AZ ADATVÉDELMI BIZTOS BESZÁMOLÓJA 2006

AZ ADATVÉDELMI BIZTOS BESZÁMOLÓJA 2006

Adatvédelmi Biztos Irodája
Budapest, 2007

Kiadja az Adatvédelmi Biztos Irodája
Felelős kiadó: Dr. Péterfalvi Attila
HU ISSN 1416 - 9762
Készült Rózsa Gábor nyomdájában
Borító design: K. Izcrám

Tartalom

BEVEZETŐ

Az éves beszámolók bevezetője mindig összegzés a tárgyalt évről, egyszersmind alapvetése a következő évnek. Ezek a sorok az országgyűlési biztosi intézmény második ciklusának utolsó teljes évéről szólnak, így egyfajta *„hosszú távú"* visszatekintésként is szolgálhatnak. Adatvédelmi biztosként abban a különös helyzetben vagyok, hogy – a megválasztásomat megelőző fél éves vitának köszönhetően, a többi biztostól eltérően – nekem nem fél, hanem majdnem egy teljes év van még hátra megbízatásomból. Ez nem változtat azonban azon a tényen, hogy a következő beszámolót már a harmadik ciklus adatvédelmi biztosa fogja benyújtani. Így ez a bevezető is összegzi az elmúlt évek tapasztalatait, ez is felvezeti a következő évet; azt az évet, melyben – reményeim szerint – sikerül megoldást találnunk néhány újonnan felmerült vagy éppen az elmúlt években folyamatosan duzzadó problémára.

Az elmúlt hat év kétségkívül legmarkánsabb jellemzője az volt, hogy a vizsgálatok száma a korábbi évek átlagához képest több mint a duplájára emelkedett, majd ezen a szinten stabilizálódott. Az ügyszámok emelkedése nagyjából azonos arányban érintette mindhárom fő területet – adatvédelem, információszabadság, jogszabály-véleményezés –, jelentős azonban a szerkezeti változás; új, hangsúlyos tevékenységként pedig megjelentek a határokon átnyúló vizsgálatok, a nemzetközi kötelezettségek és együttműködés. A szerkezeti változás leginkább az adatvédelemmel kapcsolatos ügyekben figyelhető meg: az állam mint adatkezelő egyre inkább háttérbe szorul munkánk során, míg a magánszféra adatkezelései egyre többször késztetik a polgárt arra, hogy tollat (vagy éppen klaviatúrát) ragadjon, és leírja sérelmeit. Egyre nehezebb tartani a hagyományos tagozódást is, hiszen számos esetben nem egyes adatkezelők, hanem módszerek azok, melyek kiváltják a polgárok ellenérzéseit.

Az utolsó mondat átvezet arra a jelenségre, amely egyre inkább meghatározza az adatvédők munkáját nem csupán nálunk, hanem szinte bárhol a világon. Ez pedig a technika fejlődésének adatvédelemre gyakorolt hatása. A biometrikus azonosítók, rádiójellel működő azonosító chipek, fejlett kamerarendszerek, adatelemző programok új kihívást jelentenek. Nem csupán azért, mert nehéz lépést tartani a rohamos fejlődéssel, hanem azért is, mert a gondolkodásunkon kell vál-

toztatni: a korábbi, adatkezelőkre és adatkezelésekre való irányultság helyett teljesen más szemléletet igényel az, ha egy technológiát, annak lehetséges hatásait és alkalmazási területeit vizsgáljuk. Ez a folyamat az elmúlt években a beszámolókon is éreztette hatását, a „*további érdekes ügycsoportok*" között először a kamerák, majd a biometrikus azonosítók kérdéskörét tárgyaltuk külön, most azonban immár kiemelt helyen, nagyobb terjedelemben foglalkozunk egy újszerű, és a jövőben minden bizonnyal meghatározó technológiával, a rádióhullámokon alapuló azonosítással.

Ugyancsak megfigyelhető volt az a folyamat is, amely 2006-ban nagyon markánsan megjelent: adataink már nem védhetőek határainkon belül. A közhatalmi adatkezelések közül a bűnüldözést és bűnmegelőzést szolgálók azok, melyek egyre inkább összekapcsolódnak a terrorizmus, a szervezett bűnözés elleni nemzetközi harc jegyében, de európai szinten más jellegű, gazdasági célú együttműködési folyamatok is igénylik a közös adatkezelési rendszereket, adatszolgáltatási csatornákat. A gazdasági szféra pedig már régóta nem ismeri a határokat. A „*multik*" korában élünk, a bankok, távközlési szolgáltatók, marketing cégek, de – az internetnek köszönhetően – még az áruházak is számos országban jelenlevő nagyvállalatok, melyek igyekeznek egységes szempontok szerint működni, függetlenül az egyes országokban megjelenő jogi háttértől. Ez sokszor eredményezi, hogy a máshol bevett gyakorlat nálunk jogellenes adatkezelést jelent, egyúttal szükségessé teszi a nemzetközi együttműködést is. Az ilyen jellegű ügyeinkről a korábbinál terjedelmesebb, lényegesen informatívabb „*Nemzetközi ügyek*" című fejezet szól – bár egyre nehezebb megvonni a határt a nemzeti és nemzetközi ügyek között.

Ugyancsak munkánk meghatározó tényezőjévé vált a jogalkotásban való részvételünk. Ez természetesen elsősorban az előkészítő szakaszra vonatkozik, melynek során egy-egy tervezetről nyilvánítunk véleményt. Ez a munka sokszor nehéz, hiszen jellemzőek a nagy terjedelmű munkaanyagok, illetve esetenként a véleményezésre adott rövid határidő – a néhány órás terjedelemmel – mintegy jelzi: a vélemény kérése inkább formális procedúra. Nem lehet azonban eléggé hangsúlyozni e tevékenység fontosságát: míg konkrét panaszügyekben arra van lehetőségünk, hogy a jogszabályt sértő magatartást megakadályozzuk, egy tervezetről nyilvánított vélemény és annak határozott képviselete megelőzheti azt, hogy sok állampolgár érezze sértve Alkot-

mányban biztosított jogait. A munkánk azonban nem csupán az előkészítő szakra korlátozódik: számos esetben már elfogadott jogszabály megváltoztatását kezdeményezzük a jogalkotónál. E tevékenységünk váltakozó sikert hoz, előfordult az is, hogy sikertelen egyeztetések, kezdeményezések után az Alkotmánybíróság mondta ki a végső szót.

Természetesen nem hagyta változatlanul az idő a másik fontos, védendő alapjogot, a közérdekű adatok nyilvánosságát sem. A vizsgálatok számának rohamos emelkedése az információszabadságot is érintette, a polgárok egyre öntudatosabbak ezen a téren is. Ha tudni akarnak valamit, nem félnek kérdezni a választ birtokló szervtől, ha elutasítják őket, akár harcolnak is azért, hogy tájékoztassák őket arról, amihez közük van. Jelentős változást hozott az elektronikus információszabadságról szóló törvény is, bár annak teljes körű érvényesülése még várat magára – minden bizonnyal azért, mert még az állam szerveinek is meg kell tanulni azt, hogy már nemcsak akkor kell válaszolniuk, ha kérdezik őket, hanem maguktól is tájékoztatást kell adniuk mindarról, ami a polgárokat esetleg érdekelheti. Pozitívum, hogy egyre több állami szerv honlapján található meg a szervezeti felépítés leírása, az egyes vezetők, tisztviselők elérhetőségei, a szerv munkáját meghatározó vagy annak eredményeként megjelenő dokumentumok.

Az újszerű feladatok természetesen új szemléletet is kívánnak. Egyre inkább lehetetlen egysíkú jogászi szemlélettel választ találni a kérdésekre, az adatvédőknek mindig érteni kell a vizsgált terület általános jellemzőihez, sőt, immár elengedhetetlen bizonyos szintű „*informatikai műveltség*" is. Szükséges tehát a szemlélet változása, és ez szükségessé teszi azt is, hogy a jogosítványok változzanak. Az Európai Unióhoz való csatlakozás nyomán hatályba lépett új szabályok – melyek egyfajta hatósági jogkört biztosítanak az adatvédelmi biztosnak azzal, hogy kötelező, csak bíróság által felülbírálható döntési jogkört adnak neki – mindenképpen előrelépést jelentenek. Valószínűsíthető ugyanakkor, hogy mire lejár a harmadik ciklus, és az intézmény a maga 18 évével nagykorúvá válik, további szemléletváltozásra és jogszabály-módosításra lesz szükség ahhoz, hogy az adatvédelem valóban hatékony, a modern kor követelményeinek és kihívásainak megfelelni tudó jogintézménnyé válhasson.

Azt, hogy a 2007-es év mit hoz, nem tudhatjuk. Számos régi és új kihívás áll előttünk, ezekkel szembenézni sokszor nehéz feladat. Azt mindenesetre kijelenthetem: munkatársaimmal együtt azon vagyok,

hogy az adatvédelem ne akadályként jelenjen meg, hanem a fejlődést helyes irányba mozdító tényezőként, melynek köszönhetően a technikai fejlődés előnyeit úgy évezhetjük, hogy közben jogainkról sem kell lemondanunk.

Bár az előző mondat lehetne a legjobb végszó, a bevezetőm végén egy szerkezeti változtatásra kell felhívnom az olvasó figyelmét: az ügyek és ügytípusok számának növekedése immár lehetetlenné tette, hogy az elmúlt év állásfoglalásaiból olyan válogatást állítsunk össze, amely valóban hasznos, és könnyen áttekinthető. Éppen ezért elmarad az elmúlt években megszokott *„második kötet”*, viszont az érdeklődő nagy számú állásfoglalást találhat meg honlapunkon – a technikai fejlődés és az elektronikus információszabadság szellemében.

Dr. Péterfalvi Attila

I. TEVÉKENYSÉGÜNK FŐBB ADATAI

Az Adatvédelmi Biztos Irodájához 2006-ban összesen 11654 irat (postai küldemény, levél, elektronikus levél) érkezett. A valamilyen intézkedést igénylő, vagyis *„érdemi"* iratok száma összesen 10124 volt. Az elektronikus iktatórendszerben (ELIK) 7556 iratot dolgoztunk fel, melyek nagyobbik része beérkező és a vizsgálatokhoz kapcsolódó küldemény volt. Összesen 2211 küldeményt vizsgált ügyként iktattunk. Az adatvédelmi nyilvántartásba és az elutasított kérelmek nyilvántartásába 1237 iratot küldtek az adatkezelők, melyből 753 adatkezelési bejelentés volt.

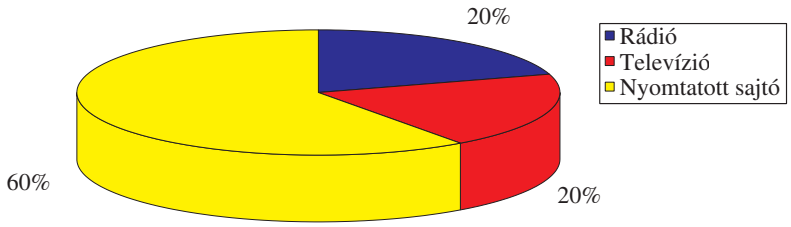
Az elektronikus levelek forgalma a következőképpen alakult. A kéretlen e-maileket, spameket leszámítva összesen 3125 valamilyen intézkedést igénylő e-mail érkezett az Adatvédelmi Biztos Irodája hivatalos postafiókjába az *„adatved@obh.hu"* címre, melyek közül 879 levelet ügyként iktattunk. Ez 149-cel több az előző évhez képest. (2005-ben 730 új ügy érkezett be villámpostán.) A jogszabály-előkészítések során a kodifikációt végzők 2006-ban szinte minden jogszabály tervezetét (278) elektronikus formában küldték meg véleményezésre, összesen 273-at. Ez az előző évhez képest (466 tervezet) jóval kevesebb ügyet jelent, ám azt is figyelembe kell venni, hogy a jogalkotás intenzitása, üteme a választások miatt 2006-ban igencsak mérséklődött. A manapság már teljesen bevetté vált gyakorlat – a szinte kizárólagossá váló elektronikus eljárás – felgyorsítja és hatékonnyá, illetve költségkímélőbbé teszi a jogszabály-véleményezési feladatkör ellátását, azonban van egy hátrányos következménye is, nevezetesen a jogszabályokat előkészítők csak az utolsó pillanatban elküldve, igen rövid határidőt hagynak a tervezetek véleményezésére, így sok esetben csak napok, illetve órák állnak az iroda rendelkezésére. Minderről részletesen a jogszabály-véleményezésekről szóló fejezetben olvashatunk. A már folyamatban levő vagy lezárt ügyekhez 512 e-mail érkezett. Az egyéb tárgyú megkeresések, tájékoztatók, elektronikus hírlevelek száma 283 volt. Külföldről minden korábbinál több, összesen 1164 e-mail érkezett, ezek a különböző uniós bizottságok, munkacsoportok, illetve az Európai Unió adatvédelmi biztosának hivatalából érkező, valamint az ombudsmanok, adatvédelmi biztosok és hatóságok nemzetközi együttműködést, kap-

csolattartását, információcseréjét szolgáló küldemények voltak, de akadt köztük konzultációs, illetve panaszbeadvány is. Miként azt az előző évek számadatai is bizonyítják egyre népszerűbbé válik az adatvédelmi biztoshoz fordulók között a beadványozás elektronikus formája. 2006-ban a beérkező beadványok közel 40 %-a e-mailben érkezett. 2006 folyamán az Országgyűlési Biztosok Hivatala a levélszerverre érkező elektronikus küldemények szűrését ellátó rendszert telepített. Összesen több mint 50 000 kéretlen üzleti, illetve egyéb célú levél érkezett elektronikus postafiókunkba, melyeknek egy jelentős részét sajnos nem képes biztonságosan kiszűrni az alkalmazott rendszer, így továbbra is nagyon sok spam érkezik hozzánk.

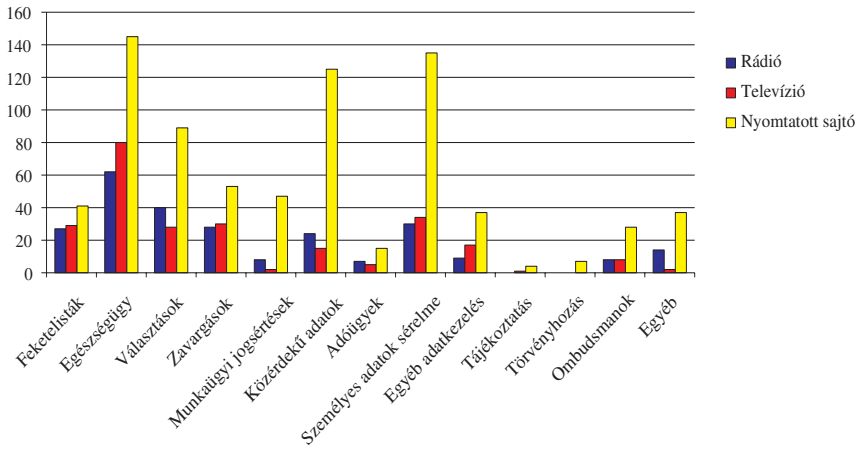
Az iroda által ügyként kezelt és iktatott iratok száma (2211) – az előző évhez viszonyítva (2350 ügy) – hat százalékkal csökkent, a több éve tartó drasztikus ügyszámemelkedés tehát látszólag megállt. Ez a megállapítás azonban csalóka, hiszen elég, ha csak a jogszabály-véleményezések fentiekben említett alacsony számára és annak okaira gondolunk. A jogszabály-véleményezések száma 469-ről 278-ra, a panaszügyeké 1149-ről 1241-re, a konzultációs ügyeké 490-ről 434-re változott. A nemzetközi ügyek száma 139-ről 145-re emelkedett. Figyelemreméltó, hogy a panaszügyek száma az előző év 240-es növekedési számához képest is tovább nőtt 2006-ban közel 100-al.

Az adatvédelmi biztos megjelenése az elektronikus médiában és a nyomtatott sajtóban a 2006. január 1. és 2006. december 31. közötti időszakban

Az adatvédelmi biztos médiaszereplései



Az adatvédelmi biztos médiaszerepléseinek fontosabb témakörei



Témakörök	Rádió	Televízió	Nyomtatott sajtó	Mind összesen
Feketelisták	27	29	41	97
Egészségügy	62	80	145	287
Választások	40	28	89	157
Zavargások	28	30	53	111
Munkaügyi jogsértések	8	2	47	57
Közérdekű adatok	24	15	125	164
Adóügyek	7	5	15	27
Személyes adatok sérelme	30	34	135	199
Egyéb adatkezelés	9	17	37	63
Tájékoztatás	0	1	4	5
Törvényhozás	0	0	7	7
Ombudsmanok	8	8	28	44
Egyéb	14	2	37	53
Összesen	**257**	**251**	**763**	**1271**

Az Adatvédelmi Biztos Irodájába érkezett ügyek megoszlása

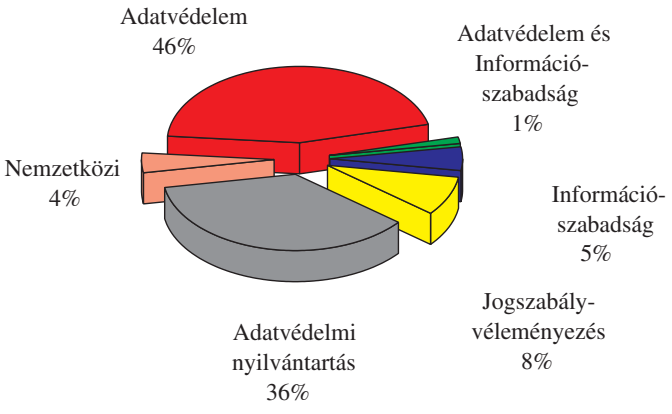
Ebben az évben a tavalyihoz hasonlóan áttekinthető és egyszerű ábrákon szemléltetjük az irat- és ügyforgalmat bemutató statisztikai elemzést. Az adatvédelmi nyilvántartás a már megszokott módon önálló fejezetben szerepel. Az összes, vagyis a 2211 ügyből az adatvé-

delmi ügyek száma 1524 (1493), a jogszabály-véleményezéseké 278 (469), az információszabadságot érintő ügyek száma 169 (196) volt, 45 beadvány mindkét alkotmányos alapjogot érintette. Az információszabadságot is érintő ügyeink száma tehát összesen 214. A nemzetközi ügyeink száma 145 (139) volt. (A zárójelben feltüntetett adatok minden esetben az előző, 2005. évre vonatkoznak.) Hivatalból összesen 27 vizsgálat indult. Az adatvédelmi nyilvántartásba küldött iratok (bejelentkezések, módosítások, törlések) száma 753 volt, az elutasított személyes, illetve közérdekű adatokra vonatkozó kérelmekről a kézirat lezárásáig 446 jelentést kaptunk. A jelentések beküldésének határideje 2007. február 1-je, de a több éves tapasztalat azt mutatja, hogy ezt követően, illetve a kézirat lezárása (február 15.) után is sok jelentés érkezik, melyek száma minden évben meghaladja a százat.

Ha az adatvédelmi biztos hatáskörébe tartozó két információs alapjogot érintő beadványok számát, illetve arányát vesszük szemügyre, akkor megállapítható, hogy az információszabadságot és a közérdekből nyilvános adatokat is érintő ügyek aránya az adatvédelemhez képest több mint 14 százalék, ez az adat az elmúlt évek adataihoz képes kis mértékű (egy százalékos) emelkedést mutat.

Az Adatvédelmi Biztos Irodájába érkezett ügyiratok és nyilvántartási kérelmek

2006 (%)



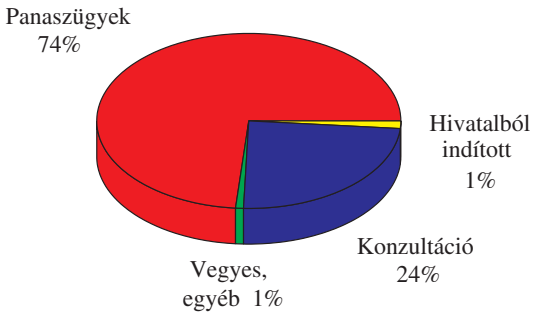
A vizsgálatok általános jellemzői

A főbb ügytípusok

A 2211 iktatott ügyirat közül ebben az évben 1241 adatvédelemmel és információszabadsággal kapcsolatos panaszügy érkezett, ez nyolc százalékos emelkedést tesz ki. Tavaly is igen jelentős számú, 1149 ilyen ügy volt. A konzultációs beadványok, K-s ügyek száma 490-ről 434-re, kis mértékben csökkent. A jogszabály-véleményezések, vagyis a J-s ügyeink száma jelentősen, 469-ről 278-ra esett vissza. A nemzetközi, vagyis az I-s ügyeink száma ismét emelkedett, 145 volt. Az arányuk nem változott, hat és fél százalék az összes iktatott ügyhöz képest. A nemzetközi és európai ügyek részletes ismertetése a beszámoló Nemzetközi Ügyek fejezetében olvasható.

Az adatvédelmet érintő 1546 ügy megoszlása a következőképpen alakult: részben vagy egészben adatvédelmi panaszügy 1139, adatvédelemmel kapcsolatos konzultációs ügy 370, hivatalból indított adatvédelmi vizsgálat 22 volt. A 15 egyéb, illetve vegyes ügy körébe az információs jogok védelmével kapcsolatos levelezések, hivatalos intézkedést, reagálást igénylő kiadványok, tájékoztatók, előadások, értekezletek, szóbeli konzultációk, tárgyalások emlékeztetői, iratanyagai tartoznak.

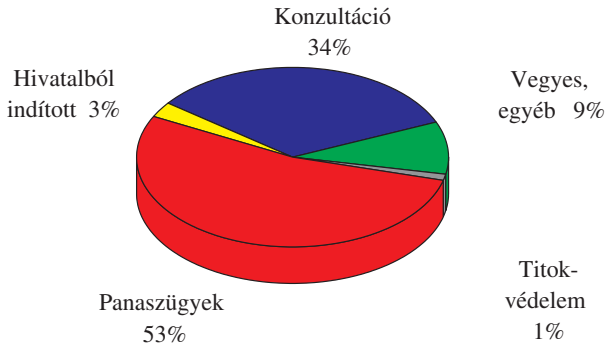
Az adatvédelmi ügyek megoszlása
2006 (%)



Az információszabadságot, vagyis a közérdekű adatok nyilvánosságát érintő ügyek száma 191. Ebből 102 panasz, 64 konzultációs ügy és 5 hivatalból indított vizsgálat volt, 18 egyéb, illetve vegyes ügy, 2 beadvány titokvédelmi tárgyú volt.

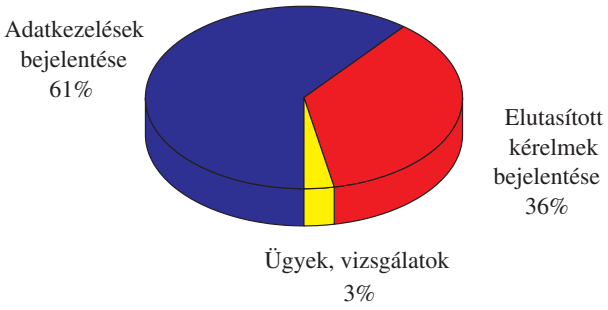
A közérdekű adatok nyilvánosságát érintő ügyiratok megoszlása

2006 (%)



Az adatvédelmi nyilvántartásba beküldött adatkezelési bejelentéseket és a szintén az adatvédelmi nyilvántartás körében feldolgozott az elutasított személyes és közérdekű vagy közérdekből nyilvános adatokra vonatkozó elutasított kérelmekről adott jelentéseket az Adatvédelmi Nyilvántartási Főosztály külön iktatási rendszerben (AVENTA), a vizsgálatot igénylő ügyektől elkülönítetten tartja nyilván. Az ELIK-ben nyilvántartott, vizsgálatot igénylő nyilvántartási ügyek (N-es ügyek) száma 38 volt. Az AVENTÁ-ba érkezett bejelentések száma 753 volt. Az adatvédelmi törvény 13. §-ának (3) bekezdése, valamint a 20. §-ának (9) bekezdése alapján az adatkezelők az érintettek személyes adataik kezelésére vonatkozó tájékoztatási kérelmének, valamint közérdekű adat megismerésére irányuló kérelmek elutasításáról és annak indokairól évente értesítik az adatvédelmi biztost. A beszámoló elkészítéséig összesen 446, 2006. évre vonatkozó jelentés érkezett. Az adatok szolgáltatására felhívó közlemény a honlapunkon, a jelentések statisztikai elemzése az adatvédelmi nyilvántartásról szóló fejezetben olvasható.

Az adatvédelmi nyilvántartás ügyiratainak megoszlása
2006 (%)

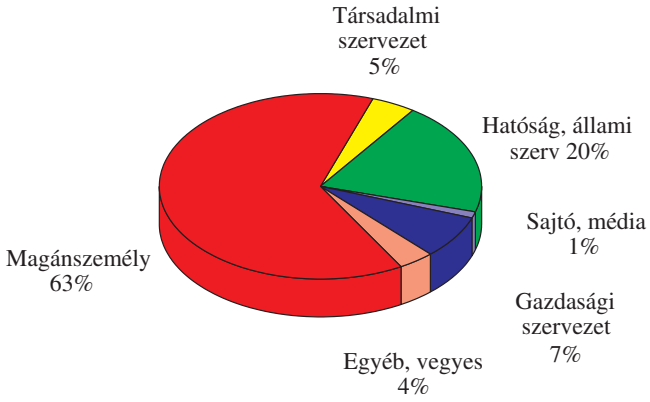


Az indítványozók aránya

Az alábbi ábra az adatvédelmi biztoshoz forduló személyek, szervezetek számáról, illetve arányáról ad tájékoztatást. 2006-ban ismét növekedett azon beadványok (panaszok, konzultációk) száma, amelyeknek indítványozói magánszemélyek/állampolgárok voltak, 1228 ilyen ügy volt (2005-ben: 1150). Az indítványozók összetétele, aránya a korábbi évekhez képest nem változott jelentősen, bár a jogi személyiséggel rendelkező indítványozók száma csökkent, ami az ügyszámok csökkenésének és ezen belül a konzultációs beadványok csökkenésének másik tényezője lehet. Mind a társadalmi szervezetek (90 beadvány), mind a sajtó részéről csökkenő indítványozói érdeklődésről számolhatunk be. Kiemelendő, hogy a sajtó, illetve a média munkatársai részéről érkező beadványok száma közel a felére, 42-ről 23-ra esett vissza.

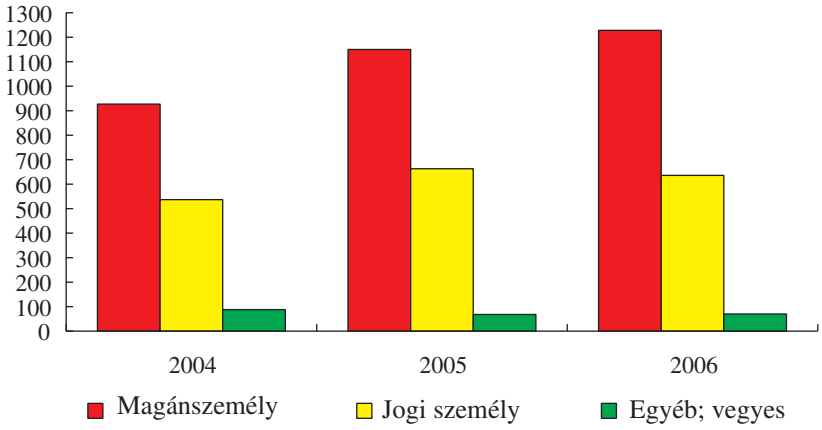
Az indítványozók aránya

2006 (%)



A jogi és a magánszemély indítványozók aránya

2004 - 2006



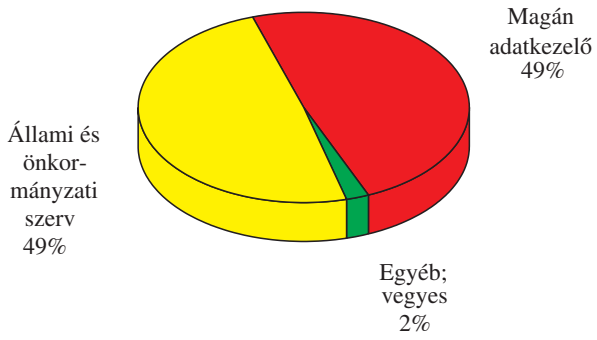
A vizsgált adatkezelők típusai

Az adatvédelmi biztos és irodája 2006-ban összesen 1976 (2005-ben 1971) adatkezelőt, illetve általuk folytatott adatkezelést vizsgált (volt olyan vizsgálat, amelyben több adatkezelő is érintett volt, illetve

volt olyan adatkezelő, amelyet érintően több különböző vizsgálat – panasz, konzultáció – is folyt). Az utóbbi három év idősor adatait összehasonlítva megállapítható, hogy nagyobb mértékben nőtt a magán adatkezelőket érintő vizsgálatok száma (897-ről 963-ra), és kis mértékben csökkent a vizsgált állami-önkormányzati adatkezelők száma 993-ról 971-re). Állandósulni látszik tehát az a folyamat, hogy a vizsgálatok száma és aránya szinte egyenlően érinti a magán és az állami, illetve önkormányzati adatkezelőket.

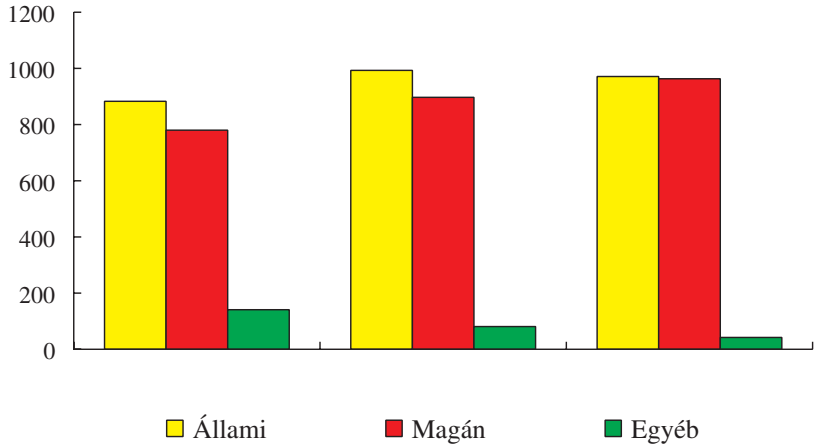
A vizsgált adatkezelők típusai

2006 (%)



A vizsgált adatkezelők típusai

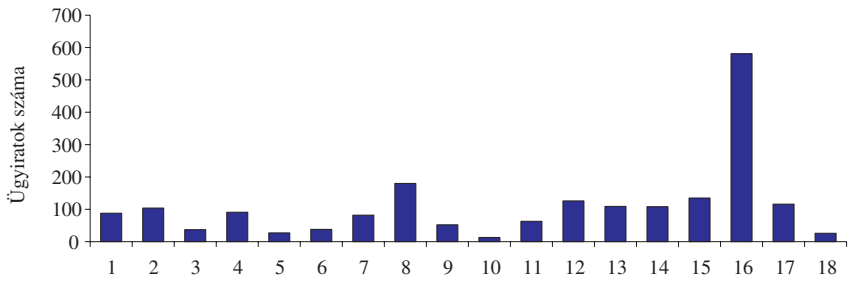
2004 - 2006



A vizsgált adatkezelők között – legmagasabb számát tekintve – 581 vizsgálattal továbbra is első helyen kell megemlíteni az egyéb adatkezelők közé sorolt munkáltatókat (68 vizsgálat), a különböző szolgáltatásokat nyújtó egyéb gazdasági társaságokat (350), áruküldőket, direkt marketing cégeket (23), illetve társasházakat (32) és a magánszemély adatkezelőket (103 vizsgálat) és az ügyvédi irodákat. Ide tartoznak a kéretlen, üzleti célú reklámot, ajánlatot tartalmazó elektronikus levelekre (spamekre) vonatkozó vizsgálatok is, melyek száma 2006-ban robbanásszerűen nőtt (magánszemélyek, illetve egyéb gazdasági társaságok adatkezelői körében). A sajtót és a médiát érintő ügyeink száma nem változott, 109 vizsgálat volt. Az egyéb közhatalmi szerveket (bíróságok, ügyészségek, dekoncentrált közigazgatási szerveket) érintő beadványok száma 66-ról 104-re emelkedett, megjegyezve, hogy a bíróságokat érintően az adatvédelmi biztosnak csak igen szűk vizsgálati jogosultságai vannak. 32-ről 52-re emelkedett az államigazgatási jogkörben eljáró egyéb szerveket érintő vizsgálatok száma. Valamelyest csökkent a pénzintézeteket érintő vizsgálatok száma, 137-ről 108-ra, és tovább csökkent a központi szerveket, minisztériumokat érintő vizsgálatok száma, 105-ről 88-ra.

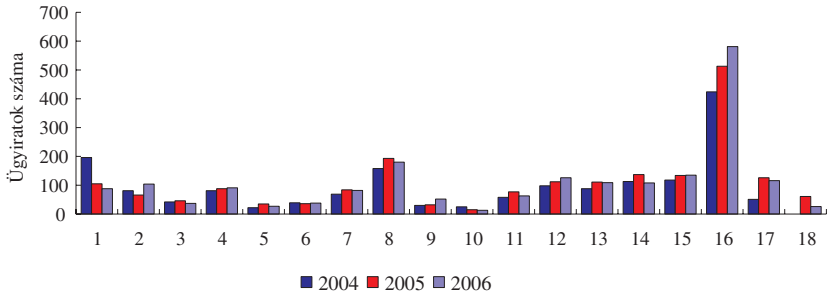
A vizsgált adatkezelők kategóriái

2006



A vizsgált adatkezelők kategóriái

2004 – 2006



1 Központi közigazgatási szerv
2 Egyéb közhatalmi szerv
3 Nemzeti adatbázis, nagy adatkezelő
4 Fegyveres és rendvédelmi szerv
5 Társadalombiztosítás/munkaügy
6 Adóhivatal, pénzügyőrség
7 Egészségügyi intézmény
8 Helyi önkormányzat és szervei
9 Államigazgatási jogkörben eljáró egyéb szerv
10 Szakosított felügyeleti szerv
11 Oktatási intézmény/kutatóintézet
12 Társadalmi szervezet
13 Sajtó/média
14 Pénzintézet
15 Közüzemi szolgáltató
16 Egyéb adatkezelő (áruküldők, társasházak, munkáltatók...)
17 Külföldi adatkezelő
18 Nincs adatkezelő

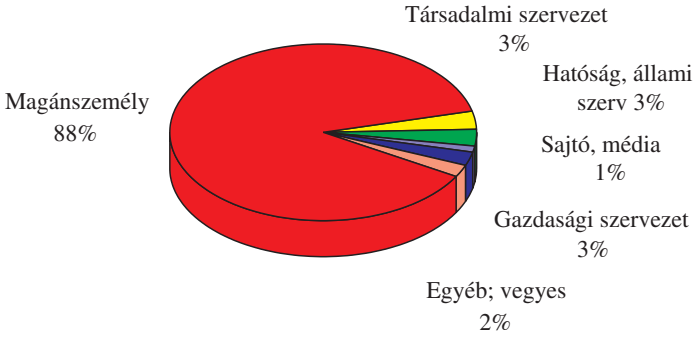
Panaszügyek

Ha az adatvédelmi biztoshoz forduló érintettet konkrét jogsérelem érte, vagy annak közvetlen veszélye állt fenn, beadványát panaszügyként kezeljük. A panaszügyek jele „*A*”, 2007-től „*P*”. A panaszügyeknek alapvetően két fajtáját különböztethetjük meg. Az egyik esetben az indítványozó vizsgálat lefolytatása nélkül a hatályos jogszabályok, a csatolt dokumentumok, illetve az általa leírtak alapján kér az ügyre vonatkozó (általános) állásfoglalást az adatvédelmi biztostól. Ebben az esetben sokszor a vizsgálattal érintett szerv nem is szerez tudomást a vizsgálatról csak akkor, ha az olyan általános jogsértést tár fel, amelyet mindenképpen orvosolni kell. Ha „*csupán*” egyéni jogsértést állapítunk meg, az indítványozó joga eldönteni, hogy kéri-e az adatvédelmi biztos közbenjárását és eljárását az ügyében, vagy saját maga fordul az adatkezelőhöz és érvényesíti jogait.

