írásbeli megkeresésre – szolgáltatást végez a titkos információgyűjtésre, illetve a titkos adatszerzésre feljogosított szervek titkos információgyűjtő, valamint titkos adatszerző tevékenységéhez*”.)

A Hatóság a felkérést elfogadta, ám a feladat végrehajtására való felkészülés során észleltük, hogy az audit tárgya olyannyira eltér a Hatóság által auditált adatkezelésektől, hogy ha ebben az esetben is a korábbiakban jól bevált audit módszert alkalmaztuk volna, akkor az ellenőrzés valószínűleg megmaradt volna a felszínes általánosságok szintjén anélkül, hogy a titkos információgyűjtés adatvédelmi szempontból releváns sajátosságait figyelembe vette volna. Sőt, az is kiderült, hogy nem áll rendelkezésre olyan formalizált módszer, amellyel egy nemzetbiztonsági szolgálat titkos információgyűjtő tevékenységének átfogó adatvédelmi ellenőrzése elvégezhető lenne. Tudomásunk szerint még sosem került sor arra, hogy egy adatvédelmi hatóság átfogó jelleggel, a gyakorlatban ellenőrizze egy titkosszolgálat titkos információgyűjtő tevékenységét.

Az előkészületek során a Hatóság számos alkalommal konzultált az NBSZ kijelölt szakértőivel, továbbá előzetesen elemezte az NBSZ titkos információgyűjtéssel kapcsolatos belső normáit. Az előzetes adatgyűjtés, valamint az igények és lehetőségek számbavételét követően a Hatóság az NBSZ szakértőivel együttműködve kidolgozta azt a módszert, amely a jogszabályi előírások maradéktalan betartása mellett alkalmas a titkos információgyűjtő tevékenység komplex adatvédelmi ellenőrzésére.

A Hatóság koncepcionális alapvetése az volt, hogy a titkos információgyűjtés adatvédelmi megítélése szempontjából lényeges momentumok jelentős része az

eszközök és módszerek gyakorlati alkalmazása során jelentkezik, ezért az átfogó ellenőrzés módszerének is gyakorlatorientáltnak kell lennie. A szóban forgó adatvédelmi audit precedensjellege okán a tervezés és a megvalósítás során a „*vagy jól, vagy sehogy*" elvet tartottuk szem előtt.

Módszertani követelményként a következő elveket határoztuk meg:

Komplexitás: Az adatvédelmi auditnak át kell fognia a titkos információgyűjtéssel kapcsolatos szolgáltató tevékenység teljes folyamatát a szolgáltatás megrendelésétől kezdve annak végrehajtásán és a megszerzett információk feldolgozásán, és a megrendelő szerv számára történő átadásán keresztül egészen az adatok törléséig. Az adatvédelmi audit tárgykörébe tartozik az NBSZ valamennyi, adatvédelmi szempontból releváns szolgáltatása. Ugyanakkor nem tárgya az auditnak az NBSZ *„back office"* működése, azaz az egyes szervezeti egységek közötti kapcsolatrendszer vagy a szolgáltatások megszervezésének belső részletei.

Együttműködés: Az NBSZ és a Hatóság együttműködésének elvi alapja az állam Alaptörvényben rögzített kötelezettsége az alapvető jogok tiszteletben tartására és védelmére. A titkos információgyűjtés eszközeinek és módszereinek alkalmazása olyan speciális, védett ismeretanyagot feltételez, amely csak az adatkezelő együttműködése esetén tárható fel az adatvédelmi audit végrehajtásához szükséges mértékben.

Átláthatóság: Az audit eredményessége érdekében az NBSZ-nek olyan speciális, titkosszolgálati tudásanyagba kell betekintést engednie, amely titkosságának fenntartása a nemzetbiztonsági szolgálatok rendeltetésszerű működésének és ezáltal Magyarország nemzetbiztonsági érdekei érvényesítésének alapvető feltétele, ezért alapvető elvárás, hogy teljesen transzparens legyen az NBSZ számára a Hatóság audit során végzett tevékenysége. Mind a Hatóság, mind az NBSZ dokumentálja az adatvédelmi audit során elvégzett tevékenységeket és a tapasztalatokat.

Adatvédelem, titokvédelem:

- Az adatvédelmi audit során nem használhatók fel a nemzetbiztonsági szolgálat konkrét ügyben végzett műveleti tevékenységére vonatkozó, illetve annak során keletkezett információk, mert erre sem az Infotv., sem az Nbtv. nem ad felhatalmazást.
- A titkos információgyűjtés eszközeinek és módszereinek ellenőrzéséhez csak az érintett személy előzetes, önkéntes és tájékozott felhatalmazása alapján használható fel személyes adat.

– Az audit során a Hatóság nem ismerhet meg olyan adatot, amelynek kezelésére az Infotv. 71. § értelmében nem jogosult, vagy amelynek ismerete az adatvédelmi ellenőrzéshez nem szükséges.
– A konkrét biztonsági, titokvédelmi és információvédelmi előírásokat előzetesen tisztázni és írásban rögzíteni kell. A feleknek gondoskodniuk kell arról, hogy az adatvédelmi audit során a munkatársak megismerjék és betartsák azokat.

A titkos információgyűjtés adatvédelmi auditálásához kidolgozott módszer lényege az, hogy az NBSZ a Hatóság által megtervezett kísérleti szituációkban, a valóságoshoz lehetőség szerint minél inkább hasonló körülmények között hajtsa végre a titkos információgyűjtéssel kapcsolatos szolgáltató tevékenységét.

A tesztek a titkos információgyűjtés valamennyi, az Nbtv. 56. §-ában felsorolt, külső engedélyhez kötött eszközére és módszerére kiterjedtek, valamint a külső engedélyt nem igénylő eszközök és módszerek közül azokra, amelyek a személyes adatok védelme szempontjából relevánsak. (De például teszt fedőintézmény létrehozására nem került sor.) A teszt szituációkat úgy alakítottuk ki, hogy az NBSZ a teszt végrehajtása során minden alkalommal valamilyen előre meghatározott, adatvédelmi szempontból lényeges kérdésben döntési helyzetbe kerüljön. A teszt szituációk megtervezésekor nem elégedtünk meg a titkos információgyűjtés során tipikusan előforduló helyzetek modellezésével, hanem valós körülmények között esetleg csak ritkán előadódó helyzetek tesztelését is felvettük az audit terv teszt katalógusába, ha az adott teszttel valamilyen adatvédelmi szempontból fontos követelmény érvényesítését lehetett ellenőrizni. Az azonban nem volt célunk, hogy a valóságos körülményektől teljesen elrugaszkodott teszt helyzeteket kreáljunk.

Az adatvédelmi követelményrendszer egyes elemeit, mint például a célhoz kötött adatkezelés követelményét, az adatminimalizálás elvét, az adatok minőségére és időszerűségére vonatkozó előírások érvényesülését az NBF tevékenységének többféle metszetében is vizsgáltuk a tesztek során:

– A titkos információgyűjtés egyes munkafázisaival összefüggésben (a megrendelés előzetes ellenőrzése, a titkos információgyűjtés végrehajtására való felkészülés, a szolgáltatás végrehajtása, az információk feldolgozása és végül a megrendelő szervhez történő eljuttatása).
– A titkos információgyűjtés egyes eszközeinek és módszereinek sajátosságaival összefüggésben (például adott eszköz vagy módszer mennyiben automatizálható, alkalmazható-e tömegesen, mennyire fókuszálható a

titkos információgyűjtés céljának eléréséhez szükséges helyszínre, személyre vagy személyi körre, időkeretek közé, adatkörre stb.).
- A megrendelő/szolgáltató kapcsolatrendszerében (például az NBSZ adatkezelőként vagy adatfeldolgozóként végzi a feladatait, mennyiben képes az adatkezelés jogszerűsége szempontjából kontrollfunkciót betölteni stb.).
- Az NBSZ szolgáltatási portfoliójának összevetése a titkos információgyűjtés Nbtv.-ben meghatározott eszközeivel és módszereivel. Lényeges, hogy mennyire pontosan határozza meg az Nbtv. az adott tevékenységet, egyértelmű-e annak elhelyezése a titkos információgyűjtés törvényben meghatározott eszközeinek és módszereinek rendszerében, világosan elhatárolható-e más eszközöktől és módszerektől, stb.

A tesztek végrehajtására való felkészülés gondos szervezést és felkészülést igényelt mind az NBSZ, mind a Hatóság részéről. A tervezés során a Hatóság figyelembe vette az NBSZ tesztek sorrendjére és végrehajtásuk időzítésére vonatkozó javaslatait és a két szervezet szakértői közösen pontosították az egyes tesztek végrehajtásának részleteit. A teszt terveket csak az NBSZ kijelölt kapcsolattartói ismerhették meg, akik titoktartási kötelezettséget vállaltak. Az előkészítést gördülő tervezéssel oldottuk meg úgy, hogy az adott titkos információgyűjtés szakterület ellenőrzése közben már a következő szakterület tesztjeinek előkészítése zajlott.

Általában a Hatóság biztosította a teszt szituációkban felhasznált eszközöket, felszereléseket, anyagokat. A Hatóság munkatársai alakították a teszt szituációkban a célszemélyeket, valamint a titkos információgyűjtés során képbe kerülő egyéb személyeket, továbbá a szolgáltatást megrendelő szervezet (rendszerint a fiktív Polgári Felderítő Szolgálat) tisztjeit.

Az NBSZ biztosította a titkos információgyűjtés speciális technikai eszközeit, amelyeket a tesztek során a munkatársaik alkalmaztak. A tesztekben résztvevő NBSZ munkatársak tudtak arról, hogy egy adatvédelmi audit eljárásról van szó, de csak annyi előzetes instrukciót kaptak, hogy mindent csináljanak pontosan úgy, ahogyan máskor. Az adott teszt konkrét céljáról és a tesztben vizsgált adatvédelmi kérdésről nem kaptak előzetes tájékoztatást.

A Hatóság csak olyan munkatársait vonta be a tesztek végrehajtásába, akik rendelkeznek személyi biztonsági tanúsítvánnyal és titoktartási nyilatkozatot tettek, valamint előzetes eligazítást kaptak a nemzetbiztonsági szolgálatok tevékenységével és objektumaival kapcsolatos biztonsági előírásokról. A célszemélyeket

és a titkos információgyűjtés során képbe kerülő harmadik személyeket alakító kollégáink írásban hozzájárultak ahhoz, hogy a tesztek során az NBSZ a titkos információgyűjtés eszközeivel és módszereivel rögzítse a személyes adataikat. Az egyes tesztek végrehajtása előtt minden NAIH munkatárs részletes forgatókönyvet kapott az adott teszthez tartozó szerepköréről (például helyszíni irányító, célszemély, járókelő, kapcsolattartó, telefonon felhívott ismerős, stb.) és konkrét feladatairól, amelyeket előzetesen megtanult, elpróbált és lehetőség szerint begyakorolt.

Egyebekben a tesztek technikai feltételeinek kialakítása az éppen vizsgált speciális eszköz vagy módszer sajátosságaihoz igazodott. Például amíg a postai küldemény csomagforgalomból való kiemelésének és átvizsgálásának tesztelése során csak a megfelelően preparált postai küldeményt kellett előkészíteni, addig a telefonlehallgatás adatvédelmi ellenőrzéséhez egy kizárólag az adatvédelmi audit céljára szolgáló, a Hatóság informatikai rendszerétől teljesen elválasztott elektronikus hírközlési tesztkörnyezetet hoztunk létre, amely a Hatóság épületében telepített telefon alközpontból és belső vezetékes hálózatból, valamint a tesztek végrehajtásához beszerzett mobiltelefon készülékekből állt. Így biztosak lehettünk abban, hogy az adatvédelmi audit során éles körülmények között modellezett telefonlehallgatások nem sérthetik a Hatóság ügyfelekkel folytatott kommunikációjának bizalmasságát.

A tesztek helyszínét az NBSZ és Hatóság közösen választotta ki. A tesztkörnyezetek néhány esetben az NBSZ objektumaiban lettek kialakítva, míg máskor a Hatóság épületében vagy egy budapesti szállodában. A külső tesztkörnyezeteket úgy választottuk meg, hogy a speciális eszközök alkalmazása során kívülálló harmadik személyek adatai ne kerülhessenek rögzítésre.

A Hatóság a valóságoshoz hasonló körülmények között vizsgálta az NBSZ titkos információgyűjtéssel kapcsolatos eljárásainak teljes folyamatát. Minden teszt úgy indult, hogy a Hatóság a nem létező Polgári Felderítő Szolgálat nevében átadta az NBSZ-nek az adott teszt fiktív tényállásának megfelelő megrendelés dokumentációját, beleértve a fiktív adatokkal kitöltött szolgálati jegyeket és a külső engedélyhez kötött titkos információgyűjtés esetén a fiktív külső engedélyt is. A tesztek előkészítése és végrehajtása során az NBSZ mindenben úgy járt el, mint az Nbtv. 8. § (1) bekezdés a) pontja szerinti szolgáltató tevékenysége során. A tesztek végrehajtását az NBSZ kijelölt munkatársa jegyzőkönyvben dokumentálta. (Ez egyébként a Hatóság feladata lenne, de csak így lehetett megoldani, hogy ne jusson a tudomásunkra olyan, a tesztek végrehajtásához egyébként sem szükséges információ, amelyet a Hatóság az Infotv. 71. §-ában foglaltak értel-

mében nem jogosult megismerni.) Ugyanakkor a Hatóság munkatársai az adott teszthez készített feljegyzésben dokumentálták azt, ha a Polgári Felderítő Szolgálat tisztjeként egyeztettek az NBSZ munkatársaival vagy például soron kívüli *„műveleti tájékoztatást”* kaptak a fiktív titkos információgyűjtésről. Ilyen módon az NBSZ és a megrendelő szervezet közötti kommunikáció és interakció is teljes körűen ellenőrizhetővé vált.

Az NBSZ a tesztek során ugyanúgy gyűjtötte, rögzítette, és dolgozta fel az információkat, mint amikor *„élesben”* végzi a szolgáltató tevékenységet. A titkos információgyűjtés tesztek eredményeként a Hatóságnak átadott dokumentációk jellegüket (például jegyzőkönyv, képfelvétel, hangfelvétel, szakértői vélemény, stb.) az információk feldolgozottságát, az adattartalmukat és formátumukat tekintve ugyanolyanok voltak, mint a tényleges titkos információgyűjtések esetében.