A másik esetben az indítványozó eleve kéri a panaszolt adatkezelés és adatkezelő vizsgálatát. Az indítványozó kilétét – amennyiben az feltétlenül szükséges –, az érintett hozzájárulásával fedjük fel a vizsgálat során. Természetesen a jogsértés súlyára, az érintettek számára tekintettel előfordul, hogy a hivatalból indítunk vizsgálatot olyan esetekben is, amelyekben azt az indítványozó eredetileg nem kérte. A konkrét jogsérelmet leíró, vagyis panaszügyként kezelt beadványok száma 2006-ban 1241 (2005-ben 1149) volt. A panaszvizsgálatok száma 2006 során nőtt, ellentétben az összes vizsgált ügy számával, amely – mint azt fent már szintén ismertettük – csökkent. A vizsgált panaszügyek indítványozóinak összetétele, aránya a következőképpen alakult. A magánszemély panaszosok aránya nem változott számottevően, ezúttal is a már megszokott 88 százalék volt. A társadalmi szervezetek 41, hatóságok, állami szervek 39, gazdasági szervezetek 34 panaszt nyújtottak be. Miként az összes indítványnál, a panaszügyeknél is megfigyelhető a sajtó, média képviselőinek lanyhuló indítványozó kedve, összesen 12 panaszügyet terjesztettek elő egész évben. Azt azért nem árt hangsúlyozni, hogy a média képviselői számtalan alkalommal keresik meg az adatvédelmi biztost és kérik ki véleményét egy-egy adatvédelmet, illetve információszabadságot érintő kérdésben, de a biztos által adott interjúk, nyilatkozatok ügyként nem szerepelnek a statisztikai rendszerben, illetve az ügyeket más érintett személy vagy szervezet indítványa alapján vizsgáljuk ki.

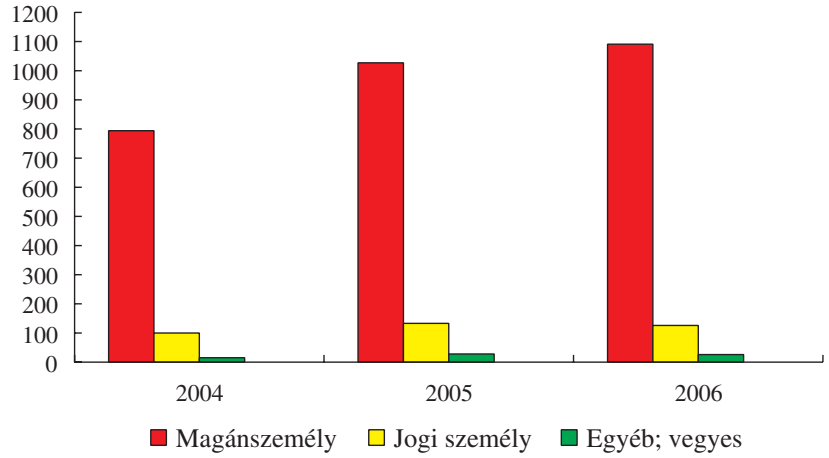
A panaszosok aránya

a 2006. év panaszügyeiben (%)



A jogi és magánszemély panaszosok aránya

Panaszügyek 2004 – 2006



A bepanaszolt adatkezelők típusai

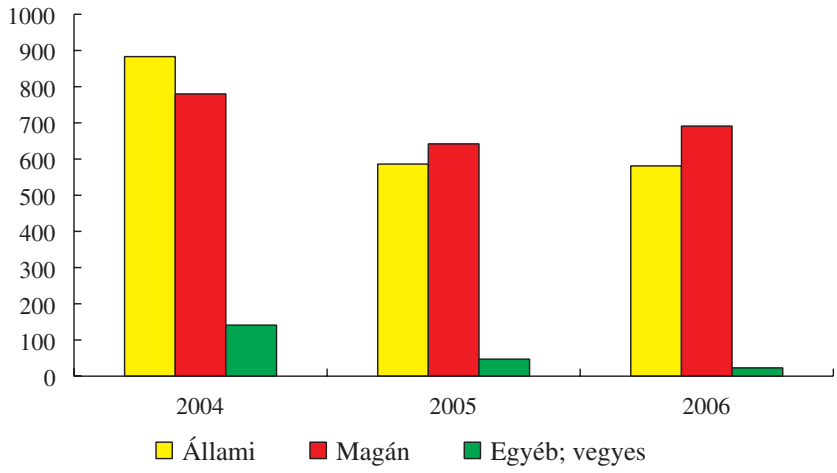
2006-ban a panaszolt adatkezelések száma nem változott számottevően, az indítványozók összesen 1295 adatkezelőt, illetve adatkezelést kifogásoltak. Egy indítvány több, illetve többféle panaszt is tartalmazhat, sőt előfordul, hogy mindkét alapjogot érinti, vagy ami szintén nem ritka, hogy a két alapjog konfliktusa, vélt vagy valós ütközése a beadvány tárgya. 2006-ban a bepanaszolt adatkezelések 45 százaléka állami, önkormányzati, 53 százaléka valamely magánszervezet vagy -személy adatkezelését érintette. Az elmúlt évek adatait, arányait is figyelembe véve ezen adat azt jelzi, hogy nemcsak hogy megfordult a magán, illetve az állami, önkormányzati adatkezelések bepanaszolásának aránya, hanem a kifogásolt magán adatkezelések száma és aránya évről évre nő.

A bepanaszolt adatkezelők típusai

a 2006. év panaszügyeiben (%)

A bepanaszolt adatkezelők típusai

Panaszügyek 2004 – 2006



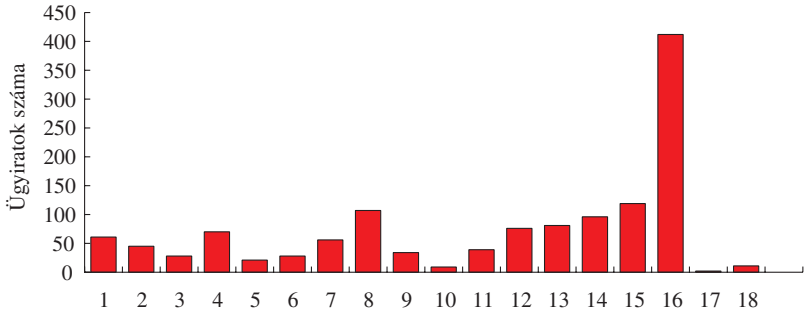
A bepanaszolt adatkezelők kategóriái

2006 folyamán a legtöbb panaszbeadvány az egyéb adatkezelőkkel szemben (magánszemélyek, egyéb gazdasági társaságok, munkáltatók, társasházak, áruküldők, közvélemény-kutatók) érkezett, összesen 412 panaszt vizsgáltunk (szemben a tavalyi 362 esettel). A közüze-

mi szolgáltatókat 119, a helyi önkormányzatok és szerveik eljárását 107, a pénzintézeteket 96, a sajtó adatkezelését 81 esetben sérelmezték a panaszosok. 2006-ban kevesebb pénzintézeteket érintő panaszt kaptunk, mint egy évvel korábban. Emelkedett a társadalmi szervezeteket, a központi közigazgatást és a közigazgatási jogkörben eljáró egyéb szerveket érintő panaszügyek száma. A legszembetűnőbb növekedést a már részletezett egyéb adatkezelők mellett a társadalmi szervezeteknél, közöttük a politikai pártoknál és az általuk kampánycélból folytatott adatkezeléseknél, illetve a központi közigazgatási és az egyéb közigazgatási szerveknél, valamint a közüzemi szolgáltatóknál figyelhetünk meg. Az egyéb közigazgatási szerveket érintő panaszok száma közel megduplázódott, melynek elsődleges oka a gázár támogatáshoz kapcsolódó adatkezeléseket kifogásoló beadványok magas száma, valamint a közigazgatási szervek közérdekű adat szolgáltatását érintő panaszok számának emelkedése. Továbbra is igen magas a média adatkezelése (81), valamint a rendvédelmi szervek (70), közöttük a rendőrség adatkezelése miatt előterjesztett panaszok száma is.

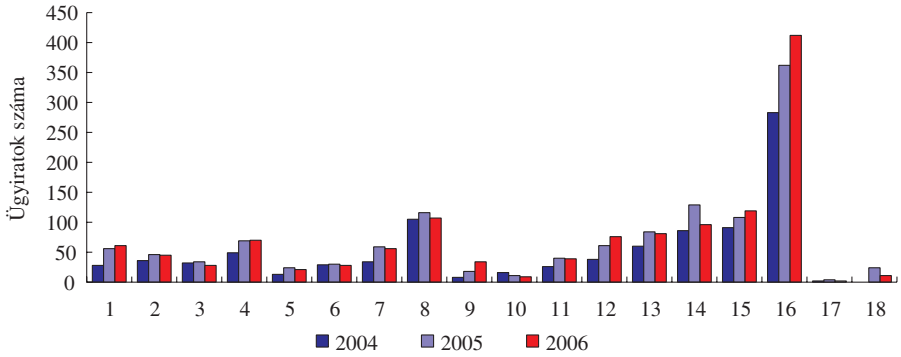
A bepanaszolt adatkezelők kategóriái

a 2006. év panaszügyeiben



A bepanaszolt adatkezelők kategóriái

Panaszügyek 2004 – 2006



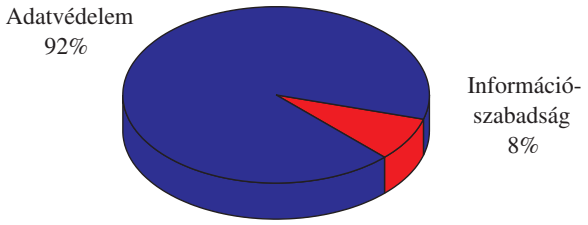
1 Központi közigazgatási szerv
2 Egyéb közhatalmi szerv
3 Nemzeti adatbázis, nagy adatkezelő
4 Fegyveres és rendvédelmi szerv
5 Társadalombiztosítás/munkaügy
6 Adóhivatal, pénzügyőrség
7 Egészségügyi intézmény
8 Helyi önkormányzat és szervei
9 Államigazgatási jogkörben eljáró egyéb szerv
10 Szakosított felügyeleti szerv
11 Oktatási intézmény/kutatóintézet
12 Társadalmi szervezet
13 Sajtó/média
14 Pénzintézet
15 Közüzemi szolgáltató
16 Egyéb adatkezelő (áruküldők, társasházak, munkáltatók...)
17 Külföldi adatkezelő
18 Nincs adatkezelő

Információs ágak a panaszügyekben

Az összes panaszügy (1241) közül személyes adataik kezelése miatt 2006-ban 1137-en tettek panaszt, vagyis 86-tal többen, mint 2005-ben. A közérdekű adatok kezelésének gyakorlatát 100 esetben kifogásolták (2005-ben „*csak*” 88-szor) az adatvédelmi biztosnál. A panaszügyekben információs ágak szerinti megoszlását tekintve is nagyon magas az adatvédelem aránya (92%-8%). A korábbi években a megoszlási állandó jellemzője volt, hogy az adatvédelmi panaszok hányada évről évre tovább emelkedett. Ez a folyamat 2004-ben megfordult, és sem 2005-ben, sem 2006-ban nem változott, mivel a közérdekű információk kezelését kifogásoló panaszbeadványok száma most is több mint 8 százalékot tesz ki szemben a korábbi 6 százalékkal. Meg-

jegyzendő, hogy míg az összes ügyet tekintve a mindkét alapjogot érintő beadványok száma 45 volt, ebből öt volt panaszügy. A panaszügyek számának további emelkedésével párhuzamosan nőnek, lépést tartanak az információszabadság érvényesülését kifogásoló panaszok, vagyis időtállónak tekinthetjük azt a tavaly leírt álláspontot, miszerint: *„az állampolgároknak közérdekű adatok iránti érdeklődése tovább fokozódik és ugyanolyan eréllyel lépnek e joguk megsértése esetén, mint a jogellenes személyes adatkezelés észlelésekor”*.

Információs ágak aránya a panaszügyekben
a 2006. év panaszügyeiben (%)

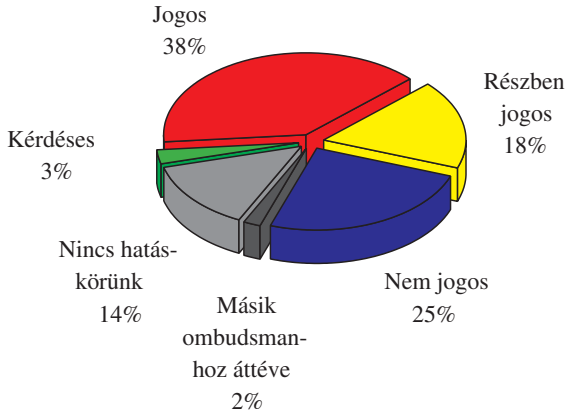


A panaszok jogossága

A már lezárt panaszügyek (1241-ből 1037-et zártunk le a beszámoló megírásáig, az előző évben ez a szám 1149/944) több mint felében, 57 százalékában – 591 esetben – állapítottuk meg, hogy jogos vagy részben jogos volt az indítványozó panasza. 2005-höz képest tehát nőtt a jogos és részben jogos panaszok száma, és kis mértékben nőtt a nem jogos panaszoké is. Jóval több olyan panaszt kaptunk, amelyet hatáskör hiánya miatt nem vizsgáltattunk ki. A másik országgyűlési biztoshoz áttett ügyek száma nem változott számottevően, viszont a kérdéses, nem eldönthető beadványok száma 116-ról 29-re csökkent.

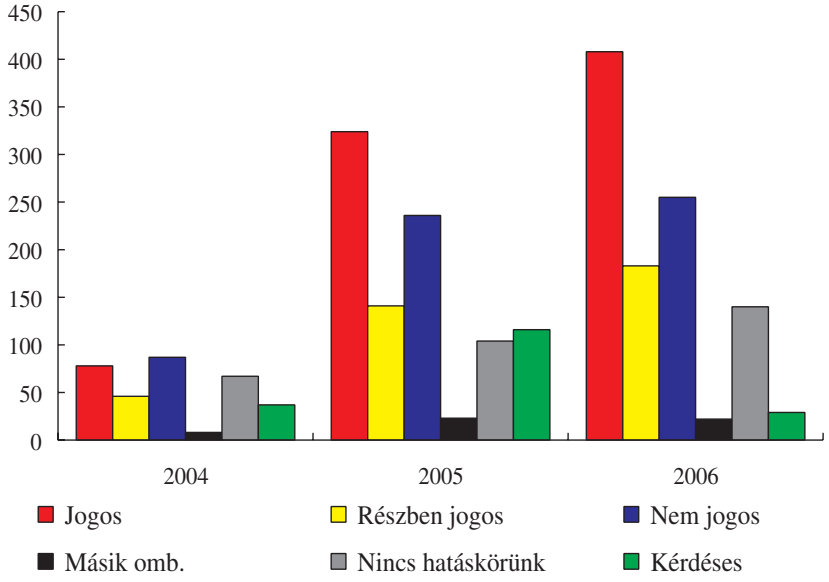
A panaszok jogossága

a 2006. év panaszügyeiben (%)



A panaszok jogossága

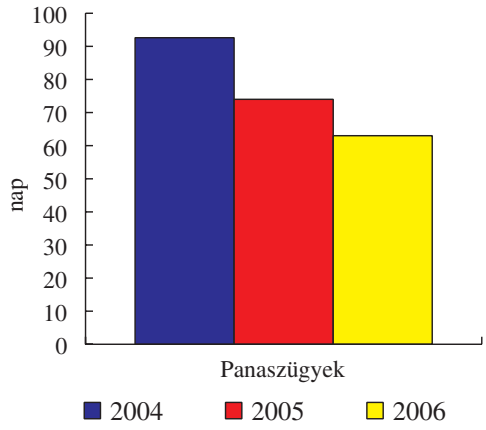
Panaszügyek 2004- 2006



Átlagos ügyintézési idő

A grafikon hároméves adatainak összehasonlítása után látható, hogy a lezárt panaszügyek átlagos ügyintézési ideje örvendetes módon ebben az évben is közel két héttel csökkent. Míg 2004-ben 92 nap, 2005-ben 72 nap, 2006-ban már csak 63 nap volt. Annak ellenére, hogy a panaszok száma 2006-ban tovább emelkedett, az ügyintézési időt tovább tudtuk rövidíteni. Ennek egyik oka, hogy a panaszosok sokszor nem kérik a gyakran elhúzódó és időigényes vizsgálatot, hanem megelégszenek az egyedi panaszuk ügyében kért és kapott biztosi állásfoglalással, melynek birtokában esetlegesen maguk veszik fel a kapcsolatot az adatkezelővel, vagy indítanak ellene peres eljárást.

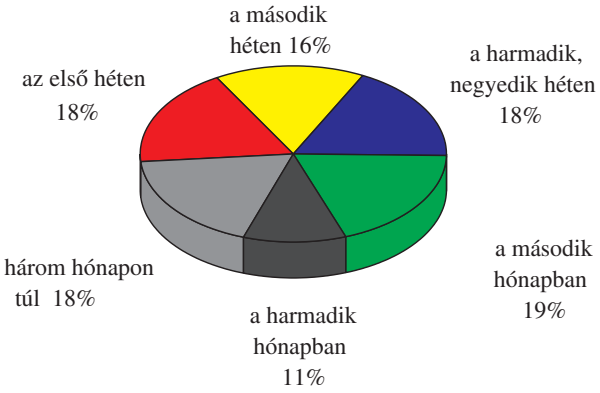
Átlagos ügyintézési idő
Panaszügyek 2004 – 2007



Az ügyintézés időtartama a 2006-os évben a következőképpen alakult. 2007 februárjáig, a beszámoló megírásáig a 2006-ban iktatott 2211 ügy közül 1142-ben az első hónapban adtunk érdemi választ a beadványt tevőnek az indítványára, ez az összes ügy több mint fele, 52 százaléka. A második hónapban további 423 beadványra válaszoltunk, amely további 19 százalékot tesz ki. Ez az összes ügy hetven százaléka.

Az ügytorlódás jelei igazán a harmadik hónapban és azon túl adott érdemi válaszok számában mutatkoznak meg (241, illetve 405 ügy). Az átlagos ügyintézési időben – mindent egybevetve – további jelentős javulás tapasztalható. Kiemelendő, hogy a három hónapon túli határidővel intézett ügyek aránya a tavalyi 25 százalékról 18 százalékra, 590-ről 405-re csökkent.

Az ügyintézés időtartama a 2006-os évben
(„Hány ügyre válaszoltunk érdemben") (%)



II. A VIZSGÁLATOK

A. Személyes adatok

A 2006. év megerősítette azt a már néhány éve megfigyelhető tendenciát, amely az ügytípusok szerkezeti átrendeződésében jelenik meg. Az adatvédelmi biztos tevékenységének első éveiben jellemző volt a nagy állami adatkezeléseket, adatkezelőket érintő vizsgálatok túlsúlya, amely mellé idővel felsorakoztak a magánszféra egyes adatkezelései: bankok, direkt marketing, munkáltatók. Ez utóbbiak jellemzője, hogy jelentőségüket nem egy-egy nagy adatkezelő adta, hanem az adatkezelések együttese. Míg például egy-egy munkáltató önmagában nem kezeli nagyszámú érintett adatát, a munkaviszonyhoz kapcsolódó adatkezelések egésze már mindenképpen indokolta – az érintettek nagy száma, a hasonló jogi háttér, rokon vonásokat mutató vizsgálatok okán – azt, hogy a munkáltatókat mint adatkezelési területet önállónak tekintsük. Hasonló a helyzet a bankok, biztosítók, távközlési szervezetek esetében is.

A magánszféra nem veszített súlyából, sőt, vizsgálataink egyre nagyobb számban irányulnak magánjogi jogviszonyokhoz kapcsolódó adatkezelésekre, miközben az új technológiák, jogértelmezési kérdések is egyre inkább itt merülnek fel. A hagyományosan nagy adatkezelőnek számító fegyveres és rendvédelmi szervek, az önkormányzatok, a társadalombiztosítás szervei, adóhatóságok egyre kevesebb munkát adnak, amely a róluk szóló fejezet rövidebb terjedelmében is megnyilvánul. Ennek többféle oka is lehet. Ezek közül az egyik, hogy az adatkezelők a kezdeti bizonytalanságoktól vagy éppen a régebbi időkből *„öröklődött”* rutintól megszabadulva megtanulták, hogy munkájuk során figyelni kell a személyes adatok védelméhez való jog érvényesülésére, és egyre inkább a jogszabályok betartásával járnak el, miközben az állampolgárok tájékoztatására is figyelmet fordítanak. Másrészt az állampolgárok megtanulták, hogy a demokratikus jogállamban az állam nem felettük áll: ismerik jogaikat, képesek azok érvényesítésére, így nem feltétlenül szorulnak arra, hogy az adatvédelmi biztostól kérjenek segítséget.

A magánszféra azonban egyre gyakrabban elbizonytalanítja az állampolgárokat. Egymást érik a legkülönbözőbb adatkezelések: ka-

merák a munkahelyeken, üzletekben, bankokban, okmányok másolása, véget nem érő adatfelvétel hitelképesség vizsgálata jegyében, *„ellenőrizhetetlen ellenőrzések”*, bonyolult adatszolgáltatási rendszerek – a mindennapjaink részévé vált, hogy ügyfélként, adósként, munkavállalóként sokan, túl sokan kíváncsiak ránk. Ezekben a viszonyokban ráadásul a függőség, a kiszolgáltatottság is megjelenik. Az állampolgár, aki jogai ismeretében, tudatosan és határozottan lép fel egy túlzó rendőri intézkedés, adóhatósági vizsgálat ellen, elbátortalanodik, ha munkáltatójával, bankjával vagy távközlési szolgáltatójával áll szemben. Nehézséget okoz a jogszabályi környezet is. Míg a közhatalom gyakorlása szigorú szabályokhoz kötött, ezekben a jogviszonyokban sok a rendezetlen kérdés, a megengedő szabály, így nehéz látni a határokat a jogszerű és a jogellenes között; sok a bizonytalan, *„szürke”* terület, melyet az adatkezelők a hatékonyság jegyében igyekeznek minél jobban kihasználni. Végezetül nem lehet elfeledkezni még egy fontos tényezőről sem: a magánszféra nagy adatkezelői közül kerülnek ki azok, akik meg tudják venni a lejfejlettebb technológiát, alkalmazni tudják a legdrágább adatelemzési módszereket is.

A bevezető végén még egy szerkesztési változtatásra is fel kell hívni az olvasó figyelmét. Az elmúlt években a beszámoló mellékletében nagyszámú ügyet ismertettünk, ezekre az utalásokat a szövegben könnyen meg lehetett találni. A vizsgálatok nagy száma és változatossága azonban egyre nehezebben kezelhető terjedelmet igényelt, miközben egyre kisebb valószínűséggel találta meg az olvasó az őt valóban érdeklő állásfoglalásokat. Ez a beszámoló már nem tartalmaz konkrét állásfoglalásokat, ugyanakkor az elektronikus információszabadságról szóló törvény alapján azok a korábbinál jóval nagyobb számban érhetők el az adatvédelmi biztos honlapján. Ezekre természetesen a megfelelő helyeken továbbra is megtalálható az utalás.

Az adatvédelmi biztos perei

A személyes adatok védelméről és a közérdekű adatok nyilvánosságáról szóló 1992. évi LXIII. törvény (továbbiakban: Avtv., adatvédelmi törvény) 2004. május 1-jén hatályba lépett módosítása egyfajta hatósági jogkört adott az adatvédelmi biztosnak. Ennek lényege, hogy a biztos már nemcsak ajánlást adhat ki, hanem kötelező döntést is hozhat, amely ellen az adatkezelő bírósághoz fordulhat. A 2006-os évben

lezárult az első ilyen per, miközben az adatvédelmi biztos egy másik ügyben is alperesként állt bíróság előtt. A következőkben e két ügy rövid ismertetésére kerül sor.

Még 2004-ben indult az a vizsgálat, amely az RTL Klub elnevezésű kereskedelmi TV-csatornán több alkalommal is sugárzásra került „*Anyacsavar*" című műsorra irányult. A műsor lényege, hogy két önként jelentkező családban az anyák egy hétre „*helyet cseréltek*", és a történteket a valóságshow-khoz hasonló módon mutatta be a televízió. Valamennyi műsor közös jellemzője volt, hogy teljesen eltérő anyagi, társadalmi helyzetben lévő családokat választottak ki, és minden családban volt kiskorú gyermek.

Az érintettek és a Magyar RTL Televízió Zrt. között megkötött szerződés alapján történő adatkezelés jogellenessége lényegében azért volt megállapítható, mivel a szerződésben nem nevesített alvállalkozók részére történő, és emellett időbeli és térbeli korlátozás nélküli adattovábbításhoz adott hozzájárulás jogszerűsége kizárt. Emellett a szerződés teljesítése során kiskorú személyek személyes adatai is a televízió kezelésébe kerültek, azonban e körben a szülők, mint törvényes képviselők által adott hozzájárulás nem elfogadható. Ennek oka, hogy a gyermekek tekintetében fennállt a pszichikai károsodás veszélye, amely szükségessé tette volna a gyámhatóság közreműködését a hozzájárulás megadása során. Az adatvédelmi biztos a televíziót a jogellenes adatkezelés megszüntetésére szólította fel. Válaszul a Magyar RTL Televízió Zrt. a biztosi intézkedés megváltoztatása érdekében keresetlevelet terjesztett a Pesti Központi Kerületi Bíróság elé, majd áttételt követően a per a Fővárosi Bíróság előtt indult meg.

A perben a felperes az adatvédelmi biztos álláspontjának jogellenességére hivatkozott. Bár a biztos készen állt arra, hogy álláspontját érdemben is megvédje a bíróság előtt, erre nem volt szükség: a felperes ugyanis akkor fordult bírósághoz, amikor a biztos még „*csak*" felszólította a jogellenes adatkezelés megszüntetésére. Az adatvédelmi törvény a bírósági út lehetőségét az adatkezelés megszüntetését elrendelő határozattal szemben nyitja meg, ilyen kibocsátására azonban nem került sor. A Fővárosi Bíróság 2006. április 10. napján kelt végzésében egyetértett ezzel az állásponttal, és a pert megszüntette. A végzés ellen a felek fellebbezéssel nem éltek.

A másik pert a Magyarországi Szcientológia Egyház indította az adatvédelmi biztos ellen, közérdekű adat kiadása iránt. Az adatvédelmi biztos 2006 májusában ajánlást bocsátott ki az egyház számára, melyben felhívta minden Magyarországon működő szcientológia egyház vagy szervezet, és a szcientológia vallás gyakorlóinak figyelmét, hogy a hitéleti tevékenységük során is ügyeljenek az adatvédelem követelményeinek betartására, különösen az adatkezeléssel érintettek megfelelő tájékoztatására. A biztos az ajánlás indokolásában hivatkozott a Nemzeti Nyomozó Iroda Bűnügyi Főosztálya által adott szakvéleményre, amely az egyház által alkalmazott *„e-meter"* hazugságvizsgáló eszközként történő felhasználhatóságával kapcsolatban készült. Az ügy részleteit az egyházakról szóló fejezetben ismertetjük, ehelyütt csak a per folyamatának bemutatására kerül sor.

Az egyház kérte a szakvélemény megküldését. Válaszában a biztos kifejtette, hogy az adatvédelmi törvény 19/A. §-a alapján a szakvéleményt nem áll módjában megküldeni, mivel az eljárás még nem zárult le, és az ajánlás fenntartásával, visszavonásával vagy megváltoztatásával kapcsolatos döntést az egyház válasza alapján lehet meghozni. Ezt követően került sor a bírósági eljárásra.

> Az egyház keresetében azt kérte a Fővárosi Bíróságtól, hogy állapítsa meg: a biztos eljárása megsértette az adatvédelmi törvény közérdekű adat kiadására vonatkozó szabályait, és kötelezze a szakvélemény kiadására. Álláspontja szerint alkotmányosan elfogadhatatlan, ha a biztos egy súlyos következményekkel járó döntést anélkül hoz meg, hogy az iratbetekintés jogát a vizsgált fél számára biztosítaná. Emellett megítélése szerint az eljárás a lelkiismereti és vallásszabadságról, valamint az egyházakról szóló 1990. évi IV. törvény szerint is aggályos, mivel a vizsgálat a vallásgyakorlás központi eleméhez kapcsolódó eszközhasználatot is érintette.
>
> A biztos ellenkérelmében kifejtette, hogy az egyház szakvélemény kiadását kérő levele kézhezvételekor az eljárással kapcsolatos döntését az ajánlás fenntartásáról, módosításáról vagy visszavonásáról – éppen a felperes érdemi válaszának elmaradása miatt – még nem hozta meg. Vagyis a kérdéses szakvélemény ekkor az adatvédelmi törvény 19/A. §-a szerinti döntést megalapozó iratnak minősült.

A Fővárosi Bíróság a perben 2006. augusztus 24. napján, majd október 19. napján tartott tárgyalást. A második tárgyaláson a biztos –

fenntartva az általa korábban előadottakat – a szakvéleményt az egyház képviselője részére átadta, mivel nyilvánvalóvá vált számára, hogy nem fogadja el az ajánlásban foglaltakat, tehát az eljárás lezárásának – és ezáltal a szakvélemény kiadásának – akadálya éppen a per megindítása miatt szűnt meg.

A bíróság a perben 2006. október 31. napján kihirdetett ítéletében, a biztos álláspontját elfogadva, az egyház keresetét jogalap hiányában teljes egészében elutasította.

Rádióhullámokon alapuló azonosítási technológiák

A XXI. század elején az információs társadalom polgára számára nem szokatlan, hogy a rohamosan fejlődő adatátviteli rendszerek a vezeték nélküli hálózatok világává alakítják a jelenlegi technológiai struktúrákat. Ma már bárki számára elérhető, hogy a különböző infokommunikációs eszközei, mint például egy mobiltelefon, laptop vagy PDA, bluetooth vagy infrakapcsolat segítségével kommunikáljanak egymással. Az elmúlt évek során megindult a fejlődés a rádióhullámok közreműködésével történő adatkommunikáció irányába is. A Radio Frequency Identification (rádióhullámokon alapuló azonosítás, RFID) ma már széles körben alkalmazott azonosítási rendszer, amely a rádióhullámok által közvetített adatok feldolgozásán alapul. A technológia lényege, hogy az RFID címke vagy chip – közismert nevén „*tag*" – rádiójelek segítségével információt közvetít a hordozó tárgyról.

Az RFID technológiai rendszer két eszköz kommunikációjára épül: az egyik az RFID „*tag*" (angol szó, jelentése: címke, cédula), a másik az RFID olvasó (reader). A tipikus RFID „*tag*" egy chipet és egy antennát tartalmaz, és ezek egy hordozórétegen vannak rögzítve. A chipen a memóriakapacitás függvényében az általános információkon túl egyedi azonosítók is elhelyezhetők, például egy termék esetében annak előállítója, gyártásának időpontja, sorszáma, rendeltetési helye. Az RFID címke leginkább a termék vonalkódjára emlékeztet, mégis kardinális a különbség a két termékazonosítási rendszer között. A vonalkód az általános termékazonosításra képes, az RFID rendszernek pedig az a célja és feladata, hogy a termék egyedi azonosítását elvégezze.

Az olvasó – ahogy a neve is mutatja – abban játszik szerepet, hogy az RFID „*tag*"-en tárolt információk digitális formában kiolvashatók

legyenek. Az olvasó antennája rádióhullámok kibocsátásával kapcsolatot keres az RFID „*tag*"-gel. A rádióhullámot érzékelő „*tag*" a memóriájában tárolt információkat analóg jelek formájában leadja az olvasónak, amely az analóg jelet digitálissá alakítja át. A digitális adatokat pedig az RFID rendszerhez csatlakoztatott számítógépes rendszer értelmezi és feldolgozza.

A technológiai alapok ugyan adottak, de az RFID rendszereknek mégis sokféle fajtája létezik. Alapvetően az aktív és a passzív rendszerek ismeretesek. Az aktív chipek önálló energiaforrással rendelkeznek, ezért az olvasóval történő kommunikációjuk azon alapul, hogy a tárolt adatokat rádióhullámokkal maguk sugározzák az olvasó felé. Ehhez képest a passzív „*tag*" önálló energiaforrással nem bír, az olvasó által kibocsátott hullámokat veri vissza. Amikor a passzív RFID egy olvasó hatókörébe ér, az olvasó által kibocsátott rádiójelek ébresztik fel álmából, és ennek hatására közvetíti a tárolt információkat. Az aktív eszköz képes arra, hogy nagyobb távolságról adjon jelet magáról, a passzív eszköz ellenben jóval kisebb és olcsóbb.

A technológia távlatai ma még beláthatatlanok. A beléptető rendszerek már számos helyen alkalmazzák a technológiát, más területek jelenleg is tesztelés alatt állnak. Vannak olyan ipari és kereskedelmi szektorok, ahol az RFID címkék és chipek használata már mindennapos gyakorlat. A kereskedelem és a logisztikai rendszerek kétségkívül haszonélvezői az RFID technológiának, hiszen a termék – például egy jármű – az előállítástól, a szállításon át, egészen a raktárakig követhető, és a teljes áru- és raktárkészlet naprakész megfigyelése elvégezhető a termékek rádiófrekvenciás azonosításával. Ezentúl az RFID technológia alkalmas a hibás, valamint a lejárt szavatosságú termék raktárkészletből való kiszűrésére is. A járművek elleni lopásvédelem egyik eszköze is lehet az RFID technológia, de a közlekedésben az utazáshoz használatos kártyákon túl, az autópályadíjak megfizetésének is mindennapos eszköze lehet. Az RFID technológia repülőtereken is alkalmazható helymeghatározásra és nyomkövetésre: az utas poggyászára helyezett RFID a csomag, a beszállókártya RFID-vel való ellátása pedig az utas helyzetének megállapítására ad lehetőséget.

> Októberben hazai és nemzetközi híradásokból értesült a biztos arról, hogy a debreceni repülőtéren az utasok nyomon követését szolgáló rendszert kívánnak kipróbálni a közeljövőben. Az utasok

> helyzete egy címke segítségével határozható meg, melyet felvételkor kapnának meg. A repülőtéren csak a technológia tesztelésére kerül sor, utasok elől elzárt területen; a folyamatban csak a fejlesztők vesznek részt, utasok nem. *(1624/A/2006)*

Az egészségügyi szektor, ideértve a gyógyszeripart is, számtalan kiaknázatlan lehetőséget rejt. A gyógyszerek egyedi azonosítóval való ellátása útján elkerülhetők lennének a gyógyszerhamisítások, az anyagszállításból eredő veszteségek, és a gyógyszer származásának hitelt éremlő igazolása is megvalósíthatóvá válna. Az egészségügyi ellátórendszer nyitott a technológia iránt, és az alkalmazás terén ígéretesek a kilátások. Az orvos kórházon belüli helyzetének meghatározása a sürgősségi ellátásokat könnyíti meg, az eszközökbe, műszerekbe való beépítés az operáció során elkövetett műhibákat segít kiküszöbölni, és a beteg személyazonosságának – különösen öntudatlan állapotban fontos – meghatározását segítheti. Ez utóbbi már a bőr alá ültetett chipek világába kalauzol bennünket.

A fentiek csak példák, a technológia lehetséges alkalmazási területeit lehetetlen számba venni. Alkalmazható bankjegyeken a hamisítások elkerülése és kiszűrése érdekében, az útlevelek esetében a biometrikus azonosítók tárolására és különféle készpénz-helyettesítő kártyarendszerekben is. Egyes svájci és osztrák sípályákon a liftek használatára jogosító kártyák tartalmaznak azonosító chipet, melyek leadásakor a síelő megkapja napi statisztikáját: mennyit síelt, milyen magasságot tett meg, mennyit pihent. A rendszer lényegében a pályákon elhelyezett olvasók adatait összesíti.

A rádiófrekvenciás azonosítási technológia kihívást jelent az adatvédelem számára, mert nem csupán tárgyak és áruk, hanem személyek ellenőrzésére, azonosítására és helyzetének nyomon követésére is lehetőséget ad. Az adatvédelem felől közelítve igazi kétarcú jelenséggel van dolgunk, mert a technológia az adatkommunikáció terén kézzelfogható előnyöket ígér, és mégis reális veszélyt jelent az egyén magánszférájára és a személyes adatok védelméhez fűződő jogára.

Az Európai Unió adatvédelemmel foglalkozó 29-es munkacsoportja 2005. január 19-én adta közre azt a munkaanyagot, amelyben az RFID technológia jellemezőinek és alkalmazásának körülményeire tekintettel megfogalmazta azokat az elvárásokat, amelyeket a technológia fejlesztőinek és alkalmazóinak szem előtt kell tartaniuk a magán-

élethez, valamint a személyes adatok védelméhez fűződő jog védelme érdekében. Az RFID technológia alkalmazása ugyanis meghatározott területeken személyes adatok gyűjtésével és kezelésével járó művelet, ezért a rádiófrekvenciás azonosítási rendszerben az adatvédelmi előírásokat figyelembe kell venni – hiszen a chipen személyes adatok is tárolhatók. A másik alkalmazási kör, ha a technológia személyek ellenőrzésére szolgál (például gyermekek vagy rabok esetében).

Az új technológia elterjedése előtt az adatvédelemnek a tájékoztatásra kell helyeznie a hangsúlyt. Ez nem csupán az adatvédelmi biztosnak, hanem a technológia fejlesztőinek, a rendszer üzemeltetőinek és forgalmazóinak is feladata. Ez nemcsak arra irányul, hogy az érintettek megismerkedjenek a technológiával, de lehetőséget kell adni arra is, hogy az egyes konkrét alkalmazásokról tájékoztatást kapjanak. Lényeges szerephez juthatnak a magánszférát védő módszerek, mint például a chip deaktiválásának lehetősége vagy olvasásának átmeneti korlátozása. Fokozott figyelmet kell fordítani az adatbiztonsági követelményekre is, elsősorban arra, hogy az információkat illetéktelenek ne olvashassák.

Az RFID technológia más, információs társadalomban született és születő technológiákhoz hasonlatosan az információk gyorsabb és hatékonyabb feldolgozására épít. Ezek a rohamosan fejlődő eszközök újra meg újra kihívást jelentenek az adatvédelem számára, mert az egyén magánszférája, az a szféra, amely technikai eszközök által érintetlen, egyre szűkül. Az adatvédelem sok esetben egy újszülött technológia mellett csupán bábáskodhat, és preventív intézkedésekkel a helyes fejlődési irányba terelheti.

Adatokkal és információkkal terhes világban élünk, amely egyszerre tágítja előttünk a horizontot, információk és ismeretek kincsestára tárul fel előttünk, mégis meztelennek érezzük magunkat, amikor magánéletünk legbensőbb titkai személyes adatok formájában különféle adatkezelések rekordjaivá válnak. Az előbb említett „*bőr alá ültetett chip*” talán túlzott aggodalomnak tűnhet – ennek ellentmond az, hogy az Amerikai Egyesült Államokban ez már olyan szinten valóság, hogy egyes tagállamokban törvény tiltja alkalmazásukat.

Nagy állami (önkormányzati) adatkezelések

A Központi Adatfeldolgozó, Nyilvántartó és Választási Hivatal

A korábban a belügyminiszter alá tartozó Központi Adatfeldolgozó, Nyilvántartó és Választási Hivatal (továbbiakban: Központi Hivatal) 2006-ban országos hatáskörű szervként a Miniszterelnöki Hivatalt vezető miniszter irányítása alá került. A szervezet adatkezelését érintő panaszok, észrevételek száma a nyilvántartásokban tárolt hatalmas mennyiségű személyes adathoz képest évről évre folyamatosan csökkenő tendenciát mutat.

A panaszosok közül a név- és lakcímadatok direkt marketing célú felhasználását kifogásolták legtöbben, az esetek zömében azonban jogszerűnek bizonyult e szervezetek eljárása. *(102/A/2006, 123/A/2006, 1639/A/2006)*

Egy polgár aziránt érdeklődött, hogy személyes adatait a személyi adat- és lakcímnyilvántartásból rosszakarója, aki a Bevándorlási és Állampolgársági Hivatalban dolgozik, jogszerűen megszerezheti-e.

> A biztos válaszlevelében arról tájékoztatta a beadványozót, hogy a polgárok személyi adatainak és lakcímének nyilvántartásáról szóló 1992. évi LXVI. törvényben a különböző szervek, hatóságok adatigénylését részletesen szabályozták, kitérve az adatlekérdezések jogalapjára is. E törvény 24. § (1) bekezdése alapján az állampolgársági ügyekben eljáró szerv a kérelmező azonosításához igényelhet adatokat a nyilvántartásból. Az adatigénylés a Bevándorlási és Állampolgársági Hivatal és területi szervei esetében tehát csak a törvényben kifejezetten megjelölt, az állampolgársági, bevándorlási eljárással kapcsolatos cél lehet, az e szervezeteknél dolgozók magáncélú adatlekérdezése jogellenes. *(2001/A/2006)*

A bűnügyi nyilvántartás vonatkozásában egy beadványozó azt kifogásolta, hogy a büntetőeljárások megszűnése után az állampolgárok miért nem kapnak automatikusan értesítést arról, hogy adataikat törölték a nyilvántartásból. A bűnügyi nyilvántartásról és a hatósági erkölcsi bizonyítványról szóló 1999. évi LXXXV. törvény (továbbiakban: Bnyt.) irányadó rendelkezéseinek ismertetése mellett a biztos hangsúlyozta, hogy a nyomozás, illetve a büntetőeljárás megszüntetése esetén a személyes adatok törlése ugyan *„automati-*

kusan" megtörténik, ez azonban nem jelenti azt, hogy erről az érintettet „*hivatalból*" értesítenék.

> Az Avtv. 6. § (2) bekezdése olyan tájékoztatási kötelezettséget ír elő az adatkezelő részére, amely az érintett kérelmén alapul – az Avtv. 11. § (1) bekezdése alapján – ez a rendelkezés tehát nem kötelezi a Központi Hivatalt „*automatikus*" tájékoztatás adására. A jelenleg Magyarországon működő „*nagy állami*" nyilvántartások egyike sem nyújt kérelem nélkül tájékoztatást az érintett részére arról, hogy megkezdték vagy megszüntették adatai kezelését. Egy ilyen tájékoztatási kötelezettség törvénybe iktatása többnyire indokolatlan, hatalmas költségeket róna az adott szervezetre. A biztos álláspontja szerint az érintett részére az Avtv.-ben biztosított tájékoztatáskérési lehetőség, illetve az adatkezelők részére előírt tájékoztatásadási kötelezettség megfelelő védelmet nyújt az állampolgárok részére arra az esetre, hogyha felmerülne bennük egy esetleges jogosulatlan adatkezelés gyanúja. *(738/A/2006)*

Szintén az adatkezelő tájékoztatási kötelezettségével kapcsolatos kérést fogalmazott meg az a panaszos, aki aziránt érdeklődött, hogy betekinthet-e a bűnügyi nyilvántartásba. A biztos állásfoglalásában foglaltak szerint az adatvédelmi rendelkezésekből nem következik, hogy az érintettnek betekintést kellene biztosítani a vonatkozó nyilvántartásokba. E kérésének technikailag is nehezen lehetne eleget tenni. Az adatkezelő eljárása akkor is megfelelő, ha az Avtv. szabályai szerint az érintett részére tájékoztatást ad. *(13/K/2006)*

A biztoshoz intézett panaszbeadványában egy polgár azt sérelmezte, hogy határátlépései alkalmával azért kell hosszabb időt várakoznia, mert adatait a határőrök lekérdezik a bűnügyi nyilvántartás gépi prioráló rendszeréből, és azzal szembesülnek, hogy egy régi elítélése szerepel a bűntettesek nyilvántartásában.

> A Bnyt. alapján a bűntettesek nyilvántartásába felvett adatokat a szándékos bűncselekmény miatt szabadságvesztésre ítéltek esetén a büntetett előélethez fűződő hátrányok alóli mentesítés (a továbbiakban: mentesítés) beálltától számított tizenöt évig kell kezelni, a c) pont pedig ezt a tárolási időtartamot a gondatlan bűncselekmény miatt szabadságvesztésre ítéltek esetén a mentesítés beálltától számított öt évben határozza meg. E rendelkezések célja éppen az, hogy a hatóságoknak – a törvényben megszabott időtartamon

belül – akkor is tudomásuk legyen egy személy *„bűnügyi”* előéletéről, ha ez illető a *„civil”* életben egyébként már mentesítésben részesült, tehát tiszta erkölcsi bizonyítványt kaphat. Egyes bűncselekmények elkövetése esetén a bűntettesek nyilvántartásában szereplő személyek adataihoz kapcsolódóan többek között olyan egyéb rendelkezéseket is tartalmazhat a nyilvántartás, mint például a határátlépés tilalma. E *„kiegészítő”* rendelkezések meglétét a hatóság szintén csak a nyilvántartás ellenőrzése útján tudja megállapítani. *(1655/A/2006)*

Rendőrség

A rendőrséggel kapcsolatos ügyek, illetve panaszbeadványok a 2006. év folyamán sem számukban, sem pedig az egyéb ügyekhez viszonyított arányukban nem mutattak jelentős változást az elmúlt évhez képest.

Továbbra is igaz, hogy a panaszok jelentős részének vizsgálatakor a biztos a rendőrség jogszerű eljárását állapította meg. Ezt a tényt különösen azért fontos kiemelni, mert a médiához illetve a külső szemlélőhöz szinte kizárólag csak azok az ügyek jutnak el, amelyekben a biztos valamilyen jogellenességet állapít meg, így a polgárokban olyan kép alakulhat ki, mintha a rendőrség sorozatosan megsértené a személyes adataik védelméhez fűződő jogukat, holott ez a kép nem reális. Az állampolgárok sok esetben téves információk és jogérzet alapján vélik úgy, hogy a rendőrség jogszerűtlenül járt el velük szemben, és a biztos gyakran tömegével utasít el azonos vagy egymáshoz nagyon hasonló jellegű panaszokat, illetve állapítja meg a rendőri eljárás és intézkedés jogszerűségét. Maga a rendőrség is komoly erőfeszítéseket tett az elmúlt néhány évben annak érdekében, hogy a biztos állásfoglalásait a mindennapi munka során megfelelően alkalmazzák, és adatvédelemmel kapcsolatos problémák felmerülése esetén, gyakran az állampolgári panaszokat megelőzendő fordulnak a biztoshoz állásfoglalásért. Az alábbiakban következzék néhány jellemző ügycsoport vagy kiemelkedő súlyú ügy bemutatása.

Az előző évekhez hasonlóan nagyszámú, az igazoltatással kapcsolatos panasz érkezett, ezek száma azonban nem kiemelkedő az összes, rendőrséggel kapcsolatos panasz számához képest. E panaszok egy részének vizsgálatakor a biztos a rendőrség jogszerű eljárását állapította meg, azonban az igazoltatással összefüggésben ebben az év-

ben meglehetősen nagy a jogos panaszok aránya. Különösen érthetetlen ez akkor, amikor ezt a kérdéskört a biztos már számtalanszor vizsgálta, és az ügyekben kiadott állásfoglalásait a rendőrség vezetése is elfogadta.

> A problémát leginkább az okozza, hogy egyes helyi rendőrkapitányságok nem veszik figyelembe a 3/1995. (III. 1.) BM rendelet azon rendelkezését, mely szerint az eljáró rendőr csak azzal a személlyel összefüggésben rögzíthet adatokat, akinél ezt további intézkedés szükségessége vagy egyéb releváns körülmény indokolja, és valamennyi igazoltatott személy adatát feljegyzik, majd ezt követően 2 évig teljesen indokolatlanul és jogszerűtlenül tárolják. A rögzítés indokai igen változatosak, és meglehetősen semmitmondóak, az általános jellegű bűnmegelőzéstől a terrorizmus elleni harcig terjednek. Volt már olyan rendőrkapitányság is, amely arra hivatkozott, hogy területükön feltételezhető körözött személyek felbukkanása. Ezen indok nem elfogadható, hiszen valószínűleg nincs olyan része az országnak, ahol ne lehetne feltételezni körözött személyek felbukkanását. A kapitányságvezető a biztos álláspontját elfogadta, és intézkedett a gyakorlat megváltoztatásáról, illetve a rögzített adatok törléséről. *(1461/A/2006)*

Az év folyamán számos panasz érkezett a rendőrségi határozatok adattartalmával kapcsolatosan is. A leggyakoribb kifogás, hogy a nyomozást megszüntető határozat „*személyi részében*" feltüntetett személyes adatok az eljárásban ellenérdekelt felek tudomására jutottak, mivel a nyomozó hatóság ugyanolyan adattartalmú határozatot kézbesített az eljárásban részt vevő valamennyi fél részére.

> A biztos már a 2005. év végén javaslatot tett az igazságügy-miniszternek a büntetőeljárásról szóló 1998. évi XIX. törvény (továbbiakban: Be.) olyan módon történő módosítására, hogy az biztosítsa, hogy az ellenérdekű felek ne juthassanak hozzá egymás személyes adataihoz az eljárás során, illetve annak lezárásakor. A javaslattal az igazságügy-miniszter nem értett egyet, álláspontja szerint fontos eljárásjogi érdekek sérülnének azzal, hogyha az eljárásban részt vevő különböző felek különböző határozatokat kapnának. A biztos álláspontja a kérdéskörrel kapcsolatosan továbbra is az, hogy a célhoz kötöttség elvére tekintettel jogszerűtlen a határozat adattartalma, amennyiben az több adatot tartalmaz annál, mint amennyi a felek adott eljárásban történő azonosításához szükséges.

> Teljesen szükségtelen és veszélyes is, hogy az ellenérdekű felek a különböző határozatokból hozzájuthatnak a másik fél személyes adataihoz, amikor azoknak gyakorlatilag semmilyen hasznuk nincs a határozat lényegét tekintve. *(2214/A/2005, 2091/A/2006)*

Gyakran jelent gondot az állampolgárok számára, hogy hozzájussanak olyan rendőrségi határozatokhoz, amelyek jogos kárigényük érvényesítéséhez lennének szükségesek – például egy közlekedési balesettel kapcsolatosan –, mivel a rendőrség adatvédelmi okokra hivatkozva megtagadja e határozatok kiadását. A szabálysértésekről szóló 1999. évi LXIX. törvény (továbbiakban: Szabstv.) 51. § (1) bekezdése alapján a szabálysértési eljárásban sértett az, akinek jogát vagy jogos érdekét a szabálysértés sértette vagy veszélyeztette. E rendelkezés alapján a balesetben érintett vétlen felet tekinthetjük sértettnek, hiszen az elkövetett szabálysértés sértette az ő érdekeit. A (2) bekezdés alapján a sértett az eljárás során az őt érintő iratokat megtekintheti, azokról másolatot kérhet, illetőleg készíthet, az eljárást lezáró határozat pedig egyértelműen a vétlen felet is érintő iratnak minősíthető. Amennyiben a balesetben részes, vétlen fél a határozatról abból a célból kíván másolatot kapni, hogy azt jogos kárigénye érvényesítéséhez felhasználja a biztosító előtt folyamatban levő eljárásban, úgy ez az adatkezelés, illetve adatátadás teljes mértékben megfelel az Avtv.-ben megfogalmazott követelményeknek. *(912/A/2006, 1807/A/2006)*

Hasonló jellegű problémával szembesült az az állampolgár is, aki polgári pert kívánt volna indítani egy neki kárt okozó szerelő ellen, azonban az illetőnek csak a nevét és *„titkosított”* mobiltelefonszámát ismerte.

> Mivel a polgári perrendtartásról szóló 1952. évi III. törvény (továbbiakban: Pp.) 121. § (1) bekezdése alapján a keresetlevélben fel kell tüntetni a feleknek a lakhelyét, ezért a bíróság hiánypótlásra visszaadta a keresetlevelet a panaszosnak, hogy pótolja az *„alperes”* adatait. A panaszos a rendőrséghez fordult, ahol a megadott információk alapján ki is derítették a szükséges adatokat, de azokat a panaszosnak adatvédelmi okokra hivatkozva nem adták ki. Bírósági megkeresés esetén a rendőrség átadta volna a kért adatokat a bíróságnak, a bíróság azonban a panaszos többszöri kérése ellenére sem intézett megkeresést a rendőrséghez az adatok kiadása végett. A panaszos a szükséges adatokat a Központi Adatfeldolgozó, Nyil-

vántartó és Választási Hivataltól is megpróbálta megszerezni, ahol azonban arról tájékoztatták, hogy csak egy név alapján nem tudnak adatot szolgáltatni. Végül a bíróság – mivel a panaszos az adatokat nem tudta beszerezni – a keresetlevelet elutasította. Az ismertetett eset során valamennyi érintett szerv a rá vonatkozó jogszabályok szerint járt el, jogszabálysértés tehát nem történt. A probléma miatt a biztos felkérte az igazságügyi és rendészeti minisztert a vonatkozó jogszabályok módosítására, hiszen azok megakadályozták a panaszost abban, hogy kártérítési igényét érvényesíthesse, illetve a bíróság számára – a keresetlevél benyújtását megelőzően – nem biztosítanak semmilyen lehetőséget az eljáráshoz szükséges, a felek által azonban jogszerűen hozzá nem férhető információk beszerzésére. *(1836/A/2006)*

Egy állampolgár azzal kapcsolatosan kérte a biztos állásfoglalását, hogy a nyomozás megszüntetését követően a Be. 193. § (1) bekezdésére hivatkozva meg kívánta tekinteni a nyomozás iratait, ezt azonban az eljáró rendőrkapitányság elutasította, és részére csak a Be. 70/B. § (2) bekezdése szerinti korlátozott iratmegismerési jogot biztosították. A rendőrség eljárása elleni panaszát a megyei főügyészség és a Legfőbb Ügyészség is elutasította, mivel véleményük szerint a rendőrség helyesen járt el.

A probléma kivizsgálása során a biztos megkereste az igazságügyi és rendészeti minisztert, aki válaszában leírta, hogy mivel a Be. 193. § (1) bekezdése esetleges vádemelést említ, ezért ebből adódik az a nézet, hogy a gyanúsított és a védő számára csak korlátozott iratmegismerési jog biztosítható abban az esetben, ha a Be. 190. §-a alapján a nyomozás megszüntetésére került sor. A Be. 191. §-a ugyanis lehetővé teszi a nyomozás folytatását, így olyan adatok, információk juthatnak a gyanúsítottnak vagy védőjének tudomására, amelyek a nyomozás érdekeit sértenék. A miniszter álláspontja szerint azonban a nyomozás iratai megismerésének lehetősége nem valamiféle öncél, hanem a jogérvényesítés valós esélyének biztosítása, hiszen csupán az iratok ismeretében dönthet a jogosult az őt megillető indítványokról, észrevételekről. Mindebből tehát az következik, hogy az iratmegismerés lehetőségét a nyomozás elvégzése után mind a vádemelési javaslat, mind a megszüntetési javaslat esetében biztosítani kell, majd az ügyész a számára biztosított jogkörben és időben dönt a vádemelés vagy megszüntetés kérdésében. A miniszter a leg-

főbb ügyész helyettesével is konzultált a kérdésben, aki arról tájékoztatta, hogy a nyomozás megszüntetésével a nyomozást elvégzettnek, befejezettnek kell tekinteni, a nyomozás érdekei ekkor már reálisan nem sérülhetnek. Igaz ugyan, hogy a Be. 191. §-a lehetőséget ad a megszüntetett nyomozás folytatására, erre azonban rendszerint új körülmény felmerülése esetén kerülhet csak sor. Ezért a legfőbb ügyész helyettese jogértelmezéssel is lehetségesnek tartja azon következtetés levonását, hogy a nyomozás megszüntetését követően a terhelt és a védő a Be. 193. §-ának (1) bekezdése szerint megismerheti az iratokat, és azokból a Be. 70/B. § (5) bekezdésének a) pontja alapján igényelhet másolatot. *(562/A/2006)*

Állampolgárok és a rendőrség részéről is érkeztek beadványok, amelyek annak a kérdésnek a tisztázására irányultak, hogy egy gépjármű forgalmi rendszáma személyes adatnak minősül-e vagy sem. Egy beadvány ennek okán az Autótulajdonosok Országos Érdekvédelmi Egyesületének adatkezelését is kifogásolta, mivel az egyesület a rendőrség körözési adatállományát – illetve annak egy részét – használja lopott autók felkutatására.

A biztos ezekben az ügyekben arra az álláspontra helyezkedett, hogy a gépjármű körözési adatok – többek között a rendszám, alvázszám, gépjármű színe és típusa – nem minősülnek személyes adatnak, hiszen amennyiben egy személy vagy egy szervezet csak ezeket az adatokat kezeli, úgy egymagában a *„saját”* adatbázisa alapján nem tudja ezeket az adatokat egy meghatározott személyhez társítani. Egy adat gyakorlatilag bármikor kapcsolatba hozható az érintettel, hogyha azt megfelelő adatbázisba helyezzük, konkrét adatkezelések vizsgálatakor azonban csak az releváns, hogy az adott adatkezelő össze tudja-e egyértelműen kapcsolni a kezelt adatokat egy természetes személlyel. Ellenkező értelmezés esetén ugyanis minden adat személyes adatnak minősülne, még a statisztikai adatok vagy például akár egy véletlenszerűen kitalált születési dátum is. Mindezek alapján tehát a kérdéses adatkör átadása a polgárőrség – illetve bármely más személy vagy szervezet – részére adatvédelmi szempontból nem kifogásolható, amennyiben az adatok címzettje saját adatállománya alapján nem tudja a kapcsolatot helyreállítani az adat és annak *„tulajdonosa”* közt. *(929/A/2006, 2038/K/2006)*

A Pécs környéki községek polgármesterei jelezték a Baranya Megyei Rendőr-főkapitányságnak, hogy településeiken nagy probléma a prostitúció megjelenése, és kérték a főkapitányság segítségét a jogszabályok betartatásában. A rendőrség folyamatosan ellenőrizte az érintett útszakaszokat, és intézkedett a jogellenes cselekmények megszüntetése érdekében. Az ellenőrzések során alaposan feltételezhető volt, hogy a prostituáltak a megszerzett jövedelmet eltitkolják, adóbevallást nem készítenek, tehát szabálysértést vagy bűncselekményt követnek el. A helyszíni meghallgatásról – mely önkéntes alapon történt – jegyzőkönyvet vettek fel, és a kitöltött jegyzőkönyveket megküldték az illetékes adóhatóságnak.

> Az üggyel kapcsolatos állásfoglalásában a biztos kifejtette, hogy rendőrségnek nem feladata az adókötelezettség teljesítésének ellenőrzése, ezzel kapcsolatos adatok gyűjtése, felvétele és továbbítása – ez az adóhatóság hatáskörébe tartozik. A rendőrség az ellenőrzések során nem vizsgálhatja sem a személyi jövedelemadóról szóló, sem az adózás rendjéről szóló törvények rendelkezéseinek megtartását. A rendőrség az adózással kapcsolatos szabályok megszegésének esetei közül csak a legsúlyosabb, bűncselekménynek számító jogsértések – például adócsalás – tekintetében járhat el. Az adózási szabályok megsértésének egyéb esetei nem minősülnek a Szabstv. szerinti szabálysértéseknek, vagyis a rendőrség nem vizsgálhatja az adózási, egészségügyi előírások betartását és nem vehet fel kifejezetten ezekre irányuló adatokat. Nem volt egyértelműen megállapítható továbbá, hogy a *„helyszíni meghallgatások”* milyen eljárási cselekménynek minősülnek, mi a törvényi jogalapjuk, ugyanis a vonatkozó törvényi szabályozás fogalmi rendszerében ilyen elnevezés nem szerepel. Tanúmeghallgatás esetén a Szabstv. 55. §-a, az eljárás alá vont személy vallomása esetén a Szabstv. 66. §-a szerint kell eljárni, de ennek feltétele valamilyen szabálysértés – pl. tiltott kéjelgés – elkövetése miatti eljárás indítása. A rendőrség biztosnak megküldött válasza nem tartalmaz információt arról, hogy szabálysértési eljárást indított-e, és ha igen, milyen szabálysértés miatt. A rendelkezésre álló iratokból az a következtetés vonható le, hogy a prostituáltakkal szemben szabálysértési eljárást nem indítottak, az ellenőrzés kifejezetten a jövedelmi, adózási adatok felvételére irányult. Vagyis a nyilatkoztatásnak nincs olyan törvényes célja, melynek érdekében ez az eljárás, az adatfelvétel indokolt. Mindezek alapján a biztos megállapította, hogy a rendőrség kifogásolt eljárása jogszerűtlen volt, mert megfelelő törvényi jogalap és cél nélkül folyt. *(2330/A/2005)*

Vám- és Pénzügyőrség

A 2006. év folyamán a Vám- és Pénzügyőrség tevékenységével kapcsolatosan viszonylag csekély számú beadvány érkezett, és e kevés beadvány túlnyomó többsége is azt az igazoltatási gyakorlatot, illetve adatkezelést kifogásolta, amely szerint a Vám- és Pénzügyőrség minden igazoltatott személy adatát rögzíti, és két évig kezeli – ellentétben a rendőrség és a határőrség eljárásával, amely szervek esetében az igazoltatott személy adatait főszabályként nem lehet rögzíteni. Amint arra már a tavalyi beszámolóban is utaltunk, a kérdéses adatkezelésre törvényi felhatalmazása van a Vám- és Pénzügyőrségnek, az tehát nem jogellenes. A körülményeket és a többi hasonló szerv eljárását szabályozó törvények előírásait figyelembe véve azonban az adatkezelés már nyilvánvalóan szükségtelen és aránytalan, így tehát nem felel meg a célhoz kötöttség elvének. Sajnálatos módon a biztosi kezdeményezés ellenére az elmúlt évben nem történt semmilyen előrelépés a jogsértő szabályozás módosítása érdekében.

A Vám- és Pénzügyőrség ellenőrzési tevékenységéhez kapcsolódóan vizsgálta a biztos azt a kérdést, hogy az egyéni vállalkozók adatai személyes adatoknak minősülnek-e vagy sem. A METRO Kereskedelmi Kft. ugyanis azt kifogásolta, hogy a Vám- és Pénzügyőrség a 2003. évi CXXVII. törvény 106. § (7) bekezdése alapján felszólította a céget, hogy adják át a Vám- és Pénzügyőrségnek jogi személyek, illetve jogi személyiség nélküli gazdasági társaságok – többek között egyéni vállalkozók – adatait ellenőrzés céljából. A METRO álláspontja szerint az egyéni vállalkozók adatai személyes adatoknak minősülhetnek.

> Az Avtv. 1/A. § (1) bekezdése alapján a törvény rendelkezései kizárólag természetes személyek adatait érintő adatkezelésekre vonatkoznak. Az egyéni vállalkozó azonban a szóban forgó helyzetben nem tekinthető természetes személynek, hiszen épp az teszi lehetővé számára, hogy a METRO ügyfelévé váljon, hogy „*kvázi*" cégként viselkedik, illetve a gazdasági életben való részvétel is azáltal válik lehetővé a számára, hogy a jog bizonyos szempontból cégnek tekinti. Természetesen előfordulhat, hogy természetes személyként védett adatai (pl. lakcím, telefonszám stb.) megegyeznek az egyéni vállalkozóként is használt adataival – így pl. a lakcíme egyben a székhelye is –, ilyen esetekben azonban ezekre az adatokra már – „*céges*" minőségükben – nem terjedhet ki a személyes adatok védelméhez fű-

ződő jog. Mindezek alapján tehát az egyéni vállalkozók adatai nem tekinthetők személyes adatoknak, így kezelésükre, illetve továbbításukra nem vonatkoznak az Avtv. rendelkezései. *(1028/A/2006)*

Állami adóhatóság

A beadványok jelentős része egyrészt azzal volt kapcsolatos, hogy az állami adóhatóságnak mely adatokat kell átadni, milyen információkat kérhet különféle eljárásai során, másrészt pedig arra vonatkozott, hogy az adóhatóság mely adatokat tehet megismerhetővé mások számára az adózási információk közül. Egy ilyen ügyben a biztos megállapította, hogy nem sért személyiségi jogokat az ellenőrzött személy az adóellenőrzés folyamán abban az esetben, ha a rokoni, baráti, üzleti partneri kölcsönadóinak nevét, adatait hozzájárulásuk nélkül az adóhatóság rendelkezésére bocsátja. *(791/A/2006.)*

Az előző évhez hasonlóan 2006-ban is több szempontból változtak a pénzügyi, adózási jogszabályok, ami természetesen kihatással volt az Adó- és Pénzügyi Ellenőrzési Hivatal tevékenységére az adatszolgáltatások, adattovábbítások, adatgyűjtések és az adatok felhasználása tekintetében. Az adatkezelést is érintő jogszabályok megalkotása során azonban a biztos nem minden esetben tudta érvényesíteni az adatvédelmi szempontokat, ugyanis gyakran előfordult, hogy e jogszabálytervezeteket – az Avtv.-ben foglaltakkal ellentétben – nem küldték meg részére véleményezésre, vagy a megküldött tervezetek esetében az egyeztetés, véleménykérés csak formális volt. Az elmúlt évek adózási tárgyú törvénymódosításait áttekintve megállapítható, hogy a hatóságok közti adatszolgáltatásra, adatátadásra vonatkozó szabályok változásai rendszerint az információs önrendelkezési jog újabb és újabb korlátozásával, egyre több személyes adat hatóságok általi kezelésével járnak. A közteherviselés és az állami bevételek biztosításának fontosságát elismerve némi aggodalomra ad okot ez a tendencia. Különösen a jelentős változásokkal, kiterjedt adatkezeléssel járó törvényjavaslatok előterjesztése során kellene nagyobb hangsúlyt fektetni a tervezett változtatások szükségességének, indokainak bemutatására, ugyanis csak az alapjogi korlátozás alkotmányos követelményeinek megfelelő adatkezelési szabályok fogadhatóak el. Aggasztó az a tendencia és jogalkotási módszer, mely szerint a hatóságok közti adatszolgáltatásra, adatátadásra felhatalmazást adó törvényi rendel-

kezések minden nagyobb módosító törvénycsomag kapcsán megváltoznak úgy, hogy kiegészülnek egy-egy átadandó adatfajtával, továbbá az adatátadásban részt vevő adatkezelő szervvel, hatósággal, de az adattovábbítások köre, mértéke bővítésének indokoltsága nincs megfelelően alátámasztva.

A jogszabályok az adóhatóság feladatává tették meghatározott adózási, társadalombiztosítási információk összegyűjtését és azok egy részének továbbítását más szervek részére. Elfogadható, ha az adóhatóság a többszörös adatszolgáltatás adminisztratív terheit csökkentendő olyan adatokat is összegyűjt, rögzít és továbbít, amelyeket azután más állami szervek fognak nyilvántartásba venni és felhasználni. Az azonban ellentétes az osztott információs rendszerek alkotmányos követelményével, ha az adóhatóság a mások számára összegyűjtött adatokat saját nyilvántartásában készletezi, felhasználja.

A jogi szabályozás változása kapcsán több beadványban is problémaként merült fel, hogy az adóhatóság és már szervek közti adatátadások, adatszolgáltatások és az adatnyilvántartás során mely azonosító kódok és hogyan használhatóak. Az adózási nyilvántartások azonosító kódja az adóazonosító jel, más szervek ezt csak korlátozottan, meghatározott esetekben ismerhetik meg, illetve kezelhetik – az adóhatóság pedig a társadalombiztosítási azonosító jelet nem használhatja. Az Országos Egészségbiztosítási Pénztár és a magánnyugdíjpénztárak adatkezelésére vonatkozóan is hangsúlyozta az adatvédelmi biztos, hogy nem fogadható el e szervek nyilvántartásainak az adóazonosító jel alkalmazásával való létrehozása, és az adóhatósággal való adatkommunikáció során kapcsolati kód képzésére és alkalmazására kell törekedni. A következő évre tervezett vizsgálat részletesebben áttekinti e témát. *(1526/K/2006, 1730/K/2006)*

A társadalombiztosítási szervek adatkezelése

A 2006. évben a korábbiakhoz képest kevesebb beadvány érkezett a társadalombiztosítási szervek adatkezelését illetően. A 2006-os év egyik legjelentősebb problémája a háziorvosok tételes betegforgalmi jelentésének, illetve a BNO-kód (Betegségek Nemzetközi Osztályozása) vényeken való feltüntetésének kötelezővé tétele volt. A kérdés részletes kifejtését az egészségügyi adatkezelésekről szóló fejezet tartalmazza.

Országos Egészségbiztosítási Pénztár

Az Országos Egészségbiztosítási Pénztárral (továbbiakban: OEP) való együttműködés hagyományosan jónak mondható, az egészségbiztosító és az adatvédelmi biztos többször is konzultált egymással.

Az OEP egyik megkeresésében az állami adóhatóság és az egészségbiztosító közötti kommunikáció körébe tartozó kérdésben kérte az adatvédelmi biztos állásfoglalását. Ennek lényege, hogy az OEP adóazonosító jelen, kapcsolati kód alkalmazása nélkül létrehozhat-e egy külön személyi nyilvántartást. Az adatvédelmi biztos válaszában megállapította, hogy a 2007. január 1-jétől hatályos törvényi rendelkezések és az adatvédelem osztott nyilvántartási elvének figyelembevételével az OEP jogszerűen megismerheti a biztosítottak adóazonosítóját, de a megismerést követően a kapcsolati kód alkalmazása elkerülhetetlen és kötelező. *(1526/K/2006)* Az állásfoglalás teljes terjedelmében a honlapon megtalálható.

Az adatvédelmi biztos átfogó vizsgálatot folytatott le a közgyógyellátás rendszerének adatvédelmi vonatkozásaival kapcsolatban. A biztos a korábbi véleményét továbbra is fenntartotta. Eszerint a Megyei Egészségbiztosítási Pénztár (továbbiakban: MEP) számára nem szükséges a közgyógyellátásra való jogosultságot megállapító határozat teljes tartalmának megismerése, ugyanis a határozatban foglalt adatok – beleértve a jövedelmi adatokat is – kezelése a MEP tevékenységéhez nem szükségesek. Kifogásolta továbbá, hogy a szociális hatáskört gyakorló jegyző tudomást szerez a háziorvosi igazolásban szereplő egészségügyi adatokról, noha azok ismerete a feladatai ellátásához nem szükséges. *(1010/H/2006)*

Nyugdíjigazgatás

Az állami nyugdíjbiztosító adatkezelését kifogásoló beadványok száma a korábbi évekhez képest viszonylag alacsony volt.

Egy panaszos kifogásolta, hogy a Nyugdíjfolyósító Igazgatóság a nyugdíj összegéről szóló értesítést általános postai levélküldeményként küldte meg a részére.

> A postáról szóló 2003. évi C. törvény szerint hivatalos irat csak az e célra rendszeresített tértivevénnyel adható fel. Tekintettel azonban arra, hogy a nyugdíj összegéről szóló értesítés kézbesítéséhez a jog-

szabály nem fűz jogkövetkezményt, nem kötelező a feladó számára, hogy az értesítést könyvelt küldeményként adja postára. Az adatvédelmi biztos álláspontja szerint a nyugdíjfolyósító azzal, hogy zárt küldeményként juttatja el a címzetteknek a levelet, eleget tesz az Avtv.-ben foglalt adatbiztonsági követelményeknek. *(266/A/2006)*

Magánbiztosítók

Az állami társadalombiztosítási szervek adatkezelésén kívül 2006-ban is egyre nagyobb teret kaptak a magánbiztosítók.

Az Allianz Hungária Biztosító Rt. egy orvosi műhibával kapcsolatos kártérítési ügyben felkérte az Igazságügyi Orvosszakértői Intézetet, hogy az érintett gyógykezelésével kapcsolatos kórházi iratok alapján – a jogosult beleegyezésével – készítsen szakértői véleményt az érintett egészségügyi állapotáról és a bekövetkezett egészségromlás mértékéről. A szakvélemény elkészültét követően a panaszos sikertelenül próbálta megszerezni a véleményt. A biztosító indoklása szerint a kért szakértői vélemény a biztosító megrendelésére készült, belső kárrendezési irat.

Az adatvédelmi biztos korábbi állásfoglalására hivatkozva megállapította, hogy az érintettről más személy megbízásából vagy megrendelésével készült szakértői vélemény az érintett által megismerhető irat. Az Avtv. 11-12. §-ai az érintett alapvető és legfontosabb információs jogaként jelölik meg a tájékoztatáshoz való jogot, ezt a jogot kizárólag törvény korlátozhatja. A biztosító társaság által elkészíttetett egészségügyi szakvélemény megismerésétől az érintett nem zárható el. Ennek alapján a biztos felszólította a biztosítót, hogy a kérdéses szakvéleményt bocsássák az érintett rendelkezésére. A biztosító válaszlevelében közölte, hogy a biztosítottra vonatkozó adatok biztosítási titoknak minősülnek, ezért titoktartási kötelezettségük a károsult felé is fennáll. A károsultra vonatkozó adatokat a károsult jogi képviselőjének megküldték. *(819/A/2006)*

Egy beadványozó kifogásolta, hogy az MKB Egészségpénztár belépési nyilatkozatán fel kell tüntetni az adóazonosító jelét, továbbá a telefonos és honlapon történő egyenleglekérdezés az adóazonosító jel segítségével történik.