A 2016 áprilisa és 2017 február közötti időszakban 34 titkos információgyűjtés teszt végrehajtására került sor. A tesztek kiértékelése 2017-ben történt, ezért arról a 2017. évi beszámolóban fogunk számot adni, már amennyire az az adatvédelmi audit eljárásra vonatkozó törvényi korlátozások, valamint a titokvédelmi előírások betartása mellett lehetséges. Előzetesen csak annyit jegyzünk meg, hogy az audit messzemenően visszaigazolta az NBSZ elkötelezettségét az adatkezelés törvényességét illetően, ugyanakkor a tesztek a titkos információgyűjtéssel kapcsolatos tevékenységek néhány olyan részletét is feltárták, amelyekkel kapcsolatban a Hatóság az adatvédelmi követelmények magas szintű érvényesítése érdekében észrevételekkel és javaslatokkal élt.

Az eredmények alátámasztják az NBSZ adatvédelmi auditálása során alkalmazott módszer létjogosultságát, mert a gyakorlatorientált tesztek olyan, adatvédelmi szempontból releváns részletekre is rávilágítottak, amelyeket a hagyományos audit módszerrel (kérdőív, interjú, belső szabályzatok elemzése) nem lehetett volna feltárni.

VII.2. A titokfelügyeleti eljárások tapasztalatai

Jóllehet 2016-ban az NBSZ adatvédelmi auditálása nagymértékben lekötötte a Hatóság titokfelügyeleti ügyintézési kapacitását, a korábbi évekhez hasonló számban érkeztek minősített adatot érintő bejelentések, amelyek között az adatvédelemre és az információszabadságra vonatkozó panaszok egyaránt voltak. A Hatóság a beadványok többségét a vizsgálati eljárás keretei között intézte,

mert nem álltak fenn a titokfelügyeleti hatósági eljárás megindításának feltételei (Az Infotv. 62. § (1) bekezdése szerint: ha a Hatóság vizsgálata alapján vagy egyébként valószínűsíthető, hogy a nemzeti minősített adat minősítése jogellenes, a Hatóság titokfelügyeleti hatósági eljárást indíthat.)

A 2016-os tapasztalatok alapján a Hatóság azt feltételezi, hogy a jövőben évente várhatóan 6-7 esetben kerül majd sor titokfelügyeleti hatósági eljárás indítására az Infotv. 31. § (6a) bekezdésében foglaltak alapján a bíróság kezdeményezésére. A 2016-ban indult titokfelügyeleti hatósági eljárások közül a Seuso kincs repatriálása kapcsán megkötött ügyvédi megbízás minősítése tárgyában indult eljárás fejeződött be. Az eljárás során a Hatóság megkereste a minősítőt a minősítés részletes indokolása és az iratmásolatok megküldése tárgyában. A minősítő ezt követően felülvizsgálta és megszüntette a szóban forgó iratok minősítését, amelyet azóta már nyilvánosságra hoztak. Erre tekintettel a Hatóság a titokfelügyeleti hatósági eljárást végzéssel megszüntette.

A 2016-ban befejeződött eljárások közül említést igényelnek még a következők:

Az egyik ügyben a minősítő az adat keletkezését követően évekkel később döntött az adat minősítéséről. A Hatóság ezzel kapcsolatban arra hívta fel a figyelmet, hogy az adat minősítését az adat keletkezését követően késedelem nélkül végre kell hajtani, ha annak törvényben meghatározott feltételei fennállnak, ugyanis az esetleges késlekedés a közérdekű adatok megismeréséhez való jog sérelméhez vezethet, továbbá a demokratikus jogállamiság részét képező jogbiztonság sérelmével is járhat.

A Mavtv. 6. § (1) bekezdése előírja a minősítés kezdeményezését annak számára, akinél a minősített adat ismérveinek megfelelő adat keletkezik. A Mavtv. nem állapít meg határidőt arra vonatkozóan, hogy az adat keletkezésétől számított mennyi idő alatt kell a minősítést kezdeményezni, ám belátható, hogy erre ésszerű határidőn belül sort kell keríteni.

A minősítési eljárás késedelmes lefolytatása sérti a közérdekű adat megismeréséhez való jog érvényesülését, mert végső soron meghosszabbodik az adat keletkezésétől a közérdekű adat megismerhetővé válásáig (a minősítés megszűnéséig) terjedő időtartam. Ha az adatot kezelő szerv megfelelő indok nélkül késlekedik a minősítési eljárás kezdeményezésével és a minősítéssel, úgy szándékos jogsértés lehetősége feltételezhető. (Más ügyekben szerzett tapasztalataink szerint előfordult már olyan is, hogy a minősítő egészen addig kivárt a minősítéssel, amíg adatigény érkezett a közérdekű adat megismerése iránt.)

Azt is érdemes figyelembe venni, hogy ha a minősítésre később kerül sor, akkor kérdéses, hogy az adat keletkezése és a minősítési eljárás megkezdése közötti időben ténylegesen ki fért hozzá az adatokhoz. A minősített adatok kezelésére és védelmére vonatkozó szigorú ügykezelési szabályokat csak a minősítés kezdeményezését követően kell alkalmazni. Ha minősített adat illetéktelen személyhez kerül, akkor utólag már alig lehet bizonyítani azt, hogy az adat megszerzésére:

– az adat keletkezése és a minősítés kezdeményezése közötti időszakban, vagy
– a minősítés kezdeményezését követően

került sor.

A minősített adattal való visszaélést csak a minősítési eljárás kezdeményezését követően lehet elkövetni, ezért a jogbiztonság szempontjából is elfogadhatatlan az olyan minősítési eljárási gyakorlat, amely lehetővé teszi azt, hogy később minősítendő adatokat hosszú ideig a nem minősített adatokkal és iratokkal együtt kezeljenek. Ha az adat a keletkezését követően akárcsak ideiglenesen, illetve csak részlegesen is kikerült az adatot keletkeztető szerv birtokából, úgy azt utólag már nem lehet jogszerűen minősíteni.

Egy másik ügyben azért fordult a Hatósághoz egy bejelentő, mert az Alkotmányvédelmi Hivatal (AH) megtagadta a tájékoztatást a nemzetbiztonsági ellenőrzése során összegyűjtött, rá vonatkozó nemzetbiztonsági kockázati tényezőt nem tartalmazó adatokról. A Hatóság vizsgálatot indított, amelynek során több alkalommal, az AH objektumában vizsgálta az érintett nemzetbiztonsági ellenőrzése során keletkezett iratanyagot és a rendelkezésre álló iratkezelési segédletek, valamint az AH munkatársaitól kért szóbeli felvilágosítás alapján az iratok kezelését, beleértve a korábban elvégzett iratselejtezések jogszerűségét, továbbá a nemzetbiztonsági ellenőrzésre és az iratkezelésre vonatkozó AH belső normák tartalmát.

A Hatóság a vizsgálat eredményeként megállapította, hogy az AH főigazgatója az Infotv. 19. §-ában, valamint az Nbtv. 48. §-ában foglaltakkal összhangban, nemzetbiztonsági érdekből korlátozta az érintett tájékoztatáshoz való jogát. A korlátozás oka az, hogy a nemzetbiztonsági ellenőrzés iratainak megismerése esetén rekonstruálható lenne a nemzetbiztonsági ellenőrzés részletes tartalma és eljárásrendje. A nemzetbiztonsági ellenőrzés részletes szabályainak titokban tartásához nemzetbiztonsági érdek fűződik, mert ha ezek nyilvánosságra kerülnének, az veszélyeztetné a nemzetbiztonsági ellenőrzések eredményességét. Ezért az érintettek tájékoztatási jogának korlátozása olyan esetben is jogszerű, ha a nemzetbiztonsági ellenőrzés nem tárt fel kockázati tényezőt.

A Hatóság a tájékoztatási jog korlátozásának jogszerűségétől függetlenül azt is vizsgálta, hogy jogszerű volt-e a nemzetbiztonsági ellenőrzés során végzett adatkezelés. A vizsgált ügyben a nemzetbiztonsági ellenőrzést az AH jogelődje, a Nemzetbiztonsági Hivatal (NBH) végezte. A Hatóság a bejelentő nemzetbiztonsági ellenőrzéséről azt állapította meg, hogy az kizárólag annak megállapítására irányult, hogy az érintettel kapcsolatosan nemzetbiztonsági kockázat fennáll-e. Az adatgyűjtés mélysége összhangban volt az érintett által betöltött, az akkori terminológia szerint *„fontos és bizalmas"* jogviszony jellegével. A nemzetbiztonsági ellenőrzés során szükségtelen, az érintett személyes adatai védelméhez való jogát sértő adatgyűjtés nem történt. Az NBH az ellenőrzésről összefoglaló jelentést készített, amely az ellenőrzés során gyűjtött adatokkal összhangban álló következtetéseket fogalmazott meg. Ez alapján került sor a kockázati tényezőt nem tartalmazó biztonsági szakvélemény kiállítására.

A nemzetbiztonsági szakvélemény elkészítése és a Hatóság vizsgálata közötti időszakban a nemzetbiztonsági ellenőrzés iratanyagának egy részét selejtezték. A selejtezés az AH belső iratkezelési előírásaival összhangban történt.

VII.3. A kétoldalú titokvédelmi egyezmények véleményezése

A minősített adat védelméről szóló 2009. évi CLV. törvény (Mavtv.) megkülönbözteti egymástól a nemzeti minősített adatokat és a külföldi minősített adatokat. A nemzeti minősített adat olyan adat, amelyet magyar közfeladatot ellátó szerv készített és minősített. A külföldi minősített adat ezzel szemben olyan adat, amelyet az Európai Unió valamennyi intézménye és szerve, továbbá az Európai Unió képviseletében eljáró tagállam, a külföldi részes fél vagy nemzetközi szervezet által készített és minősített. A két kategória közötti különbségtétel azért lényeges, mert amíg a nemzeti minősített adat esetében annak minősítése a közérdekű adat megismeréséhez való jog érvényesülését korlátozza, addig a külföldi minősített adat esetében a törvényi szabályozás tulajdonképpen azt az elvet érvényesíti, hogy ezek az adatok nem lehetnek a közérdekű adat megismeréséhez való jog tárgyai. A Hatóság ellenőrzési és titokfelügyeleti hatósági jogköre is csak a nemzeti minősített adatokra terjed ki, a külföldi minősített adatokra azonban nem. A külföldi minősített adatok magyarországi szerv általi átvétele esetén a külföldi minősített adatokkal való rendelkezési jog továbbra is a külföldi minősítőt illeti meg. Az adatot átvevő magyar szerveknek az a feladata, hogy a külföldi minősített adat védelméről gondoskodjanak. Erre Magyarország nemzetközi egyezményekben vállal kötelezettséget.

A fentiek értelmében fontos, hogy a titokvédelmi egyezmények világosan elkülönítsék egymástól a nemzeti és a külföldi minősített adatokat, valamint az azokra vonatkozó rendelkezési jogköröket. Ebből a szempontból problematikus, hogy 2016 óta több olyan kétoldalú nemzetközi titokvédelmi egyezmény előkészítése történt meg, amely közös, konszenzuális rendelkezési jogkört biztosít a feleknek az együttműködésük során létrejött adatok minősítésével kapcsolatban.

A Hatóság álláspontja szerint a felek együttműködésében a két fél szervei vesznek részt. E szervek a saját államuk szabályai szerint keletkeztetnek minősített adatot. Az államok közötti kétoldalú együttműködés ugyanis nem mossa el az államok joghatósága közötti határvonalakat és nem hoz létre a két államtól független szervezeti, illetve jogrendet. A kétoldalú nemzetközi titokvédelmi megállapodások túlnyomó többsége arra az elvre épül, hogy a részes államok maguk rendelkeznek az együttműködés során rendelkezésre bocsátott adataikkal. Ez az elv összhangban van az állami szuverenitással és nemzetközi kapcsolatok általános rendezőelveivel.

Az együttműködés során keletkezett adatok esetében a minősítés felülvizsgálatának és megszüntetésének a felek kölcsönös egyetértéséhez való kötése hátrányos a közérdekű adatok nyilvánossága szempontjából, mert ennek alapján a külföldi fél olyankor is megakadályozhatja a minősítés felülvizsgálatát és megszüntetését, amikor az a magyar jog szerint kötelező lenne. Különösen problematikus, ha a titokvédelmi egyezmény nem határozza meg a minősítés megszüntetésének anyagi jogi feltételeit, mert ennek az lehet a következménye, hogy az egyezményben részes felek valamelyike esetleg politikai megfontolás alapján, vagy egyéb, jogon kívüli okból megakadályozhatja az együttműködés során keletkezett adat minősítésének megszüntetését a másik országban is. A kifogásolt szabály nincs összhangban a Mavtv.-vel sem, ugyanis a Mavtv. nem teszi lehetővé a minősítői jogkör külföldi szervvel való megosztását.