Az adatvédelmi biztos egy korábbi állásfoglalására hivatkozva a következőket állapította meg: Az adózás rendjéről szóló 2003. évi XII. törvény (továbbiakban: Art.) tételesen felsorolja, hogy az érintett kivel köteles közölni adóazonosító jelét. Az Art. vonatkozó rendelkezése értelmében a magánszemély akkor köteles közölni az adóazonosító jelét, ha ezzel összefüggésben az igazolást kiállító szervet adatszolgáltatási kötelezettség terheli. Az adatszolgáltatási kötelezettség csak ilyen tartalmú igazolás kiadása esetén áll fenn. Mindebből következően, ha a magánszemély nem kíván adókedvezményt igénybe venni, szabadon dönthet arról, hogy közli-e az adóazonosító jelét vagy sem.

Az adóazonosító jel call centeres általános ügyfélazonosítóként való használata adatvédelmi szempontból szintén aggályos. A személyazonosító jel helyébe lépő azonosítási módokról és az azonosító kódok használatáról szóló 1996. évi XX. törvény szerint az adatkezelő az érintettel, illetve más adatkezelővel való, meghatározott célú kapcsolattartása során csak azt az azonosító kódot használhatja, amelyre a feladatot meghatározó törvény felhatalmazza. Törvényi felhatalmazás hiányában az azonosító kódot csak az érintett előzetes, írásbeli hozzájárulása alapján lehet felhasználni. Az érintettet a hozzájárulás megtagadása, illetve visszavonása miatt hátrány nem érheti, a hozzájárulásért bármiféle előny kilátásba helyezése tilos. Az adatkezelés egyébként sem nélkülözhetetlen, tekintettel arra, hogy az ügyfél tagi kóddal is rendelkezik. A vizsgálat eredményeképpen a biztos felszólította az adatkezelőt az adatkezelési gyakorlat felülvizsgálatára és a szükséges intézkedések megtételére. *(1220/A/2006)*

Önkormányzatok

A 2006. évben a helyi önkormányzatokat érintő vizsgálatok száma és aránya nem változott az elmúlt évekhez képest. Fontos ugyanakkor kiemelni azt, hogy ebben az esztendőben önkormányzati választásokat is tartottak, és a helyi választási szervek, illetve a választási eljárásban résztvevők adatkezelését is számos beadvány kifogásolta, ezen ügyeket a választásokról szóló alfejezetben ismertetjük. Azon ügyek ismertetésére, melyekben az önkormányzat mint munkáltató jelenik meg, a Munkáltatók című alfejezetben kerül sor.

Az önkormányzatoknál dolgozó szakemberek továbbra is gyakran kérnek konzultációs lehetőséget, jogi állásfoglalást a biztostól.

Számtalan önkormányzati, jegyzői konferenciára és szakmai továbbképzésre szóló meghívásnak teszünk eleget, és segítjük, támogatjuk az egységes és helyes jogalkalmazói gyakorlat kialakítását az adatvédelem terén is. Bár a honlapunkon számos, az önkormányzatok adatkezelését érintő állásfoglalás olvasható, melyekből az adatvédelmi biztos joggyakorlata teljes körűen megismerhető, mégis a már korábbi években tárgyalt és eredményesen lezárt ügyek, ügycsoportok újra és újra napirendre kerülnek. Valószínű, hogy az önkormányzati adatkezelők egy része, vélhetően akkor, ha ez valamilyen helyi konfliktus forrása, vagy azzá válhat, „*személyre és esetre szabottan*" kérik a biztosi állásfoglalást, mert valamiért a már közzétett biztosi álláspont érvényesítéséhez nem elég, ha a hasonló tényállást taglaló jogesetet az adatkezelő maga közli az érintettekkel vagy az adatok kezelését igénylőkkel. Az adatkezelők ugyanis gyakran szembekerülnek az adatok továbbítását igénylő önkormányzati szervekkel, képviselőkkel. Emiatt az ismétlődő ügyek száma viszonylag magas, viszont e folyamat jelezheti az adatvédelmi „*szak*"-ombudsman iránti bizalom további erősödését, mivel ha kell, az adatkezeléseket törvényesen folytatni akarók mögé állunk. Egy másik sajnálatos jelenség is folytatódott, illetve felerősödött. Nevezetesen: nőtt azon beadványok, elsősorban panaszügyek száma, amelyeket hatáskör hiányában nem tudunk kivizsgálni, illetve más országgyűlési biztoshoz áttenni. Ezek a szociális ellátást igénylő, válsághelyzetbe került embertársainktól érkező segítségkérő levelek. Természetesen minden lehetséges információt, segítséget, jogi tájékoztatást megadunk a biztoshoz fordulóknak, és ha lehetőség van rá, akkor az ügyet az illetékes szervhez áttesszük.

Önkormányzati adóhatóság

Egy állampolgár tájékoztatást kért arról, hogy a polgármesteri hivatal adóhatósága jogszerűen kérheti-e adópótlék eltörléséhez az általa használt adatlapon szereplő valamennyi adatot, köteles-e a kérelmező az összes feltett kérdésre válaszolni és felfedni saját és családja tagjainak vagyoni viszonyait.

> Az Art. alapján a tőke-, pótlék-, illetőleg bírságtartozás mérséklésére irányuló kérelem esetén az adóhatóságnak vizsgálnia kell, hogy az adózó és a vele együtt élő közeli hozzátartozók megélhetését a tartozás megfizetése súlyosan veszélyezteti-e, vagyis a kedvezmény

elbírálása érdekében kérhet adatokat a jövedelmi viszonyokról és a vagyoni helyzetről. Az eljáráshoz kötődő adatkezelés során figyelembe kell venni a célhoz kötöttség elvét is. A vizsgált estben használt nyomtatvány adatköre nem mindenben felelt meg ezen elvnek. A jövedelemre, vagyonra vonatkozó adatok kezelése elfogadható a megélhetési veszélyhelyzet vizsgálatához, azonban egyes adatok esetében (például: igazolvány száma, foglalkozás, jelenlegi és korábbi munkahely, pénzkövetelés) valószínűsíthető, hogy azok valójában nem szükségesek a kérelem elbírálásához. Természetesen az adózónak lehetősége van arra, hogy személyes adatairól ne nyilatkozzon, ebben az esetben azonban az adóhatóság kérelmét a rendelkezésre álló adatok alapján bírálja el. A biztos kezdeményezte a kért adatkör szűkítését. *(191/A/2006)*

Egy önkormányzati képviselő tájékoztatást kért arról, hogy képviselői minőségében tájékoztatást kérhet-e a helyi adóhatóság eljárásáról, mivel a jegyző több esetben is indítványozta iparűzési és súlyadó hátralék esetén az adótartozások elengedését.

Ha az adózási adat nem magánszemélyre, hanem valamely szervezetre, cégre vonatkozik, akkor kezelésére nem vonatkoznak az Avtv. szabályai. Ellenben az adótitok védelmére vonatkozó szabályokat valamennyi adatra alkalmazni kell, így adózási adatokat csak az Art. 54. §-ában meghatározott esetekben lehet mások tudomására hozni. A képviselő-testület és a képviselők tevékenységéhez, tájékoztatásához (például: költségvetési kérdések, rendeletalkotás esetén) elegendő anonimizált, összesített adatok, elemzések átadása. Ezen adatokat nemcsak a képviselők, hanem bárki megismerheti. Az önkormányzat helyi adók vonatkozásában fennálló adómegállapítási joga nem teszi szükségessé meghatározott személyek adózási adatainak kezelését. A helyi önkormányzatokról szóló 1990. évi LXV. törvény (továbbiakban: Ötv.) 19. § (2) bekezdése informálódási jogot biztosít a képviselőknek egyrészt *„önkormányzati ügyekben”*, másrészt *„a képviselői munkájához szükséges”* mértékben. A képviselői minőség azonban önmagában nem jogosít személyes adatok megismerésére és kezelésére. Az Avtv.-vel csak olyan értelmezés van összhangban, amely szerint a képviselő konkrét ügyben – az erre hatáskörrel rendelkező bizottság tagjaként, illetve a képviselő-testület ülésén – a személyes adatok kezelését igénylő eljárás részeként ismerheti meg a személyes adatokat. Az adóhatósági jogkör gyakorlása nem jelentheti az adótitok jogosulatlan továbbítá-

sát, nyilvánosságra hozását. Amennyiben adótitkok mások tudomására jutnak, akkor e harmadik személyek sem jogosultak arra, hogy az adatokat továbbítsák vagy nyilvánosságra hozzák.

Az Art. alapján a helyi adómérséklési és adóelengedési ügyekben a jegyző jár el a törvényben foglaltak végrehajtása érdekében, és a képviselő-testületnek nincs adómérsékléssel kapcsolatos feladata. Vagyis a képviselő-testület akkor kezelhet, ismerhet meg személyes adatokat, ha tevékenységéhez kapcsolódóan, meghatározott célból erre törvény felhatalmazza. *(540/A/2006)*

Szociális ügyek, gyámügy

Egy kisebbségi önkormányzati képviselő azért kérte az adatvédelmi biztos állásfoglalását, mert a képviselő-testület döntése alapján a kisebbségi képviselők adatvédelmi akadályok miatt nem vehettek részt a szociális bizottság munkájában.

Az Ötv. 1. §-a szerint a helyi önkormányzat – a törvény keretei között – önállóan szabályozhatja, illetőleg egyedi ügyekben szabadon igazgathatja a feladat- és hatáskörébe tartozó helyi közügyeket, önállóan alakíthatja szervezetét és működési rendjét. Döntését az Alkotmánybíróság, illetve bíróság kizárólag jogszabálysértés esetén bírálhatja felül. A szociális igazgatásról és szociális ellátásokról szóló 1993. évi III. törvényben meghatározott szociális feladat- és hatásköröket a helyi önkormányzat képviselő-testülete, a települési önkormányzat polgármestere, a települési önkormányzat jegyzője látja el. A szociális nyilvántartás vezetése a jegyző feladata, melyből csak a szociális hatáskört gyakorló szervek és más felsorolt szervek, intézmények részére eseti megkeresésük alapján szolgáltathatók adatok. Vagyis ha a kisebbségi önkormányzat képviselőjét nem választják be a települési önkormányzat szociális bizottságába, akkor nem vehet részt a bizottság érdemi munkájában, és ekként nem rendelkezik az Avtv.-ben előírt törvényi felhatalmazással arra, hogy az önkormányzati hatósági ügyek elbírálása során a polgárok szociális nyilvántartásban is kezelt személyes adatait megismerje. *(949/A/2006)*

Hasonló ügyben kért állásfoglalást egy kistelepülés önkormányzatának igazgatási ügyintézője arról, hogy a települési képviselő, illetve a képviselő-testület megismerheti-e a szociális nyilvántartásban szereplő azon személyes adatokat, melyeket a polgármester a képviselő-testü-

let által a rá átruházott szociális igazgatási feladat és hatáskör ellátása során kezelt, vagyis pontosan kinek, miért és mennyi segélyt adott.

Az Ötv. 35. §-a szerint a polgármester az önkormányzati, valamint az államigazgatási feladatait, hatásköreit a képviselő-testület hivatalának közreműködésével látja el és dönt a jogszabály által hatáskörébe utalt államigazgatási ügyekben, hatósági jogkörökben. Az Ötv. 11. §-a szerint a képviselő-testület önkormányzati hatósági ügyben hozott határozata ellen fellebbezésnek nincs helye, de a polgármester önkormányzati jogkörben hozott hatósági határozata ellen a képviselő-testülethez lehet fellebbezést benyújtani. Az Ötv. 19. § (1) bekezdés c) pontja alapján a települési képviselő kezdeményezheti, hogy a képviselő-testület vizsgálja felül a polgármesternek – a képviselő-testület által átruházott – önkormányzati ügyben hozott döntését. Az Ötv. 19. §-a (2) bekezdése informálódási jogot biztosít a települési képviselő számára egyrészt *„önkormányzati ügyekben"*, másrészt *„a képviselői munkájához szükséges"* mértékben. Mint minden más adatkezelésre, a képviselők azon kéréseire is vonatkoznak az Avtv. szabályai, amelyek személyes adatok kezelésével járnak. A képviselő önálló feladat- és hatáskörrel nem bír, *„képviselői munkája"* elsősorban a képviselő-testület és bizottságai döntési kompetenciájába tartozó egyes ügyek döntéseinek előkészítésében, végrehajtásuk szervezésében és ellenőrzésében való részvételt jelenti. Az Avtv.-vel azonban csak olyan értelmezés van összhangban, amely szerint a képviselő konkrét ügyben – az erre hatáskörrel rendelkező bizottság tagjaként, illetve a képviselő-testület ülésén – a személyes adatok kezelését igénylő eljárás részeként ismerheti meg a személyes adatokat.

A vizsgált esetben így a személyes adatok továbbítása jogellenes lett volna, mivel egyik törvény sem hatalmazza fel a települési képviselőt arra, hogy egyénileg, személyes ellenőrzés lefolytatása céljából, egyedi ügyre vonatkozó adatszolgáltatást kérjen és kapjon a jegyző által vezetett szociális nyilvántartásból. Amennyiben a képviselő-testület úgy dönt, hogy a képviselő kezdeményezésére, a polgármester által átruházott szociális hatáskörben meghozott döntést felülvizsgálja, akkor az ügy iratai, illetve a felülvizsgálathoz szükséges, nyilvántartott személyes adatok a képviselő-testületnek kizárólag e cél érdekében továbbíthatók. Ugyanez vonatkozik arra az esetre is, ha az ügyfél fellebbez, és a képviselő-testülettől a szociális ügyben átruházott hatáskörben meghozott polgármesteri határozat *„felülvizsgálatát"* kéri. A biztos álláspontja szerint kizárólag a statisztikai adatok segítségével adott polgármesteri beszámoló felel meg az Avtv. szabályainak. *(1870/K/2006)*

Az egyik fővárosi gyámhivatal vezetője, egy folyamatban lévő eljárásban, a szülői felügyeleti jogokkal nem rendelkező apa irat-betekintési jogával kapcsolatban fogalmazott meg kérdéseket. A gyámhivatal kapcsolattartási ügyben döntésének meghozatalához előzetes pszichológusi véleményt kért egy kiskorúról, aki „*szorongó, félelmekkel teli az apával szemben*", a szülői felügyeleti jogokat gyakorló anya a gyermek vizsgálati eredményei tükrében az apa tájékoztatását kifejezetten ellenezte.

Az adatvédelmi biztos hasonló ügyekben kialakított állásfoglalásaiban már korábban hangsúlyozta, hogy – a szülők gyakori „*félreértése ellenére*" – a gyermekvédelmi-gyámhatósági eljárásokban a főszereplő minden esetben egyértelműen a gyermek, aki valamilyen okból külső, állami segítségre szorul. A segítségnyújtás előfeltétele pedig, hogy az ő személyre szabott speciális helyzetét és igényeit szakértők felmérjék és szakvéleményükben rögzítsék. A gyermekvédelmi törvény az alapelveknél kiemeli, hogy a gyermekek védelmét ellátó helyi önkormányzatok, gyámhivatalok, bíróságok, rendőrség, ügyészség, pártfogó felügyelői szolgálat, más szervezetek és személyek e törvény alkalmazása során a gyermek mindenek felett álló érdekét figyelembe véve, törvényben elismert jogait biztosítva járnak el. A gyámhatóságokról, valamint a gyermekvédelmi és gyámügyi eljárásról szóló 149/1997. (IX. 10.) Korm. rendelet 13/A. § -a alapján a gyámhatóság az irat-betekintési jogot a közigazgatási hatósági eljárás és szolgáltatás általános szabályairól szóló 2004. évi CXL. törvény 68-69. §-ában foglaltakra hivatkozva (a gyermekek védelméről és a gyámügyi igazgatásról szóló 1997. évi XXXI. törvény 136. §-ának (5) bekezdésben meghatározott esetet pedig külön is nevesítve) a szülő tekintetében végzéssel korlátozhatja.

A vizsgált esetben a gyámhatóság feladata és felelőssége annak a kérdésnek az eldöntése, hogy az apa milyen terjedelemben ismerheti meg a kiskorúról készített pszichológusi szakvélemény tartalmát. Ennek célja, hogy a hatósági döntés alapjául szolgáló vélemény lényegével tisztában legyen, ügyféli jogai így ne csorbuljanak, és a gyermekéről is megfelelő információt nyerjen – mindezt úgy, hogy a kiskorú gyermek érdekei (ideértve az apával való kapcsolatát is) a tájékoztatás során (vagy éppen emiatt) ne sérüljenek. Ennek az alapvetően szakmai kérdésnek az eldöntésekor akkor jár el helyesen a hatóság, ha pszichológus szakértőt vesz igénybe, és ebben a kérdésben is kikéri a szakvéleményét. *(1189/K/2006)*

Egyéb, igazgatási célú adatkezelések

Egy jegyző konzultációs beadványában a veszélyes és veszélyesnek minősített eb tartásáról és a tartás engedélyezésének szabályairól, valamint az ebek veszélyessé minősítésével összefüggő szakhatósági eljárásról szóló jogszabályok adatvédelmi szempontú anomáliáira hívta fel a figyelmet. Az indítványozó álláspontja szerint e speciális viszonyokat szabályozó jogi normák nincsenek összhangban az adatvédelmi előírásokkal.

Az adatkezelést elrendelő jogszabályok között az állam- és közbiztonságról szóló 1974. évi 17. törvényerejű rendelet (továbbiakban: tvr.) megfelelő jogforrási szint a veszélyes és veszélyessé minősített ebek tartásának engedélyezési eljárásával, és a veszélyessé minősítésével összefüggő szakhatósági eljárással kapcsolatos adatkezelések tekintetében. A tvr. felhatalmazó rendelkezéseket is tartalmaz, mely szerint a veszélyessé minősítéssel összefüggő szakhatósági közreműködés szabályait a földművelésügyi miniszter állapítja meg. Ezen a felhatalmazáson alapul az ebek veszélyessé minősítésével összefüggő szakhatósági eljárásról és az ebek egyedi azonosításának díjáról szóló 15/1997. (III. 5.) FM rendelet. Továbbá a tvr. alapján a kormány felhatalmazást kapott, hogy a veszélyes és veszélyessé minősített eb tartása engedélyezésének és tartásának részletes feltételeit és módját, valamint ezek ellenőrzésének rendjét rendeletben határozza meg. Ezen a felhatalmazáson alapul a 35/1997. (II. 26.) Kormányrendelet, amely meghatározza az engedélyezési eljárás részletszabályait.

A vizsgált jogszabályokról elmondható, hogy önmagában az adatkezelés kormányrendeleti vagy miniszteri rendeleti szintű szabályozása nem sérti az adatvédelem garanciális alapelveit, ha a kötelező adatkezelést elrendelő jogszabály kielégíti az Avtv. 3. § (3) bekezdésében foglalt kritériumokat, és a törvényi felhatalmazás kiterjed az eljárással összefüggő adatkezelés részletszabályainak megalkotására is. A tvr. 1997-ben hatályba lépett rendelkezései tartalmilag nem felelnek meg a később hatályba lépett Avtv. módosításnak. Különösen abban a tekintetben nem, hogy a tvr. nem nevesíti adatkezelőként az állat-egészségügyi szakhatóságot és az Országos Állat-egészségügyi Intézetet, továbbá nem határozza meg, hogy ezek a szervezetek az engedélyezési és veszélyessé minősítési eljárásban milyen feltételekkel kezelik az eb tulajdonosának személyes adatait. Az állat-egészségügyi állomás adatkezelését a szakha-

tósági közreműködésre tekintettel a tvr. felhatalmazó rendelkezéseiből ugyan le lehet vezetni, azonban szükséges a tvr. kiegészítése. Az Országos Állat-egészségügyi Intézet adatkezelése viszont különösen aggályos, mert az adatkezelés jogalapja a tvr. felhatalmazó rendelkezéséből már nem következik, és az adatkezelést elrendelő jogforrási szint (kormányrendelet) nem felel meg a *„törvényben elrendelt adatkezelés"* követelményének. A központi nyilvántartás a személyes adatok védelméhez fűződő joggal összefüggésben olyan mértékű korlátozást jelent, amelyet törvényben (a tvr.-ben) az adatkezelés feltételeinek meghatározásával szükséges szabályozni. Az adatvédelmi biztos kezdeményezte a földművelésügyi és vidékfejlesztési miniszternél a jogszabály módosítások előterjesztését. A miniszter az adatvédelmi biztos álláspontjával teljes mértékben egyetértett, és jelezte, hogy e tárgykörben egy teljesen új törvény megalkotását fogja kezdeményezni. *(412/A/2006)*

Egy önkormányzat köztisztviselője arról kért állásfoglalást, hogy a körjegyzőséghez tartozó településeken telephellyel, székhellyel rendelkező kereskedők adatait kiadhatja-e a Növény- és Talajvédelmi Szolgálat részére. A zöldség-gyümölcs forgalmazásával foglalkozó kereskedők gazdasági tevékenységüket – az egyéni vállalkozók kivételével – nem természetes személyként végzik, ezért a kereskedők adatai fő szabály szerint nem minősülnek személyes adatnak, vagyis kizárólag az egyéni vállalkozók adatainak kezelésére vonatkozott a kiadott biztosi állásfoglalás.

Az Avtv. rendelkezései alapján adatkezelésnek minősül, ha a jegyző a Növény- és Talajvédelmi Szolgálat részére az egyéni vállalkozó kereskedők adatait kiadja, ezért erre az érintettek hozzájárulásának hiányában kizárólag törvényi felhatalmazás alapján nyílhat lehetőség. Az Európai Közösségek Bizottsága 1148/2001/EK rendelete 3. cikkelyének (4) bekezdése szerint, a kereskedőknek biztosítaniuk kell a tagállamok által az adatbázis létrehozásához és frissítéséhez szükségesnek ítélt információt. A tagállamok meghatározzák azokat a feltételeket, amelyek szabályozzák a nem az adott tagállam területén alapított, de ott kereskedelmi tevékenységet folytató kereskedők bekerülését az adatbázisba. Vagyis a bizottsági rendeletből nem következik a jegyző adatszolgáltatási kötelezettsége, mivel az európai jogszabály kizárólag a kereskedők számára teszi kötelezővé a szükséges információk biztosítását. A növényvédelemről szóló 2000. évi XXXV. törvény ugyancsak nem ír elő a jegyző számára adatszolgál-

> tatási kötelezettséget, így ez sem szolgáltat az adatkezeléshez megfelelő jogalapot. Az egyéni vállalkozásról szóló 1990. évi V. törvény 4/A. §-a alapján a körzetközponti jegyző az egyéni vállalkozókról nyilvántartást vezet, melynek adatai – a telefon- és telefaxszám kivételével – nyilvánosak. Azonban a kialakult adatvédelmi gyakorlat szerint a nyilvános személyes adatok tekintetében is érvényesülnie kell a célhoz kötött adatkezelés elvének, amely a vizsgált esetben megvalósult, mivel a Növény- és Talajvédelmi Szolgálat részéről az adatok igénylésére hivatalos feladatainak ellátásának céljából, a szükséges mértékben került sor. Vagyis a jegyző nem sérti az érintettek információs önrendelkezési jogát, ha a vállalkozói igazolvánnyal rendelkező egyéni vállalkozó kereskedők nevére, székhelyére és telephelyére vonatkozó adatokat továbbítja a Növény- és Talajvédelmi Szolgálat részére. De mivel a mezőgazdasági termelőtevékenység és az ahhoz kapcsolódó szolgáltatás vállalkozói igazolvány nélkül is gyakorolható, így a nyilvántartásban nem szereplők adatait – törvényi felhatalmazás híján – kizárólag az érintettek hozzájárulása esetén adhatja ki a jegyző. *(506/K/2006)*

Ugyancsak az egyéni vállalkozók adatainak felhasználását érintette az a beadvány, amelyben egy jegyző azt kérdezte az adatvédelmi biztostól, hogy a közbeszerzési értékhatárt el nem érő beszerzéseik költségkímélő, hatékony lebonyolítása céljából az adatvédelmi jogszabályok betartása mellett jogszerűen létrehozhatnak-e olyan adatbázist, amely a településen székhellyel, telephellyel rendelkező egyéni vállalkozók, társas vállalkozások nevét, címét és tevékenységi körét tartalmazza.

> Mivel a társas vállalkozások adatainak nyilvántartása adatvédelmi aggályokat nem vethet fel, az Avtv. személyes adatokra vonatkozó rendelkezéseit kizárólag az egyéni vállalkozók adataira kell alkalmazni. Az Avtv. rendelkezéséből adódóan az egyéni vállalkozók neve, székhelye és tevékenységi köre az egyéni vállalkozásról szóló törvény alapján közérdekből nyilvános adat. Az adatok nyilvánosságát – a cégnyilvántartáshoz hasonlóan – a gazdasági tevékenység biztonsága mint közérdekű cél teszi indokolttá. A polgármesteri hivatal által létrehozni kívánt nyilvántartással ez a közérdekű cél nem sérül, mivel az adatok felhasználására változatlanul a gazdasági forgalomban, az önkormányzati beszerzések megvalósítása során kerülne sor. Ezért adatvédelmi szempontból nincs akadálya a nyilvántartás létrehozásának. *(878/K/2006)*

A polgármesteri hivatalok adatkezelése

Egy állampolgár arról kért állásfoglalást, hogy a polgármesteri hivatal vezethet-e nyilvántartást azokról a személyekről, akik a polgármesterek és az önkormányzati képviselők vagyonnyilatkozataiba betekintettek, illetve a betekintést igénylő érintettnek igazolnia kell-e személyazonosságát.

> Az Avtv. 19. § (4) bekezdése szerint közérdekből nyilvános adat az állami vagy helyi önkormányzati feladatot, valamint jogszabályban meghatározott egyéb közfeladatot ellátó szerv feladat- és hatáskörében eljáró személynek a feladatkörével összefüggő személyes adata, továbbá egyéb, közfeladatot ellátó személynek e feladatkörével összefüggő személyes adata. Ezen adatok megismerésére e törvénynek a közérdekű adatok megismerésére vonatkozó rendelkezéseit kell alkalmazni. A törvény alapján a közérdekű adatok megismeréséhez az igénylőnek nem kell semmilyen érdeket igazolnia, és az adatkezelő az igény teljesítését nem teheti attól függővé, hogy az igénylő az információt mire kívánja felhasználni. Az Avtv. nem hatalmazza fel az adatkezelőt arra sem, hogy az adatigénylő személyazonosságát ellenőrizze, adatait rögzítse. *(821/A/2006)*

Egy városi önkormányzat képviselő-testületi ülésein gyakorlattá vált, hogy a testületi ülésről készült jegyzőkönyv eredeti példányával együtt kezelték a hallgatósággal aláíratott jelenléti ívet. Bár az önkormányzat szervezeti és működési szabályzata nem tartalmazott semmilyen rendelkezést arról, hogy a jelenléti ívet kinek kell aláírnia, azt a megjelenő érdeklődő állampolgárokkal is aláíratták. Az adatfelvétel előtt a jegyzőkönyvvezető elmondta az érintetteknek, hogy jegyzőkönyvvezetés és az esetleges kérdésükre adott válasz miatt kérik az aláírásokat. A felvett jelenléti ívet a jegyzőkönyv mellékleteként bárki számára hozzáférhetővé tették a polgármesteri hivatalban, illetve a városi könyvtárban.

> Az Avtv. alapján a név, az aláírás és az az adat, hogy valaki részt vesz a képviselő-testület ülésén személyes adat, függetlenül attól, hogy az aláírás olvasható-e vagy sem. E személyes adatok az Avtv. szabályai szerint kizárólag az érintett hozzájárulásával (mivel ezen adatok kezelésére az Ötv. nem ad felhatalmazást a képviselő-testületnek), a célhoz kötöttség elvének betartásával kezelhetők, beleértve a kezelt adatok nyilvánosságra hozatalát is. A biztos megállapította, hogy a testületi ülésen megjelenő érdeklődő érintettek sze-

mélyes adatainak felvételét és nyilvánosságra hozatalát nem alapozza meg a (formálisan) megadott hozzájárulásuk sem, mivel az adatok kezelése nem felel meg a célhoz kötöttség elvének. Az adatkezelés egy a jövőben esetlegesen bekövetkező esemény (az érintett szót kap a testület ülésén) dokumentálása céljából, készletező és a cél elérésére alkalmatlan módon folyt, mivel a feltárt gyakorlat alapján felvett jelenléti ív nyilvánvalóan nem lehet alkalmas arra, hogy a később hozzászólót azonosítsa. Másfelől az érintett hozzászólónak – amennyiben szót kap – jogában áll eldönteni, hogy a hozzászólását névvel vagy név nélkül kívánja-e elmondani, illetve előzetesen tájékoztatni kell arról, hogy a hozzászólását (esetleg hangfelvétel útján is) jegyzőkönyvbe veszik. Ezt követően a hozzászóló érintett által a nyilvános testületi ülésen a közszereplése során általa közölt vagy a nyilvánosságra hozatal céljából általa átadott adatok tekintetében megadott hozzájárulását az Avtv. 3. §-a alapján vélelmezni kell. Ez vonatkozik az érintett lakcímének kezelésére is, amennyiben írásban küldik el a választ, nem célszerű a nyilvánosságra hozott jegyzőkönyvben *„felvenni és tárolni”* az érintett nevét és lakcímét. *(1332/A/2006)*

Az önkormányzat vagyonával való gazdálkodásához kapcsolódott az alábbiakban ismertetett eset. Egy állampolgár annak vizsgálatát kérte, hogy történt-e visszaélés személyes adataival, amikor Terézváros Önkormányzata az egyik Andrássy úti épület privatizációja során kiszolgáltatta az épületben található önkormányzati bérlakások lakóinak adatait – köztük a lakásbérleti szerződéseket is – a befektető kft. részére. A jegyző álláspontja szerint a befektető mint új tulajdonos jogosult megismerni a lakásbérleti szerződések adatait. Az önkormányzat tájékoztatta a bérlőket a tulajdonos személyében bekövetkezett változásról, a bérleti szerződések átadása szerződéses kötelezettség volt, a bérlakások tulajdonosának személye az adásvétel által megváltozott, az új tulajdonos adatkezelővé vált, vagyis a korábbi adatkezelő önkormányzat helyébe lépett az egyébként változatlan jogviszonyban.

A bérleti szerződésben feltüntetett név- és lakcímadatot polgári jogi jogügylet alapján valóban kezelheti az adott gazdasági társaság, a törvényes jogalapot a Polgári Törvénykönyv és a bérleti szerződés együttesen teremti meg. Azonban egyéb adattovábbítás (például: telefonszám, okmányazonosító) jogalapja csak a bérlő hozzájárulása lehet. A kezelendő (továbbított) adatkör meghatározásánál

> tekintettel kell lenni a célhoz kötöttség elvére is. Ennek megfelelően csak a bérleti szerződés teljesítéséhez szükséges adatkör átadása fogadható el. S bár az önkormányzat tájékoztatta a lakókat az adásvételről és az új tulajdonos/adatkezelő személyéről, azonban ez a levél a bérleti szerződéssel és annak adataival kapcsolatos egyéb információt nem tartalmazott, ezért a tájékoztatás nem felelt meg az Avtv. szabályainak. *(31/A/2006)*

Egy jegyző tájékoztatást kért arról, hogy megsérti-e az önkormányzat az Avtv. szabályait, amennyiben a település saját internetes oldalán található hivatalos fóruma csak előzetes regisztráció után vehető igénybe. A regisztráció során az érintetteknek kötelezően meg kellett adniuk név (felhasználónév), jelszó, e-mail cím, teljes név, lakcím és telefonszám adataikat. Az egyik felhasználó az Európa Tanács 1999/5-ös ajánlására hivatkozva arra hívta fel az önkormányzat figyelmét, hogy az említett szolgáltatás névtelenül vagy fedőnévvel is igénybe vehető.

> A biztos az internetes regisztrációval kapcsolatosan 2004-ben kiadott állásfoglalásában már hangsúlyozta, hogy az önkormányzatnak mint tartalomszolgáltatónak nem kötelessége felelősséget vállalni a szabad vélemény-nyilvánításhoz való jog gyakorlásával elkövetett jogsértésekért, így a felhasználók személyazonosságának megállapítása sem tartozik az ő tartalomszolgáltatói feladatkörébe. Amennyiben a fórumon olyan hozzászólás jelenik meg, amely sérti bárkinek a személyiségi jogait, vagy jogszabályba ütközik, a tartalomszolgáltató köteles azt a tartalmat eltávolítani. A jogsértő személyének a megállapítása a nyomozóhatóság feladatkörébe tartozik, a tartalomszolgáltatótól csupán a regisztrálással kezelt adatok szolgáltatása várható el, a hozzászóló valós kilétének felfedése nem a tartalomszolgáltató feladata. A hozzászólások eldurvulásának elkerülését egyébként sem szolgálja a lakcím, telefonszám, és e-mail cím, valamint a polgári név együttes kezelése, mert a személyes jelenlétet nélkülöző internetes közegben a személyazonosítás ezen adatok alapján sem állapítható meg minden kétséget kizáróan. Az önkormányzatnak az a törekvése, hogy a felhasználók azonosításának érdekében az oldal használatát előzetes regisztrációhoz kösse, adatvédelmi szempontból elfogadható, azonban az adatkezelését köteles a célhoz kötöttség és adatminimum elvéhez igazítani. *(1585/K/2006)*

A különböző internetes fórumok adatkezeléseiről bővebben szól az *„Internet”* fejezet.

Szektorális adatkezelések

Egészségügy

Az egészségügyi adatkezelések fejezete 2006-ban azzal kezdődik, amivel a tavalyi beszámolóban záródott: az uniós ellenőrzések ügyével. Egy vizsgálat például azért indult, mert egy háborús traumát szenvedett emberek pszichiátriai kezelését felvállaló alapítványtól a Belügyminisztérium projektellenőrzés címén bekérte a kezeltek nevét. A vizsgálat során kiderült azonban, hogy (mint oly sok más esetben) az Európai Bizottság állásfoglalásának megfelelően itt is elegendő, ha a minisztérium képviselője csak azt ellenőrzi, hogy az alapítvány által ellátott személy valóban szerepel-e az állami nyilvántartásban, de az érintett személyes adatai már nem kerülnek rögzítésre. *(1598/K/2005)*

Ez a példa is azt mutatja, hogy az ellenőrzések lebonyolítása nem feltétlenül kell, hogy együtt járjon személyes adatok kezelésével. Egészségügyi állapotra utaló különleges adatok esetében pedig mind a jogalkotótól, mind a jogalkalmazótól elvárható lenne, hogy megfelelő érzékenységgel, körültekintéssel válassza meg eszközeit a közpénzek útjának követéséhez.

Ezzel szemben a jelenlegi helyzet lesújtónak is minősíthető. Az Adatvédelmi Biztos Irodája mindig is együttműködött a közpénzek ellenőrzési rendszereinek hatékony kidolgozásában. A társadalombiztosítás rendszerében – az OEP-től megkapott információk szerint – évente 150 millió receptet írnak fel, 120 millió orvos-beteg találkozót dokumentálnak, a kifizetések összege 1500 milliárd forint. Ezek mindegyikénél szükségszerű az adatkezelés. Ennek eredményeképp végül a nagy állami nyilvántartások körében a legnagyobb rendszerjellegű nyilvántartás jön létre. Elkerülhetetlen tehát ennek a stratégiai jelentőségű, a biztosítottak intim szférájához tartozó különleges adatokkal működő rendszernek a megfelelő kezelése, védelme és *„karbantartása”*. Adatvédelmi szempontból többféle alkotmányos megoldás szóba jöhet, így elfogadható a pénzügyi-szakmai ellenőrzések teljes vagy részleges különválasztása is. Ehhez képest 2006-ban az egészségügyi politika a finanszírozási gondokra olyan új adatbegyűjtési tervekkel reagált, melyekről általánosságban mindenképpen megállapítható, hogy az adatvédelem alapvető elve, miszerint *„csak olyan személyes adat kezelhető, amely az adatkezelés céljának megvalósulásához elen-*

gedhetetlen, a cél elérésére alkalmas, csak a cél megvalósulásához szükséges mértékben és ideig" [Avtv. 5. § (2)], nem jelent meg a jogalkotó számára követelményként.

A társadalombiztosítási szervek kiemelt adatkezeléseinek átfogó vizsgálata 2006 októberében zárult le. Az állampolgári panaszbeadványok (több mint 30 egyéni panasz!) többsége az alább ismertetett négy kérdéskört együttesen érintette.

Sokan kifogásolták, hogy a háziorvosok 2006. szeptember 1-jétől kötelesek havi rendszerességgel adatot szolgáltatni a Megyei Egészségbiztosítási Pénztárakon keresztül az OEP-nek.

Mivel az adatvédelmi törvény kritériumait a kormányrendeleti szintű felhatalmazás megsérti, a háziorvosi kötelező adatszolgáltatás formai alkotmányossági okok miatt egyértelműen jogellenesnek volt minősíthető. Tartalmi okokból sem megnyugtató azonban az egységes jelentési rendszer jelenlegi szabályozása. Az adatkezelés célhoz kötöttségének elve alapján a finanszírozó kizárólag az általa finanszírozott ellátásokról kell hogy valamilyen módon tudomást szerezzen, így a háziorvosok munkájának a szűk értelemben vett gondozáson kívüli részével kapcsolatban az adattovábbítás célja nem meggyőző (a népegészségügyi szűréseket az ÁNTSZ külön forrásból végzi, a látleletek kibocsátását, a jogosítványhoz szükséges orvosi vizsgálatot, lőfegyverhasználati engedélyezési eljárás során kötelező orvosi vizsgálatot stb. a társadalombiztosítási szervek nem finanszírozzák.).

További súlyos kifogás az adatbiztonsági szempontokkal összefüggésben merült fel. Több háziorvos beszámolója szerint a társadalombiztosítási szervekkel történő kommunikáció (mely esetenként kétoldalú, hiszen például az orvosok rendszeresen megkapják az általuk felírt vények gyógyszertári adatait a biztosított taj-számon történő azonosítása mellett) számítógépes adathordozó, floppy lemez postázásával történik. A gyakorlat szerint ez normál postai küldeményként érkezik, vagyis a betegadatok semmiféle külön védelemben nem részesülnek. Más orvosok azt kifogásolják, hogy a jelentést konstruáló számítógépes program „*szabadon*" kutat az orvosi nyilvántartások adataiban, és az adatkezelő háziorvos – mivel a jelentés kizárólag a program segítségével generált kódszámokban jelenik meg – nem tud meggyőződni arról, hogy a küldött anyag a valóságban milyen adatokat tartalmaz.

A panaszok másik körében sokan kifogásolják, hogy a vényköteles, de társadalombiztosítási támogatással nem rendelkező gyógyszerek esetében annak ellenére bekerülnek adataik a társadalombiztosítási szervek nyilvántartásába, hogy valójában betegként semmilyen jogviszonyban nem állnak a társadalombiztosítás rendszerével. Három gyógyszer esetében kivételként közgyógyellátás keretében itt is van támogatás.

> A vizsgálat során kiderült, hogy ennek indoka főként technikai: szolgáltatói oldalról egycsatornás jelentési rendszer működik, amely nem képes arra, hogy a nem finanszírozott gyógyszerek listáját leválogassa. Ennek következtében a jogi szabályozás is csak egyetlen vénytípust ismer. Az OEP részéről egyfajta *„profiltisztítás"* jegyében egyértelmű annak a támogatása, hogy a társadalombiztosítási támogatással nem rendelkező gyógyszerek és ellátások ne szerepeljenek a nyilvántartásában.

A harmadik kérdéskör a vényköteles recepteken a BNO-kód (Betegségek Nemzetközi Osztályozása) kötelező feltüntetése. A tervezett szabályozás szerint a vényt az orvosnak kell kitölteni és a gyógyszerész elvileg ellenőrzi, hogy a felírt gyógyszer megfelel-e a betegség kezelésére a BNO-kód alapján. Az OEP szakértői is elismerték azonban, hogy jogszabály ilyen kötelezettséget nem ró a patikusra, sőt, a 250 betegség kezelésére vonatkozó szakmai protokollt az Egészségügyi Minisztérium is csak nemrég tette közzé. A felhatalmazó jogszabály rendeleti szintjére vonatkozó formai kifogások mellett a minisztériumtól érkező válaszok továbbra sem adtak megnyugtató tartalmi választ a kötelező feltüntetés indokára vonatkozóan.

Végezetül a tárgyhoz kapcsolódik – bár állampolgári panaszok nem érintették – az OEP-től kikerülő adatok köre. Egy 2004-es miniszteri rendelet az OEP számára kapcsolati kód-alapon történő rendszeres, tételes jelentési kötelezettséget ír elő az Egészségügyi Minisztérium, az Egészségügyi Stratégiai Kutató Intézet és az Országos Szakfelügyeleti Módszertani Központ felé. Az adattovábbítás személyazonosításra alkalmatlan módon, kapcsolati kóddal történik. A rendszer tehát – a fentiek alapján – úgy működik, hogy az OEP az állampolgárok által igénybe vett egészségügyi ellátásokról (ideértve a gyógyszerfogyasztást is) rendszeresen, egyénre lebontva jelent a minisztériumnak.

Felmerül a kérdés, hogy a pontossága és mérete miatt igen nagy piaci értéket képviselő, egyénekre lebontott és folyamatosan karbantartott adatbázis rendszeres átadásának mi a célja. A kérdés fontosságát alátámasztja az a tény, hogy amennyiben a kapcsolati kódokat dekódolják – ami természetesen csak jogellenes módon, bűncselekmény elkövetésével történhet, de elvileg a lehetősége nem zárható ki – a társadalombiztosítási ellátást igénybe vevő polgárok különleges adatai védelméhez fűződő alkotmányos joga veszélybe kerülhet.

A vizsgálat – mely pozitív minisztériumi fogadtatás hiányában még korántsem zárult le – számos olyan problémára fényt derített, mely valamennyi pontnál általános érvénnyel megállapítható. Kifogásolható mindenekelőtt, hogy a különleges adatok kötelező kezelésének szabályozását a jogalkotó sorozatban rendeleti úton próbálja megoldani, törvényi szintű előírás helyett. Nem tudni, hogy az összegyűjtött adatállományok a jövőben milyen célokat fognak szolgálni, milyen elvek és kritériumok mentén kerül majd sor az adatok feldolgozására. Az adatkezelési célok meghatározása hosszú távú fejlesztési koncepciók keretén belül képzelhető el, ehelyett sok esetben tettenérhető a pótmegoldás, a *„tűzoltás”*: nem az eredendő problémát hárítják el, hanem utólag ellenőriznek felesleges adatok alapján. *(1301/A/2006)*

2006-ban sor került egy hivatalból indított vizsgálatra is a közgyógyellátás rendszerének adatvédelmi összefüggéseiről. Egy rendkívül bonyolult rendszerről van szó, melyben adatkezelést végez az egészségügyi megalapozottságot igazoló háziorvos, a közgyógyellátási jogosultságról döntő jegyző, a szakhatóságként eljáró és az igazolványt kiállító MEP, a központi nyilvántartást vezető OEP, valamint a gyógyszerkiadást megelőzően a jogosultsági feltételeket ellenőrző gyógyszertár is.

> Még egy ilyen bonyolult rendszerben is arra kell törekedni, hogy minden döntéshozó kizárólag annyi és olyan személyes és különleges adathoz férjen hozzá, ismerjen meg, amennyire feladata ellátásához feltétlenül szüksége van. A biztos 2006. júliusi ajánlásában ezért leszögezte, hogy a közgyógyellátási jogosultságot megállapító jegyző nem ismerheti meg az érintett egészségügyi adatait – az egészségügyi rászorultság tényének kivételével –, ezt a jogszabálynak egyértelműen ki kell mondania. Az egészségbiztosítási szerv ugyanilyen indokok alapján nem jogosult a közigazgatási határozat azon részének megismerésére, melyen az érintett szociális helyze-

> tére vonatkozó adatok szerepelnek. A gyógyszertár által pedig a közgyógyellátási jogosultság ellenőrzése során kizárólag a törvényben meghatározott adatok rögzíthetőek, az OEP ezen túl adatrögzítést nem rendelhet el. *(1010/H/2006)*

Természetesen egyéb, „*klasszikus*" ügyek is szép számmal előfordultak ebben az évben. Az érintettek kifogásolták, hogy több orvosi rendelőben új módszereket is „*bevetettek*", mint például a betegek fényképes nyilvántartása *(1748/A/2006)* vagy a rendelőben elhangzottakról hangfelvétel készítése *(1803/A/2005)*. Mindkét esetben megállapítható volt, hogy a választott eszköz nem alkalmas a törvényes adatkezelési célok elérésére.

Szomorú tény, hogy sok szülő egymás közti megoldatlan konfliktusához a gyermeket vagy a gyermek személyes, különleges adatait is eszközül kívánja felhasználni, elsősorban a gyámhivatali eljárás keretében. Ezekben az ügyekben mindig a gyermek érdekeire kell elsősorban tekintettel lenni, esetleges érdekellentét esetében akár a törvényes felügyeleti joggal rendelkező szülő irat-megismerési joga is korlátozható *(587/K/2006, 1189/K/2006)*. A panaszok és konzultációs kérelmek gyakorisága miatt a gyermekvédelmi jelzőrendszerben az egészségügyi szolgáltatók jelzési kötelezettségével összefüggésben 2006 májusában a biztos állásfoglalást adott ki, mely tartalmazza a Családügyi, Szociális és Esélyegyenlőségi Minisztérium által elkészített módszertani útmutatót is. A gyakorlati útmutatót a biztos az állásfoglalásban jelzett kitétellel és megjegyzésekkel ajánlotta elfogadásra. *(308/K/2006)*

A fentieken kívül voltak olyan, egészségügyi adatokkal kapcsolatos vizsgálatok is, amelyek ismertetése más területekkel való kapcsolódásuk okán nem a jelen fejezetben olvashatók. Így például a biztos – „*régi-új*" problémaként – 2006 végén a MABISZ és a PSZÁF bevonásával vizsgálatot indított az életbiztosítási szerződések megkötése során felvett adatok köréről, erről bővebben a „*Biztosítók*" fejezetben lehet olvasni. A 2006. őszi tüntetések sérültjeinek különleges adataival kapcsolatos rendőrségi megkeresések ügye „*Az őszi zavargások kapcsán felmerült adatvédelmi kérdések*" című fejezetben olvasható.

Munkáltatók

A munkavállalók adatainak kezelésével kapcsolatos beadványok száma ez évben is meghaladta az előzőekét, más szektorális adatkeze-

lésekhez képest jelentős emelkedést mutatva. Az Adatvédelmi Biztos Irodájával telefonon konzultáló munkavállalók, munkáltatók száma is igen magas volt. A konzultációkból többek között az derült ki, hogy a munkavállalók egyre tudatosabban figyelnek magánszférájuk védelmére munkahelyükön, ugyanakkor az egzisztenciális kiszolgáltatottságuk miatt ez a jogérzék sokszor pusztán az észlelésre korlátozódik, és nem terjed ki az aktív jogérvényesítésre.

Az érintettek személyiségi jogaikat egyes adatkezelések kapcsán kevésbé tudják érvényesíteni. A munka világán belül azok a személyek vannak a leginkább kiszolgáltatott helyzetben, akik korábbi munkahelyüket valamilyen oknál fogva elvesztették, s maguk és családjuk eltartása érdekében mihamarabb új munkahelyet kell keresniük. A jeligés álláshirdetésekkel, valamint a magán-munkaközvetítők adatkezelésével kapcsolatos adatkezelések, azok utólagos nyomon követése évről évre visszatérő kérdésként merült fel az állampolgárok beadványaiban. A biztos a két adatkezelői kör eljárásával kapcsolatban ajánlást tett közzé.

A jeligés álláshirdetésnek az a sajátja, hogy a hirdetést feladó személy személyazonossága – illetőleg ha a feladó cég, annak kiléte – nem válik ismertté az érintett pályázó előtt, mindössze egy hagyományos vagy elektronikus postacímet tartalmaz, melyre a kért személyes adatokat meg kell küldeni. A jelentkező nem szerez tudomást arról, hogy pontosan hova, kinek küldi meg személyes – esetenként különleges – adatait, s arról sem, hogy az adatkezelő a továbbiakban a személyes adatokat milyen célra kívánja felhasználni. Az álláshirdetéseknek tartalmaznia kell a feladó személyének, valamint ha nem azonos vele a későbbi adatkezelő, akkor annak pontos megjelölését, azt az információs módot, formát, melyen keresztül az érintett tájékozódhat az adatkezelés céljáról, a személyes adatainak kezeléséről, illetőleg amelyen kérheti annak megszüntetését.

A munkahelykeresés további tipikus formája a munkaközvetítőkön keresztül történő álláskeresés. Ennek a magánkeretek között működő formája a magán-munkaközvetítői tevékenység, mely során a munkavállaló jóllehet ismeri a személyes adatait kezelő személyt, egzisztenciálisan kiszolgáltatott helyzete ugyanakkor nem változik, s ebből fakadóan olyan személyes adatokat is megad a munkaközvetítő számára, melyek kezelése sokszor cél nélküli. A beadványokból az is kitűnik, hogy egyes esetekben a magán-munkaközvetítő az érintett kifejezett kérelme ellenére sem szünteti meg a személyes

adatok kezelését, vagy olyan személyeknek is megküldi azokat – például külföldi munkáltatónak –, amelyhez az érintett nem járult hozzá, s melyről nincs tudomása.

A gyakorlat során a magán-munkaközvetítők az egyes konkrét állásokhoz szükséges adatoknál szélesebb adatkört kezelnek, arra való tekintettel, hogy az érintett adatait több munkáltatónak is megküldik. A magán-munkaközvetítők által az egyes konkrét munkaköröknél szükséges, tágabb kört átfogó adatkezelések – ha a személyes adatok kezelése a várható munkakörök tükrében ténylegesen indokolható – nem jogellenesek, nem tekintendők cél nélküli adatkezeléseknek. Ugyanakkor a kezelt személyes adatok a munkát kínáló személyeknek nem adhatók át teljes körűen, csak azok, melyek a konkrét munkaviszony kapcsán az alkalmasság megítéléséhez valóban szükségesek. A külföldre történő munkaközvetítés során az adattovábbítást végző személynek vizsgálnia kell azt, hogy az a harmadik ország, melynek területére a személyes adatokat továbbítják, biztosítja-e a megfelelő szintű védelmet a személyes adatok kezelése során. Amennyiben ilyen jellegű védelem nem biztosított, akkor a személyes adatok továbbítása csak akkor tekinthető jogszerűnek, ha az érintett a kifejezett hozzájárulását megadta. Amennyiben a tevékenység célja megvalósult – vagyis a munkaközvetítés sikeres volt –, illetőleg ha az érintett azt kéri, az adatkezelőnek a személyes adatok kezelését meg kell szüntetnie. Abban az esetben, ha a személyes adatokat a magán-munkaközvetítő abból a célból továbbra is kezelni kívánja, hogy a jövőben újabb állásajánlattal keresse meg a munkavállalót, azt csak akkor teheti meg jogszerűen, ha az adatkezeléshez az érintett személy hozzájárulását megadta. *(167/A/2006)*

A munkavállalók adatainak kezelésével foglalkozó másik ajánlás a sztrájk szervezésével kapcsolatos adatkezelést érintette. Több érdekképviseleti szervezet kért állásfoglalást abban a kérdésben, hogy az általuk szervezett sztrájk kezdete előtt a munkáltató a munkavállalóktól vagy tőlük megkérheti-e a sztrájkban résztvevők listáját. Általánosságban megállapítható, hogy a sztrájk szervezésével összefüggésben a személyes adatok átadása csak abban az esetben tekinthető jogszerűnek, ha az érintett ahhoz kifejezetten és önként – vagyis külső, jogkorlátozó ráhatástól mentesen – hozzájárult. Az adattovábbítás jogszerűségét utóbb az adatkezelőnek, vagyis a sztrájkot szervezőnek kell bizonyítania, ezért célszerű a hozzájárulást az érintettektől írásban megkérnie.

A sztrájkról szóló 1989. évi VII. törvény (továbbiakban: Sztv.) 6. § (3) bekezdése értelmében a sztrájk miatt kiesett munkaidőre – eltérő megállapodás hiányában – a dolgozót díjazás és a munkavégzés alapján járó egyéb juttatás nem illeti meg. Azt az adatot tehát, hogy ki vesz részt a sztrájkban, a munkáltató bérszámfejtés céljából – a bérszámfejtési határidő figyelembevételével – utólag jogosult kezelni. Nem igényelheti azonban előzetesen a munkáltató a sztrájkban részt vevő munkavállalók személyes adatait.

Az elégséges szolgáltatás nyújtása mint adatkezelési cél vizsgálatakor szükséges figyelembe venni azt a bírósági jogértelmezést, mely szerint a sztrájk jogellenességét önmagában a felek tárgyalásának az eredménytelensége nem alapozza meg. A sztrájk jogszerűségét, illetve jogellenességét kizárólag az Sztv. 3. §-a alapján kell elbírálni (BH 1991. 255.). Ez okból az elégséges szolgáltatás teljesítése céljából történő egyeztető eljárás során a szervező és a munkáltató rögzítheti a szükséges számszaki adatokat arra vonatkozóan, hogy az egyes munkaegységekben hány embernek kell dolgoznia. A munkavállalók név szerinti megnevezése azonban ehhez a célhoz nem szükséges.

A vállalat vagy üzem polgári jogi kötelezettségeivel kapcsolatban meg kell jegyezni, hogy a sztrájk miatti késedelembe esés nem jelenti az érintett munkáltató feltétlen felelősségét. Amennyiben bizonyítja, hogy a késedelem elhárítása érdekében úgy járt el, ahogy az adott helyzetben általában elvárható, nem tartozik kártérítéssel. *(381/H/2006)*

Az elmúlt években megjelenő, ez évben pedig egyre több beadvány tárgyát képező adatkezelési forma a dolgozó földrajzi helyzetének meghatározása GPS-eszközök, illetőleg a rendelkezésére bocsátott mobiltelefon cellainformációja által.

A munkáltató változó munkahely – így tipikusan gépjárművek – esetében, logisztikai célból kezelheti a gépjármű tartózkodási helyét, az ellenőrzés kivitelezésekor azonban vizsgálni kell, hogy az a szükségesség és arányosság követelményének megfelelő jogkorlátozást eredményez-e. Nem lehet tehát valamennyi változó munkahelyű munkavállalót GPS-szel vagy más nyomkövetővel nyomon követni, csak akkor, ha az a munkakörből fakadóan valóban szükséges, és az ellenőrzés más, enyhébb jogkorlátozást eredményező módon nem valósítható meg. A munkáltató ellenőrzési jogköre tehát nem lehet azonos a munkavállaló megfigyelésével. Az adatkezelés jogalapjának meglétén túl kiemelten kell vizsgálni azt, hogy a

> létrejövő adatkezelés megfelel-e a célhoz kötött adatkezelés követelményének. A célhoz kötöttség elvéből következik, hogy a *„készletre”*, előre nem meghatározott jövőbeni felhasználásra való adatgyűjtés és tárolás alkotmányellenes.
>
> A fentiekből következően a GPS-rendszer, illetőleg a mobiltelefon használatakor létrejövő cellainformációk használatának a jogosultsága mindig csak a konkrét eljárás részleteinek az érdemi vizsgálatakor állapítható meg. Munkaidőn kívüli időszakban a munkavállaló tartózkodási helyének esetleges nyomon követéséhez azonban a munkáltatónak sem törvényi jogalapja, sem megfelelő célja nincs, ezért az ilyen jellegű adatkezelés jogellenesnek minősül. *(68/A/2006, 559/A/2006, 1496/A/2006, 1664/A/2006, 1767/A/2006)*

A cellainformációkon alapuló *„flottakövető”* szolgáltatást valamennyi mobil távközlési szolgáltató biztosítja megfelelő feltételek megléte esetén. Általában elmondható, hogy a szolgáltatók felhívják a megrendelő figyelmét a jogszerű adatkezelés követelményeire, és azok megsértése akár a szolgáltatás megszüntetését is eredményezheti. Ennek jegyében különösen figyelemreméltó, hogy pont az egyik szolgáltató volt az, amelyik – állítólag tesztelési célból – kezelte és tárolta a dolgozók telefonjainak földrajzi helyzetére vonatkozó információkat. Az adatkezelés titokban történt, arra véletlenül derült fény egy, az érintettek és a társaság közötti munkaügyi per kapcsán. Az érintettek ezért a munkáltató-szolgáltató ellen személyiségi jogi pert indítottak, mely során a bíróság – a biztos állásfoglalásához hasonló tartalmú ítéletében – elmarasztalta a szolgáltatót. *(920/K/2006)*

Szintén az előző évek tendenciáját követve, a beadványok között kiemelkedően nagy számban fordult elő a munkahelyi kamerázás, a hagyományos és elektronikus levelezőrendszerek, a munkavállaló számára átadott számítógépen tárolt adatok, valamint a munkahelyi telefon használatának ellenőrzésével kapcsolatos vizsgálatok száma.

Egy egyetemen körlevelet küldtek körbe, melyben felhívták az egyetemi közösség figyelmét egy közelgő szoftverellenőrzésre. A körlevélhez csatoltak egy Excel táblázatot, amelyben a dolgozók nevéhez rendelve feltüntették az általuk használt összes, nem az egyetem által installált szoftvert. A levél a beadványozó értelmezése szerint azt sugallta, hogy a felsorolt programok *„kétes eredetűek”*, célja pedig az volt, hogy mindenki távolítsa el számítógépéről az illegálisan telepí-

tett programokat. A programlistán olyanok is szerepeltek, melyek a felhasználó vallásos vagy más világnézeti meggyőződésére („*Katolikus naptár*", „*Islamic screensaver*"), illetőleg szexuális szokásaira („*LiveSexCam*") engednek következtetni. Előfordult továbbá az is, hogy egyes dolgozók nevéhez olyan programokat rendeltek hozzá, melyeket nem ő, hanem a gépet előzőleg használó munkavállaló installált. A nyilvánosságra hozott listán nem szerepelt az egyetem felső vezetősége, illetve a számítástechnikai osztály dolgozója számítógépére telepített programok listája. A tájékoztató szerint azért, mert ezeken a számítógépeken nincsenek „*kétes eredetű programok*".

> Az adatvédelmi biztos állásfoglalása szerint a körlevél beadványban ismertetett módon történő továbbítása büntető szankcióként is értelmezhető, melyhez azonban a munkáltató nem rendelkezik jogalappal. Abban az esetben ugyanis, ha a munkáltató olyan körülményt észlel, amely a munkavállaló szabályellenes magatartását támasztja alá, a dolgozóhoz kell fordulnia, a kérdést vele kell rendeznie, de nem állíthatja őt nyilvános pellengérre. Ha a munkavállaló szabályellenes magatartása bebizonyosodik, akkor a munkáltatónak joga van a munkaviszonyra irányadó jogszabályokban ismertetett szankciókat alkalmazni, ezeket azonban olyan módon köteles megtenni, amely nem sérti az érintett személyiségi jogait. *(866/A/2006)*

Egy munkáltató a munkahelyről írt e-mailek megismerhetőségével kapcsolatosan azzal a kérdéssel fordult a biztoshoz, hogy ha az ilyen tárgyú hivatalos leveleket a munkáltató megismeri, azzal sérülnek-e a levél címzettjének a személyiségi jogai. A címzett személy ugyanis nem feltétlenül van tisztában azzal a ténnyel, hogy a levélben szereplő, vele kapcsolatos személyes adatokat harmadik személy megismerheti.

> Két fél közötti jogviszonnyal kapcsolatos adatokat – jogaik érvényesítése végett – a felek jogosultak megismerni. Ebből fakadóan, a munkáltató megbízásából, a munkavállaló által hivatalos ügyekben írt és fogadott elektronikus levelek tartalmát a munkáltató jogosult megismerni, az ilyen jellegű levelekbe betekinteni. E jogosultságának érvényesítése mellett azonban biztosítania kell a levelezésben érintett harmadik személy azon jogát is, hogy az adatkezelés rész-

leteiről tájékoztatást kapjon. Jóllehet az ilyen jellegű tájékoztatásnak a hazai joggyakorlatban még nincs elfogadott formája, ugyanakkor az adatvédelmi biztos felhívta figyelmet arra a lehetséges megoldásra, miszerint a címzett részére küldött levél alján, annak mellékleteként egy tájékoztatót helyezzenek el. *(1393/K/2006)*

A személyi jövedelemadóról szóló 1995. évi CXVII. törvény (továbbiakban: Szja tv.) 2006. szeptember 1-jétől hatályos 69 § (1) bekezdésének mb) pontja, valamint (12) bekezdése értelmében természetbeni juttatásként adóköteles a munkahelyi telefonok magáncélú használata. Az új rendelkezés hatálybalépése után számos munkáltató fordult a biztoshoz, és arról kért állásfoglalást, hogy az adózási kötelezettség teljesítése során milyen formában kezelhetik a munkavállalók telefonhívásainak adatait.

A munkáltató a munkavállalók részére átadott telefonon lefolytatott magáncélú telefonhívásokat mint természetbeni juttatást adhatja a munkavállalók számára, de a magáncélú hívások költségeinek megtérítését is kérheti.

Ha a munkáltató az egyes konkrét munkavállalók magáncélú telefonhívásainak a költségeit nem tudja meghatározni, akkor a Pénzügyminisztérium honlapján közzétett, az Adó- és Pénzügyi Ellenőrzési Hivatallal együtt megadott, a cégtelefonok magáncélú használatával összefüggő adókötelezettségről szóló tájékoztató (továbbiakban: tájékoztató) értelmében azt 20 %-ban állapíthatja meg. Ebben az esetben azonban, tekintettel arra, hogy a magán-, illetőleg a hivatalos hívások adatai a telefonhívások listáján nem választhatók külön – melyet maga a tájékoztató is jogszerű követelményként szab meg – a hívások adatai a telefonhívások listázásával nem kezelhetők. A munkáltató tehát csak a telefonköltségek adatait kezelheti, és az esetleges adóügyi ellenőrzés során azt köteles az ellenőrzést lefolytató személy részére átadni. A tájékoztatóban megjelölt, 20%-nál alacsonyabb magánhasználat is megállapítható, azonban az ezt igazoló dokumentumokat olyan formán köteles a munkáltató nyilvántartani, amely megfelel az Art., illetőleg az Avtv. rendelkezéseinek is.

Az Avtv. rendelkezéseiből fakadóan, a munkáltató az adózási kötelezettségeinek teljesítése céljából ebben az esetben sem kezelheti a magánjellegű telefonhívások adatait, ezért az ellenőrzés során csak azt rögzítheti, hogy a magán-, illetőleg a hivatalos hívások milyen

költséget eredményeztek. Ezt egyrészt úgy tudja megoldani, ha a magán-, illetőleg a hivatalos hívásokat külön kóddal látja el. A hivatalos kódú hívásokat jogosult kezelni, a magán jellegű hívások adataiból azonban csak a költségekkel kapcsolatos adatokat kezelheti. Az Art. rendelkezéseiből fakadóan a munkáltató az adóügyi ellenőrzést végző személynek a hivatalos hívások adatait tartalmazó listát, illetőleg a magánjellegű hívások összegét tartalmazó dokumentumokat adhatja át.

Azokon a munkahelyeken, ahol a kódolás nem megoldható, elfogadható az a gyakorlat, miszerint a munkavállaló által használt telefon híváslistáját lezárt borítékban adják át – azt előzetesen a munkáltató nem kezelheti –, és a magánhívások telefonszámait a munkavállaló olyan formában törli, hogy azokat a későbbiekben ne lehessen azonosítani, a költségek azonban megállapíthatók. További lehetséges megoldás lehet a telefon-tükörkönyv vezetése, vagyis amikor a munkavállaló számára a munkáltató előírja, hogy a telefonhasználat részleteit, így azt, hogy mikor, milyen célból kezdeményezett hívásokat, egy erre rendszeresített nyomtatványon vezesse.

Amennyiben a munkáltató a magáncélú használat ellenértékét – vélelmezett értékét – megtérítteti a munkavállalóval, nem kell közterheket fizetnie. Ebben az esetben a munkáltató nemcsak a közterhek megfizetése alól mentesül, de az azzal kapcsolatos adatkezelésektől is, vagyis az Szja tv. rendelkezéseinek betartása céljából nem lehet a munkavállalók telefonhasználatával kapcsolatos adataikat kezelni, és azt harmadik személynek továbbítani. *(1672/K/2006)*

Több munkavállaló, érdekképviseleti szervezet fordult a biztoshoz amiatt, hogy a munkáltató postai küldemény formájában küldi meg a munkavállalók részére a munkabér-elszámolást. Az egyik beadvány szerint a munkavállalók jogos érdeke az, hogy a munkabér elszámolására vonatkozó adatokat csak és kizárólag maguk ismerhessék meg, ezt az érdeket azonban a postai küldemény formájában megküldött bérelszámolás – mivel az abban szereplő adatokat az érintett akarata ellenére családtagja, illetőleg egyéb harmadik személy is megismerheti – sértheti.

Az Avtv. 10. §-ában foglalt adatbiztonsági követelményből következik az, hogy a postai küldeményt olyan megjelöléssel kell ellátnia a feladónak, melynek következtében a címzett azt bizonyosan megkapja. Az, hogy az érintett munkavállaló nevére megküldött postai

> küldeményt más személy – így családtagjai – felbontják, nem a munkáltató adatkezelésének megítélése kérdéskörébe tartozik. Amennyiben egy harmadik személy az érintett munkavállaló hozzájárulása nélkül bontja fel a nevére érkező postai küldeményt, akkor azzal a személyiségi jogait, így mindenekelőtt a levéltitokhoz való jogát sérti meg. *(352/A/2006)*

A köz- és a magánszférában dolgozók helyzetét összehasonlítva, a beadványok alapján továbbra is megállapítható, hogy az utóbbi körbe tartozókat – az irányadó jogszabályi háttér hiányossága miatt – adataik kezelése kapcsán továbbra is nagyobb számú jogsérelem éri. Ugyanakkor ez évben is érkeznek olyan beadványok, melyek a közszférában dolgozó munkavállalókat érintő jelentős súlyú jogsérelmekről számoltak be.

Egy önkormányzatnál a választásokat követően teljes képviselő-testületi váltás történt. Az új testület valamennyi tagja egyben egy helyi egyesület tagja is. Az újonnan megválasztott alpolgármester a képviselő-testület nevében a helyi önkormányzat valamennyi dolgozó munkaköri leírását, önkormányzati munkaviszonyának kezdő időpontját, bruttó munkabérét megkérte írásban, mely adattovábbítás meg is történt. Az átadott adatokat a beadványozó tudomása szerint az egyesület valamennyi tagja megkapta.

> A képviselő-testület, az alpolgármester, valamint az az egyesület, amelynek a képviselők tagjai, az Avtv. rendelkezéseinek értelmében harmadik személyeknek minősülnek, ezért részükre személyes adat csak akkor továbbítható, ha ilyen irányú törvényi felhatalmazás lehetővé teszi. A köztisztviselők jogállásáról szóló 1992. évi XXIII. törvény rendelkezései értelmében a helyi önkormányzat alpolgármestere – illetőleg képviselő-testülete – nem jogosult a képviselő-testület hivatalánál foglalkoztatott köztisztviselők személyes adatainak a megkérésére, valamint annak továbbítására harmadik személyek részére. Az ilyen adatkéréseket az adatkezelőnek – vagyis a jegyzőnek – meg kell tagadnia. *(1618/A/2006)*

Oktatásügy

Az oktatásügyben működő adatkezelők sokszínű képet mutatnak: ide tartoznak az óvodák, iskolák és a felsőoktatási intézmények

is; adatgyűjtés, és -tárolás, nyilvánosságra hozatal és adatbiztonsági kérdések egyaránt felmerülnek. Sajnálatos, hogy a mai napig találunk olykor-olykor olyan adatkezelőt, akinek csak igen csekély ismerete van az adatvédelem alapjairól, és a biztosi vizsgálat kapcsán csodálkozik rá ezekre a szabályokra; mások pedig ismervén ugyan az alapelveket, abból gyakran életszerűtlen következtetéseket vonnak le.

> A fentiekre példaként hozhatók azok az indítványok, melyekben tanárok teszik fel a kérdést a biztosnak, hogy vajon igaz-e, hogy *„megtiltotta"* a dolgozatok otthoni javítását. Természetesen a biztos ilyen állásfoglalást nem adott ki, azonban az indítványozók figyelmét felhívta arra, hogy speciális szabály hiányában az adatvédelem általános szabályai szerint kötelesek az adathordozók (dolgozatfüzetek) kezelésében eljárni. Eszerint az abban szereplő adatokat illetéktelen személy számára nem továbbíthatják, nem tehetik lehetővé annak megismerését és természetesen nyilvánosságra sem hozhatják. Ez azonban nem jelenti egyúttal azt is, hogy a tanárnak kötelező lenne a dolgozatokat az iskolában javítania. *(138/K/2006, 1508/Z/2006)*

Az oktatási intézmények sem maradnak el a kamerás megfigyelés terén más adatkezelőktől, azonban kellő megfontoltság is mutatkozik e rendszer kezelésében.

> Erről tett tanúbizonyságot a Debreceni Egyetem Orvos- és Egészségtudományi Centrum Általános Orvostudományi Kar Anatómiai Intézete, melyet az a nagy port felvert vád ért, hogy a hallgatók oktatási időn kívül oda bejárva emberi szerveket hoznak ki a boncteremből. Ennek visszaszorítása és felderíthetősége érdekében az egyetem kamerás megfigyelőrendszert kívánt telepíteni a boncterembe, és erről kérte ki a biztos véleményét.
>
> A biztos kifejtette, hogy személyes adat – törvényi felhatalmazás hiányában – csak akkor kezelhető, ha az érintett ahhoz önkéntes és tájékozott beleegyezését adta. Az érintettek hozzájárulása beszerezhető oly módon is, hogy a belső szabályzatban, illetőleg a boncterem bejáratánál, jól látható helyen elhelyezik a munkaidőn kívül történő képrögzítésről szóló tájékoztatást. A tájékoztatáson meg kell jelölni az adatkezelés pontos célját, azt, hogy mely időszakban történik képrögzítés, ki az adatkezelő, vagyis ki jogosult a rögzített képfelvételek megtekintésére, mely esetekben ellenőrzik a felvétele-

ket, és meddig kezelik azokat. A videofelvételeket csak akkor lehet felhasználni, ha azt meghatározott törvényes cél szükségessé teszi. Szükséges továbbá azokat a személyeket is megjelölni, akik az utólagos ellenőrzést elvégezhetik. *(585/K/2006)*

Egy budapesti gimnázium a nagy értékű számítástechnikai berendezések lopása ellen úgy kíván védekezni, hogy a terem plafonjára erősített (távirányítással kezelhető) gépeket figyeli csak a kamera, a teremben tartózkodókat nem, és csak az a személy jelenik meg a kamera látóterében, aki jogellenesen közelít a kamera felé. *(1124/K/2006)*

A különböző felmérésekkel és adatgyűjtésekkel szemben több szülő is emelt kifogást, mivel általában az iskolától nem kaptak megfelelő tájékoztatást az adatkezelés céljáról és módjáról.

Ilyen volt a SuliNova Kht. felmérése is, mely szerint egy új és korszerű intelligenciavizsgálat adaptálása kezdődött. A rendszer alkalmas lesz a magyar gyermekek értelmi képességeinek objektív felmérésére. E felmérés előkészítéséhez a SuliNova Kht. témavezetője és programvezetője a jegyzőtől a 6-16 éves korú gyermekek adatait (nevét és elérhetőségét) kérte.

Mivel cselekvőképtelen, illetve korlátozottan cselekvőképes személyek adatairól van szó, az adatkezelést nem törvény rendeli el, és csak távoli összefüggésben van szó közoktatási célról, a biztos felhívta az Oktatási Minisztérium helyettes államtitkárának figyelmét arra, hogy az érintettek előzetes tájékoztatásától ebben az esetben sem lehet eltekinteni. *(688/K/2006, 712/A/2006)*

Egy pécsi gyakorló iskola igazgatója kérte a biztos állásfoglalását az iskolában végzendő szociometriai felméréshez.

A biztos tájékoztatta az indítványozót, hogy – immáron évtizedes – gyakorlata szerint azt tartja elfogadhatónak, ha az adatfelvételben és annak kiértékelésében az iskola tanárai nem vesznek részt. Az adatkezelésnek és az adatok kiértékelésének célja a nevelő munka hatékonyabbá tétele, így e célból az adatvédelmi törvény célhoz kötöttségi követelményét figyelembe véve nem indokolt, hogy az egyedi adatokat a tantestület tagjai megismerjék. A felmérés elvégzéséhez szükséges olyan adatkezelési szabályzat kialakítása is, mely tartalmazza az adatkezelés folyamatát, az érintett jogai gyakorlati

érvényesíthetőségének biztosítékait, valamint az adatvédelmet biztosító technikai és szervezési intézkedéseket. *(204/K/2006)*

Ide tartozónak tekinthetjük a felsőoktatásról szóló 2005. évi CXXXIX. törvény előírása alapján az intézmények pályakövetési kötelezettségét is. Az ebben való részvételhez kért állásfoglalást egy egyetem rektor-helyettese, mert a rendszer indulásakor szükséges személyes adatokra vonatkozóan még nincs meg az érintettek hozzájárulása, mivel a felmérésben a korábban végzett hallgatók vesznek részt. A hallgatói nyilvántartási rendszerben szereplőknek azonban – a célhoz kötött adatkezelés követelményének megfelelően – nem lehet erre vonatkozóan személyre szóló levet küldeni, azonban annak nincs akadálya, hogy a rendszeren keresztül körlevélben hívják fel a hallgatók figyelmét a felmérésben való részvétel lehetőségére. *(1868/K/2006)*

Az oktatásban résztvevők – tanárok, tanulók – adatainak a világhálón való közzétételével kapcsolatosan is érkezett indítvány a biztoshoz.