VII.4. A Nemzeti Biztonsági Felügyelettel folytatott szakmai konzultáció

A minősített adatok kezelésével kapcsolatban Magyarországon két szervezet rendelkezik hatósági jogkörrel. A Hatóság a személyes adatok védelméhez, valamint a közérdekű és a közérdekből nyilvános adatok megismeréséhez való jog érvényesülésének ellenőrzése és elősegítése céljából az Infotv.-ben meghatározottak szerint vizsgálati vagy titokfelügyeleti eljárást folytat. A másik szervezet

a Nemzeti Biztonsági Felügyelet (NBF), amelynek feladata a Mavtv. 20. § (1) bekezdése szerint a minősített adat védelmének hatósági felügyelete, a minősített adatok kezelésének hatósági engedélyezése és felügyelete, valamint a telephelyi iparbiztonsági hatósági feladatok ellátása. A két szervezet feladatkörének elhatárolása érdekében az Infotv. 62. § (1b) bekezdése úgy rendelkezik, hogy a Hatóság titokfelügyeleti hatósági eljárása az NBF Mavtv.-ben meghatározott feladatait nem érinti. A másik oldalról a 20. § (2) bekezdés r) pontja szerint az NBF együttműködik a Hatósággal a közérdekű adatok megismeréséhez fűződő alkotmányos jog tiszteletben tartása és az információszabadság érvényesülése érdekében. E szabályok alapján a két szervezet feladat- és hatásköre világosan elhatárolható, ugyanakkor a szabályozás megteremti a szervezetek közötti szakmai együttműködés jogi feltételeit. Ez utóbbi azért szükséges, mert mind alapjogvédelmi szempontból, mind a jogbiztonság, mind a minőségi jogalkalmazás szempontjából lényeges, hogy a két szervezet összehangolt, egyeztetett jogértelmezésen alapuló joggyakorlatot folytasson. Ennek érdekében a két szervezet szakértői időről időre egyeztetéseket tartanak, amelyeken a minősítéssel, illetve a minősített adatok kezelésével kapcsolatos jogi követelményeket veszik sorra. A 2016-ban folytatott szakmai eszmecseréken egyebek mellett a következő kérdések kerültek terítékre:

A Mavtv. 4. § (3) bekezdése felhatalmazza az ott felsorolt beosztásokat betöltő minősítőket arra, hogy a minősítői jogkörüket belső szabályzatban az alárendeltségükbe tartozó, vezetői megbízással rendelkező, illetve vezetői beosztásba kinevezett más személyre és a minősített adat felülvizsgálatába bevont felülvizsgálati szakértőre írásban átruházzák. Ezzel kapcsolatban a Hatóság és az NBF a konzultáció eredményeként egyetértett abban, hogy a minősítő csak a minősített adat felülvizsgálatával kapcsolatos jogkörét ruházhatja át a felülvizsgálati szakértőre. A minősítő más jogköreinek felülvizsgálati szakértőre való átruházására nem kerülhet sor. A jogkör átruházásakor írásban, pontosan meg kell jelölni, hogy a jogkör átruházása mire (például milyen legfeljebb minősítési szintű adatokra, illetve milyen minősített iratanyagra) vonatkozik és mi a határideje. A jogkör átruházása nem jelenti azt, hogy a minősítőnek erre az időre megszűnne a felülvizsgálati jogköre. A minősítő jogosult a felülvizsgálati szakértő átruházott jogkörben meghozott felülvizsgálati döntését felülbírálni. A felülvizsgálati jogkör átruházása megszűnik a határidő elteltével, de a minősítő ezt megelőzően is bármikor jogosult a felülvizsgálati jogkör Mavtv. 4. § (3) bekezdése szerinti átruházását megszüntetni. A felülvizsgálati jogkör átruházásának megszüntetésére ugyanolyan formai és tartalmi követelmények vonatkoznak, mint e jogkör átruházására.

A Mavtv. 8. § (1) bekezdése is lehetővé teszi a felülvizsgálati szakértő igénybevételét, ám a Mavtv. 4. § (3) bekezdésétől eltérően ebben az esetben a felülvizsgálati szakértő nem rendelkezik felülvizsgálati döntési jogkörrel, hanem kizárólag minősített adat felülvizsgálati döntés-előkészítést végez a minősítő számára. További eltérések a Mavtv. 4. § (3) bekezdésében foglaltakhoz képest:

- A 8. § (1) bekezdése alapján bármely minősítő igénybe vehet felülvizsgálati szakértőt, míg a 4. § (3) bekezdése alapján csak az ott megjelölt beosztásokat betöltő minősítők.
- A 8. § (1) bekezdése esetén nem szükséges (de nem is kizárt) belső szabályzatban utalni a felülvizsgálati szakértőre.

A Mavtv. 5. § (7) bekezdése lehetőséget ad a minősítés meghosszabbítására az ott meghatározott, minősítési szint szerint differenciált feltételekkel. Lényeges szem előtt tartani, hogy a minősítés meghosszabbítására (a Mavtv.-ben meghatározott feltételek fennállása esetén) egy megismételt minősítési eljárás keretében kerülhet sor. A minősítés meghosszabbítása esetén a meghosszabbítás Mavtv.-ben meghatározott maximális időtartamát a minősítés meghosszabbítására vonatkozó döntés időpontjától kell számítani.

A minősítő a Mavtv.-ben előírt rendszeres felülvizsgálati kötelezettsége a minősítés meghosszabbítását követően is fennáll.

VIII. Nemzetközi ügyeink

VIII.1. A NAIH nemzetközi szerepvállalásai

Az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény 38. § (4) bekezdés e) pontja alapján a NAIH törvényben meghatározott szervekkel vagy személyekkel együttműködve képviseli Magyarországot az Európai Unió közös adatvédelmi felügyelő testületeiben. A nemzetközi kapcsolattartás és az európai adatvédelem fő szereplői közé tartoznak a nemzeti adatvédelmi hatóságok, az Európai Adatvédelmi Biztos és az Európa Tanács, melyekkel a NAIH napi szinten együttműködik.

VIII.2. Budapesti Tavaszi Konferencia

A Bevezetőben már említettük a Budapesti Tavaszi Konferenciát http://www.naih.hu/budapest-springconf/, mint 2016 kiemelkedő nemzetközi eseményét. 1991 óta minden évben összegyűlnek az európai adatvédelmi hatóságok az aktuális és közös szakmai kérdések megvitatására. A konferencia tagjai formális akkreditáció útján nyernek felvételt, az esemény nyitó része sajtó nyilvános, de ezt követően a tanácskozás zártkörű, azon csak a regisztrált tagok és meghívott előadók, valamint a fogadó szervezet szakértői vehetnek részt. 2006 után 2016. május 26-27-én ismét Budapest – vagyis a NAIH – látta vendégül a több, mint 100 regisztrált résztvevőt.

A Budapesten megvitatott két fő téma a nemzetbiztonsági szolgálatok személyes adatokhoz történő hozzáférése és a nemzetközi együttműködés kérdéskörei voltak. Az Európai Unió új adatvédelmi rendelkezései alapjaiban fogják megváltoztatni a személyes adatok védelmére vonatkozó szabályokat, melyek közvetlenül alkalmazandók lesznek minden tagállamban és a nemzeti adatvédelmi hatóságok szükségszerűen szorosabb együttműködésben látják majd el tevékenységüket. A hatóságok készülnek erre a szerepre, a szükséges források előteremtése érdekében pedig tárgyalnak a költségvetésért felelős tagállami szervekkel. A külföldre irányuló adattovábbítások témájában elfogadott nyilatkozat megerősíti az Európai Unió és az Európa Tanács azon törekvését, hogy az európai polgárok számára akkor is az Európában biztosított védelmet nyújtsák, ha az adataikat más kontinensre továbbítják. A külföldre irányuló adattovábbítások nem adhatnak kibúvót az európai védelmi szint lerontására.

VIII.3. Nemzetközi projektek

VIII.3.1. Arcades-projekt

Az Európai Unió Bizottsága által támogatott, 2014-ben indult Arcades-projekt *(„ARCADES"„Introducing dAta pRoteCtion AnD privacy issuEs at schoolS in the European Union", „Bevezetés az adatvédelembe és az adatvédelmi problémákba az Európai Unió iskoláiban")* 2016-ban sikeresen lezárult. A tanároknak szánt közös, illetve külön magyar oktatási segédanyagok, adatvédelmi kézikönyvek szabadon letölthetők a NAIH oldaláról: http://naih.hu/arcades/dokumentumok.html). A legjobb adatvédelmi tanórák felvételei szintén megtekinthetők a honlapunkon: http://naih.hu/arcades/videok.html. A projekt záró motívuma és egyben a verseny fődíja a 2016 márciusában megtartott barcelonai ünnepélyes záró konferencia volt, ahol minden résztvevő ország beszámolt a saját eredményeiről.

VIII.3.2. Macedón projekt – a macedón adatvédelmi hatóság számára történő ismeretek átadására

Az EUROPAID által finanszírozott „*Support to access to right on protection of personal data in Macedonia (EuropeAid/135668/IH/SER/MK)"* elnevezésű pályázat keretében, amelyben a NAIH konzorciumi partnerként vesz részt, 2016-ban sor került az első szakértői tanulmányutakra a Macedón Köztársaságban. A három NAIH szakértő témái: nemzetközi adatvédelmi együttműködés, a két információs jog összhangjának megteremtése, valamint a bíróságok, ügyészségek és az ombudsman adatkezeléseinek egyes kérdései. A szakértői munka 2017-ben is folytatódik.

VIII.3.3. Részvétel Málta schengeni értékelésében

Málta schengeni joganyagnak való adatvédelmi megfelelőségi ellenőrzésére 2016. szeptember 5-9. között került sor helyszíni ellenőrzés keretein belül, amelyen a NAIH szakértője is részt vett. A 10 főből álló delegációba különböző tagállamokból és az Európai Bizottságtól érkeztek szakértők, míg az Európai Adatvédelmi Biztos képviselője megfigyelőként volt jelen. Az ellenőrzés áttekintette a vonatkozó joganyagot és annak helyi hatóságok által történő alkalmazásának gyakorlatát. A szakértők helyszíni látogatást tettek a Máltai Adatvédelmi

Hatóságnál, a Külügyminisztériumnál, az N.SIS hatóságnál, a SIRENE Irodánál és Máltai Informatikai Ügynökségnél (a máltai közigazgatás informatikai rendszereinek üzemeltetéséért felelős szervnél). A jelentést a Tanács Schengen Bizottsága tárgyalja majd meg részleteiben, ezt követően a végső jelentést a Bel- és Igazságügyi Tanács fogja elfogadni.

VIII.4. A Schengeni Információs Rendszerrel (SIS) kapcsolatos állampolgári megkeresések

A SIS, mint a belső határok eltörléséből és a külső határok megszigorított ellenőrzéséből eredő biztonsági kockázatokat kezelő rendszer, szigorú adatvédelmi szabályok alapján működik. Ezek betartását az Európai Adatvédelmi Biztos (EDPS) és a tagállami adatvédelmi hatóságok – Magyarországon a NAIH – rendszeresen ellenőrzik. Ha bárki tájékoztatást kíván kapni arról, hogy adatai szerepelnek-e a SIS-ben, vagy az ott található adatok helyesbítését, törlését kéri, kérelmét a meghatározott formanyomtatvány kitöltésével benyújthatja bármely kormányhivatalban, rendőrkapitányságon, illetve magyar külképviseleten. A kérelmeket első fokon a Nemzetközi Bűnügyi Együttműködési Központban (NEBEK) szervezeti egységeként működő SIRENE Iroda bírálja el, amely a kért tájékoztatás nyújtását indokolt esetben megtagadhatja, de tájékoztatni köteles a kérelmezőt ennek tényéről és jogalapjáról. A SIRENE Iroda döntésével szemben a NAIH-nál lehet felülvizsgálatot kezdeményezni. 2016-ban összesen 16 alkalommal fordultak hozzánk felülvizsgálati kérelemmel, ebből négy alkalommal magyar, a többi esetben külföldi érintettről volt szó. Területi megoszlást tekintve érkeztek beadványok közel- és távol-keleti, afrikai és dél-amerikai országok állampolgáraitól, illetve a Nyugat-Balkán és Ukrajna térségéből. A Hatóság felülvizsgálati eljárást összesen 5 alkalommal indított, a többi esetben általános tájékoztatást nyújtott a beadványozóknak a Nemzeti SIRENE Irodához fordulás jogáról.

Két megindított felülvizsgálati eljárásban a NAIH megállapította, hogy a kérelmező a magyar-szerb határ illegális átlépése miatt szerepel a SIS rendszerben, a rá vonatkozó jelzést pedig a törvényi előírásoknak megfelelően helyezték el és kezelik a magyar hatóságok. Két másik esetben magyar állampolgárok az általuk jóhiszeműen vásárolt gépjármű forgalomba helyezése során szembesültek azzal, hogy az körözött járműként szerepel a SIS rendszerben. A NAIH vizsgálata kiderítette, hogy a jelzéseket mindkét esetben törölni kellett volna már a rendszerből – erre utólag sor is került.

VIII.5. Részvétel az uniós adatvédelmi felügyeleti munkacsoportok tevékenységében

VIII.5.1. 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 egy vegyes típusú koordinációs ellenőrző csoport létrehozását írja elő, amely SIS II koordinációs ellenőrző csoportként (Coordinated Supervision Group) alakult meg még 2013 folyamán.

A SIS figyelmeztetéseket (úgynevezett *„alert-ek”*) tartalmazó moduljával kapcsolatban a munkacsoport kidolgozott egy kérdéseket tartalmazó audit keretrendszert, amelynek használatával a tagállami hatóságok egységes módszertan szerint tudják ellenőrizni a nemzeti SIS üzemeltetéséért felelős hatóságokat.

A munkacsoport megvitatott egy lengyel joggyakorlatban felmerült problémát. Lengyelországban nem csak bűnüldözési célokból, hanem olyan közigazgatási hatósági eljárások során is ellenőrzik a SIS-ben a kérelmezővel kapcsolatos információkat, mint a fegyverhasználati engedélyek kiadása. Ennek látszólagos jogalapját a fegyverhasználati engedélyek kiadását szabályozó nemzeti törvény adja, amely szerint az eljárás során ellenőrizni kell, hogy az igénylő nem veszélyes-e az ország köz- illetve nemzetbiztonságára. A törvényben ugyanakkor nem szerepel explicit módon a SIS. A munkacsoport álláspontja szerint a lengyel joggyakorlat ellentétes az uniós joggal, mivel a SIS II rendelet és határozat alapján kizárólag bűnüldözési célokra lehet a rendszert használni.

Feltérképezésre került, hogy az egyes tagállamokban a nemzeti költségvetés esetleges korlátozásainak volt, illetve van-e hatása a schengeni joganyag érvényesülésével kapcsolatos adatvédelmi felügyeletre. Általánosságban elmondható, hogy a nemzeti hatóságok nem kaptak a schengeni felügyelettel kapcsolatos plusz erőforrást – ezzel kapcsolatban készül egy nemzeti parlamenteknek címzett közös nyilatkozat.

Az Európai Bizottság képviselője beszámolt a munkacsoportnak a SIS II központi rendszerével kapcsolatos legújabb fejlesztésekről. Az AFIS (Advanced Finger-

print Identification System) bevezetése jól halad, a központi rendszer üzemeltetését végző eu-LISA ügynökség megkezdte a technikai feltételek megteremtését.

VIII.5.2. Europol Közös Ellenőrző Hatósága (JSB Europol)

A jövőbeli legfontosabb változás, hogy 2017. május 1-től az új Europol-rendelet hatálybalépésével az *„Europol Együttműködési Testület”* (Europol Cooperation Board, röviden: ECB) fogja átvenni a JSB Europol feladatait. Az új testület adminisztrációs és titkársági feladatait – ideértve a felhalmozott dokumentáció átvételét – az Európai Adatvédelmi Biztos (EDPS) látja el, mely állandó képviselővel lesz jelen az üléseken. Felmerült, hogy az ECB-n belül létrejönne egy állandó bizottság, amelynek az ECB elnöke, az EDPS képviselője, valamint néhány erre jelentkező tagállami képviselő lenne a tagja.