Egy középiskola igazgatója indítványában azt kérdezte, hogy az oktatóknak és a tanulóknak milyen adatai hozhatók nyilvánosságra. A biztos tájékoztatta az igazgatót arról, hogy a tanárok adatainak nyilvánosságára vonatkozóan a közalkalmazottak jogállásáról szóló 1992. évi XXXIII. törvény 83/B. § (2) bekezdését kell alkalmazni, mely szerint a közalkalmazotti alapnyilvántartás adatai közül a munkáltató megnevezése, a közalkalmazott neve, továbbá a besorolására vonatkozó adat közérdekű, ezeket az adatokat a közalkalmazott előzetes tudta és beleegyezése nélkül nyilvánosságra lehet hozni. A tanulók adatainak nyilvánosságra hozatalára nincs törvényi felhatalmazás, és annak nincs törvényes célja sem, ezért azt kizárólag az érintettek megfelelő tájékoztatáson alapuló, önkéntes és határozott beleegyezése alapján lehet megtenni. *(577/K/2006)*

Szintén honlapon való közzététel ügyében fordult a biztoshoz egy egyetem, mert a hallgatók tudományos dolgozatait, illetve tudományos tevékenységgel folytatott adataikat kívánnák nyilvánosságra hozni.

A biztos válaszában kifejtette, hogy ezt csak az érintett hozzájárulásával lehet megtenni. A hozzájárulás az érintett kívánságának

olyan önkéntes és határozott kinyilvánítása, amely megfelelő tájékoztatáson alapul, és amellyel félreérthetetlen beleegyezését adja a rá vonatkozó személyes adatok – teljes körű vagy egyes műveletekre kiterjedő – kezeléséhez. A hallgatókat tehát hozzájárulásuk megadása előtt adekvát módon fel kell világosítani az adatkezelés céljáról, különös tekintettel arra, hogy a nyilvánosságra hozott adatok tekintetében az önrendelkezésből fakadó jogait érdemben nem tudja gyakorolni.

Mindezeken túl lehetőséget kell a hallgatónak biztosítani arra, hogy adatainak és dolgozatainak nyilvánosságra hozatalához külön-külön járulhasson hozzá, mivel a két csoport nem szükségszerűen kapcsolódik össze, így azok kezelésének egy hozzájárulásba foglalása nem fér össze az információs önrendelkezési jog alapelveivel. *(1534/K/2006)*

Immár évek óta folyik a vizsgálat a győri Szent István Egyetem adatkezelési gyakorlatának ügyében. A 2004 óta folyó vizsgálatban az egyetem és az érintett egyetemi kollégium vezetői minimális együttműködési hajlamot sem mutatnak (például hónapok elteltével válaszolnak csak a megkeresésekre), így a vizsgálatot még mindig nem sikerült lezárni.

Az egyetem egyik kollégiumában ujjlenyomat-vizsgáló beléptetőrendszert vezettek be, majd azóta már a kollégium parkolóját, portáit, folyosóit és lépcsőfordulóit is kamerás megfigyelő-rendszerrel szerelték fel. Az ujjlenyomat-vizsgáló rendszerrel kapcsolatos biztosi álláspont szerint – melynek értelmében az adatminimalizálás követelményét figyelembe véve a már meglévő adatok alapján a hallgató azonosítható – az arckép, kártyaszám és Neptun-kód mellé nem szükséges a belépéshez még az ujjlenyomat öt azonosító pontjának kezelése is. A rektor a beléptetési rendszert az adatvédelmi elveknek megfelelően átalakíttatta. *(378/A/2004, 1736/A/2006)*

A kamerás megfigyelés ügyében a vizsgálat még tart. *(814/A/2006)*

Távközlési szervezetek

A távközlési szektor adatkezelését érintő panaszok száma a korábbi évekhez viszonyítva csökkent. A személyazonosító igazolványok másolásával összefüggő biztosi állásfoglalás és a tavalyi évben lezárult átfogó vizsgálat eredményének tekinthető, hogy a korábbi évek visz-

szatérő ügycsoportját képező igazolványmásolásokkal kapcsolatos panaszok száma csökkenő tendenciát mutat. Továbbra is jellemző ügycsoportot képeznek a szerződéskötéssel, valamint a telefonos zaklató hívásokkal kapcsolatos panaszok.

Évről évre visszatérő problémát jeleznek azok az állampolgároktól, bíróságoktól, nyomozó hatóságoktól érkező kérdések, amelyek az eljárás lefolytatását és a tényállás felderítését elősegítő forgalmi adatok továbbításának jogi lehetőségét kutatják. Az elektronikus hírközlésről szóló 2003. évi C. törvény (továbbiakban Eht.) 157. §-a igen szigorúan szabályozza a forgalmi és számlázási adatok kezelésének rendjét, érvényre juttatva azt a jogalkotói szándékot, amely a hírközlési rendszer használata során keletkezett adatokat magas szintű védelemben kívánja részesíteni.

> E szakasz (6) bekezdés c) pontja szerint a forgalmi és számlázási adatok átadhatók a nemzetbiztonság, a honvédelem és a közbiztonság védelme, a közvádas bűncselekmények, valamint az elektronikus hírközlési rendszer jogosulatlan vagy jogsértő felhasználásának üldözése céljából az arra hatáskörrel rendelkező nemzetbiztonsági szerveknek, nyomozó hatóságoknak, az ügyésznek, valamint a bíróságnak. Ennek az adatszolgáltatásnak a biztosítása céljából a törvény 157. § (8) bekezdése alapján három évig köteles a szolgáltató az adatokat megőrizni.

A fentiek alapján, a biztos megállapította, hogy a veszélyes fenyegetés szabálysértés esetén a vonatkozó törvényi rendelkezések nem adnak lehetőséget arra, hogy az eljáró bíróság számára adatot szolgáltassanak.

> Az elmúlt években mind a sérelmet szenvedett állampolgárok, mind bírák, bírósági vezetők számos esetben jelezték azt, hogy az elkövető kilétének megállapítása, illetve a bizonyítás nem lehetséges akkor, ha a fenyegetés telefonon keresztül történik, ugyanis az Eht. alapján nem adhatók át a hívó fél adatai bíróságnak; ezt a korábbi jogi szabályozás sem tette lehetővé. Ilyenkor a bíróság csak akkor tud eljárni, ha a feljelentő ismeri (pl. hang, vagy kijelzett hívószám alapján) az elkövetőt, és ezt bizonyítani is tudja. *(1794/K/2006)*

A jelzett probléma feloldása érdekében a biztos jelezte az igazságügyi és rendészeti miniszternek, hogy adatvédelmi szempontból nem lenne aggályos a vonatkozó törvények módosításával az adatszolgáltatás lehetővé tétele.

A törvényi rendelkezések értelmében a nyomozó hatóság sem jogosult az előfizetői adatok megismerésére, ha a nyomozás az emberi méltóságot és a becsületet sértő cselekmény üldözése céljából történik, és a cselekmény elkövetési módja az elektronikus hírközlő hálózat felhasználása. Erre tekintettel az internetszolgáltató a becsületsértés miatt indított büntetőeljárásban nem adhatja ki jogszerűen az előfizetői adatokat, mert az eljárás magánvádas bűncselekmény miatt van folyamatban.

> A becsületsértés miatt folyamatban lévő büntetőeljárásban a nyomozó hatóság fordult a biztoshoz konzultációs beadvánnyal, mert az ügyben érintett hírközlési szolgáltató megtagadta a jogsértő tartalmat az internetes oldalon közzétevő felhasználó előfizetői adatainak kiadását. Az Eht. 157. § (6) bekezdés c) pontja alatt úgy rendelkezik, hogy az elektronikus hírközlési szolgáltató az előfizetői adatokat csak közvádas bűncselekmények esetén az arra hatáskörrel rendelkező nemzetbiztonsági szerveknek, nyomozó hatóságoknak, az ügyésznek, valamint a bíróságnak adhatja át. A Be. 52. § (1) bekezdése alapján a könnyű testi sértés, a magántitok megsértése, a levéltitok megsértése, a rágalmazás, becsületsértés és kegyeletsértés esetén a vádat mint magánvádló a sértett képviseli, feltéve, hogy az elkövető magánindítványra büntethető. *(1719/K/2006)*

A hírközlési szolgáltató forgalmi és számlázási adatok továbbítására vonatkozó beadványára a biztos elmondta, hogy három éven túl azok a forgalmi és számlázási adatok, amelyeket törvényes jogcímen (például számviteli törvény) kezel a hírközlési szolgáltató, büntetőügyben eljáró bíróságnak a Be. 71. §-a, polgári ügyben eljáró bíróságnak a Pp. 163. § (1) bekezdés és a 164. § (2) bekezdés alapján jogszerűen továbbíthatók.

> A biztos állásfoglalásában kifejtette, hogy három éven túl a hírközlési szolgáltatónak az Eht. 157. § (6) bekezdésének c) pontjában definiált adatkezelési célja megszűnik, és ezzel együtt a forgalmi és számlázási adatok további kezelésének a jogalapja is. Az Avtv. 14. §

(2) bekezdés d) pontja szerint személyes adatot törölni kell, ha az adatkezelés célja megszűnt, vagy az adatok tárolásának törvényben meghatározott határideje lejárt. Ez a hírközlési szolgáltató gyakorlatában annyit jelent, hogy a törvényben előírt adatkezelési időtartam elteltét követően a hívásrekordokat tartalmazó adatbázisból az Eht. 157. § (6) bekezdés c) pontjára hivatkozva adatszolgáltatás nem teljesíthető.

Azonban nem ez az egyetlen jogszabályi felhatalmazás, melynek alapján a szolgáltató forgalmi és számlázási adatot kezel. Az elektronikus hírközlési szolgáltató által kiállított számla az általános forgalmi adóról szóló 1992. évi LXXIV. törvény 13. § (1) bekezdés 16-17. pontja szerint tartalmazza például a vevő nevét, címét, a teljesítés időpontját, a termék (szolgáltatás) megnevezését, valamint besorolási számát, a termék (szolgáltatás) mennyiségi egységét és mennyiségét. Az Eht. 142. § (1)-(2) bekezdése, és a 16/2003. (XII. 27.) IHM rendelet 15. §-a lehetővé teszi a helyi, helyközi, belföldi távolsági és nemzetközi hívások díjainak, valamint a mobil rádiótelefon-hálózatokban végződtetett hívások díjainak elkülönített feltüntetését. Az előfizető kérésére kiállított hívásrészletező tartalmazza a hívott számot, a hívás kezdő időpontját és a hívás időtartamát is. Ezt a számlát mint a könyvviteli elszámolást alátámasztó számviteli bizonylatot a szolgáltató a számvitelről szóló 2000. évi C. törvény 169. § (2) bekezdése alapján legalább nyolc évig köteles megőrizni.

Az ÁFA törvény és az ágazati szabály szerint kiállított tételes számla, illetve hívásrészletező tartalmaz tehát olyan adatot, amely forgalmi és számlázási adat.

A forgalmi és számlázási adat több jogcímen továbbítható a bíróságnak. A Be. általános jelleggel hatalmazza fel a büntető ügyben eljáró bíróságot az adatkérésre, polgári peres eljárásban bonyolultabb a helyzet megítélése.

A Pp. a bizonyítási eljárás során a felek rendelkezési elvét helyezi előtérbe. Ez azt jelenti, hogy a bíróság hivatalból bizonyítást csak törvényben meghatározott esetekben rendel el. Ezt a néhány törvényes kivételt leszámítva a polgári perben a bíróság bizonyítékok megszerzése érdekében nem jogosult megkeresni az érintett hírközlési szolgáltatót, mert a bizonyítás a feleket terheli; esetleges bírósági megkeresés esetén pedig a szolgáltatónak meg kell tagadnia az adatszolgáltatást. *(987/K/2006, 1470/A/2006)*

A forgalmi és számlázási adatok szigorú kezelésének rendjét tükrözi, hogy a hívó fél előfizetői száma még a hívott előfizető számára sem ismerhető meg korlátlanul. A hívó előfizetői számot a szolgáltató a számlázás és a kapcsolódó díjak beszedése, az előfizetői szerződések figyelemmel kísérése céljából a törvényi rendelkezésnek megfelelően 2 év 30 napig őrzi, és csak a törvényben meghatározott esetekben továbbíthatja az adatkezelésre jogosult szerveknek. Ennek értelmében az előfizető csak az általa hívott számok listáját ismerheti meg (hívásrészletező), és tájékoztatást ezekről kérhet.

Az Eht. 157. §-ának szigorú adatvédelmi előírásai miatt a hívott előfizető a telefonjára érkezett hívószámok listáját csak a hívó felek hozzájárulása alapján kaphatja meg tekintettel arra, hogy ezek a hívó fél személyes adatainak minősülnek. Ugyanezen okból tilthatják meg az előfizetők eseti vagy állandó jelleggel, hogy számukat a hívott készülék kijelezze. *(147/A/2006, 783/A/2006, 1071/A/2006, 1206/A/2006, 1470/A/2006)*

A biztos a 2006-os évben több olyan panaszbeadvánnyal foglalkozott, amelyeknek tárgya az volt, hogy milyen jogi feltételek mellett ismerhető meg vagy válhat hozzáférhetővé a szöveges üzenetek (SMS) tartalma az előfizető vagy az előfizetőn kívüli személy számára.

Egyes beadványok arról számolnak be, hogy a hírközlési szolgáltató egy adott hívószámra érkezett, illetve a hívószámról indított szöveges üzenetek tartalmát kilistázta, és illetéktelen személynek – ellenszolgáltatásért cserébe – átadta. A vizsgálat során a szolgáltató jogellenes adatkezelése nem volt megállapítható. *(429/A/2006, 1204/A/2006)*

Egy előfizető azért fordult az adatvédelmi biztoshoz, mert a mobilszolgáltatója megtagadta az előfizetői hívószámára egy meghatározott hívószámról érkezett szöveges üzenet tartalmának kinyomtatását. Jogi megközelítésben lényeges különbséget kell tennünk az SMS tartalmának (az SMS szövege), valamint az elküldés körülményeinek (időpont, küldő telefonszáma, cellainformációk stb.) az adatvédelmi megítélése között. Az Eht. 155. § (3) bekezdése értelmében *„a szolgáltató a továbbított közlések tartalmát csak olyan mértékben ismerheti meg és tárolhatja, amely a szolgáltatás nyújtásához műszakilag elen-*

gedhetetlenül szükséges". A hivatkozott jogszabályhely alapján tehát magának a közlésnek a tárolására csak addig van lehetőség, amíg az a szolgáltatás teljesítéséhez szükséges. Ezt követően a továbbított üzenetet minden rendszerből törölni kell.

> Az ügyben érintett hírközlési szolgáltató a megkeresésre adott válaszlevelében elmondta, hogy az üzenetközpont működése nem teszi lehetővé, hogy a feladott üzenetek tartalmi részéhez bárki hozzáférjen. A konkrét előfizetői kártyára érkező és arról küldött üzenetek még kódolt formában sem állnak összegyűjtve rendelkezésre egyetlen berendezésen sem, tehát semmilyen módon nem készíthető azok tartalmáról lista. Az üzenet tartalmi része a kódolt továbbítás miatt nem hozzáférhető más hálózati rendszerekben, azt a kézbesítés után a fogadó fél mobil készülékén lehet elolvasni. A biztos megállapította, hogy jogszerűen járt el a hírközlési szolgáltató, amikor a szöveges üzenet elküldését és kézbesítését követően megtagadta a szöveges üzenet kinyomtatását és kiadását az érintett előfizetőnek. *(1263/A/2006)*

Az SMS szövegének a tárolásához képest eltérő jogi megítélés alá esnek az SMS szolgáltatás küldésének és díjazásának a körülményei (hívásrekordok), ugyanis az Eht. 157. §-a alatt található rendelkezés értelmében a szolgáltatók a küldés időpontját, a hívó és a hívott előfizetői számokat stb. az SMS díjazása, a díjak beszedése és az előfizetői szerződés figyelemmel kísérése céljából a törvényben előírt ideig tárolják.

A hazai szabályozás összhangban van az Európai Parlament és Tanács 2002/58/EK irányelvével, melynek 5. cikke rögzíti a közlések bizalmasságának elvét. Eszerint a tagállamoknak a nemzeti szabályozásukban biztosítaniuk kell a nyilvános hírközlő hálózatok és a nyilvánosan elérhető elektronikus hírközlési szolgáltatások segítségével történő közlések és az azokra vonatkozó forgalmi adatok titkosságát. Kivételt képeznek azok a tagállami jogszabályi intézkedések, amelyek olyan korlátozásokat jelentenek, amelyek egy demokratikus társadalomban a nemzetbiztonság, a nemzetvédelem, a közbiztonság védelme érdekében, valamint a bűncselekmények, illetve az elektronikus hírközlési rendszer jogosulatlan használatának megelőzése, kivizsgálása, felderítése és üldözése érdekében szükségesek és arányosak.

A terrorizmus és a szervezett bűnözés elleni küzdelmet célzó európai kezdeményezések keretében 2006. március 15-én elfogadott irányelv célkitűzése, hogy a szolgáltatóknak az egyes forgalmi adatok megőrzésére vonatkozó kötelezettségeit harmonizálja, valamint biztosítsa azt, hogy ezen adatok az egyes tagállamok nemzeti joga által meghatározott súlyos bűncselekmények kivizsgálása, felderítése, üldözése céljából rendelkezésre álljanak. Az irányelv tehát a forgalmi adatok megőrzése vonatkozásában tagállami jogszabályi harmonizációra törekszik, mert az adatok megőrzését előíró nemzeti rendelkezések közötti jogi és technikai különbségek vannak.

Az irányelv azonban csak a hírközlés vagy a hírközlési szolgáltatás során keletkezett vagy feldolgozott forgalmi és helymeghatározó adatokra vonatkozik, és nem az olyan adatokra, amelyek a közölt információ tartalmát képezik. A megőrzés idejére vonatkozó tagállami szabályozás 6 hónaptól 2 évig terjedhet, ennek elteltével az adatokat szigorúan törölni kell. A tagállamok adatvédelmi biztosaiból álló munkacsoport véleményében arra helyezte a hangsúlyt, hogy az adatkezelés feltételeit pontosan kell meghatározni, és az nem eredményezhet nagymértékű adatbányászatot.

A biztos egy ügy kapcsán megállapította, hogy egyik jogszabály sem kötelezi az előfizetőt arra, hogy a számhordozás és a szolgáltatóváltás körülményeiről és indokairól az átadó szolgáltatóját tájékoztassa. Ennek értelmében az előfizető erre nem köteles, azonban semmi akadálya nincs annak, hogy véleményét a szolgáltatójával közölje. Az átadó szolgáltató a szolgáltatások minőségének javítása céljából készíthet ilyen jellegű felmérést, azonban a számhordozást kezdeményező előfizetőt nem kényszerítheti ilyen nyilatkozatra, és a számhordozás lebonyolítása sem tehető függővé ettől a nyilatkozattól.

> Az Eht. 150. §-a a hírközlési szektorban a verseny szabadsága érdekében lehetővé teszi az előfizető számára azt, hogy úgy válthasson egyik szolgáltatóról a másik szolgáltatóra, hogy előfizetői hívószámát megtarthassa. A számhordozás részletes szabályait a 46/2004. (III. 18.) kormányrendelet tartalmazza. A számhordozás megtagadására a kormányrendelet 5. § (9) bekezdésében foglalt esetekben kerülhet sor.
>
> A hozzájáruló nyilatkozat megtételére az előfizető jogosult, mert az információs önrendelkezési jog őt illeti meg a saját személyes ada-

tai tekintetében. Ezt az alkotmányos alapjogot nem gyakorolhatja helyette a hírközlési szolgáltató alkalmazottja, ezért a nyilatkozat megtételét sem vállalhatja át az előfizető helyett. A nyomtatvány hozzájáruló nyilatkozata az előfizető előzetes megkérdezése nélkül, az előfizető kifejezett, egyértelmű és önkéntes nyilatkozata nélkül nem érvényes. *(1286/A/2006)*

A korábbi évekhez hasonlatosan érkeztek beadványok a cellainformációkkal összefüggő adatkezelések tárgyában is. A mobil távközlési szolgáltatók a szolgáltatás nyújtása során kezelik a cellainformációkat, mely lehetőséget ad a SIM-kártya földrajzi helyzetének meghatározására. A meghatározás pontossága a kártya helyzetétől függ, néhány métertől néhány kilométerig terjedhet. Több esetben kérték a biztos állásfoglalását (szolgáltatók, munkáltatók, munkavállalók) arra vonatkozóan, hogy a cellainformáció felhasználható-e arra, hogy ezáltal a munkáltató a munkavállaló helyzetét meghatározza. A biztos állásfoglalásában meghatározta azokat a garanciákat, amelyek mentén az úgynevezett flottakövető szolgáltatást a munkáltató igénybe veheti a távközlési szolgáltatótól. Az állásfoglalások részletes ismertetése a munkáltatók adatkezeléséről szóló fejezetrészben található.

Internet

Az elmúlt évben az előző évekhez képest az internetet érintő beadványok számának növekedése lelassult. Azonban a panaszok száma így is magas, és ennek továbbra is elég jelentős részét teszik ki a kéretlen elektronikus levelekre vonatkozó beadványok. A világháló használata egyre inkább elterjedté válik az állampolgárok körében; az internet sokrétűsége és változatossága visszatükröződik az ügyek sokszínűségén. A régi ügycsoportok – mint például a fórumok adatkezelése – mellett megjelentek újabb beadványtípusok, így például a közösségépítő weboldalak adatkezelésével vagy az IP-cím szolgáltató általi ellenőrzésével kapcsolatos ügyek.

Idén is sok panasz érkezett az internetes fórumokkal kapcsolatban, amelyek újfent a szabad véleménynyilvánítás, illetve a személyhez fűződő jogok ütközésével összefüggő kérdéseket vetettek fel.

Egy vőfély beadványában azt sérelmezte, hogy a www.mennyegzo.hu internetes portál fórumán személyes adatait nyilvánosságra

hozták, és tiltakozása ellenére is használták. Az adatkezelő arra hivatkozva nem akarta törölni az adatokat a hozzászólásokból, hogy ezzel a szabad véleménynyilvánítás sérülne. Az adatvédelmi biztos válaszában kifejtette, hogy a vélemény, értékítélet kifejezése nem adatvédelmi kérdés, ez a szabad véleménynyilvánítás körébe tartozik. Ezért adatvédelmi szempontból nincs jelentősége annak, hogy egy vélemény jó vagy rossz, kellemes vagy kellemetlen az egyénre nézve. Az információs önrendelkezési jog megillet bárkit, így a kritikával illetett és a kedvező véleményt kapott egyént is. Az interneten bárki közzéteheti véleményét, a szabad véleménynyilvánításhoz fűződő alkotmányos alapjog biztosítja számára, hogy véleményét bárhol, bármilyen fórumon szabadon elmondja és terjessze, de más alkotmányos alapjogok által kijelölt határok között. Többek között védendő érték a magánszféra, amelybe az egyén személyiségi jogai, becsülete, magántitka és személyes adatai is beletartoznak, vagyis az érintett nemcsak az adatvédelmi törvényben, hanem a Polgári Törvénykönyvben (továbbiakban: Ptk.) biztosított jogérvényesítési lehetőségeivel is élhet, sőt felmerülhet a büntetőjogi felelősségre vonás is (becsületsértés, rágalmazás, vagy visszaélés személyes adattal). *(192/A/2006)*

Több panaszos kifogásolta, hogy kérésük ellenére egyes honlapok fórumairól nem törlik regisztrációjukat (nicknevet), illetve hozzászólásaikat. Az elektronikus kereskedelmi szolgáltatások, valamint az információs társadalommal összefüggő szolgáltatások egyes kérdéseiről szóló 2001. évi CVIII. törvény (továbbiakban Elkertv.) szerint az információs társadalommal összefüggő adatkezelésekre az adattakarékosság és az adatelkerülés elve alkalmazandó, tehát az internetes szolgáltató a lehető legkevesebb adatot köteles kezelni a szolgáltatás nyújtása során, illetve ha a szolgáltatás lehetővé teszi, az adatok kezelését mellőzni kell. Az interneten szokásos eljárás az anonimizálás, illetve a pszeudonimizálás, ezek a személyazonosság elrejtését szolgálják. A pszeudonimitás (például nicknév használata) azokban az adatkezelésekben alkalmazandó, ahol a teljes anonimitásnak – a közérdek (például bűnüldözés) vagy más védendő érték (személyiségi jogok védelme) miatt – nincs helye. Tipikusan a fórumok használatában terjedt el. Ilyenkor a valós személyazonosító adatokat egy szabadon választott jelölés (nick) fedi el annak érdekében, hogy csak törvényes feltételek mellett (például büntetőeljárás) és csak szükség esetén sor kerüljön a személyazonosság helyreállítására. A nicknév személyes adat, ha a mögötte rejtőző természetes személy azonosított vagy azonosítható. Ha a felhasználó által szabadon választott jelölés (nick) mellett más személyazonosító

adatok (mint például e-mail cím) kezelésére nem kerül sor, akkor a személyazonosság helyreállítására kizárólag a felhasználó képes. Akár úgy, hogy személyazonosságát az oldalon vagy bárhol máshol visszakereshető módon felfedi, akár úgy, hogy a nicknév és más személyes adatai között a kapcsolatot létrehozza. A szolgáltatás nyújtásához elengedhetetlenül szükséges forgalmi adatokat (IP-cím, a kapcsolat dátuma, időpontja, tartama stb.) a szolgáltató csak a szükséges ideig kezelheti. Ezeknek az adatoknak a cél nélküli megőrzése az Avtv.-ben meghatározott adatminőség elvébe is ütközik, hiszen az adatokat úgy kell tárolni, hogy az érintettet csak a tárolás céljához szükséges ideig lehessen azonosítani. A személyes adatokat – így a nicket is – a fórum üzemeltetője az Avtv. alapján törölni köteles. *(1156/A/2006, 1175/A/2006)*

Szintén az internetes fórumokhoz kapcsolódóan megjelent egy új típusú beadványcsoport. E panaszok azt kifogásolták, hogy különböző fórumok üzemeltetői a moderálási szabályok érvényesítése során az IP-címet ellenőrizve tiltották ki a felhasználókat.

Egy ilyen ügyben a beadványozó azzal összefüggésben kért állásfoglalást, hogy bár személy szerint őt tiltották ki egy fórumról, ennek ellenére a számítógépet használó másik fórumozó sem tudott saját felhasználói nevével belépni az oldalra, pedig az ő regisztrációja eltérő IP-címről érkezett. A biztos az ügyre vonatkozóan megállapította, hogy az internet hálózatában az IP-címek egy-egy számítógépre utalnak, melyet az internethez hozzáférést biztosító szolgáltató rendel az előfizetőhöz abból a célból, hogy azonosítsa az előfizetőt. Az IP-cím, akárcsak a felhasználó neve, beceneve (nick), jelszava és e-mail címe is személyes adat.

Számos internetes oldal moderálási alapelvei előírják, hogy a fórumon való hozzászólás regisztrációhoz kötött, melynek során a felhasználó önként adja meg adatait és fogadja el a moderálási alapelveket. Ezek az elvek lehetővé teszik, hogy a moderátorok a szabályszegés súlyától függően akár végleg vagy határozott időre kitilthassanak egyes felhasználókat a rendelkezésükre álló információk bármelyikének a felhasználásával. Azon felhasználók ellen, akik nem tartották be a moderálási alapelvekben rögzítetteket, a moderátornak joga van fellépni úgy, hogy a rendelkezésükre álló eszközökkel megakadályozzák az alapelvek vagy törvények ismételt megsértését. A kitiltás elképzelhetetlen a felhasználó személyes

> adatainak kezelése nélkül. A szolgáltató ebből a célból jogszerűen kezeli és ellenőrzi a kitiltott felhasználó regisztrált adatait, ideértve azt az IP-címet is, amelyről a regisztráció történt. Mivel azonban a kitiltás egyetlen meghatározott látogatóval szemben alkalmazott szankció, a kitiltott személy azonosításához és a szankció alkalmazásához valamennyi rá vonatkozó (felhasználói fiókban tárolt) személyes adat egybevetése szükséges. Így egyes személyes adatok (például az IP-cím) kiragadása nem csupán célt téveszt, hanem sérti az adatminőség követelményét is. *(867/A2006, 297/A/2006)*

Egy panaszos azzal kapcsolatban kérte az adatvédelmi biztos tájékoztatását, hogy az interneten használatos különféle azonosítók személyes adatnak minősülnek-e. A személyes adat fogalmi eleme, hogy kapcsolatba hozható legyen az érintettel. Bizonyos adatok esetében ez a kapcsolat ideiglenesen megszűnik a személy és az adat között, hiszen például a nicknév esetén pont a személyazonosság elrejtése a cél. Azonban szükség esetén, és ha törvény erre felhatalmazást ad, helyreállítható a kapcsolat az adat és az érintett között. Az elektronikus levélcím, a telefonszám, az msn, az icq és a skype azonosító személyes adat, mert egy természetes személlyel összefüggésbe hozható adatok. A felhasználó az internetes társadalomban ezekkel az azonosítókkal vesz részt, ahogy az „*off-line*" életben a polgári nevével vagy fizikai elérhetőségével. *(1422/K/2006)*

Az elmúlt egy-két évben rohamosan terjedő és egyre népszerűbb kapcsolatépítő portálok számos új kérdést vetnek fel, így az adatvédelmi biztos hivatalát sem kerülhették el az ilyen jellegű oldalak használata során felmerült panaszok. E közösségi weboldalakra történő regisztráció során az érintettek önkéntesen számos adatot megadnak, melyek részben kötelezőek és nyilvánosak, míg más személyes adatok a felhasználó döntése alapján kerülnek kezelésre, és csak akkor válnak a másik fél számára ismertté, ha a felhasználó ahhoz hozzájárul.

Még 2005 végén érkezett egy beadvány, mely azzal kapcsolatban fogalmazott meg kérdést, hogy az iWiW közösségi portálon új adatkezelési gyakorlatot vezettek be, melynek következtében a közösségi háló valamennyi regisztrált tagja láthatja a tagok ismeretségi körét, míg korábban ez a nyilvánosság csak egy tag ismerősei számára volt elérhető.

A biztos állásfoglalásában kifejtette, hogy az oldal használata a tagok önkéntes hozzájárulásán alapul. Az Avtv. értelmében a hozzájárulás önkéntes, ha megfelelő tájékoztatás előzte meg, és az érintett félreérthetetlen beleegyezését adta a személyes adatai kezeléséhez. A vizsgálat megállapította, hogy a honlap adatvédelmi nyilatkozata egyértelműen meghatározza a kezelt adatok körét, és tartalmazza az arra vonatkozó információt is, hogy ezek az adatok publikusak, ennek következtében az adatkezelés jogalapjához nem fér kétség.

Az adatkezelőt azonban tájékoztatási kötelezettség terheli az adatvédelmi politikájának megváltoztatása esetében is. Az információs önrendelkezési jog lényege, hogy személyes adatával mindenki maga rendelkezik, tehát mindenki szabadon dönti el, hogy személyes adatait kik kezeljék, és azokat kik ismerhetik meg. Ennek biztosítása érdekében az adatkezelő minden egyes érintettet tájékoztatni köteles arról, hogy a korábban alkalmazott adatvédelmi szabályait megváltoztatja. Ennek elmulasztása a tájékoztatási kötelezettségének megszegését jelenti. Így a biztos felszólította az adatkezelőt, hogy az új adatkezelési szabályokról értesítse a felhasználókat annak érdekében, hogy az érintettek információs önrendelkezési jogukkal élve szabadon dönthessenek arról, hogy a megváltozott adatvédelmi alapelvek mellett is kívánnak-e az iWiW közösségi hálózatának tagjai maradni. *(1923/A/2005)*

Több beadvány érkezett az iWiW jogutódlásával kapcsolatban. Az állampolgárok arra keresték a választ, hogy jogszerű volt-e a jogelőd és a jogutód cég eljárása, amikor nem értesítették előre a felhasználókat az üzletrész-átruházásról. A biztos válaszában felhívta a figyelmet arra, hogy a jogutód társaságot illetik a jogelőd gazdasági társaság jogai és terhelik a jogelőd társaság kötelezettségei.

A jogutódlással egy adott jogi helyzet, ideértve a társaság adatkezeléseit is, teljes terjedelmében a jogutódra száll át. Az adatkezelőt, vagyis az iWiW üzemeltetőjét tájékoztatási kötelezettség terheli arra vonatkozóan, hogy az adatkezelés körülményeiben változás történt. Azonban a tagok személyében bekövetkezett változás csak a társaság belső viszonyaiban jelent változást, és az nem jelenti a társaság külső jogviszonyának – ideértve az érintettel fennálló és adatkezelést igénylő jogviszony – módosulását. Így megállapítható, hogy az adatkezelő nem köteles előzetesen tájékoztatni a felhasználókat a jogutódlás tényéről. A folytatólagos adatkezeléssel kapcso-

latban a biztos leszögezte, hogy mivel jogutódlás esetén a törvény erejénél fogva átszállnak a jogutódra a jogelődöt megillető jogok és terhelő kötelezettségek, így a jogelőd adatkezelőnek adott hozzájárulások továbbra is jogalapot jelentenek az adatkezeléshez. Ugyanígy a tagok személyében bekövetkezett változás sem teszi a hozzájáruló nyilatkozatokat hatálytalanná. Az érintett információs önrendelkezési jogával élve az adatkezelés bármely szakaszában elzárkózhat a további adatkezeléstől. Akár a „*tulajdonosváltás*" előtt, akár azt követően is. *(728/A/2006, 741/2006)*

Kéretlen elektronikus levelekkel („*spamek*") kapcsolatban továbbra is nagy mennyiségben érkeznek panaszok. Változást jelent a területre vonatkozóan, hogy 2006. január 1-jétől egyértelműbb szabályozást vezetett be az Elkertv. módosítása. Így a jogszabály a reklám fogalmát felcserélte az elektronikus hirdetés fogalmával, amely már sokkal pontosabban és tágabban határozza meg a kéretlen e-maileket. Továbbá újdonság a szabályozásban, hogy az elektronikus hirdetéssel kapcsolatos jogsértések esetén a Nemzeti Hírközlési Hatóság jár el, hasonló jogosítványokkal, mint korábban a Fogyasztóvédelmi Felügyelőség tette.

Idén a spammel kapcsolatos ügyek nagy részét tette ki az olyan elektronikus levelekkel összefüggő panasz, melyben a további levelek küldéséhez kérnek előzetes hozzájárulást, illetve engedélyt. Ez azt mutatja, hogy az adatkezelők egy jelentős hányada nincs tisztában, vagy nem akar tudomást venni a kéretlen e-maileket szabályozó törvényi rendelkezésekről. A beadványok egy másik része konzultációs jelleggel kéri az adatvédelmi biztos állásfoglalását az előzetes engedélykérő levelekkel kapcsolatban.

Az ilyen típusú e-mailek is elektronikus hirdetések, hiszen az Elkertv. kimondja, hogy annak minősül bármely olyan közlés, amelynek célja, hogy közvetve vagy közvetlenül népszerűsítsen egy vállalkozást, szervezetet, kereskedelmi, ipari vagy kézműipari tevékenységet folytató vagy szabályozott szakmát gyakorló személyt, annak áruját, szolgáltatását, tevékenységét.

E törvény szerint mindenfajta hirdetés elektronikus levelezés (e-mailen) vagy azzal egyenértékű egyéni kommunikációs eszköz útján (például mobiltelefonra szöveges üzenetben) kizárólag az igénybe vevő egyértelmű, előzetes hozzájárulásával küldhető.

A rendelkezés azt a kedvezményt teszi, hogy a hozzájáruló nyilatkozat bármely olyan módon is megtehető, amely lehetővé teszi az igénybe vevő azonosítását, valamint a hozzájárulás önkéntes és a megfelelő tájékoztatás birtokában történő kifejezését (honlapon történő feliratkozás). A jogszabály az egyén magánszféráját helyezi a védelem középpontjába, és ennek érdekében a döntési autonómia az egyént illeti meg. Tehát csak akkor küldhető számára levél, ha ebbéli szándékát az adott hirdető vonatkozásában külön nyilatkozattal kifejezte. A törvény nem tesz különbséget aközött, hogy a hirdető egyetlen alkalommal vagy rendszeresen küldi ajánlatait, ahogy a szabály alkalmazása szempontjából az is lényegtelen, hogy mi a közlés tartalma.

Az adatvédelmi biztos a jogszabálysértő gyakorlat elkerülése érdekében állásfoglalásaiban javasolta, hogy az adatkezelők a megkeresések más formáit használják fel a hozzájárulások gyűjtésére, például honlap készítésével tegyék vállalkozásukat elérhetővé. *(224/A/2006, 331/A/2006, 924/A/2006, 1465/A/2006)*

Végezetül említést kell tenni arról, hogy az év végén 31 panasz érkezett amiatt, hogy ismeretlen személyek e-mailen több tízezer adatot – cégek, magánszemélyek e-mail címét – tartalmazó adatbázist kínáltak megvételre. Az ajánlatok külföldi ingyenes levelezőrendszereken létrehozott címekről érkeztek, így a biztosnak nem állt módjában a küldő kilétének felderítése, e-mailen azonban felhívta a figyelmét arra, hogy tevékenysége – az elektronikus levelezés során küldött reklámokra vonatkozó, fent ismertetett szabályok alapján – jogellenes. Tekintettel a panaszok nagy számára a biztos közleményt adott ki, amely a honlapon olvasható.

Hitelintézetek

A hitelintézetek adatkezelését érintő állampolgári panaszok száma az idén kis mértékben ugyan, de csökkent. Az elmúlt évhez hasonlóan sajnálatos módon még mindig érkeznek az Adatvédelmi Biztos Irodájába olyan beadványok, melyek a személyazonosító okmányok banki fénymásolását kifogásolják. A pénzügyi szolgáltatók adatkezelésével kapcsolatos ügyek közel 40 %-át 2005-ben a központi hitelinformációs rendszer működését érintő panaszok tették ki. Kedvező tendencia, hogy a központi hitelinformációs rendszer szabályainak 2005 végén történt átdolgozását, ügyfélbaráttá tételét követően ez az

arány egy-két százalékra csökkent; és azok a beadványok, melyeket e tárgyban vizsgáltunk, nem bizonyultak megalapozottnak.

A pénzügyi szolgáltatók oldaláról 2006-ban is javaslatok fogalmazódtak meg a központi hitelinformációs rendszer adattartamának kibővítésére oly módon, hogy arra a jövőben azon állampolgárok személyes adatai is felkerüljenek, akik megbízhatóan, szerződésszerűen törlesztik hiteleiket. A pénzügyi szervezetek képviselőivel és a Magyar Bankszövetséggel folytatott – több évre visszanyúló – konzultációk során a biztos többször is kifejtette, hogy a pozitív adóslista súlyos alkotmányossági kérdéseket vet fel, így annak felállítását határozottan ellenzi. A pozitív adóslista mellett felhozott leggyakoribb érv az, hogy a bankok ennek segítségével hatékonyabban tudnák értékelni a hitelezés kockázatát, amely az ügyfelek irányában úgy jelentkezne, hogy a kockázat csökkenésével a folyósított hitelek kamata is csökkenhet. A biztos álláspontja szerint az adatkezeléssel elérni kívánt cél nem indokolja az alapvető jog korlátozását. A javaslat egy több millió adatból álló adatbázist eredményezne, melynek meghatározó része – a szerződésszerűen teljesítő adósok esetében – cél nélküli, készletező adatgyűjtés lenne. Ez év januárjában a Pénzügyi Szervezetek Állami Felügyelete, illetve a Magyar Bankszövetség a személyes adatok védelmét súlyosan érintő kérdésben az állampolgári jogok országgyűlési biztosához fordult állásfoglalásért. Az adatvédelmi biztos korábbi álláspontját – az általános biztos és a Pénzügyi Szervezetek Állami Felügyelete támogató álláspontjának tudomásulvétele mellett – mindaddig nem vizsgálja felül, amíg nem látja egyértelmű bizonyítékát annak, hogy a pozitív lista jár olyan előnyökkel az állampolgárok számára, ami indokolja alkotmányos jogaik korlátozását. *(91/K/2006)* Az állásfoglalás teljes szövege megtalálható a honlapon. A biztos munkatársai ezt a véleményt képviselték azon az egyeztetésen is, melyet a pozitív adóslista felállításával kapcsolatban 2006 szeptemberében az Igazságügyi és Rendészeti Minisztérium kezdeményezett. *(1334/K/2006)*

A hitelintézetek direkt marketing célú adatkezelésével összefüggésben nagyszámú panasz érkezett a biztoshoz, ezért e tárgyban hivatalból is vizsgálat indult, melynek során a biztos megállapította, hogy a hatályos jogszabályi rendelkezések nem egyértelműek, az elektronikus levelezés vonatkozásában pedig kifejezetten ellentétesek egymással.

A hitelintézetekről és a pénzügyi vállalkozásokról szóló 1996. évi CXII. törvény (továbbiakban: Hpt.) 201. § (5) bekezdése szerint a pénzügyi intézmény nem küldhet ügyfelének közvetlen postai vagy elektronikus levelezési úton reklámanyagot, ha ezt az ügyfél kifejezett rendelkezéssel kizárta. A Hpt. 201. § (5) bekezdése a direkt marketing célú adatkezelést illetően azt teszi lehetővé, hogy az ügyfél tiltakozzék ellene. A Hpt.-ben és az adatvédelmi törvényben biztosított tiltakozási jog az érintettet az adatkezelés minden szakaszában – így az adatkezelés kezdetén is – megillető jog. A biztos álláspontja szerint tehát a pénzügyi szolgáltatók kötelesek ügyfeleik számára a tiltakozási jog gyakorlására lehetőséget biztosítani mind a szerződés aláírásakor, mind pedig a jogviszony fennállása alatt. Szerencsés megoldás lenne, ha a direkt marketing célú adatkezelés vonatkozásában a hitelintézetek üzletszabályzataiban olyan tartalmú tájékoztatás szerepelne, mely szerint a reklámcélú adatkezelés ellen az ügyfél bármikor tiltakozhat. Gyakran előforduló eset, hogy a szerződés aláírásával az ügyfelek hozzájárulnak ugyan a reklámcélú adatkezeléshez, de önrendelkezési joguk csorbát szenved, mert erről külön nem nyilatkozhatnak. A szerződésbe foglalt hozzájárulás – különösen ebben a formában – megtévesztő, mert azt sejteti, hogy azzal szemben nincs tiltakozási lehetőség. A biztos felhívta továbbá arra is a figyelmet, hogy a Hpt. idézett rendelkezése kifejezetten ellentétes az Elkertv. előírásaival. Eszerint ugyanis elektronikus levelezés vagy azzal egyenértékű egyéni kommunikációs eszköz útján kizárólag az igénybe vevő egyértelmű, előzetes hozzájárulásával küldhető elektronikus hirdetés. A fenti megállapításokkal a Pénzügyi Szervetek Állami Felügyelete is egyetértett. *(379/H/2006)*

Arról is beszámolunk, hogy a Pénzügyi Szervetek Állami Felügyeletével sikeresen zárult az a többfordulós egyeztetés, melynek kiindulópontja egy, az adatvédelmi biztos vizsgálati jogosultságát korlátozó felügyeleti állásfoglalás volt. A Felügyelet – az adatvédelmi törvény rendelkezéseit figyelmen kívül hagyva – azt az álláspontot képviselte, hogy a biztos nem rendelkezik egyértelmű törvényi felhatalmazással banktitoknak minősülő adatok megismerésére. Az Avtv. 26. §-a szerint az adatvédelmi biztos a feladatai ellátása során az adatkezelőtől minden olyan kérdésben felvilágosítást kérhet, az összes olyan iratba betekinthet, illetve iratról másolatot kérhet, adatkezelést megismerhet, amely személyes adatokkal összefügghet. Az idézett

szakasz nem határoz meg különböző vagy kivételt képező adatkezelői kategóriákat (pl. ügyvédi irodák, bankok, biztosítók, stb.), amelyek esetében ezen eszközök ne lennének alkalmazhatóak. Ebből pedig egyenesen következik, hogy a hitelintézetek, mint általában véve vett adatkezelők – függetlenül a bank titoktartási kötelezettségétől – kötelesek a biztos megkeresésének eléget tenni. Az adatvédelmi biztos tehát a bejelentő külön okiratba foglalt adatkezelési felmentvénye hiányában is jogosult a bepanaszolt adatkezelést megismerni. A Felügyelet végül tartalmilag visszavonta korábbi állásfoglalását. *(1248/A/2005)*

Több olyan indítvány is érkezett a biztoshoz, mely arra a gyakorlatra hívta fel a figyelmet, hogy egyes kereskedelmi cégek a bankkártyával fizető vásárlók bankkártyaszámát számítógépes rendszerükben rögzítik.

> Amennyiben a tranzakciókhoz tartozó kártyaszámokat olyan módon tárolják, hogy azok nem kapcsolhatók egy konkrét vásárlóhoz, úgy gyakorlatilag az adatkezelés kívül esik az Avtv. hatályán. Más a helyzet azonban akkor, ha a tárolt kártyaszámokhoz az érintett neve is kapcsolódik, hiszen ekkor már a kártyaszám is személyes adat. Tekintettel arra, hogy adatkezeléshez a kereskedelmi cégek nem kérik ki az érintettek hozzájárulását, és törvény sem nyújt felhatalmazást erre, ezért a kártyaszámok személyhez kapcsolható módon, tehát személyes adatként való tárolása jogellenes. Ezekben az ügyekben a biztos felszólította az adatkezelőket, hogy a kártyaszámok tárolását vagy olyan módon oldják meg, hogy azokat még véletlenül se lehessen egy adott személyhez kapcsolni, vagy pedig – ha az általa javasolt mód nem megfelelő – a kifogásolt adatkezelést szüntessék meg és semmisítsék meg az eddig *„begyűjtött"* kártyaszámokat. A kártyaszámok azonosítható módon történő tárolása ugyanis nemcsak adatvédelmi szempontból jogszerűtlen, de komoly biztonsági kockázatot is rejt magában. *(453/K/2006, 954/A/2006)*

Az internetes banki szolgáltatások gyors terjedésével összefüggésben ez év végén sajnálatos módon megszaporodtak az úgynevezett *„adathalászattal"* kapcsolatos állampolgári bejelentések. Legjellemzőbb elkövetési magatartás, hogy a csalók különböző eszközökkel – általában a számla zárolására figyelmeztető e-mail útján – ráveszik a gyanútlan számlatulajdonost, hogy árulja el jelszavát, adjon meg bizalmas adatokat, illetve számítógépén töltsön le, indítson el bankinak

látszó alkalmazást az elektronikus üzenetben kapott link segítségével. A biztos a panaszosoknak írt válaszában elsősorban a prevenció fontosságát emelte ki. Nyomozati jogkör hiányában ezekben az ügyekben nem indult vizsgálat. A beadványozókat azonban tájékoztattuk, hogy a nyomozó hatóságoknál jogosultak büntető feljelentést tenni. *(1997/A/2006, 2030/A/2006)*

Számos beadvány érintette a bankok adatgyűjtési gyakorlatát, valamint az általuk a szerződéskötéskor kért egyes adatkezelési felmentvényeket.

A CIB Bank Zrt. esetében a beadványozó azt sérelmezte, hogy hitelkártya igényléshez személyi azonosító igazolványán kívül lakcímkártyája mindkét oldalának fénymásolatát is be kellett nyújtania, tehát azt az oldalt is, amelyen személyi azonosító száma található. A kártyaigényléshez szükséges űrlapon, az ügyfél nyilatkozatai közt található továbbá egy olyan pont, mely szerint az ügyfél hozzájárulását adja, hogy a bank a CIB csoport tagjai részére név, lakcím adatát, valamint a bankkal kötött szerződései, illetve igénybe vett szolgáltatásai típusára, továbbá azok összegére vonatkozó adatait átadja, feldolgozza, kezelje. Az adattovábbítás és adatkezelés célja, hogy a CIB csoport tagjai termékeikkel és szolgáltatásaikkal az üzletfelet közvetlenül keressék meg. A biztos megkeresésére adott válaszában a bank adatvédelmi felelőse kifejtette, hogy az ügyfél megtilthatja akár a szerződéskötés alkalmával, akár pedig azt követően, hogy adatait a fent leírt módon és célból a CIB csoporton belül átadják. A szerződéskötésnek nem feltétele a hozzájárulás megadása. A banknak nincs szüksége a személyi azonosító szám ismeretére, illetve nyilvántartására, ezért valószínűleg véletlen folytán kerülhetett sor a lakcímkártya második oldala fénymásolatának a bekérésére. Az adatvédelmi felelős kezdeményezte a belső szabályzatok oly módon történő módosítását, hogy azokból egyértelműen kitűnjön, hogy a kérdéses adatra, illetve másolatra nincs szükség. *(1034/A/2006)*

Egy másik ügyben az indítványozó az MKB Bank Nyrt. panaszbejelentő nyomtatványának adatigénylését tartotta túlzottnak. A kérdéses nyomtatványon *„kompenzációs igény”* esetén az ügyfél köteles megadni adóazonosító jelét, illetőleg taj-számát. Az MKB Bank felvilágosítása szerint kompenzációs igény alatt értenek minden olyan kompenzációt, amikor a bank a panaszos részére bármilyen oknál fogva jóváírást végez, vagy követelést enged el. Minden egyes

kompenzációs igény esetén egyedileg kerül elbírálásra annak megállapítása is, hogy a kompenzáció adóköteles jövedelmet keletkeztet-e a panaszos részére vagy sem. A jövedelemnek minősülő kompenzációs igénynek járulék vonzata is lehet, amelyről a taj-szám feltüntetésével kell adatot szolgáltatni. A biztosi vizsgálat eredményeként a bank felülvizsgálta korábbi gyakorlatát, és az alábbi intézkedéseket foganatosította: az adóazonosító jelet és a taj-számot törölték a panaszbejelentő nyomtatványról, és csak azt követően kérik be a panaszostól, miután bebizonyosodott, hogy a javára megállapított kompenzációt adó- és járulékfizetési kötelezettség terheli. Törlésre kerültek továbbá a panaszkezelő rendszerben szereplő, a panaszosoktól előre bekért taj-számok és adóazonosító jelek is. *(132/A/2006)*

A pénzügyi szektorban is igen elterjedt a telefonos ügyfélszolgálatok működtetése. A telefonos ügyfélszolgálatokhoz érkező hívásokat legtöbbször a hitelintézetek is rögzítik. Az ügyfelek számára biztosítani kell, hogy a hozzájárulásukkal készített hangfelvételt másolatban megkaphassák.

Az OTP Bank Nyrt. egyik ügyfele az sérelmezte, hogy a *„Lakáshitel vonal”*-on rögzített beszélgetésének hanganyagát a bank nem küldte meg részére. A bank az elutasítást azzal magyarázta, hogy a hívások hanganyagát csak vitás esetek rendezésére használják fel, és a jelen ügyben *„nem látnak okot a hanganyag felhasználásra, hiszen az ügyfél a beszélgetés során felvetett kérdéseire megfelelő tájékoztatást kapott, melyet el is fogadott”*.

Fontos követelmény, hogy a rögzített hanganyag mindkét fél által hozzáférhető és felhasználható legyen, amennyiben annak bizonyítása válik szükségessé, hogy mi hangzott el a rögzített beszélgetés során. Ha rögzítik a beszélgetést, az adatkezelőnek biztosítania kell az ügyfél rendelkezési jogát. Abban az esetben, ha az érintett kifejezetten a hanganyag másolatban történő kiadását kéri, az adatkezelőnek a beszélgetésről készült hangfelvételt kell rendelkezésére bocsátani, a hangfelvételről készült jegyzőkönyv azt nem helyettesítheti. A biztos elfogadhatatlannak tartotta azt a gyakorlatot, mely szerint a pénzügyi szolgáltató ítéli meg, hogy az adott esetben indokolt-e a hanganyag ügyfél által történő felhasználása. A tájékoztatás kéréséhez való jog az információs önrendelkezési jogból fakadó részjogosultság, melyet az érintett szabadon gyakorolhat. *(752/A/2006)*

Biztosítók

A biztosítók tevékenységével kapcsolatos beadványok száma jelentősen nem változott 2006-ban, és ezek a beadványok nem is jeleznek lényegesen új problémákat a biztosítási szektor adatkezelésével kapcsolatban, az eddig rendszeresen felmerülő adatvédelmi jogsértések azonban ez évben is visszatértek. Így sok ügy a biztosítók adatéhségéről, illetve a személyes adatok védelméhez való jog konfliktusáról szólt. Természetesen egyfelől érthető, hogy a biztosítók a biztosítási események elbírálásához, a szerződések (pl. életbiztosítás) megkötéséhez minél több személyes, sőt különleges adatot kívánnak kezelni, ez az igényük és ezzel kapcsolatos intézkedéseik azonban sokszor nem felelnek meg a célhoz kötött adatkezelés követelményének.

Egy konkrét ügyhöz kapcsolódóan panasz érkezett az Aviva Életbiztosító Zrt. adatkezelésével kapcsolatban. A panaszos véleménye szerint a biztosító az életbiztosítások megkötése során számos olyan egészségügyi, tehát különleges adatot kér az ügyfelektől, amelyek nem szükségesek a biztosítási kockázat elbírálásához.

A biztosítókról és a biztosítási tevékenységről szóló 2003. évi LX. törvény (továbbiakban: Bit.) 155. §. (1) bekezdése szerint a biztosító, a biztosításközvetítő és a biztosítási szaktanácsadó ügyfeleinek azon biztosítási titkait jogosult kezelni, 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 a törvény által meghatározott egyéb cél lehet. E rendelkezés szerint sokszor csak a konkrét esetek pontos ismeretében lehet eldönteni az adatkezelések jogszerűségét. A vizsgálat megállapította, hogy a biztosító adatigénylése az életbiztosítások esetén nem felel meg a célhoz kötöttség követelményének. Az ügyben kiadott állásfoglalás szerint az idézett jogszabályhely alapján ítélendő meg, hogy a biztosító adatkérése indokolt-e. A biztos álláspontja szerint például a szövettani vizsgálat eredménye a biztosító által vállalt kockázat felméréséhez szükséges lehet, hiszen egy daganatos megbetegedés valószínűsége befolyásolhatja a biztosítási esemény bekövetkezését. Ugyanakkor az olyan egészségügyi adatokat, amelyek ebből a szempontból nem vagy csak igen közvetetten bírnak jelentőséggel, a biztosító nem követelheti ügyfelétől. Ide tartoznak például a szülésekről, nőgyógyászati műtétekről, menopausa tünetek-

ről szóló kórházi iratok, ügyfél-nyilatkozatok. Elmondható tehát, hogy nincs olyan jogszabály, amely tételesen felsorolná azokat az adatokat, amelyeket a biztosító életbiztosítás megkötése előtt ügyfelétől kérhet, ugyanakkor a szolgáltatandó adatok körének határait a Ptk., az Avtv., valamint a célhoz kötött adatkezelés elve kijelöli. Amennyiben a biztosító olyan egészségügyi adatokat is tárol, amelyek a biztosítási esemény bekövetkezését nem befolyásolják, cél nélkül kezel adatokat, ezáltal jogellenes adatkezelést végez. A felelősség ebben az esetben az adatkezelőt terheli.

A vizsgálat megállapította azt is, hogy a biztosító a biztosított esetleges genetikai vizsgálatáról történő adatkérése, illetve a biztosított családtagjainak egészségi állapotára vonatkozó kérdések szintén a célhoz nem kötöttség okán jogellenesek.

Az adatvédelmi biztos állásfoglalásában kitért arra a sokszor visszatérő problémára is, hogy a biztosítók olyan adatkezelési nyilatkozatot iratnak alá ügyfeleikkel, amelyben azok a jövőre nézve, a titokkör pontos megjelölése nélkül adnak felmentést az őket kezelő orvosoknak a titoktartási kötelezettség alól. Az Adatvédelmi Biztos Irodájának megalakulása óta nagy számban érkeztek panaszok az ehhez hasonló blankettajellegű orvosi felmentvény ellen.

Több adatvédelmi biztosi állásfoglalás egyértelműen kimondta, hogy az érintetteknek a hozzájáruló nyilatkozat megadása előtt tudomással kell bírniuk arról, hogy adataikat kik, milyen célból és milyen meghatározott adatkört érintően fogják kezelni, illetve feldolgozni. Így nem követelhető, hogy a biztosítottak a jövőre nézve felmentést adjanak az orvosi titoktartás alól egy olyan személynek, akit a nyilatkozat megtételének időpontjában még nem is ismernek. Ugyanígy nem követelhető az sem, hogy az érintettek olyan adataik kezeléséhez járuljanak hozzá, amelyek csak a felhatalmazást követően keletkeznek. A megfelelő tájékoztatás hiányán túl az ilyen nyilatkozat kérése sérti az Avtv.-ben foglalt azon rendelkezést is, hogy az adatok felvételének mindenkor tisztességesnek és törvényesnek kell lennie.

Az adatvédelmi biztos a fentebb ismertetett aggályok miatt megkereste a biztosítót, és kérte, hogy sérelmezett adatvédelmi rendelkezéseit vizsgálja felül. A biztosító a megkeresésre adott válaszában kifejtette, hogy az adatvédelmi biztos, mivel nem orvos, nem kompetens annak a megítélésében, hogy bizonyos egészségügyi adatok szükségesek-e a biztosítónak egy életbiztosítás kockázatának és így

díjának meghatározásában. A biztosító előadta, hogy a biztosítottak családtagjaira vonatkozó kérdésekre adott válaszok nem minősülnek személyes adatoknak, mert azok a későbbiekben nem hozhatók összefüggésbe konkrét személlyel. A biztosító a titoktartás alóli felmentéssel kapcsolatban előadta: „*Bár az Avtv. rendelkezései nem nyújtanak eligazítást arról, hogy az érintettnek a nyilatkozatát az egyes személyes adatok kezelése előtt vagy után kell beszerezni, a biztosítási szerződésre vonatkoztatva azonban megállapítható, hogy értelemszerűen az érintett az olyan adatok kezeléséhez adja a hozzájárulását, amelyek szükségszerűen a nyilatkozatát követően keletkeznek, tekintettel arra, hogy csak a nyilatkozat beszerzését követően kerül sor az érintett orvosi vizsgálatára és a vizsgálat eredményét tartalmazó adatok kezelésére.*"

Az ügy kapcsán az adatvédelmi biztos megkereste a Pénzügyi Szervezetek Állami Felügyeletét. A PSZÁF szakmai álláspontjában az adatvédelmi biztos álláspontját szigorúnak találta, és egyebek mellett hangsúlyozta, hogy a biztosítási veszélyközösség jó minőségének fennmaradáshoz és így a biztosítási díj alacsonyan tartásához is komoly érdekek fűződnek, ennek meglétéhez pedig fontos, hogy a biztosító megfelelő áttekintést kapjon a biztosított helyzetéről, egészségi állapotáról. Az egyeztetés, illetve a biztosítók adatkezelését elemző vizsgálat még nem zárult le, de a PSZÁF illetékeseivel lefolytatott legutóbbi egyeztetés alapján úgy tűnik, sikerül kompromisszumos, a biztosítók és a biztosítottak érdekeit egyaránt figyelembe vevő megoldást kialakítani. Ezáltal várhatóan szigorodni fognak a biztosítotti egészségügyi adatok közvetlen cél hiányában történő felhasználásának és továbbításának feltételei. *(938/A/2006)*

Egy másik ügy a gépjármű-felelősségbiztosítással kapcsolatos kérdésekkel foglalkozik. A felelősségbiztosítás jelenlegi szabályozása alapján nincs a biztosítottnak arra lehetősége, hogy a részletes számítógépes javítási kalkuláció adatait megismerje, mivel azok elsősorban a károsult személyes adatának minősülnek az adatvédelmi biztos álláspontja alapján.

A panaszos szerint „*A jelenlegi eljárás lehetőséget biztosít arra, hogy egyes károsultak a biztosító embereivel összejátszva indokolatlanul magas javítási számlákat számoljanak el, és ezzel nemcsak a biztosítót, de közvetve valamennyi biztosítottat megkárosítják.*"

A biztos válaszában kifejtette, hogy a gépjármű üzemben tartójának kötelező felelősségbiztosításáról szóló 190/2004. (VI. 8.) kormányrendeletnek valóban van egy olyan rendelkezése, mely szerint az üzemben tartó jogosult arra, hogy a biztosítónak a teljes kárkifizetés összegéről szóló írásbeli értesítését követő hat héten belül a teljes károsszeget a biztosítónak megfizesse, és így a bonus-malus osztályba sorolását ne rontsa. Erre figyelemmel a biztosítótársaságot tájékoztatási kötelezettség terheli, ez azonban a teljes kárkifizetés összegére vonatkozik, nem pedig a kárfelvételi jegyzőkönyvben, valamint a javítási kalkulációban szereplő egyes tételekre.

A fenti ügy kapcsán konzultációra került sor a Pénzügyi Szervezetek Állami Felügyeletével. A konzultáció során a biztos tájékoztatta a felügyeletet, hogy korábbi álláspontját fenntartja, egyben jelezte a panaszos által felvetett problémát. A felügyeletnek írott levelében a biztos kifejtette, hogy amennyiben a fenti adattovábbítás szükségességét, elengedhetetlenségét a Pénzügyi Szervezetek Állami Felügyeletének már lezárt vizsgálatai vagy egy esetlegesen erre irányuló jövőbeli célvizsgálata is alátámasztja, úgy a biztos nem látja akadályát annak, hogy a károsult és a károkozó információs önrendelkezési jogának konfliktusát feloldandó, a Bit. biztosítási titokra vonatkozó szabályai – a célhoz kötött adatkezelés követelményét szem előtt tartva – kiegészítésre kerüljenek. *(247/A/2006)*

Ez évben is zárultak le olyan vizsgálatok, amelyekben a biztosítók jogellenes okmánymásolását állapította meg a biztos. Az adatvédelmi biztos ezekben az esetekben sokadszorra is felhívta a biztosítók figyelmét arra, hogy az okmánymásolás a személyes adatok védelméhez fűződő jog sérelmét jelenti, ha ahhoz nem szerzik be az érintett önkéntes, határozott, tájékozott hozzájárulását. Az ügymenet oldaláról nézve jelentkező célszerűségi, gazdasági megfontolások, az alkalmazottak munkájának ellenőrzésére irányuló szándék az Alkotmányban biztosított alapvető jog korlátozását mérlegelve súlytalan érvek, alkotmányjogilag értelmezhetetlen kategóriák. Következésképpen a személyes adatok védelméhez fűződő jogot nem lehet ezeknek alárendelni. *(1069/A/2005, 1205/A/2005)*

Sajtó

A sajtóval kapcsolatos ügyek tartalmi megoszlásában 2006-ban is megfigyelhető, hogy a beadványok többségében az országos, illetve

helyi lapokban megjelenő személyes adatok, fotók sajtó általi nyilvánosságra hozatalát kifogásolják a panaszosok. A beadványok másik jelentős részében pedig a televíziók műsorszerkesztési módszereit sérelmezik a polgárok.

Több panaszos azért fordult hozzánk, mert a beleegyezésük nélkül jelent meg róluk – illetve más esetben kiskorú gyermekeikről – készült fotó az újságokban, és ezért a lapokkal szembeni jogorvoslati lehetőségekről kértek felvilágosítást az érdekeltek.

Egy panaszos azt kifogásolta, hogy a HÉTközlap című helyi lap a kisnémedi óvodáról írt cikkében megjelentette gyermeke fényképét és a kép alatt közölte annak nevét is. A panaszos óvodás korú gyermeke a közzétett fotón alsónadrágban látható, amint az óvodai logopédus foglalkozik vele. A panaszos szerint a megjelent fotó sérti gyermeke személyiségi jogait, és a fénykép újságban való megjelentetéséhez nem kérték, de nem is adta volna a hozzájárulását.

Egy másik esetben a panaszos azt sérelmezte, hogy a Théma című újságban 2005. május 18-án, valamint 2006. május 10-én olyan fotókat közöltek egy cikkhez, amelyeken ő egyértelműen felismerhető kutyasétáltatás közben, és a fotók újságban való megjelentetéséhez egyik esetben sem adta a hozzájárulását. A panaszos előadása szerint második alkalommal egy olyan cikk illusztrációjaként jelent meg az egy évvel korábban készült fotója, amelyben a kutyásokat a nagy mennyiségű *„kutyagumi”* miatt marasztalják el. Panaszosunk a második eset után telefonon megkereste az újságot, hogy tiltakozzon a fotói nyilvánosságra hozatala, illetve a rá nézve sértő szövegkörnyezetben való megjelentetése ellen. A panaszos állítása szerint nem kapott megfelelő tájékoztatást – a tudta és beleegyezése nélkül – róla készült fotók további sorsáról, illetve arról, hogy a következőkben figyelembe veszie a Théma kft., hogy továbbra sem adja hozzájárulását a róla készült fotók közléséhez.

> Az adatvédelmi törvény szerint személyes adat akkor kezelhető, ha ahhoz az érintett hozzájárul, vagy azt törvény vagy – törvény felhatalmazása alapján, az abban meghatározott körben – helyi önkormányzat rendelete elrendeli. Tehát mind a fényképfelvétel elkészítéséhez, mind felhasználásához, nyilvánosságra hozásához törvényi felhatalmazás vagy a lefényképezni kívánt személyek hozzájárulása szükséges, kivéve, ha törvény közérdekből elrendeli a nyilvánosságra hozatalt. Kétség esetén azt kell vélelmezni, hogy az

érintett a hozzájárulását nem adta meg. A nyilvánosságra hozatal fogalmát e körben kiterjesztően kell értelmezni (sokszorosítás, forgalmazás, kiállítás, sugárzás, internet, stb.). Az Avtv. szabályai összhangban vannak a Ptk. rendelkezéseivel. A Legfelsőbb Bíróság egyik határozata szerint a képmás nyilvánosságra hozatalának tilalma nem vonatkozik a nyilvános eseményekről, rendezvényekről, táj- és utcarészletekről készült felvételekre, amikor az ábrázolás módja nem egyéni, hanem a felvétel összhatásában örökít meg a nyilvánosság előtt lezajlott eseményeket. A nyilvánosságra hozatalhoz a felvételen megörökített személy hozzájárulására van viszont szükség, ha megállapítható a felvétel egyedisége, egyéni képmás jellege.

A fenti jogszabályi rendelkezések, valamint a beadványokhoz mellékelt újságcikkben szereplő fotók alapján megállapítható volt, hogy az első ügyben a panaszos kiskorú gyermeke, a második esetben a panaszos egyértelműen felismerhető a fotókon, melyek közléséhez egyik érintett sem adta a hozzájárulását.

Az előbbiek alapján az Avtv. 25. §. (2) bekezdésére hivatkozva az adatvédelmi biztos felszólította a bepanaszolt lapok főszerkesztőit a jogellenes adatkezelési tevékenységük megszüntetésére. *(536/A/2006, 810/A/2006)*

A személyhez fűződő jogok védelmét és elsőbbségét deklarálja a sajtóról szóló 1986. évi II. törvény (továbbiakban: Stv.) 3. § (1) bekezdése is, mely szerint *„a sajtószabadság gyakorlása nem járhat mások személyhez fűződő jogainak sérelmével”*.

Ezzel kapcsolatos az a beadvány, amelyben a panaszos a Népszabadság Rt. eljárását sérelmezte. A Népszabadság 2006. február 13-i számában Rab László tollából írás jelent meg *„Egy a 400 ezerből”* címmel. A cikk nyilvánosságra hozta a panaszos nevét, valamint azt az információt, hogy a panaszos – aki a Fidesz 400 ezer munkanélkülit demonstráló választási plakátjához, hirdetéséhez modellként képmását adta – budapesti vállalkozó, másodállásban statiszta és autókölcsönzésből él, nem munkanélküli, és az *„arcát”* az Armada Modellügynökségtől vásárolta a hirdető politikai párt.

A panaszos beadványához csatolta a Népszabadság szerkesztőségébe is eljutatott nyilatkozatát, mely szerint szerződés alapján vállalta, hogy a megbízó párt a róla készült fotót felhasználja, ennek megfelelően csak az arcát (képmását) adta ehhez a szerephez. Leve-

le szerint a plakátokon megjelenített szövegekért, azok tartalmáért nem tartozik felelősséggel. A cikk szerzőjének elmondta, és a szerkesztőnek is kifejtette, hogy nem kíván interjút adni, továbbá nem járul hozzá, hogy neve, címe, bármely más személyes adata vagy akár a foglalkozása tevékenységi köre bekerüljön az újságba.

Vörös T. Károly főszerkesztő álláspontja szerint az érintett személyes adatai nyilvánosságra hozatalának törvényes jogalapja az Stv. 2. § (1) bekezdésében foglaltak teljesítése, miszerint mindenkinek joga van arra, hogy tájékoztatást kapjon szűkebb környezetét, házáját stb. érintő kérdésekben. A sajtó feladata a hiteles, pontos, gyors tájékoztatás. A panaszos tiltakozásának figyelmen kívül hagyását a főszerkesztő azzal indokolta, hogy az Alkotmány biztosítja a sajtó szabadságát, beleértve a szerkesztés szabadságát is. Álláspontja szerint itt két alapjog – személyes adatok védelme és sajtószabadság – ütközéséről van szó, ezért a panaszos nevének mellőzése sértette volna ezen alapvető jogot. A Népszabadság álláspontja szerint egyébként nem életszerű, hogy kizárólag csak az újságban megjelent információk alapján vált beazonosíthatóvá az érintett, mivel a megjelent plakátok alapján mind lakókörnyezetében, mind pedig ügyfelei által széles körben korábban is ismert volt.

Az üggyel kapcsolatban az adatvédelmi biztos kifejtette, hogy személyes adat nyilvánosságra hozatalához az érintett kifejezett hozzájárulásának hiányában egyértelmű törvényi felhatalmazásra van szükség. E szabályokat figyelmen kívül hagyta a Népszabadság, amikor a 2006. február 13-i számában törvényes jogalap nélkül, a panaszos kifejezett tiltakozása ellenére nyilvánosságra hozta a panaszos személyes adatait. Az adatvédelmi biztos a panaszost tájékoztatta a jogérvényesítési lehetőségekről; a Népszabadság főszerkesztőjét pedig felszólította, hogy a jövőben tartózkodjanak a hasonló jogsértésektől. *(273/A/2006)*

Évek óta visszatérő probléma a televíziós műsorokban szerepelő polgárok személyes, sok esetben szenzitív adatainak nyilvánosságra hozatalával kapcsolatos műsorkészítési, műsorszerkesztési gyakorlat. A kereskedelmi televíziók valóságshow és egyéb riportműsoraival összefüggő beadványok mellett az idén a közszolgálati televízió egyik műsorával kapcsolatosan is érkezett panasz.

A panaszos beadványában előadta, hogy miután bejelentette munkahelyén, hogy veszélyeztetett terhes, a munkáltatója felmondott neki. Történetét megírta a Magyar Televíziónak, és az esetről készült

riport áprilisban került adásba *„A tévé ügyvédje”* című műsorban. Volt munkáltatójával – a műsor vetítése előtt – azonban a panaszos peren kívül egyezséget kötött, amelyben a részére fizetendő kártérítés kifizetéséhez a munkáltató azt a feltételt támasztotta, hogy a cég neve és egyéb adatai az ügy kapcsán ne kerüljenek nyilvánosságra. E feltétel betartása érdekében a panaszos írásban többször megkereste a műsor felelős szerkesztőjét, és kérte, hogy a volt munkáltatójával kapcsolatos információk ne hangozzanak el a műsorban. A műsor szerkesztője ezt többször, írásban meg is ígérte – amit a beadványhoz csatolt iratok tanúsítottak –, ennek ellenére a műsorról készült videofelvétel első vágóképében hosszú másodpercekig, jól azonosíthatóan látszott az érintett cég neve és címe. Emiatt a volt munkáltató nem fizette ki a panaszos részére a peren kívüli egyezségben meghatározott kártérítési összeget.

> Az adatvédelmi biztos álláspontja szerint a panaszos volt munkáltatójának neve és címe a vele való kapcsolatba hozhatóság okán a panaszos személyes adatának minősült a műsor levetítése során, az a tevékenység pedig, amellyel a műsor ezeket az adatokat nyilvánosságra hozta, adatkezelésnek minősült. Jelen ügyben a műsornak nem volt törvényi felhatalmazása adatkezelésre, ezért ahhoz, hogy a panaszos volt munkahelyének pontos nevét és címét nyilvánosságra hozza, a panaszos hozzájárulására lett volna szükség. A panaszos ezt a hozzájárulást azonban nem adta meg, sőt többször kifejezetten kérte írásban, hogy ezen adatait a riportban ne hozzák nyilvánosságra. A panaszos adatkezelésre vonatkozó rendelkezése hatályosult is a műsor szerkesztője felé, mivel többször is ígéretet tett ennek teljesítésére. Ennek okán jelen ügyben jogellenes adatkezelés valósult meg. Az adatvédelmi biztos felszólította a műsor felelős szerkesztőjét, hogy a jövőben fokozottan vegyék figyelembe, hogy tevékenységük során sok esetben adatkezelés valósul meg, a műsor készítői, illetve a televízió pedig adatkezelőnek minősülnek, ezért be kell tartaniuk az Avtv. előírásait. A panaszost arról tájékoztatta, hogy az Avtv. 18. §-a szerint az adatkezelő az érintett adatainak jogellenes kezelésével vagy a technikai adatvédelem követelményeinek megszegésével másnak okozott kárt köteles megtéríteni, a kár megtérítése iránt pert lehet indítani adatkezelő ellen. *(830/A/2006)*

Levéltár, tudományos kutatás

Az elmúlt évi indítványdömping után e tárgykörben – különösen az úgynevezett ügynök-ügyek elcsitulása miatt – az ügyek száma a korábbiaknak megfelelően alakult.