A JSB Europol megtárgyalta az Europol éves adatvédelmi vizsgálatának megállapításait, kiemelve, hogy az Europol által kezelt adatok minősége – a többmilliárdnyi adat mennyiségének köszönhetően – sok esetben nem ütötte meg az elvárható szintet, sokszor kifejezetten silány minőségű adatokat továbbítanak a tagállamoknak. A mennyiség pedig kihatással van a rendszer hatékony működésére is, mivel az adatokat nagyon sokáig tárolják. A JSB Europol belső képzések szervezését ajánlotta a munkatársak számára az adatminőség javítása érdekében.

Végül említést kell tenni a 2016 december elején nyilvánosságra került, de igazából még 2009 előtt történt úgynevezett *„Europol adatszivárgási ügyről”*. Az Europol egyik alkalmazottja egy prezentáció készítéséhez szükséges adatokat átmásolta egy pendrive-ra, majd otthon az alkalmazott házastársa által előfizetett felhő-alapú tárhely-szolgáltatásba helyezte át azokat. Mivel a szolgáltatást nem védték jelszóval, az adatokat bárki szabadon megtekinthette az interneten keresztül. Az incidenst egy újságíró is észrevette. Az Europol az ügy kapcsán akkor úgy nyilatkozott, hogy az érintett adatok műveleti kockázatot nem jelentettek, mivel azok régiek voltak (Theo van Gogh holland filmrendező 2004-es meggyilkolásához és az azzal kapcsolatban elítélt holland iszlamistákhoz köthető információkról volt szó). A JSB Europol kiemelte, hogy valószínűleg nem csak emberi hiba történt, mivel az érintett időszakban az Europol nem rendelkezett megfelelő belső biztonsági szabályozással, azt csak 2010-ben alkották meg. Ráadásul erről az incidensről (a holland televízióban nemrég levetített dokumentumfilm kapcsán) a JSB csak most, hosszú évek után értesült. Ennek valószínűsíthető oka, hogy a jelenleg és az incidenskor hatályos Europol határozat alapján az Europolnak nincs adatvédelmi incidensjelentési kötelezettsége a JSB felé.

VIII.5.3. Váminformációs Rendszer Adatvédelmét Felügyelő Munkacsoport (JSA Customs és CIS SCG)

A JSA Customs, mint az EU *„régi harmadik pillérébe”* tartozó adatokat kezelő váminformációs rendszert ellenőrző hatóság feladatait 2017. május 1. után átveszi a Vámügyi Információs Rendszer Koordinációs Ellenőrzési Csoportja (CIS SCG). A JSA Customs tehát formálisan megszűnik. A CIS SCG a tagállamok adatvédelmi hatóságainak képviselőiből és az Európai Adatvédelmi Biztos (EDPS) hivatalának képviselőiből áll.

A váminformációs adatbázissal kapcsolatos megkeresést, panaszt az ülésen részt vevők által képviselt adatvédelmi hatóságok egyike sem kapott az elmúlt években, ezért felveszik a kapcsolatot az illetékes nemzeti hatóságokkal – Magyarország esetében a Nemzeti Adó- és Vámhivatallal.

VIII.5.4. Eurodac Rendszer Adatvédelmét Felügyelő Munkacsoport (Eurodac SCG)

Az Európai Bizottság képviselője beszámolt az ujjnyomatokat tároló Eurodac rendszer adatvédelmi felügyeletét ellátó Eurodac SCG-nek az új szabályozás kidolgozás alatt álló koncepciójáról. Várható jövőbeli változások az Eurodac rendszerben:

- A tagállamok területén illegálisan tartózkodó személy adatai tárolhatók lennének. (Jelenleg a tagállamok területén elfogott illegális migránsok esetében csupán az adatok összevetése lehetséges az Eurodac rendszerben rögzített, menedékkérőkre vonatkozó adatokkal.)
- Az ujjnyomat mellett további biometrikus azonosítóként rögzíthető lenne arcképmás is (hosszú távú cél egy arcfelismerő szoftver bevezetése), és szankcionálható lenne, ha valaki megtagadja az arcképe vagy ujjnyomata rögzítését.
- Az ujjnyomatok mellett a személyes adatok (így például név, születési dátum, állampolgárság, személyazonossági adatok, vagy úti okmányok) is rögzíthetők lennének a központi Eurodac rendszerben, ezen adatok ujjnyomat- vagy arcképtalálat esetén lennének hozzáférhetők.
- Az ujjnyomat-vétel alsó korhatára 14 évről 6 évre csökkenne a kísérő nélküli kiskorúak azonosítása, valamint a családjaiktól elszakadt gyermekek családjainak mihamarabbi megtalálása érdekében.
- A javaslat nem változtatna a menedékkérők adatai megőrzésének idején (10 év), az illegális migránsok adatait azonban 5 évig tárolná a rendszer

(a Vízuminformációs Rendszer és a létrehozandó Be- és Kiléptetési Rendszer rendelkezéseihez hasonlóan). Nem törölnék a rendszerből azok adatait, akik számára valamelyik tagállam tartózkodási engedélyt állít ki (az esetükben az adatok megjelölésének lenne helye, így az érintett személyt át lehetne adni annak a tagállamnak, amely kiállította a tartózkodási engedélyt), illetve azokét, akik elhagyták a tagállamok területét.

- A nemzetközi védelemben részesített személyek jelölt adataihoz való bűnüldözési célú hozzáférés továbbra is megszűnne 3 év elteltével, de ez a korlát nem lenne alkalmazandó azon illegális migránsok esetében, akik részére ideiglenes tartózkodási engedélyt állított ki valamely tagállam. A javaslat – a visszatérések megkönnyítése érdekében – az adatok harmadik országokkal való megosztásának szabályait is módosítja, de nem teremt közvetlen hozzáférést e harmadik országok számára.

A Közös Európai Menekültügyi Rendszer reformja tehát folyamatban van, 2017-ben előrelépés várható e téren. A munkacsoport jelezte, hogy mivel gyakorlatilag egy teljesen új adatbázis létrehozását tervezi az EU, ezért fontos lenne azzal kapcsolatban egy előzetes adatvédelmi hatásvizsgálat lefolytatása még annak működésbe lépése előtt.

Az Eurodac rendszer tagállami ellenőrzésével kapcsolatban elkészült egy vizsgálati terv minta, amelyet a tagállami hatóságok a nemzeti ellenőrzéseknél tudnak használni útmutatóként.

VIII.5.5. Vízuminformációs Rendszer Adatvédelmét Felügyelő Munkacsoport (VIS SCG)

Az Európai Bizottság képviselőjének tájékoztatása szerint az eddig lefolytatott tagállami schengeni értékelések (Schengen Evaluation) hiányosságként feltárták, hogy általában a nemzeti adatvédelmi hatóságok ellenőrzésük során legtöbbször nem vonnak be informatikai szakértőt, emellett a VIS-el kapcsolatos érintetti panaszbeadvány, illetve hozzáférési joggyakorlással kapcsolatos megkeresés hiányában nincs erre vonatkozó megfelelő eljárási rend sem.

A tagállamok nem EU-s országokban található külképviseleteire alkalmazandó jog kérdése abban az esetben merül fel, ha a tagállam külképviselete kiszervezi az egyik adatkezeléséhez tartozó adatfeldolgozói munkát egy nem uniós országban működő cégnek. A jogi elemző munka után a közös álláspontot a 2017 tavaszán esedékes ülés tárgyalja meg.

VIII.5.6. 29-es Adatvédelmi Munkacsoport BTLE (Határok, utazás és bűnüldözés) alcsoportja

Az alcsoport kiemelten foglalkozik a személyes adatoknak az illetékes hatóságok által a bűncselekmények megelőzése, nyomozása, felderítése, üldözése vagy büntetőjogi szankciók végrehajtása céljából végzett kezelése tekintetében a természetes személyek védelméről és az ilyen adatok szabad áramlásáról, valamint a 2008/977/JHA tanácsi kerethatározat hatályon kívül helyezéséről szóló európai parlamenti és tanácsi Irányelv (Bűnügyi Irányelv) hatálybalépésének várható hatásaival.

A legfontosabb változás, hogy az Irányelv hatálya szélesebbé válik (2. cikk), hiszen kiterjed a nem állami, de bűnüldözési célból adatokat kezelő gazdasági társaságokra, szervezetekre is. Az újfajta adatkezelési szemlélet (4-7. cikk) egyrészről az adatvédelmi alapelvek újszerű megfogalmazásában, másrészt az adatkezelők számára előírt olyan speciális kötelezettségek előírásában nyilvánul meg, mint az adatok tárolására és a felülvizsgálatra vonatkozó határidők, az adatalanyok különböző kategóriáinak megkülönböztetése és a személyes adatok és a személyes adatok minőségének ellenőrzése közötti különbségtétel. Az adatkezelés jogszerűségének biztosítása kiemelt szerepet kap, amellyel összefüggésben a szükségesség és célhoz kötött adatkezelés alapelvi rendelkezései határoznak meg konkrét kötelezettségeket, míg további feltételeket tartalmaz az Irányelv a különleges adatok és az automatizált döntéshozatal vonatkozásában is.

Részletesebb szabályok kerültek elfogadásra az adatalanyok jogai vonatkozásában (III. Fejezet), amelyek az érintetti jogoknak az eddiginél szélesebb körű érvényesülését hivatott elősegíteni, nagyobb védelmet biztosítva az adatalanyok számára.

Az Irányelv IV. fejezete olyan újfajta kötelezettségeket ír elő a Rendelethez hasonlóan, mint *a beépített és alapértelmezett adatvédelem, a magánélet-védelmi hatástanulmány és az előzetes konzultáció az adatvédelmi hatósággal*. Ezek tartalmának meghatározása egyedi esetekben eltérő lehet, de minden bizonnyal egy teljesen újfajta adatkezelést eredményez majd, amely nagyobb mértékben veszi majd figyelembe a magánszféra és a személyes adatok védelméhez fűződő jogok érvényesülését.

Szintén részletes és szélesebb körű kötelezettséget ír elő az Irányelv az *adatkezelési tevékenység nyilvántartására* (24. cikk) és *azok naplózására* (25. cikk) is.

Új jogintézményt vezet be a 26. cikk: *az adatvédelmi hatóság általi kötelező előzetes jóváhagyást,* míg a 28. cikk az *adatvédelmi incidens kötelező jelentését* írja majd elő, amely rendelkezések az adatvédelmi hatóságokkal való még szorosabb együttműködésre és az általuk javasolt szempontrendszer még szélesebb körű érvényre juttatására kötelezi majd az adatkezelőket. *A belső adatvédelmi felelős kötelező kijelölése* szintén jelentős garancia. A *külföldre történő adattovábbítások* száma várhatóan nő majd, míg előzetes jóváhagyásukra, ellenőrzésükre vonatkozóan az Irányelv új feltételrendszert állít fel. Ezekkel összefüggésben az adatvédelmi hatóságok előzetes kontrollja az eddiginél nagyobb szerepet kaphat.

Az Irányelv végrehajtásáért felelős *Ellenőrző Testület* független uniós szervként nagyobb hatáskörrel rendelkezik majd az egyes nemzeti adatkezelések vonatkozásában és várhatóan aktívabb ellenőrzést is folytat majd le a jelenleg létező koordinatív rendszerben működő szerveknél.

Kevés kivétellel a legtöbb tagállamban az irányelv nemzeti jogba való átültetésére az adatvédelmi hatóságoknak nincs közvetlen ráhatásuk, a jogszabály megszövegezésében közvetlenül nem vesznek részt, az a témában kompetens minisztérium feladata.

Az alcsoport a fentieken túl megvitatta, hogy az Európai Unió és az Amerikai Egyesült Államok között megkötött, a nemzetközi adattovábbítás jogalapját adó, a Bizottság EU-USA adatvédelmi pajzs (*„Privacy Shield"*) egyezményének alapján nem egyértelmű, hogy az érintett hogyan érvényesítheti a jogait: panaszával vajon fordulhat-e majd közvetlenül az Európai Adatvédelmi Testülethez (EDPB), vagy először a nemzeti hatóságát kell megkeresnie. Szükség van egy egységes formanyomtatványra minden tagállam részéről a panaszkezeléshez, továbbá egy olyan biztonságos csatornára melyen keresztül az adatok kommunikációja megvalósítható.

Végül az alcsoport kiemelten foglalkozik az Európai Unió és az Amerikai Egyesült Államok között megkötött úgynevezett *„Umbrella Agreement"* elnevezésű egyezménnyel is, amely az első olyan nemzetközi szerződés, amelyben az USA nem amerikai állampolgárok számára biztosít az amerikai állampolgárokhoz hasonló jogokat. A védelem csak európai uniós állampolgárokra vonatkozik, mégis egy precedens nélküli minimum szintet jelent majd az atlanti bűnügyi együttműködés körében kezelt adatok vonatkozásában. Amerikai részről a törvényalkotás befejezettnek tekinthető. A szerződésben foglaltak betartásának ellenőrzésével kapcsolatban a jövőben szükség lesz úgynevezett közös ellenőrzések lefolytatására, amelynek lényege, hogy a Bizottság, az EDPB és a tagállamok kiválasztott kép-

viselői kiutaznak az USA-ba és ott egy helyszíni ellenőrzés keretein belül vizsgálják meg a megfelelőséget. Probléma lehet, hogy az ellenőrzésen részt vevőktől az USA meg fogja valószínűleg követelni a legmagasabb fokú nemzetbiztonsági átvilágításnak való megfelelést, és hogy az ellenőrzésen elhangzottak, valamint a vizsgálati jelentés is minősített adat lesz, így a résztvevők azokat nem tudják a nyilvánosságnak kommunikálni.

VIII.5.7. A 29-es Adatvédelmi Munkacsoport nemzetközi adattovábbítás alcsoportja (ITS)

2016-ban kiemelt téma volt az Amerikai Egyesült Államokba történő adattovábbítás feltételrendszerének vizsgálata.

A Safe Harborral összefüggő eljárásokkal kapcsolatos ad-hoc munkacsoporti ülésen a magyar, a német szövetségi, a hamburgi, a hesseni, a spanyol, és a francia adatvédelmi hatóságokat képviselő szakértők megvitatták, hogy az egyes tagállami hatóságoknál konkrétan hány olyan eljárás van folyamatban, ahol az adatkezelők vagy adatfeldolgozók a Safe Harbor EU Bíróság általi érvénytelenítését (az ún. Schrems-ítélet) követően is e jogalapra hivatkoznak az USA-ba történő adattovábbítások során.

Az alcsoport az év elején a Schrems-ítélet következményeinek részletes elemzését követően, a BTLE alcsoporttal együttműködve elemezte *„Privacy Shield"* egyezménnyel kapcsolatos határozat tervezetét, a *„kereskedelmi"* aspektusokra, vagyis az uniós adatkezelők/adatfeldolgozók által az USA-ban letelepedett szervezetek részére történő adattovábbítás feltételrendszerére és jogorvoslati lehetőségeire koncentrálva. A továbbított adatokhoz az USA hatóságai általi hozzáféréssel kapcsolatos rendelkezéseket a BTLE alcsoport vizsgálta meg. A Privacy Shield határozat-tervezettel kapcsolatos véleményét[82] a 29-es Munkacsoport 2016. április 13-án hozta nyilvánosságra. Ebben üdvözölte a korábbi keretrendszerhez (a Safe Harborhoz) képest történt előrelépéseket, azonban néhány fontos kérdéssel kapcsolatban – például alapelvek, jogorvoslati rendszerek – módosításokat is javasolt. A Bizottság 2016/1250 végrehajtási határozata a 95/46/EK európai parlamenti és tanácsi irányelv alapján az EU-USA adatvédelmi pajzs által biztosított védelem megfelelőségéről 2016. július 12-én került elfogadásra, ezt követően az alcsoport a határozat által megalkotott és az uniós tag-

82 WP238in.:http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendati/files/2016/wp238_en.pdf

állami adatvédelmi hatóságokból álló jogorvoslati fórum, az *„EU Informal Panel”* eljárási rendjéről folytatott egyeztetéseket, valamint kidolgozott egy egységes formanyomtatványt a Privacy Shield-del kapcsolatban a tagállami hatóságokhoz érkező panaszok hatékonyabb intézése érdekében.

Az alcsoport szakértői emellett nagy figyelmet fordítottak a kötelező szervezeti szabályozással (BCR) kapcsolatos kérdésekre is. Konkrét ügyekkel kapcsolatban számos, a WP 107-es munkadokumentum szerinti együttműködési eljárás lefolytatására került sor, másrészt általánosságban is megvitattak számos kérdést az egységes jogértelmezés érdekében. A szakértők emellett elkezdték a BCR-ral kapcsolatos munkadokumentumok (WP 74, WP 107, WP 108, WP 153, WP 154, WP 155) felülvizsgálatát az új európai adatvédelmi rendeletfényében - az átdolgozott munkadokumentumok 2017-ben lesznek elérhetők a 29-es Munkacsoport honlapján.

VIII.5.8. 29-es Adatvédelmi Munkacsoport technológiai alcsoportja (TS)

2016-ban a GDPR-ra történő felkészülés jegyében az alcsoport feladata volt több fontos vélemény tervezet előkészítése (adat-hordozhatósághoz való jog gyakorlati megvalósulása, adatvédelmi hatásvizsgálat) és az alcsoport megkezdte a munkát az incidens jelentéshez és az adatvédelmi tanúsítási rendszerhez kapcsolódó vélemények előkészítésére. Ugyancsak az alcsoport lett kijelölve az ePrivacy irányelv felülvizsgálatának, illetve az új ePrivacy Rendelet tervezet véleményezésére.

A TS emellett még számos érdekes technológiai újítással foglalkozott – természetesen – adatvédelmi szempontból. Az okos eszközök wifi és bluetooth kommunikációs csatornák felhasználásával végzett felhasználói követésének (location tracking) adatvédelmi kockázatainak elemzése több problémát is megvilágított, úgymint az adatkezelés átláthatóságának a hiányát, az érintettek azonosíthatóságának a magas fokát, a magánszféra nagyfokú kiszolgáltatottságát, a profilalkotás, a rendőrségi adatigénylés, az adatkezelő meghatározásának nehézségét. A technika használatának azonban vannak elfogadható változatai is, így például Norvégiában egy külön alkalmazást kell feltelepíteni az okos eszközre, amely az adott bluetooth követést végző fizikai eszközzel (bluetooth beacon) kommunikál.

A TS 2016-ban felülvizsgálta a WP 29-es Munkacsoport korábbi, a munkáltatói adatkezelésekről szóló véleményeit és megkezdte egy, a legújabb technológiák kihívá-

sait is magába foglaló, a munkavállalók ellenőrzésének adatvédelmi kockázataival foglalkozó vélemény tervezet elkészítését. Új kihívást jelentenek a munkavállalók megfigyelésére (employee monitoring) kifejlesztett olcsó és elterjedt megoldások, amik már figyelemmel vannak az otthoni munkavégzés, a saját eszköz használata (bring your own device), a munkahelyi telemetria és analitika módszereire is.

Az alcsoport a fentieken túlmenően konzultációt kezdeményezett több területen is az érintettekkel, így például az egymással kommunikáló gépjárművek *(„connected cars”*) adatvédelmi kérdésköreiről, vagy az Okos Városok *(„smart cities”*) koncepciókról.

A napirenden továbbra is megtalálható volt a nagy IT cégek (például: Facebook, Google, Microsoft) gyakorlatainak, újításainak adatvédelmi megfelelőségi elemzése. Ezek közül kiemelkedik a belga hatóság Facebook elleni eljárása, amely egy bírósági ítélettel zárult. Az ítélet kimondta, hogy a Facebook által használt DATR cookie alkalmazása jogellenes (ez a *„süti”* a be nem jelentkezett érintetteket követi, ha olyan honlapra lépnek, ahol Facebook social plugin API-ja telepítve van, például egy *„like gombon”* vagy egy nyilvános Facebook oldalon keresztül). A cookie a felhasználó gépére elhelyezésre kerül és követi böngészési szokásait. A Facebook által hivatkozott adatbiztonsági cél valós ugyan, de sem az arányosság, sem a megfelelő tájékoztatás követelményének nem felelt meg és a belga bíróság nem fogadta el, hogy csupán távoli biztonsági szempontokra hivatkozva ilyen széleskörű adatkezelések történjenek.

VIII.5.9. A 29-es Adatvédelmi Munkacsoport hatóságok közötti együttműködéssel foglalkozó alcsoportja (Cooperation subgroup)

Az Európai Unió új adatvédelmi rendelete a tagállamok közötti hatósági együttműködést lényegesen szorosabbá teszi, és az ehhez kapcsolódó eljárásait is rögzíti. Az alcsoport legfontosabb feladata 2016-ban, hogy az új eljárások alkalmazása érdekében iránymutatásokat dolgozzon ki a tagállami hatóságok számára. A négy fő téma: az ún. egyablakos ügyintézés menete a határokon átnyúló adatkezelések esetében (one-stop-shop), a hatóságok együttműködése ún. kölcsönös segítségnyújtás keretében (mutual assistance), a hatóságok közös műveletei (joint operations), valamint a közigazgatási bírság kiszabásának közös európai uniós szempontrendszere. Az első három témakörben az alcsoport javaslatára a Munkacsoport munkaanyagokat fogadott el, amelyeket 2017-ben tesztelni fognak a hatóságok, és szükség esetén módosítják a hatóságok munkatársainak szánt iránymutatásokat.

A közigazgatási bírság kiszabásának szempontrendszere számos tagállamban újdonságot jelent, hiszen nem mindenütt van jelenleg lehetőség adatvédelmi természetű jogsértés esetén bírságot kiszabni. A rendelet egységes alkalmazására törekednek a tagállami hatóságok a jogvédelem azonos szintjének megvalósítása érdekében, biztosítva az adatkezelők számára a jogbiztonságot, egyszersmind azért is, hogy elejét lehessen venni a legkedvezőbb környezetet biztosító tagállamok közötti válogatást (forum shopping). A magyar hatóság szempontjából is kiemelkedő jelentőségű kérdésről van szó, hiszen a jelenleg 20 millió forintos bírságplafon 20 millió Euróra emelkedik 2018 májusától. Az egységes szempontrendszer kidolgozása 2017-ben folytatódik.

VIII.5.10. A távközléssel foglalkozó nemzetközi adatvédelmi munkacsoport (International Working Group on Data Protection in Telecommunications)

Az úgynevezett berlini munkacsoport egy új vélemény tervezetet vitatott meg, amely az e-learning során kezelt személyes adatokról szól. A platformok adatvédelmi kockázatai közül kiemelendő, hogy online környezetben a tanulmányokhoz nem kapcsolódó személyes adatokat is gyűjt a rendszer, amely akár különleges adatokat is érinthet (például tanulási zavar, politikai vélemény, stb.). Egyre több magántársaság jelenik meg a piacon, amely a gyermekek adatainak további felhasználásáért és direkt marketing megkeresésekért kínálja ingyenesen az oktatási platformokat. A magánszereplőkkel az adatkezelői felelősség is elmosódik, többnyire az ilyen szolgáltatások felhő alapú informatikát használnak, amelyben az érintettek adatainak továbbítása és kezelése nem átlátható.

Az okos tévék adatvédelmi kérdéseivel kapcsolatban megállapították, hogy a legtöbb esetben már a készülék üzembe helyezésével rengeteg személyes és analitikai adat áramlik a gyártóhoz és egyéb szereplőkhöz. Emellett a hangfelismerő és személyes asszisztens funkcióknak is van adatvédelmi kockázata.

Az Európai Bizottság és más nemzeti adatvédelmi hatóságok mellett a berlini munkacsoport is foglalkozott a *„connected cars”* koncepciójával, amely alapjában véve a gépjárművek mozgásának, a vezetők viselkedésének a nyomon követését és elemzését jelenti, illetve a gépjárművek egymás közötti automatikus kommunikációját elsősorban a forgalom biztonsága, zavartalansága (például a vezető figyelmeztetése vezetési hibákra, veszélyes csomópontokban segítségnyújtás) és a kényelmesebb közlekedés érdekében (például intelligens útjelzők, dugóelkerülés, baleset esetén automatikus segélyhívás, stb.). A kérdések azért

égetőek, mert az érintettek semmit nem tudnak a készülékeik, eszközeik kommunikációjáról.

VIII.5.11. Délkelet-európai Rendőri Együttműködési Egyezmény (Police Cooperation Convention for Southeast Europe - PCC SEE)

Az Egyezményt 2006. május 5-én írta alá hét ország: Albánia, Bosznia-Hercegovina, Macedónia, Moldova, Montenegró, Románia és Szerbia, Magyarország pedig a Délkelet-európai Rendőri Együttműködési Egyezmény kihirdetéséről szóló 2012. évi XCII. törvény 2012. december 11-i hatályba léptetésével csatlakozott. Cél, hogy az EU közös vívmányaira, valamint az EU tagállamok között alkalmazott legjobb gyakorlatokra építve növeljék a biztonságot a térségben, és felkészítsék a nyugat-balkáni országokat az európai uniós tagságra. Az Egyezmény alapján a Szerződő Felek fokozzák együttműködésüket a közbiztonságot fenyegető veszélyek elhárítása, valamint a bűncselekmények megelőzése, felderítése és rendőrségi nyomozása során. Az Egyezmény végrehajtására létrehozott legfőbb döntéshozó szerv, a Miniszteri Bizottság létrehozta az adatvédelmi munkacsoportot, amelynek feladata a kölcsönös értékelési eljárás részleteinek kidolgozása és az Egyezmény adatvédelemmel kapcsolatos rendelkezései érvényesülésének monitorozása. Minden szerződő fél – így Magyarország is – két tagot jelöl a Munkacsoportba, amelyből az egyik a nemzeti adatvédelmi hatóság, míg a másik a bűnüldöző hatóságok adatvédelemben jártas képviselője kell, hogy legyen. A 2015 decemberi ülés megállapította, hogy az Egyezmény 31. cikkének megvalósulását garantáló kölcsönös adatvédelmi értékelést minden Szerződő Fél sikeresen teljesítette, így az Egyezmény jogalapot teremthetne a személyes adatok cseréjéhez, azonban – tekintettel arra, hogy annak számos nem EU tagállam is részese – szükséges egy részletesebb, megfelelő adatvédelmi garanciákat teremtő jogi struktúra kialakítása. Nyitott kérdés még, hogy az Egyezmény adatvédelmi végrehajtási megállapodása tartalmazzon-e a továbbítható bűnügyi személyes adatokkal kapcsolatban egy részletes listát vagy elegendő egy általános felhatalmazás?

VIII.5.12. TFTP

2016 márciusában került sor az Európai Unió és az Amerikai Egyesült Államok között az Európai Unióból származó pénzügyi üzenetadatoknak a terrorizmus finanszírozásának felderítését célzó program céljából történő feldolgozásáról és az Amerikai Egyesült Államok részére való átadásáról szóló megállapodás

(TFTP) 4. Közös Felülvizsgálatára, amelyben a NAIH munkatársa adatvédelmi szakértőként vett részt a 29-es Adatvédelmi Munkacsoport küldötteként. A Felülvizsgálat részletei minősített adatok, de a Felülvizsgálatról az Európai Bizottság jelentést készít, amelyet elfogadásra terjeszt be az Európai Tanács és az Európai Parlament elé.

VIII.5.13. A nemzeti utasadat információs (PNR) rendszerrel kapcsolatos fejlemények

Az EU PNR Irányelv 2016. május végén lépett hatályba azzal, hogy a tagállamoknak az irányelv nem hagy felkészülési időt. Jelenleg három kivétellel (Egyesült Királyság, Románia és Magyarország) még a legtöbb tagállam nem ültette át az irányelvet a nemzeti jogába és nem hozta létre az utasadatok elemzésére a nemzeti utasadat ellenőrző hatóságot (úgynevezett: Passenger Information Unit, röviden: PIU).

Magyarországon a 2015. évi XXXV. törvény rendelkezései alapján 2016. július 17-én állt fel új hatóságként a Terrorelhárítási Információs és Bűnügyi Elemző Központ (TIBEK), amelyen belül az Ügyeleti és Utasadat Főosztály látja el a nemzeti PIU feladatait. A TIBEK nemzeti PIU-ként a légitársaságoktól átveszi és kezeli az utasadatokat, amikkel elemző-értékelő tevékenység keretében kockázatelemzést végez. Az utasadatok kezelésének célja a terrorizmussal, a szervezett bűnözéssel összefüggő bűncselekmények, valamint az illegális migráció területén megjelenő szervezett bűnözői csoportok és bűnszervezetek által elkövetett bűncselekmények felderítésének és nyomozásának, illetve az illegális migráció megelőzésével, megakadályozásával kapcsolatos feladatok elősegítése, továbbá a nemzetbiztonságot veszélyeztető törekvések és tevékenységek elhárításának az elősegítése.

A TIBEK 2016. szeptember 29-én konferenciát tartott a Belügyminisztériumban az új hatóság és ezen belül a nemzeti PIU működésével kapcsolatban. Jelenleg a rendszerbe minden olyan légitársaság küld adatokat, amelyek a schengeni térségen kívülre szerveznek járatokat. Az adatokat előre beállított profilok alapján automatikusan elemzi a rendszer, majd jelzi az operátornak, ha gyanús adatot talált. A rendszerben manuálisan is lehet keresni, de csak akkor, ha az arra jogosult hatóságtól (nyomozó hatóságok, titkosszolgálatok, ügyészség, bíróság) kapott megkeresést a TIBEK. A rendszerből való adatigénylésre kizárólag az irányelvben felsorolt súlyos bűncselekményekkel kapcsolatos nyomozások, vizsgálatok

kapcsán kerülhet sor (a magyar Btk.-ban ez összesen 26 nevesített bűncselekményt jelent). Az irányelv teljes körű átültetése a nemzeti jogba még folyamatban van, a vonatkozó jogszabályok teljes harmonizációjára a Belügyminisztérium tájékoztatása alapján 2017-ben kerül sor.

VIII.6. Részvétel az Európa Tanács munkájában

VIII.6.1. A 108-as Egyezmény reformja

Az Európa Tanács személyes adatok gépi felhasználása során az egyének védelméről szóló, 1981. január 28-i 108. számú egyezménye (108-as Egyezmény) reformjának ügye többször szerepelt a 108-as Egyezmény Tanácsadó Bizottságának (T-PD) napirendjén. Bár az új szövegben szakértői szinten a részes felek megállapodtak, 2016 során két delegáció is fűzött a módosításhoz fenntartásokat, vagy nem vonta vissza azokat, amelyeket korábban ahhoz tett, így a szöveg végső jóváhagyására 2016-ban sem volt lehetőség. Az egyeztetések szakértői szinten folynak tovább.

VIII.6.2. Európa Tanács Terrorizmussal foglalkozó Szakértői Bizottsága (CODEXTER)

A CODEXTER 2016 során létrehozta a Különleges Nyomozási Technikákkal foglalkozó (SIT) albizottságát, melynek feladata az Európa Tanácsnak a terrorizmus és súlyos bűncselekmények elleni harcban a különleges nyomozási technikák alkalmazásáról szóló Rec (2005)10 számú ajánlásának felülvizsgálata a 2005 óta végbement technikai és technológiai fejlődés fényében, illetőleg hogy hogyan lehetne kiterjeszteni az ajánlás hatályát a pénzügyi nyomozási technikákra is.

VIII.7. Nemzetközi vonatkozású jogszabálytervezetek véleményezése

A NAIH 2016-ban több nemzetközi vonatkozású jogszabálytervezetet is véleményezett a jogalkotó megkeresése nyomán. Ezek közül egyrészt kiemelendő a

Magyarország és a Thaiföldi Királyság között létrejött kiadatási egyezmény kihirdetéséről szóló törvény véleményezésre megküldött szövege.

A törvénytervezetben az adatvédelmi előírások szerint az egyezmény alkalmazásához szükséges személyes adatok feldolgozása és kezelése a szerződő felek nemzeti jogszabályai alapján történik, az adatokat továbbító szerződő felek további feltételeket szabhatnak a továbbított adatok feldolgozására vonatkozóan. Egyebekben az egyezmény a személyes adatok védelmére vonatkozó előírásokat nem tartalmaz. Ezzel kapcsolatban a NAIH felhívta arra a figyelmet, hogy az alapvető jogok védelmének az Alaptörvényben meghatározott rendszerével nem egyeztethető össze az, hogy valamely jogalkalmazó szerv diszkrecionális jogkörébe utalja az egyezmény az adatkezelési, illetve adatvédelmi szabályok meghatározását.

Magyarország és a Vietnami Szocialista Köztársaság között létrejött, az elítélt személyek átszállításáról szóló egyezmény kihirdetéséről szóló törvény, valamint a Magyarország és a Vietnami Szocialista Köztársaság között létrejött kiadatási egyezmény kihirdetéséről szóló törvény véleményezésre megküldött szövege tekintetében a személyes adatok továbbítása a külföldi adattovábbítás Infotv.-ben valamint az Európai Parlament és a Tanács 95/46/EK adatvédelmi irányelvében szereplő feltételrendszere alapján lehetséges. A törvénytervezet nem tartalmaz külön rendelkezéseket a személyes adatok védelméről, arra a Magyarország és a Vietnami Szocialista Köztársaság között létrejött kölcsönös bűnügyi jogsegélyről szóló, e beszámoló megírásakor még ki nem hirdetett egyezmény személyes adatok védelmét szabályozó cikkében megfogalmazottakat kívánják alkalmazni. A Hatóság álláspontja, hogy a szóban forgó egyezményekben kívánatos lenne meghatározni a személyes adatok védelmének jogi garanciáit (az adatkezelés célhoz kötöttsége, a tájékoztatáshoz való jog, az érintettek jogai), figyelemmel a külföldi adattovábbítás jogszabályokban meghatározott feltételrendszerére. Jogsegélyt csak folyamatban lévő, egyedi büntetőeljárás keretében, és csak a konkrét eljárás alá vont személlyel kapcsolatban lehet kérni. A NAIH felhívta a jogalkotó figyelmét arra, hogy Magyarország Uniós kötelezettségeiből fakadóan harmadik országba irányuló adattovábbítás során a 95/46/EK irányelv által biztosított védelem szintjét szükséges garantálni.

VIII.8. Bitcoin technológiával kapcsolatos ügyek

A NAIH 2016-ban két ügyben is felkérésre állásfoglalást adott ki a Bitcoin-rendszer, mint magánszférát védő technológia vonatkozásában. A Bitcoin egy bárki által szabadon használható digitális fizetőeszköz, amely azonban csak virtuálisan létezik, így nevéhez hűen teljes mértékben bitekből és bájtokból áll. Fizikai megtestesülésével, érmeként vagy bankjegyként sehol sem találkozhatunk vele. Szemben a hagyományos pénzügyi intézetekkel, amelyek az ügyfelek magánszféráját az utalásokra vonatkozó információk visszatartásával védik, ezt a Bitcoin rendszerében az biztosítja, hogy a címek tulajdonosaira vonatkozó információk egyáltalán nem ismertek. Ha egy felhasználó elkezdi használni a virtuális érmék küldésére és fogadására szolgáló Bitcoin szoftvert, akkor az semmilyen információt nem fog kérni a személyes adatokat illetően, és nem kell a felhasználónak magát regisztrálnia a hálózatra sem.

Az első ügy egy USA-beli ügyvédi iroda megkeresése volt, amely az új technológiának a magánszféra védelmére gyakorolt hatásában kérte ki a NAIH véleményét. Összességében elmondható, hogy a technológiával kapcsolatban Magyarországon még nem került sor konkrét jogalkotói aktus kibocsátására, ez azonban nem akadálya jelenleg annak, hogy a magánszemélyek és vállalkozások szabadon használják a rendszert saját céljaikra. A jövőben a visszaélések megelőzése érdekében azonban mindenképpen üdvözlendő lenne a technológia értékelésére alkalmas jogszabályi környezet megalkotása.

A második ügyben a Dombóvári Járásbíróság kereste meg a NAIH-ot egy folyamatban lévő büntetőeljárással kapcsolatban állásfoglalás és szaktanácsadói vélemény kibocsátása végett. A konkrét esetben több millió forint elkövetési értékre csaltak ki a sértettől Bitcoinokat. A büntetőeljárás során eldöntendő kérdés az volt, hogy egy adott Bitcoin mennyiség az elkövetés időpontjában vajon rendelkezett-e a piacon pontosan meghatározható értékkel? A NAIH állásfoglalásában erre egyértelműen igennel válaszolt.

VIII.9. Drónok

A pilóta nélküli repülőgépek (Unmanned Aircraft System (UAS) vagy Remotedly Piloted Aircraft System (RPAS), összefoglaló nevükön drónok használata egyre jelentősebb adatvédelmi aggályokat kelt. Az európai adatvédelmi hatóságok az 1990-es évek óta foglalkoznak a drónok magánszférára gyakorolt hatásával,

hiszen ezekkel az eszközökkel, – különösen, mióta már szinte divatcikké váltak – a zártláncú kamerák megfigyelésénél is sokkal súlyosabb módon sérthetik a magánéletünket, privátszféránkat.[83] Az általuk végzett megfigyelés érzékelhetetlen, tolakodó (intruzív), önkényes és folyamatos lehet, ráadásul maga az eszköz szinte bárki számára elérhető, megvásárolható.

A NAIH 2014 novemberében bocsátotta ki a drónok használatáról szóló, adatvédelmi kérdéseket feldolgozó ajánlását[84], mely a járművekre szerelhető kiegészítőkkel megvalósuló atipikus adatkezelést, a civil felhasználás adatvédelmi kérdéseit járja körül.

A drónokat Európában egyre gyakrabban használják polgári és kereskedelmi célokra különböző ágazatokban, a szabályozási keret azonban továbbra is összehangolatlan. Alapvető nemzeti biztonsági szabályok vonatkoznak ugyan rájuk, vagy épp folyamatban van kialakításuk, de e szabályok unió-szerte eltérőek, számos kulcsfontosságú óvintézkedést nem koherens módon szabályoznak, ezért előreláthatólag 2019-től a tagállami szabályozásokat (amennyiben ilyen az adott tagállamban hatályban lesz) felváltja majd egy EU-s rendeleti szintű egységes szabályozás. A rendelet tervezetet az Európai Repülésbiztonsági Ügynökség (EASA) készíti elő. 2015 végén az EASA egy kockázati tényezőkön alapuló hatásvizsgálat alapján 3 kategóriára osztotta a drónokat (open/alacsony kockázatú, specific/közepes kockázatú, certified/magas kockázatú), az egyes kategóriákra eltérő engedélyezési, felügyeleti és regisztrációs szabályok vonatkoznak majd. A rendelet-tervezet adatvédelmi aspektusainak kialakításában különböző nemzetközi szakmai műhelyeken keresztül a NAIH is aktívan részt vesz.

A hazai jogi szabályozásának kialakítása 2016-ban elkezdődött. A légiközlekedésről szóló 1995. évi XCVII. törvény módosításáról szóló 2016. évi CXXXVI. törvényben definiálták a drón fogalmát, mely szerint *„pilóta nélküli légijármű: olyan polgári légijármű, amelyet úgy terveztek és úgy tartanak üzemben, hogy vezetését nem a fedélzeten tartózkodó személy végzi.”*[85]

A Nemzeti Közlekedési Hatóság által összeállított jogszabálytervezet a 0,25 kg feletti súlyú drónokat készül szabályozni és tartalmaz több, a NAIH által megfogalmazott adatvédelmi megoldást is. Elkülönül a kereskedelmi valamint a magáncélú

83 International Working Group on Data Protection in Telecommunications 675.47.25., Adatvédelem légi megfigyelés esetén, Munkadokumentum, 54. ülés, 2013. szeptember 2-3.
84 https://www.naih.hu/files/ajanlas_dronok_vegleges_www1.pdf
85 2016. évi CXXXVI. tv. 18. § (2)

felhasználás, az uniós rendelettervezethez hasonlóan három különböző, kockázatelemzésen alapuló kategóriát állít fel és rendelkezik a felelősségbiztosítás kérdéséről. A magyar légtérben jelenleg hivatalosan csak eseti vagy korlátozott légtér igénybevételére vonatkozó engedéllyel, valamint tevékenységi jóváhagyással szabad drónt röptetni, maximum 150 méteres magasságig és 25 kilogrammnyi tömeghatárig. A Légügyi Hivatal biztosítja a kért koordináták által határolt terület légterét, ahol más légi jármű a drónhasználat ideje alatt nem jelenhet meg.

A NAIH véleménye szerint a leendő jogi szabályozásban érvényesíteni kell azt a garanciális alapelvet, hogy az adatkezelés során személyes adatot csak célhoz kötötten és csak meghatározott időpontra, földrajzi területre, személyi körre kiterjedően lehet gyűjteni és kezelni, ezzel összefüggésben pedig szükség van a légiközlekedési hatóság által lefolytatott engedélyezési eljárásra. Valamennyi adatkezelési cél tekintetében figyelemmel kell lenni az arányosság követelményére. A magáncélú felhasználás során drónnal megvalósított adatkezelés nem vonható ki az adatvédelmi garanciák alól, a kedvtelésből üzemeltetett drónok felhasználója nem hivatkozhat arra a kivételszabályra, mely szerint a természetes személy kizárólag saját személyes céljait szolgáló adatkezelésre az adatvédelmi szabályok nem alkalmazandók.[86]

Az adatkezelésekre analógia útján alkalmazandó az *EUB Ryneš v Úřad* ügyben hozott ítélete, mely szerint minden olyan esetben, amikor a drón kilép a szűk értelemben vett magánterületről, az adatvédelmi szabályok alkalmazása indokolt az egyének védelme érdekében.[87]

Németországban a légiközlekedési törvény[88] módosításának közigazgatási és társadalmi egyeztetése folyamatban van. A módosítás a magáncélú drónhasználat szabályait kívánja lefektetni, a kereskedelmi célú üzemeltetéssel e módosítás nem foglalkozik. Az új szabályok a magyar és az európai szabályokhoz hasonlóan érvényes felelősségbiztosítást írnak elő, bizonyos esetekben (kereskedelmi célú használat esetén minden alkalommal) a német légügyi hatóságnál repülési engedélyeztetési eljárás lefolytatása szükséges. A drónokat üzemeltető kereskedelmi vagy magán célú felhasználó is egyaránt köteles tiszteletben tartani a német szövetségi adatvédelmi törvényt.

Az Egyesült Államok Szövetségi Légügyi Hatóságának (Federal Aviation Administration) modernizációjáról szóló 2012-es törvény értelmében a drón egy

86 Infotv. 2. § (4) bekezdése
87 Ryneš ítélet, C-212/13, EU:C:2014:2428
88 Luftverkehrs-Ordnung (LuftVO)

személyzet vagy utas nélküli légi járműből, valamint az annak biztonságos és hatékony üzemeltetéséhez szükséges elemekből álló szerkezet.[89] A 25 kg alatti tömegű drónokat szabályozó törvény[90] 2016. augusztus 29-én lépett hatályba.

Az amerikai közlekedési minisztérium légügyi hatósága által készített jogszabály célja a drónhasználat során felmerülő, más légi járművekkel, az emberekkel és vagyontárgyakkal kapcsolatos kockázati tényezők csökkentése. A törvény a magyar tervezethez hasonlóan folyamatos vizuális kapcsolatot követel az adatkezelő és az egység között, valamint tiltja a repülési tevékenységben közvetlenül nem résztvevő személyek feletti működtetést, mely szabály egyaránt alkalmas a személyi sérülések lehetőségének csökkentésére valamint az egyén magánszférájának védelmére. Az amerikai légügyi hatóság az engedélyezési eljárás, valamint a kereskedelmi használathoz szükséges jogosítvány megszerzése során adatvédelmi oktatásban is részesíti az adatkezelőt.

89 FAA Modernization and Reform Act of 2012, Pub. L-. No. 112-95. § 331(9)

90 BILLING CODE 4910-13-P; RIN 2120–AJ60 Operation and Certification of Small Unmanned Aircraft Systems, Part 107

IX. Mellékletek

IX.1. NAIH emlékérem 2016

2016. január 28-án a *„Nemzeti Adatvédelmi és Információszabadság Hatóság Emlékérem”* adományozásáról szóló 19/2012. sz. NAIH szabályzata alapján az ezüst emlékérmet a Budapesti Gépészeti Szakképzési Centrum Mechatronikai Szakközépiskola pedagógusa, Vereb Márta és hét diákja kapta az ARCADES adatvédelmi pályázat keretében nyújtott, az internetes adatvédelem, valamint a fiatalok biztonságos és jogtudatos internethasználatával kapcsolatos ismeretek népszerűsítése során végzett kiemelkedő tevékenységéért.

A NAIH ezüst emlékérem átadása a Magyar Tudományos Akadémián
2016. január 28-án

IX.2. Az adatvédelmi nyilvántartás

A 2016. január 1-től létrejött új szervezeti struktúrában az adatvédelmi nyilvántartással kapcsolatos teendők ellátása az Adatvédelmi Főosztálytól az Informatikai, Ügyviteli és Nyilvántartási Főosztály feladatkörébe került. Az operatív feladatokat 2016-ban 2 fő adatvédelmi szakértő látta el.

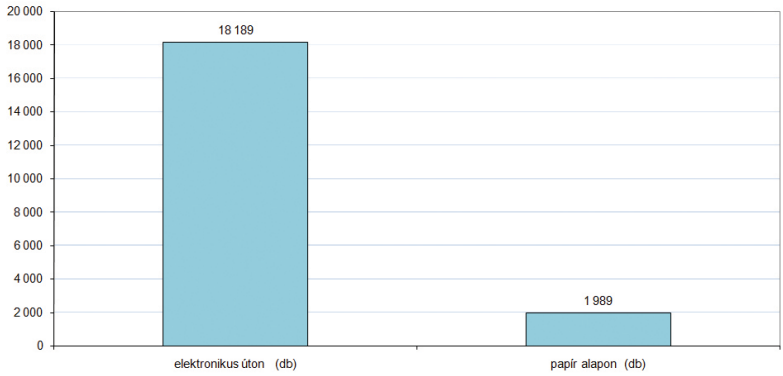
Az adatvédelmi nyilvántartás ügyiratszám statisztikája:

	elektronikus úton (db)	**papír alapon (db)**	**összesen: (db)**
Nyilvántartásba vételi kérelem / hiánypótlás	15.063	896	15.959
Módosítás / törlés	1.390	495	1.885
Konzultációs kérdés	1.736	598	2.334
Összesen:	**18.189**	**1.989**	**20.178**

Az előző évekhez képest tovább csökkent a papír alapon beérkezett kérelmek száma, amiből egyértelműen következik, hogy egyre több adatkezelő használja a Hatóság honlapján elérhető *„NAIH_Avatár”* bejelentkezés kitöltő keretprogramot. A bejelentéseket továbbra is célszerűbb elektronikus úton beküldeni, hiszen azok továbbítása és a nyilvántartásba vételi határozat vagy hiánypótlás előkészítése így gyorsabb, továbbá az elektronikus űrlap kitöltő programja a bevitt adat mezők előzetes ellenőrzésével segítséget nyújt a kérelem helyes kitöltéséhez.

Az adatkezelések adatvédelmi nyilvántartásba történő bejelentésének menetében a már bejelentett adatkezelések módosításának, törlésének, valamint a hiánypótlások teljesítésének módjában a korábbi évekhez képest nem történt változás.

Nyilvántartásba vétel kapcsán keletkezett ügyiratok megoszlása



Nyilvántartással kapcsolatos konzultációs megkeresések

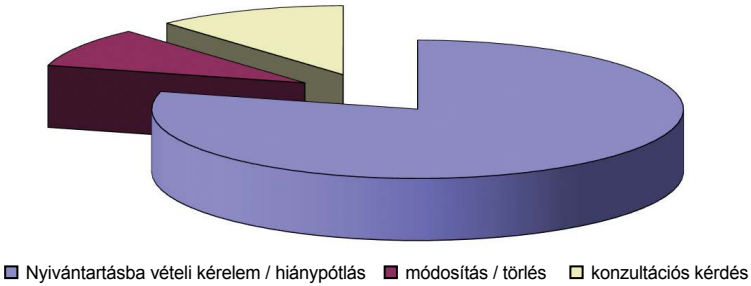
2016-ban összesen 2334 adatvédelmi nyilvántartással összefüggő, de nem közvetlenül adatkezelések bejelentésével kapcsolatos megkeresés érkezett a Hatósághoz, melyek jelentős része konzultációs kérdésnek minősült. Ezekben az érintettek a különböző célú – hírlevél küldés, web áruház üzemeltetés, kamerarendszer működtetés, *„whistle blowing”* rendszer (visszaélés jelentéstételi rendszer) működtetése – adatkezelések adatvédelmi nyilvántartásba vételéről, az adatkezelési tájékoztató elkészítéséről, valamint a már bejelentett adatkezelések tartalmáról kértek tájékoztatást.

Az adatlap kitöltése

Annak ellenére, hogy a nyilvántartással kapcsolatos törvényi rendelkezések és a gyakorlat könnyebb értelmezésének elősegítése érdekében a korábban a honlapon közzétett részletes kérelem kitöltési útmutató és a *„Gyakran ismételt kérdések”* mellett a Hatóság közzétette a honlapján az adatvédelmi nyilvántartásba történő bejelentkezésről szóló állásfoglalását is (http://naih.hu/adatvedelmi-allasfoglalasok,-jelentesek.html), továbbra is jelentős számban érkeznek az adatlap kitöltésével kapcsolatos megkeresések.

Mindezek mellett jelentős számban érkeztek pontatlanul vagy hiányosan kitöltött nyilvántartásba vételi adatlapok is, melyeknek leggyakoribb hiányossága, hogy az adatkezelés jogalapjánál és időtartamánál törvényi hivatkozás esetén nem jelölik meg az adatkezelők a pontos törvényhelyet.

Az adatvédelmi nyilvántartással kapcsolatos megkeresések megoszlása



IX.3. Elutasított tájékoztatási kérelmek és adatigénylések

Az Infotv. 14. § a) pontja szerint az adatkezelések által érintett személyek kérelmezhetik az adatkezelőnél a személyes adataik kezeléséről szóló tájékoztatás nyújtását. Ezekben az esetekben az adatkezelő részletes tájékoztatást ad az általa kezelt személyes adatok köréről, az általa megbízott adatfeldolgozó által feldolgozott adatokról, az adatok forrásáról, az adatkezelés céljáról, jogalapjáról, időtartamáról, az adatfeldolgozó nevéről, címéről, az adatkezeléssel összefüggő tevékenységéről, továbbá az adattovábbítás jogalapjáról és címzettjéről. Az adatkezelő azonban az Infotv.-ben meghatározott esetekben – például honvédelmi, nemzetbiztonsági, bűnüldözési, vagy gazdasági-pénzügyi érdekekből – megtagadhatja az érintett tájékoztatását. Az Infotv. 16. § (3) bekezdése az adatkezelő kötelezettségeként írja elő, hogy a tájékoztatást elutasító kérelmekről a Hatóságot évente a tárgyévet követő év január 31-ig értesítse.

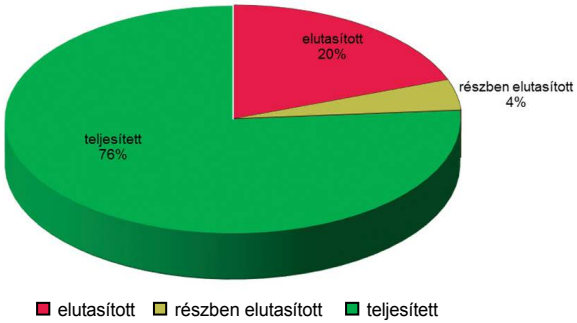
Az Infotv. 26. §-a biztosítja az állampolgárok közérdekű és közérdekből nyilvános adatok megismeréséhez való jogát. A közérdekű adatok megismerése iránti igényt szóban, írásban, vagy elektronikus úton bárki kezdeményezheti. Az Infotv. azonban az imént ismertetett, az adatkezelőt terhelő tájékoztatás nyújtáshoz hasonlóan a közérdekű adatok megismerését az adatfajták meghatározásával egyebek mellett honvédelmi, nemzetbiztonsági, pénzügyi, devizapolitikai érdekekből, vagy például külügyi kapcsolatokra tekintettel korlátozhatja. Az adatkezelő kötelessége, hogy az igény megtagadásáról értesítse az igénylőt, az elutasított kérelmekről, valamint az elutasítások indokairól nyilvántartást vezessen, és az abban foglaltakról minden év január 31-ig tájékoztassa a Hatóságot.

Noha az Infotv. az adatkezelő kötelezettségeként fogalmazza meg az elutasított kérelmekről szóló tájékoztató Hatósághoz való megküldését, e kötelesség megszegését nem szankcionálja a törvény. Az előző évektől eltérően a 2016-os évre vonatkozóan megküldött és 2017.02.23-ig beérkezett tájékoztatók adatait dolgoztuk fel.

IX.3.1. A közérdekű adatigénylések elutasítása

közérdekű adatigénylés				
elutasított (db)	részben elutasított (db)	teljesített (db)	összes db	adatkezelők száma
484	109	1900	2493	228

Közérdekű és közérdekből nyilvános adatok
teljesítésére/elutasítására vonatkozó adatok összesítve a 2016. évben



A Hatósághoz 2016-ra vonatkozóan 2017. február 23-ig 228 db közérdekű adatigénylésre vonatkozó tájékoztatás érkezett.

A közérdekű adatok megismerésére irányuló kérelmeket – a teljesség igénye nélkül – legtöbb esetben az alábbi okokra hivatkozva tagadták meg az adatkezelők:

– nem közérdekű adatra vonatkozott az adatigénylés;
– az igényelt adatok a törvény értelmében nem nyilvános adatok;
– a nyilvánosságot korlátozó határidő nem telt le;
– az igényelt adatok nem a szerv kezelésében vannak;

– az igényelt dokumentum minősített adatot tartalmaz;
– az igényelt adat üzleti titoknak minősül;
– az igényelt adat vonatkozásában a megkeresett szerv nem minősül adatkezelőnek.

IX.3.2. Személyes adatok kezeléséről szóló tájékoztatás teljesítése/elutasítása

2016-ra vonatkozóan összesen 31 adatkezelő küldte be tájékoztatását a Hatósághoz. Tekintettel arra, hogy az Infotv. nem írja elő az adatkezelők számára az elutasítás indokairól szóló tájékoztatás kötelezettségét, így ezekről részletes információk nem állnak rendelkezésre.

A személyes adatok kezelésével összefüggő adatigénylések				
elutasított személyesadat igénylés (db)	részben elutasított személyesadat igénylés (db)	teljesített személyesadat igénylés (db)	összes	adatkezelők száma
3861	48	174490	178399	31

Jól látszik a tájékoztatásokból készült összesített adatokból, hogy az adatkezelők a személyes adatokra vonatkozó adatigényléseket jellemzően teljesítik:

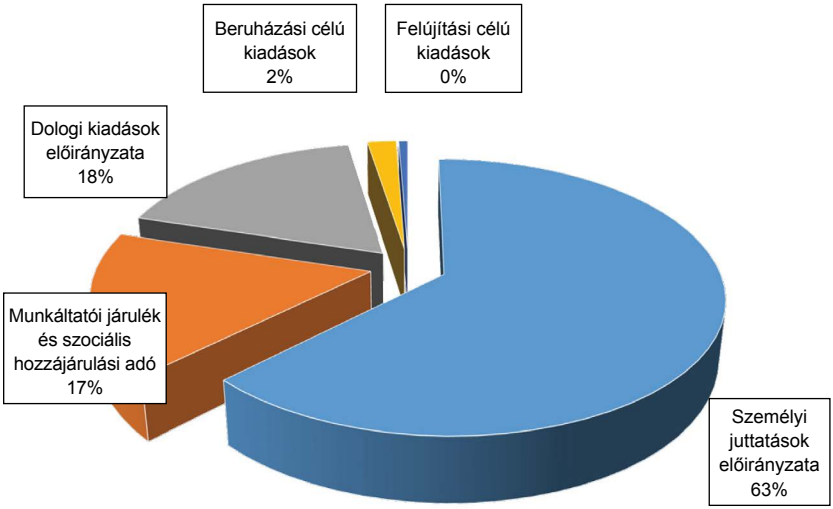
elutasított	részben elutasított	teljesített
2,16%	0,03%	97,81%

IX.4. A Hatóság költségvetése, gazdálkodása és személyi állománya

A Nemzeti Adatvédelmi és Információszabadság Hatóság működésének és gazdálkodásának 5. évét zártuk 2016. december 31-ével.

A NAIH 2016. évi költségvetése 2016. évben 573 500eFt volt, melynek %-os megoszlását mutatja a következő táblázat kiemelt előirányzatonként:

Kiemelt előirányzatok megoszlása



A 2016. évi kiemelt előirányzatok 63%-át a személyi juttatások kiemelt előirányzata tette ki. A munkáltatói járulék és szociális hozzájárulási adó 17% volt. A kiemelt dologi előirányzatok az összes költségvetés 18%-át tették ki. A beruházási kiadások 2%-a a teljes éves költségvetésnek. A felújításra tervezett előirányzat nem érte el az egy százalékot.

A 2016. évi bevételi és kiadási előirányzatok évközi változása, a teljesítési adatokkal együtt (eFt-ban)

Megnevezés	Eredeti előirányzat	Módosított előirányzat	Teljesítés	Kötelezettséggel terhelt 2016. évi maradvány
Eredeti előirányzat	573 500			
Egyéb működési célú támogatások		4 507	4 507	
Egyéb felhasználási célú támogatás fejezettől		9 500	9 500	
Egyéb szolgáltatási díj		6 384	6 384	
Szolgáltatások bevételei		4 240	4 240	
Kiszámlázott forgalmi adó bevétel		1 335	1 335	
Egyéb működési bevételek		9 156	9 156	
2015. évi költségvetési maradvány		46 935	46 935	
Bérkompenzáció		244	244	
Egyéb bevételek összesen		82 301	82 301	
Központi, irányító szervi támogatás	573 500	655 801	655 801	
Bevételi előirányzatok mindösszesen:	573 500	655 801	655 801	-
Személyi juttatások előirányzata	359 800	375 549	370 571	4 978
Munkáltatói járulék és szociális hozzájárulási adó	97 100	107 510	105 279	2 231
Dologi kiadások előirányzata	101 600	126 259	105 587	20 672
Beruházási célú kiadások	11 500	46 483	24 045	22 438
Felújítási célú kiadások	3 500	-	-	
Kiadási előirányzatok összesen:	*573 500*	*655 801*	*605 482*	*50 319*

A bevételi előirányzat és teljesítési adatai a 2016. évben

A 2016. évi eredeti bevételi előirányzat 573 500eFt volt. Az eredeti költségvetési támogatást több tényező befolyásolta, mely visszanyúlik a megelőző évre. Teljes egészében felhasználtuk a 2015. évi maradványt, amely 46 935eFt volt. A 2015. évben megrendezett Drón Konferencia támogatására 4 507eFt-ot kaptunk a Miniszterelnökségtől utólagos elszámolásra.

A 2015. évi fejezeti tartalék visszahagyásra került 2016. decemberében a Kormány által. Ebből a Hatóság épületének külső felújításához kapcsolódó árnyékolás technika kiépítése, valamint a 2018-ban hatályba lépő uniós adatvédelmi rendeletben foglaltak megvalósításához szükséges infrastruktúra, ezen belül az informatikai eszközök beszerzése fog megtörténni.

A Hatóság audit szolgáltatási és a BCR bevétele összesen 10 624eFt volt. Az uniós kiküldetések visszatérülése pedig 9 156eFt-ot tett ki. A 655 801eFt módosított bevételi előirányzat teljesítése megtörtént 2016. december 31-ig. Az Arcades-projekt elszámolásának pénzügyi teljesítése áthúzódott 2017. évre.

A kiadási előirányzatok és teljesítési adataik

A 2016. évi költségvetés eredeti előirányzata 573 500eFt volt, melyből a kiemelt eredeti személyi előirányzat 359 800eFt. A módosított személyi előirányzat 375 549eFt. A 2016. évi költségvetésbe már beépült a titokfelügyeleti alapfeladat ellátásának finanszírozása.

A munkáltatói járulék és szociális hozzájárulási adó eredeti előirányzata 97 100eFt, mely év közben 107 510eFt-ra módosult az intézményi átcsoportosítás által.

Az eredeti dologi kiemelt előirányzat 101 600eFt, volt a költségvetés szerint. A módosított dologi kiadások előirányzata 126 259eFt. A 2016. évi költségvetés eredeti dologi kiadások előirányzatában szerepel az európai adatvédelmi biztosok és hatóságok konferenciájának megrendezésére kapott 16mFt.

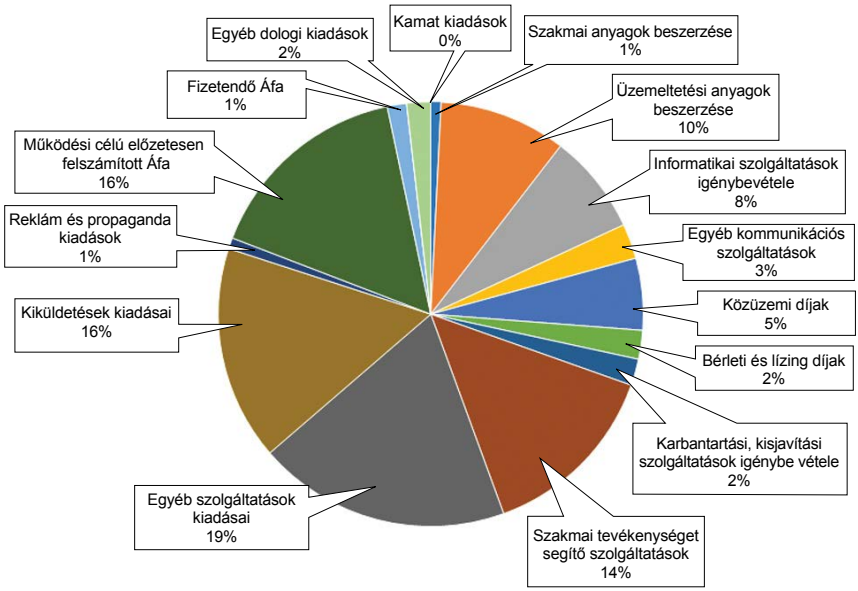
Az eredeti beruházási célú kiadási előirányzat 11 500eFt volt, mely a 2015. évi maradvány igénybevétele, a 3 500eFt felújítási célú kiadási előirányzat átcsoportosítása, valamint a 9 500eFt fejezeti tartalék visszahagyása következtében 46 483eFt-ra emelkedett.

A 2015. évi maradvány felhasználása sikeresen lezárult a 2016. évben. Ebből a biztonsági és beléptető rendszer teljes kiépítése, és az informatikai rendszer további fejlesztése valósult meg. A maradványból a Titokfelügyeleti Főosztály működésének infrastruktúráját teremtettük meg, valamint a Gazdálkodási és Humánpolitikai Főosztály számára történt egy gazdálkodási és számviteli integrált rendszer beszerzése.

A dologi kiadások megoszlása

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

Teljesült dologi kiadások megoszlása



A dologi kiadások nagyobb részét, az az 20 346eFt-ot, az egyéb szolgáltatások teszik ki, mely 19% a teljes dologi kiadásokhoz képest. A kiküldetési kiadások mértéke 17 216eFt, azaz 16%. A működési célú előzetesen felszámított áfa 16 760eFt. A szakmai anyagok beszerzésére, mely 14%, 10 232eFt-ot költöttünk. A 2016. évi 50 319eFt év végi maradvány, teljes egészében, kötelezettségvállalással terhelt maradvány. Az összegben szerepel a 9 500eFt fejezeti tartalék visszahagyása is, mely december közepén került kihirdetésre.

A bírságbevételek alakulása

A Hatóság által kiszabott és befolyt bírság teljes egészében átadásra kerül a központi költségvetés részére. A 2016. évre áthúzódó, be nem folyt bírság 109 820eFt volt. 2016. évben ténylegesen befolyt 12 400eFt bírság.

A Hatóság létszámának alakulása

A Hatóság 2016. december 31-i létszáma 73 fő volt. A 2015. évi létszámhoz képest a növekedést egyrészt a Titokfelügyeleti Főosztály létrehozása másrészt a 2018. évi uniós adatvédelmi rendeletre való felkészülés indokolja.

IX.5. A Hatóság elnökének részvétele szakmai konferenciákon, rendezvényeken

2016. január 21. – Budapest, Pázmány Péter Katolikus Egyetem, Adatrobbanás, Műhelykonferencia – A helyzet felülről – Adatbőség vs. információszabadság.

2016. február 5. – Budapest, ACCE adatvédelmi konferencia – Újdonságok az adatvédelem területéről.

2016. március 8-9. – Párizs, 13th International symposium on citizen participation and collaboration in promoting open government – Citizen participation facing the transparency challenge.

2017. március 17. – Budapest, Mathias Corvinus Collegium – Jog az internet világában: kihívások és lehetőségek című konferencia – kerekasztal beszélgetés.

2016. április 5. – Budapest, (Parlament) – A NAIH 2015. évi beszámolójának bemutatása.

2016. április 7. – Brüsszel, Annual Conference EU Data Protection Law – roundtable discussion.

2016. április 15-17. – Pozsony, GLOBSEC Global Security Conference – roundtable discussion.

2016. május 26-27. – Budapest, Az Európai Adatvédelmi Biztosok Tavaszi Konferenciája – Practical aspects of the data protection audit of secret information collection.

2016. május 31. – Budapest, NBSZ Nemzeti Kibervédelmi Intézet – Az adattörlés adatvédelmi jogi szempontból.

2016. szeptember 5-8. – Portó, 5th International Conference on Electronic Government and the Information Systems Perspective, EGOVIS 2016 – Transparency of the public sphere – dilemmas and soultions in Hungary.

2016. szeptember 15. – Budapest, ELTE ÁJK, Aula Magna – Szabó Máté 60. születésnapja alakalmából szervezett Ünnepi Konferencia – Az alapjogok védelme az információszabadság tükrében.

2016. szeptember 30. – Budapest, Nemzeti Közszolgálati Egyetem – Kutatók éjszakája – Véleményszabadság vs. Adatvédelem.

2016. október 26. – Budapest, Magyar Honvédség IV. Adatvédelmi Továbbképzés – Az adatvédelem aktualitásai.

2016. november 15. – Budapest, Acta Humana, *„A jó állam aspektusai”* című konferencia – Az alapjogok védelme az információszabadság tükrében.

2016. november 29. – Budapest, NAIH, A Belső adatvédelmi felelősök konferenciája – Aktualitások az adatvédelem és az információszabadság területén.

IX.6. Fényképek a Hatóság eseményeiről

A *„Legjobb adatvédelmi tanóra”* pályázat nyertesei a barcelonai ARCADES projekt záró konferencián, 2016. január 28-án.

Az európai adatvédelmi biztosok és hatóságok Budapesten megrendezett tavaszi konferenciája 2016

Péterfalvi Attila elnök és Jurij L. Bosickij a Kijevi Jogi Egyetem rektorának találkozója, 2016. szeptember 23.

IX.7. A beszámolóban említett jogszabályok és rövidítések jegyzéke

- 108-as egyezmény, az Európa Tanács Adatvédelmi Egyezménye: az egyének védelméről a személyes adatok gépi feldolgozása során Strasbourgban, 1981. január 28-án kelt Egyezmény, Magyarországon kihirdette az 1998. évi VI. törvény, 1998. február 27-én.
- A 2016/680-as irányelv, az Európai Parlament és a Tanács (EU) 2016/680 irányelve (2016. április 27.) a személyes adatoknak az illetékes hatóságok által a bűncselekmények megelőzése, nyomozása, felderítése, a vádeljárás lefolytatása vagy büntetőjogi szankciók végrehajtása céljából végzett kezelése tekintetében a természetes személyek védelméről és az ilyen adatok szabad áramlásáról, valamint a 2008/977/IB tanácsi kerethatározat hatályon kívül helyezéséről.
- a Délkelet-európai Rendőri Együttműködési Egyezmény kihirdetéséről szóló 2012. évi XCII. törvény.
- a jogalkotásról szóló 2010. évi CXXX. törvény.
- a jogszabályok előkészítésében való társadalmi részvételről szóló 2010. évi CXXXI. törvény.
- a közérdekű adat iránti igény teljesítéséért megállapítható költségtérítés mértékéről szóló 301/2016. (IX. 30.) Korm. rendeletet.
- a közlekedéssel összefüggő egyes törvények módosításáról szóló 2016. évi CXLIV. törvény.
- A légiközlekedésről szóló 1995. évi XCVII. törvény módosításáról szóló 2016. évi CXXXVI. törvény.
- a nemzeti felsőoktatásról szóló 2011. évi CCIV. törvény.
- a nemzeti vagyonról szóló 2011. évi CXCVI. törvény.
- a nemzetiségek jogairól szóló 2011. évi CLXXIX. törvény.
- a nyilvánosan elérhető elektronikus hírközlési szolgáltatások nyújtása, illetve a nyilvános hírközlő hálózatok szolgáltatása keretében előállított vagy feldolgozott adatok megőrzéséről és a 2002/58/EK irányelv módosításáról szóló 2006. március 15-i 2006/24/EK európai parlamenti és tanácsi irányelv.
- az állami vagyonról szóló 2007. évi CVI. törvény.
- az általános forgalmi adóról szóló 2007. évi CXXVII. törvény (ÁFA tv.).
- az előzetes és utólagos hatásvizsgálatról szóló 24/2011. (VIII. 9.) KIM rendelet.
- az Európai Parlament és a Tanács 95/46/EK adatvédelmi irányelve.
- az önkormányzati ASP rendszerről szóló 257/2016. (VIII. 31.) Korm. rendelet.

- Bit., a biztosítókról és a biztosítási tevékenységről szóló 2014. évi LXXXVIII. törvény.
- Btk., a Büntető Törvénykönyvről szóló 2012. évi C. törvény.
- Eht., az elektronikus hírközlésről szóló 2003. évi C. törvény.
- Eht., mód. az elektronikus hírközlésről szóló 2003. évi C. törvény módosításáról szóló 2016. évi CXXVIII. törvény.
- Ekertv., az elektronikus kereskedelmi szolgáltatások, valamint az információs társadalommal összefüggő szolgáltatások egyes kérdéseiről szóló 2001. évi CVIII. törvény.
- Fgytv., a fogyasztóvédelemről szóló 1997. évi CLV. törvény.
- GDPR: az Európai Parlament és a Tanács 2016/679 rendelete a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK rendelet hatályon kívül helyezéséről (általános adatvédelmi rendelet).
- Hvt., A honvédelemről és a Magyar Honvédségről, valamint a különleges jogrendben bevezethető intézkedésekről szóló 2011. évi CXIII. törvény.
- Infotv., az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény.
- Kkvtv., a kis- és középvállalkozásokról, fejlődésük támogatásáról szóló 2004. évi XXXIV. törvény.
- Magyarországnak a Nyílt Kormányzati Együttműködés kezdeményezés keretében a 2015–2017. évekre tett vállalásairól szóló második akciótervéről szóló 1460/2015. (VII. 8.) Korm. határozat.
- Mavtv., a minősített adat védelméről szóló 2009. évi CLV. törvény.
- Mvt., a munkavédelemről szóló 1993. évi XCIII. törvény.
- Nbtv., a nemzetbiztonsági szolgálatokról szóló 1995. évi CXXV. törvény.
- Rtv., a Rendőrségről szóló 1994. évi XXXIV. törvény.

Tartalomjegyzék

Nemzeti Adatvédelmi és
Információszabadság Hatóság

1125 Budapest, Szilágyi Erzsébet fasor 22/c
Levelezési cím: 1530 Budapest, Pf.: 5

Telefon: +36 (1) 391-1400
Fax: +36 (1) 391-1410

Internet: http://www.naih.hu
e-mail: ugyfelszolgalat@naih.hu

Kiadja: a Nemzeti Adatvédelmi és Információszabadság Hatóság
Felelős kiadó: Dr. Péterfalvi Attila elnök
ISSN 2063-403X (Nyomtatott)
ISSN 2063-4900 (Online)