A nyilvánosság és kutathatóság fogalma gyakran összemosódik, noha a kutatás területén nem tekinthetjük ezeket azonosaknak. Egy indítványozót kérdésére válaszul a biztos arról tájékoztatott, hogy általánosságban nem mondható ki, hogy minden levéltári anyag egyúttal közérdekű adat lenne, csupán azok, amelyek levéltárba kerülésük idején is annak számítottak.

A levéltárak használatának szabályairól a köziratokról, a közlevéltárakról és a magánlevéltári anyag védelméről szóló 1995. évi LXVI. törvény (továbbiakban: Ltv.) rendelkezik, mely kimondja, hogy a közlevéltárban őrzött, az 1990. május 1-je után keletkezett, a keletkezés naptári évétől számított harminc éven túli, az 1990. május 2-a előtt keletkezett, a keletkezés naptári évétől számított tizenöt éven túli levéltári anyagban – bizonyos kivételekkel –, továbbá időbeli korlátozás nélkül abban a levéltári anyagban, amelyet már nyilvánosságra hoztak, illetőleg, amelynek tartalmát az adatvédelmi törvény szerint mindenki megismerheti, a kutatni kívánt téma megjelölését tartalmazó kérelemre bármely természetes személy ingyenesen kutathat, és a kutatásra kiadott levéltári anyagról saját költségén másolatot készíttethet. Az 1990. május 1. után keletkezett, a keletkezés naptári évétől számított harminc év lejárta előtt a belső használatra készült, valamint a döntés-előkészítést tartalmazó levéltári anyagban folytatható kutatást az átadó szerv hozzájárulásával a levéltári anyagot őrző közlevéltár engedélyezi. Jogutód nélkül megszűnt szerv levéltári anyagában a kutatást a levéltári anyagot őrző közlevéltár engedélyezi. *(1895/K/2006)*

Az 1956-os forradalom és szabadságharc ötvenedik évfordulójára való tekintettel több kiadvány készült, melyeknek szerzői, szerkesztői kértek a biztostól adatvédelmi szempontú útmutatást.

A történelmi események szereplői adatainak nyilvánosságra hozatalának esetében – az állandó biztosi gyakorlat szerint – több szempontot kell figyelembe venni. Az egykor közfeladatot ellátó szervezetek szolgálatában állók személyi körének neve, beosztása, illetve más adata engedélyük vagy hozzátartozóik engedélye nélkül köz-

zétehető. Az egykori forradalmárok adatait – amennyiben élnek – csak abban az esetben lehet közzétenni, ha ahhoz hozzájárultak, vagy az adatok már jogszerűen nyilvánosságra kerültek. Az elhunytak adatainak védelmét nem az adatvédelmi törvény biztosítja, hanem a polgári jogban található kegyeleti jog intézménye. Ennek értelmében a halál után is biztosítani kell az elhunyt méltóságának védelmét, mely azonban az idő múlásával lassan elenyészik. *(1218/K/2006)*

Hasonlóan kell eljárni a forradalom és az azt követő megtorlások áldozatainak adataival is. *(611/K/2006)*

Az év talán – e tárgykörben – legizgalmasabb indítványát az Állambiztonsági Szolgálatok Történeti Levéltárának főigazgatójától kaptuk, aki arról kért állásfoglalást, hogy vajon az adattovábbítás megismeréséhez való jog alapján az egykori hálózati személy megismerheti-e azoknak az adatait, akik aktájából adatokat kaptak. A kérdés jelentősége abban áll, hogy a hálózati személy adatait az egykori megfigyelt megismerheti.

A biztos válaszában kifejtette, hogy a törvény elsődleges megközelítése szerint valóban joga lenne az egykori hálózati személynek megismerni, hogy ki tekintett bele a személyes adatait tartalmazó aktába. Az adatvédelem alapja azonban az Alkotmány, melynek 59. §-a mindenki számára biztosítja a személyes adatok védelméhez való jogot. Ennek értelmezéséhez szem előtt kell tartani az Alkotmánybíróság állandó gyakorlatát is, mely kimondja, hogy az emberi méltósághoz való jog oszthatatlan és redukálhatatlan. Ez a jog az emberi méltóság védelmének egyik nevesített eleme, ezért az érintett személyek jogainak ütközése esetén a védelemben elsőbbséget kell biztosítani az egykori megfigyelteknek, mivel az ő jogaikat – tekintettel az iratok keletkezésének idejére és körülményeire – súlyosan sértené az egykori megfigyelőknek nyújtandó tájékoztatás. Ezzel szemben az egykori megfigyelők méltóságán – a biztos véleménye szerint – e tájékoztatáshoz fűződő joguk korlátozása miatt érdemi sérelem nem esik. *(1438/K/2006)*

Közüzemi szolgáltatók

Az elmúlt három évhez hasonlóan idén is számos panaszbeadvány érkezett a közüzemi szolgáltatók adatkezelésével kapcsolatban.

A korábbi évekhez képest növekedett a panaszok száma, különösen a gázszolgáltatók adatkezelését kifogásolják az állampolgárok. A gázártámogatással kapcsolatos panaszok többségében az állampolgárok arról érdeklődnek, hogy jogszerű-e, hogy a gázszolgáltató, illetve a közös képviselő tudomást szerez az érintettek jövedelmi viszonyairól. Az erről szóló, 231/2006. (XI. 22.) Korm. rendelet tervezetét nem küldték meg az adatvédelmi biztos részére véleményezésre, ezért utólag, 2006. december 1-jén tette közzé álláspontját a rendelet szabályaira vonatkozó észrevételeiről.

> A biztos szerint egy bonyolult, nagy adminisztrációval járó rendszer jön létre, melyben sok adatkezelő (Magyar Államkincstár, APEH, közreműködő szerv, szolgáltatók, közös képviselők) vesz részt, az érintettek számára nehezen követhető az adataik sorsa és kezelésének módja. Az adatkezelés folyamatának részletei nincsenek átgondolva, nincs meghatározva például az adatkezelés időtartama. A kialakított szabályozás több szempontból sincs összhangban a törvényi előírásokkal.
>
> Nem célja az adatvédelmi biztosnak a támogatási rendszer működésének megakadályozása, azonban szükségesnek tartja a kialakított szabályozás felülvizsgálatát, újbóli áttekintését a hiányosságok kiküszöbölése érdekében. Javaslatot tett törvényi szabályozás előkészítésére úgy, hogy pontosan meg legyen határozva az adatnyilvántartás, az adatáramlás rendje, az adatkezelők tevékenysége. A törvényi szabályozási szintet indokolja az is, hogy nagy mennyiségű adatkezelésről és nagy állami nyilvántartás felállításáról van szó, az érintettek száma és a kezelendő személyes adatkör kiterjedt. A szabályozás felülvizsgálatától, annak törvényi szintre emelésétől a szociális és munkaügyi miniszter nem zárkózott el. *(1824/J/2006)*

Több állampolgár kifogásolta, hogy a TIGÁZ Zrt. oly módon kezeli az érintettek személyi igazolványának számát és telefonszámát, hogy nem tünteti fel az adatlapon az adatszolgáltatás önkéntes voltát, valamint az adatkezelés célját. A földgázellátásról szóló 2003. évi XLII. törvény 39. § (5) bekezdése ugyanis részletesen leírja, hogy a közüzemi fogyasztó közüzemi szerződésének milyen adatokat kell tartalmaznia.

> A biztos szerint az érintettek részére egy, a jelenleginél teljesebb, átfogóbb tájékoztatás nyújtása szükséges. Mindenképpen ki kell tér-

ni arra, hogy a két, a panaszosok által sérelmezett módon igényelt adat megadása önkéntes, és közölni kell az érintettekkel e két adat kezelésének a célját is, amely valóban lehet a fogyasztói elégedettség vizsgálata (telefonszám), illetve a közüzemi díjak hatékonyabb beszedése, behajtása (személyi igazolvány száma). Nem világos továbbá, hogy a TIGÁZ a közvélemény-kutató cégek részére történő adattovábbítást a fogyasztó előzetes hozzájárulásához köti-e. Az adatvédelmi biztos álláspontja szerint az ilyen adattovábbításhoz is mindenképpen kell az érintettek hozzájárulása.

A TIGÁZ Zrt. az állásfoglalást nem fogadta el, a biztost felhívták annak felülvizsgálatára. Az adatvédelmi biztos újabb levelében leszögezte: álláspontját változatlanul fenntartja. *(1571/A/2006)*

Ezzel szemben az ELMŰ és a Fővárosi Gázművek készségesen eleget tett az adatvédelmi biztos észrevételeinek a közüzemi felmondó nyilatkozatok adatkérésével kapcsolatban. Mindkét társaság kéri az érintettek telefonszámát, de annak céljáról (egyeztetések, kapcsolattartás) és önkéntes voltáról tájékoztatják az érintetteket. Az ELMŰ továbbá kéri a személyi igazolvány számát is, de az érintettek tudomására hozzák, hogy ennek megadása sem kötelező, ennek hiányában is elfogadják a szerződés felmondását.

A panaszosok továbbra is rendszeresen kifogásolják, hogy a közszolgáltatók a tulajdonosváltozásról való meggyőződés érdekében lefénymásolják az adásvételi szerződést, illetve egyéb, a tulajdonosváltozást igazoló dokumentumokat (hagyatéki végzés, halotti anyakönyvi kivonat, bérleti szerződés, stb.). Mivel a közszolgáltató az adatokat csak célhoz kötötten, a cél megvalósulásához elengedhetetlen mértékben kezelheti, ezért a törvényben előírt személyes adatokon túli adatkezelés jogellenes. A tulajdonosváltás hitelt érdemlő igazolását a szolgáltató megkövetelheti, de ennek kapcsán nem juthat olyan személyes adatok birtokába, melyek kezelése a cél eléréséhez szükségtelenek. A bemutatott dokumentumokról másolat úgy készíthető, ha azon csak a lényeges adatok látszanak, az egyéb adatokat a szolgáltató nem kezelheti. *(160/A/2006, 358/A/2006)*

Egy hulladékkezelést végző Kft. konzultációs kérelemmel fordult az adatvédelmi biztoshoz, melyben a társaságuk üzemeltetésében álló gyűjtő-szállító járművek kamerával való felszerelésével kapcsolatban kért állásfoglalást. A kamerás megfigyelést abból a

célból valósítanák meg, hogy társaságuk munkavállalóinak munkavégzését ellenőrizzék.

Adatkezelésnek minősül a fénykép-, hang-, vagy képfelvétel készítése is. Azon személyek esetében, akiket munkavállalóként kérnek fel ilyen hozzájárulás megadására, önkéntességről nem beszélhetünk, hiszen a munkavállalói viszony alárendelt helyzetéből következően az önkéntesség megléte aggályos. Ezért a munkavállaló megfigyelési célból való kamerázása jogszerűtlen. A munkavállaló munkájának kamerával való ellenőrzése azonban az előbbi indokon túl azért sem tekinthető jogszerűnek, mert az ellenőrzésnek ez a módja a munkavállaló alkotmányos alapjogait (jelen esetben elsősorban a személyes adatok védelméhez fűződő jogot) súlyosan és aránytalanul korlátozza. Az érintettek másik csoportja azoké, akik nem munkavállalók, de a kamerák látóterébe kerülve felvétel készülhet róluk. A tárgyalt esetben azonban – egy mozgó járműről lévén szó – nehezen kivitelezhető, hogy a kamerás megfigyelés tényéről való tájékoztatás az érintettekhez eljusson. Ennél a csoportnál hiányzik továbbá az adatkezelés célja is. A tervezett adatkezelés ezért az ismertetett feltételek mellett jogellenes. A munkavállalók ellenőrzésére nem megfelelő és jogszerű eszköz kamerás megfigyelésük. Jelen esetben a megfigyelést vagyon-, illetve élet-, és egészségvédelmi célok sem indokolják. *(1389/K/2006)*

Többen kifogásolták követelések kezelésével foglalkozó cégek, illetve a Díjbeszedő Rt. adatkezelését is.

A követelés-kezeléssel kapcsolatban a biztos állásfoglalásaiban kifejtette: a szolgáltató jogosult ezzel a tevékenységgel külön vállalkozást megbízni, de az adatok átadásához vagy törvény felhatalmazására vagy az érintett – akár szerződésben megadott – hozzájárulására van szükség. A követelés-kezeléssel foglalkozó társaság köteles arra, hogy az érintetteket megfelelő módon tájékoztassa. Ez utóbbi azért is fontos, hogy az ügyfél meggyőződhessen arról, hogy az őt megkereső társaság felé is rendezheti tartozását.

A vizsgálatok során megkeresett társaságok a biztos állásfoglalását elfogadták. *(658/A/2006, 946/A/2006)*

A Díjbeszedő Rt. tevékenységét kifogásoló panaszosokat a biztos tájékoztatta arról, hogy az rt. kizárólag adatfeldolgozást végez, döntéseket nem hoz a követelésekkel kapcsolatban. Az adatfeldolgozás törvényes, ha az adatvédelmi törvény szabályainak megfelelően történik. *(628/A/2006)*

Panaszosok kifogásolták, hogy az egyik gázszolgáltató kötelezi a fogyasztókat a gázmérő szekrények oly módon történő elhelyezésére, hogy azok a kerítésen keresztül leolvashatóak legyenek.

> A gázfogyasztás mértéke a kapcsolatba hozhatóság okán személyes adatnak minősül. Egy gázmérő bárki által leolvashatóan történő elhelyezése nyilvánosságra hozatalnak, ezért adatkezelésnek minősül. Jelen esetben a társaság törvényi felhatalmazás nélkül kötelezi egy személyes adat nyilvánosságra hozatalára a fogyasztókat, ezért ezen adatkezelés jogalapja csak a fogyasztók hozzájárulása lehet, de csak abban az esetben, ha számukra felkínálnak olyan elhelyezési lehetőséget is, amelynek során gázfogyasztásukról nem tájékozódhat bárki. *(1176/A/2006)*

Érdeklődtek az állampolgárok annak jogszerűsége felől is, hogy egyes közüzemi szolgáltatók mellékelhetnek-e reklámanyagokat a számlalevelek mellé.

> Az nem kifogásolható, ha a közüzemi szolgáltató a saját szolgáltatásához kapcsolódó reklámokat küld ki a számlalevél mellékleteként. Ugyanis a közüzemi szerződés megkötése során a közüzemi szolgáltató arra vállalt kötelezettséget, hogy az ügyfél számára megfelelő szolgáltatást nyújtson. Amennyiben a szolgáltató a mellékelt reklámok segítségével tájékoztatja az ügyfeleket a közüzemi szolgáltatás fejlesztéséről vagy valamilyen újdonság bevezetéséről, akkor ez az ügyfél érdekét is szolgálja, hiszen a szolgáltatás megfelelő színvonala ezáltal is jobban biztosítható.
>
> Az olyan reklámanyagok küldésére azonban törvény nem ad felhatalmazást, amelyek nem a fenti célt szolgálják, ezért – az érintett hozzájárulásának hiányában – az ilyen küldemények továbbítása jogellenes adatkezelési tevékenységnek minősül. *(913/A/2006)*

Volt olyan panaszos, aki azt kifogásolta, hogy egy budapesti szolgáltató havi számláit boríték nélkül dobja be a postaládájába.

> Az Avtv. előírásainak csak olyan számlaforgalmi szabályozás felel meg, amely garantálja, hogy a szolgáltató által kézbesített számlákon szereplő személyes adatokat csak az arra feljogosított személyek továbbíthatják, és azokhoz illetéktelen személyek nem férhet-

nek hozzá. E követelményeket az biztosíthatja, ha a kézbesítő személy zárt borítékban juttatja el a számlákat az állampolgárokhoz.

Természetesen a szolgáltatás teljesítése és az ehhez kötődő számlázási eljárás során a személyes adatokhoz hozzáférő személyeket titoktartási kötelezettség terhel minden, a tudomásukra jutó személyes adat tekintetében. *(1159/A/2006)*

Társasházak, lakásszövetkezetek

Az elmúlt évben tekintélyes számban érkeztek beadványok a társasházak, illetve lakásszövetkezetek adatkezelésével kapcsolatban. Mindenképp figyelemre méltó jelenség ez, hiszen 1997 óta az e témában érkező panaszok aránya nem érte el azt a szintet, amely indokolta volna a társasházak külön fejezetben való tárgyalását. Az azóta eltelt időben az Országgyűlés elfogadta a társasházakról szóló 2003. évi CXXXIII. törvényt (továbbiakban: Tht.) és a lakásszövetkezetekről szóló 2004. évi CXV. törvényt (továbbiakban: Lszt.). Ugyanakkor sem a lakásszövetkezetekre, sem a társasházakra vonatkozó szabályozás nem járja át kellő körültekintéssel a személyes adatok kezelésére vonatkozó szabályokat, így az állampolgárok által feltett kérdések megválaszolásánál az adatvédelmi törvény szabályozását kell alapul venni.

Talán az egyik legtöbbször felmerülő probléma a közös költséggel tartozók nevének nyilvánosságra hozatala, kifüggesztése. A panaszok egy részénél a közös képviselő kért előzetes tájékoztatást arról, van-e arra lehetőség, hogy a lakók a tájékoztató levél mellékleteként megkapják a nemfizetők listáját, valamint olyan panaszok is előfordultak, ahol a már kifüggesztett listát kifogásolták az érintettek.

Arról, hogy a társasházban, illetőleg a lakásszövetkezetben tulajdonnal rendelkezők milyen formában ismerhetik meg a közös költségek vagy a kommunális kiadások viselésében hátralékkal rendelkezők személyét, 1996-ban a biztos ajánlást adott ki. Bár az ajánlás kiadásakor még a korábbi társasházi törvény volt hatályban, az adatkezelésre vonatkozó megállapítások ma is irányadóak. A panaszosokat ezekben az ügyekben a biztos arról tájékoztatta, hogy a nem fizető, illetőleg a hátralékkal rendelkező tulajdonostársak személyére vonatkozó adatokat törvényi felhatalmazás hiányában nem lehet nyilvánosságra hozni, azokat csak az érintett tulajdonostársak ismerhetik meg. A Tht. 28. §-a szerint az éves elszámolás el-

fogadásáról a közgyűlés határoz. Szükségszerű tehát, hogy az éves elszámolás benyújtásakor, illetve annak elfogadása érdekében a közgyűlés megismerhesse az elszámolásban szereplő adatokat, így a közös költségekhez való hozzájárulás előírását és teljesítését a tulajdonostársak nevének feltüntetésével. Ekkor tehát a közgyűlés tagjainak, vagyis a tulajdonostársaknak van lehetőségük arra, hogy megismerjék azt, hogy név szerint melyik tulajdonostársnak mennyi közös költség hátraléka van. Ez történhet például a könyvelés megtekintésével, vagy úgy, hogy zárt (kizárólag a tulajdonostársak részvételével megtartott) közgyűlésen ismertetik a hátralékkal rendelkező tulajdonostársak nevét. Amennyiben a közös költség fizetésében hátralékkal rendelkező tulajdonostársak adatait ily módon ismertették, nem állapítható meg jogsérelem. *(184/A/2006, 287/A/2006, 591/A/2006, 776/K/2006, 1484/A/2006, 1813/A/2006, 1818/A/2006, 1966/K/2006)*

A beadványok másik nagy csoportjában azon panaszok álltak, amelyben az érintett a társasházban működő kamerák működését kifogásolta, vagy a kamerák működtetésének jogszerűségével kapcsolatban kért állásfoglalást.

A kamerák telepítésének legfőbb okaként általában a betörések elleni védekezést jelölték meg a társasházi közös képviselők. Sok esetben a kamerarendszert a felvételek rögzítése nélkül egyfajta elijesztő, megelőző funkció betöltésére használnák a lakóközösségek vagyonuk védelme érdekében. A kamerás megfigyelés útján számos személyes adat birtokába jut a megfigyelő rendszer üzemeltetője, sok esetben azonban nem minden lakó járul hozzá ahhoz, hogy ilyen jellegű, rájuk vonatkozó adatokat megismerjenek, tároljanak. A kamerás rendszer üzemeltetője a rögzítés révén adatkezelővé válik, tevékenysége akkor jogszerű, ha ahhoz az érintett hozzájárul, vagy azt törvény elrendeli.

Törvényi felhatalmazás hiányában az adatkezeléshez az érintettek hozzájárulására van szükség: minden lakónak szükséges a hozzájárulása ahhoz, hogy a közös használatú magánterületen, mint amilyenek a garázs, illetve a bejárati ajtók előtti tér, képfelvételeket rögzíthessen a rendszer, valamint jól látható, még a belépés előtt elolvasható helyre el kell helyezni azt a figyelmeztetést, hogy az adott területet kamerával figyelik. Ezen felül tájékoztatást kell adni az érintett kérésére az adatkezelés minden részletéről. Fontos még, hogy a kamera látómezeje nem irányulhat közterületre. A kizárólag

saját tulajdonában, illetve használatában álló területen a lakó végezhet megfigyelést, de akkor is megfelelő módon fel kell hívnia az odalátogatók figyelmét az adatkezelés tényére, és tájékoztatást kell adnia a fentebb ismertetett körülményekről. *(99/A/2006, 533/A/2006, 864/K/2006, 1099/A/2006, 1907/K/2006)*

Az Lszt. adatvédelem terén mutatkozó hiányosságaira utal egy már 2003 óta húzódó ügy, amely szintén az adatkezelés szabályozatlanságából indult ki. A vizsgálat ugyan 2006-ban lezárult, de az idáig vezető út sokkal rövidebb lett volna, ha van a háttérben egy olyan törvényi szabályozás, amely maradéktalanul megoldást jelent minden olyan felmerülő problémára, amely az állampolgárok igazságérzetét e témakörben sérti.

A panaszos egy garázsszövetkezet által üzemeltetett ki- és beléptető rendszer jogszerűségét kifogásolta. Panaszában leírta azt, hogy kamerákat szereltek fel minden egyes garázs előterébe, melyek segítségével rögzítették az érkező járművek rendszámát, valamint azok indulási és érkezési idejét. Az így nyert adatokról készített nyilvántartás rendőrség részére történő továbbításáról is döntés született. A biztos állásfoglalása tartalmilag nem tért el a fentebb már leírt, a kamerák üzemeltetése kapcsán kialakított álláspontól. A szövetkezet először felfüggesztette az adatrögzítést, majd a közgyűlésük egyik határozatára hivatkozva újra működtetni kezdte a garázstelep kapurendszerének számítógépes nyilvántartását. Az ügyvezető válasza szerint a közgyűlés döntése valamennyi tagra kiterjedő hatállyal bír, és a közgyűlés hatáskörébe tartozik a létesítmény használatáról való döntés, illetve a testület döntése ellen tiltakozást senki nem jelentett be, és az nem törvénysértő. A közgyűlés valóban szabályozhatja a beléptető rendszert, illetve annak használatát, azonban ez csak a hatályos jogszabályok betartásával történhet. Mind a testület döntése, mind a szövetkezet működése törvénysértő, mivel nincs tekintettel az adatvédelmi törvény előírásaira. A közgyűlés csak abban az esetben dönthet személyes adatok kezeléséről, ha valamennyi szövetkezeti tag jelen van és beleegyezik az adatkezelésbe, ez azonban több száz fős taglétszámnál gyakorlatilag lehetetlen. A kapurendszer működéséről a tagoknak adott tájékoztatás nem elegendő, a *„hallgatás beleegyezés”* módszer nem megfelelő, mivel az adatkezeléshez történő hozzájárulásnak csak az érintett önkéntes, kifejezett, félreérthetetlen beleegyezése tekinthető. Személyes adatok kezelésének másik módja, ha törvény

rendelkezik erről. Az Lszt. nem tartalmaz olyan szabályt, amely a kifogásolt adatkezelést előírná, csupán a 43. §-ban meghatározott személyes adatok kezelését teszi lehetővé a tulajdonosok, bérlők nyilvántartása céljából. Mindezek alapján megállapítható volt, hogy a szövetkezet beléptetési rendszerének működtetéséhez – azokat kivéve, akik ehhez kifejezetten hozzájárultak – nincs megfelelő jogalap, és a szövetkezet adatkezelése jogellenes. *(532/A/2006)*

A társasházakkal, illetőleg a lakásszövetkezetekkel kapcsolatos beadványok egy részében az érintettek arról kértek tájékoztatást, hogy mely felhatalmazás alapján, illetőleg mely cél elérése érdekében lehet a lakókról lakónyilvántartást vezetni.

A Tht. 22. §-a alapján a szervezeti-működési szabályzat előírhatja, hogy a tulajdonostárs köteles a közös képviselőnek vagy az intézőbizottság elnökének bejelenteni egyes adatokat (többek között az ingatlan-nyilvántartás nyilvános adatait), melyekről a közös képviselő vagy az intézőbizottság elnöke nyilvántartást vezethet; a törvény a kezelhető adatkört és az adatszolgáltatás szabályait is pontosan meghatározza. Vagyis a szervezeti és működési szabályzat a jogszabállyal összhangban rendelkezhet lakónyilvántartás vezetéséről, de az adatkör nem haladhatja meg a törvényben meghatározottakat. Így például a tulajdonostársaktól nem igényelhető születési helyük, ideiglenes lakcímük, munkahelyük, adóazonosító jelük, taj-számuk, telefonszámuk. *(174/A/2006, 604/A/2006, 708/K/2006, 1358/A/2006, 1441/A/2006)*

Nem egy olyan beadvány érkezett, melyben a panaszok alapja az volt, hogy a társasházban lakóknak joguk van-e megismerni az egyedi vízórával rendelkező lakók fogyasztására vonatkozó külön adatokat. A társasház összes fogyasztása megismerhető, azonban az megtudható-e, hogy adott hónapban ki, milyen mennyiséget fogyasztott és ezért mennyit fizetett? Van-e erre törvényi felhatalmazás, illetve alátámaszthatja-e ezt bármilyen jogszerű cél?

Az adatvédelmi törvény alapján megállapítható, hogy a közüzemi szolgáltatás igénybevételekor a lakók vízfogyasztásának mennyisége, illetve a fogyasztásért fizetendő összeg nagysága személyes adatnak minősül, amely az érintett hozzájárulása hiányában törvény felhatalmazása alapján kezelhető. A Tht. erre vonatkozó felhatalmazást nem ad, ugyanakkor előírja, hogy a szervezeti-működési

szabályzatnak tartalmaznia kell a tulajdonostárs külön tulajdonának használatára, hasznosítására, a külön tulajdonon belül nem mérhető közüzemi és más szolgáltatások díjának elszámolására és megfizetésére vonatkozó szabályokat.

A fentiek alapján elmondható, hogy a társasház szervezeti-működési szabályzatában kell meghatározni azokat a mérési és elszámolási szabályokat, melyek alapján az egyes lakásokra jutó vízfogyasztási költségeket meg lehet állapítani. Az egyéni fogyasztást a társasház teljes vízfelhasználásának értékéből különböző arányszámokkal lehet kiszámolni, ami függhet az egyes lakásokban lakók számától, és/vagy a lakás alapterületétől. Mivel a társasház egészére jutó vízfelhasználási mennyiség, az egyes külön tulajdonú lakások területe, valamint az arányszámok minden tulajdonostárs számára megismerhetőek, ezért elvileg kiszámítható az egyes tulajdonosok által felhasznált víz és az ezért fizetendő összeg. Azonban a tényleges értékek ettől eltérhetnek, és ezek az értékek olyan személyes adatnak minősülnek, melyek csak az érintett hozzájárulásával ismerhetőek meg.

Összefoglalva megállapítható, hogy törvény nem ad lehetőséget arra, hogy akár a közös képviselő, akár valamelyik tulajdonostárs hozzáférjen az egyéni (tényleges) vízfogyasztásra vonatkozó adatokhoz. Továbbá akkor sincs lehetőség az egyes lakásokban felszerelt mérőórák leolvasására, ha a társasház szervezeti és működési szabályzata vagy határozata rendelkezik róla, mivel ezek elfogadásához csak egyszerű szavazattöbbség szükséges, és így az ellenzőktől nem kényszeríthető ki, hogy beengedjék a leolvasót a lakásba. *(1512/A/2006)*

Egyházak

Az elmúlt évek beszámolói közül eddig mindössze kétszer – 1997-ben és 1998-ban – foglalkoztunk külön alfejezetben az egyházak adatkezeléseivel, meglehetősen rövid terjedelemben. 2006-ban azonban több olyan beadvány érkezett, amely azt mutatta, hogy az egyházak mint adatkezelők esetében is felmerülnek olyan vitás kérdések, melyek igénylik a biztos közreműködését. Fontos kiemelni, hogy az ügyek nagy része nem panaszügyeken alapult, elsősorban egyházi vezetők, tisztségviselők fordulnak a biztoshoz állásfoglalást kérve. Ezzel kapcsolatban érdemes megjegyezni, hogy 2005-ben, a Szcientológia Egyház adatkezelésének vizsgálata során többen vitatták annak lehe-

tőségét, hogy az adatvédelmi biztos vagy más állami szerv vizsgálhassa az egyházak tevékenységét.

Az ilyen jellegű ügyek kapcsán a biztos mindig szem előtt tartotta azt, hogy hazánkban a vallás szabadsága alkotmányos alapjog, amely magában foglalja az egyházak szabad működését is. Az alkotmányos alapjogoknak ugyanakkor egymásra tekintettel kell érvényesülniük, így a személyes adatok védelméhez való jogot az egyházak adatkezelései tekintetében is biztosítani szükséges; az adatvédelmi biztosnak pedig jogában áll bármilyen adatkezelést megvizsgálnia, sőt, állampolgári beadvány esetén ez kötelessége. A vizsgálatok egyikének sem lehetett és nem is volt tárgya az egyházak hitéleti tevékenysége, és nem érintették az egyház önmeghatározását, küldetésével kapcsolatos kérdéseket.

Ez az elv megjelenik az adatvédelmi törvényben is, amely szerint nem kell bejelenteni az adatvédelmi nyilvántartásba azt az adatkezelést, amely egyház, vallásfelekezet belső szabályai szerint történik – ebbe a körbe tartoznak elsősorban a hitéleti tevékenységgel összefüggő nyilvántartások. Minden olyan adatkezelés azonban, amely más törvényen, esetleg speciális jogviszonyon alapul, nem mentes a bejelentési kötelezettség alól.

> Több konzultációs kérdés érkezett az adatvédelmi biztoshoz az adományok, közcélú adományok utáni kedvezmény igénybevételére jogosító igazolások kapcsán. Az igazolás kiadásának szabályait az Szja tv. tartalmazza, amely meghatározza annak tartalmát, felhasználásának módját is. Az igazolásokhoz kapcsolódó adatkezelés így nem az egyház belső szabályain, hanem az Szja tv.-n alapul, vagyis azt be kell jelenteni az adatvédelmi nyilvántartásba. *(81/N/2006)*

Több beadvány érintette az egyházak kezelésében lévő, levéltári anyagnak minősülő dokumentumok, nyilvántartások kezelését. Ebben a körben elsősorban a különböző egyházi anyakönyvek (melyek a születéssel, kereszteléssel, házasságkötéssel, elhalálozással stb. kapcsolatos adatokat tartalmazzák) kezelése, illetve az egyes adatok törlésére vonatkozó kötelezettség kérdéses.

> Egy konzultációs ügy kapcsán az adatvédelmi biztos leszögezte: levéltári anyag nem csak levéltár birtokában lehet. Az Ltv. alapján az a nem közfeladatot ellátó szerv, amely a tulajdonában vagy birtoká-

ban lévő maradandó értékű iratainak tartós megőrzése céljából levéltárat létesít, vagy tart fenn, és vállalja a törvényben foglalt követelmények teljesítését, a kultúráért felelős miniszternél kezdeményezheti magánlevéltárának nyilvános magánlevéltárként történő bejegyzését. A nyilvános magánlevéltárként történő bejegyzést a miniszter engedélyezi. Ha valamely egyház vagy egyházi jogi személy a törvényben előírt követelményeket nem teljesíti, iratanyaga nem minősül nyilvános magánlevéltárnak. Az egyes iratok ugyanakkor ettől függetlenül tekinthetők maradandó értékű iratnak, amelyek őrzésére vonatkoznak az Ltv. szabályai. Az egyházi anyakönyvek – tekintettel azok tudományos jelentőségére – esetében mindenképpen indokolt a kiemelt védelem, ezen belül az is, hogy elhelyezésük, védelmük, kutatásuk az Ltv. hatálya alá tartozzon. Ennek érdekében az egyházaknak, egyházi jogi személyeknek célszerű kezdeményezni nyilvános magánlevéltár létesítését. Ennek kapcsán fontos hangsúlyozni, hogy az iratok nem kerülnek ki az egyház birtokából, tulajdonából. *(1532/K/2006)*

A levéltári anyagok esetében máshogy alakulnak a személyes adatok kezelésére vonatkozó kötelezettségek is. Az Avtv. meghatározza azokat az eseteket, amikor az adatkezelő az adatokat törölni köteles (pl. az érintett azt kéri, vagy az adatkezelés célja megszűnt). A törlési kötelezettség ugyanakkor – a jogellenes adatkezelés kivételével – nem vonatkozik arra a személyes adatra, amelynek adathordozóját levéltári őrizetbe kell adni. Így a levéltári anyagnak minősülő egyházi anyakönyvek esetében az érintett nem kérheti adatai törlését. *(1208A/2006)*

A fentiek kapcsán hangsúlyozni kell, hogy a maradandó értékűnek nem tekinthető és levéltári őrizetbe nem kerülő dokumentumban a törlési kötelezettség továbbra is fennáll; ugyanez a helyzet akkor is, ha az adatkezelés jogellenes. Ennek lehetséges esete az, ha az egyház tagjaitól más személyekre vonatkozóan az érintettek hozzájárulása nélkül gyűjt adatokat, vagy tagjaira vonatkozóan azok tudta nélkül kezel személyes adatokat. *(1145/K/2006)*

Egy állampolgár a Magyarországi Evangélikus Egyház Országos Közgyűlése által létrehozott Tényfeltáró Bizottság adatkezelésével kapcsolatban kérte a biztos állásfoglalását. A Tényfeltáró Bizottság az egyház múltjának feltárását célzó levéltári kutatás eredményéről tájékoztatni kívánta a közvéleményt.

> Az adatvédelmi törvény alapján a tudományos kutatást végző szerv vagy személy személyes adatot csak akkor hozhat nyilvánosságra, ha az érintett abba beleegyezett, vagy az a történelmi eseményekről folytatott kutatások eredményeinek bemutatásához szükséges. A kutatásokra vonatkozóan erre a szabályra utal az Ltv., illetve az elmúlt rendszer titkosszolgálati tevékenységének feltárásáról és az Állambiztonsági Szolgálatok Történeti Levéltára létrehozásáról szóló 2003. évi III. törvény (továbbiakban: Ásztltv.) is. Az Ásztltv. alapján a közszereplőkre vonatkozó, illetve közszereplésekkel kapcsolatos egyes személyes adatok nyilvánosságra hozhatóak.
>
> A közszereplői minőség eldöntése – az érintett nyilatkozatának függvényében – elsősorban a kutatást engedélyező levéltár kompetenciájába tartozik, vita esetén a döntés a bíróság feladata. Az adatvédelmi biztos tehát nem foglalhat állást abban a kérdésben, hogy az egyházi személy közszereplőnek tekinthető-e. A probléma alapvetően a törvényből fakadó értelmezési nehézségekből adódik, amelyekre az adatvédelmi biztos 2003. december 15-én kiadott ajánlásában felhívta a jogalkotó figyelmét. *(879/K/2006)*

2006-ban a legnagyobb nyilvánosságot kétségkívül a Szcientológia Egyház által alkalmazott e-méter adatvédelmi kérdéseiről kiadott ajánlás kapta. A vizsgálat során az egyház vitatta a biztos hatáskörét a lelkiismereti és vallásszabadságra hivatkozva. Ezzel kapcsolatban a biztos kifejtette, hogy az Avtv., illetve az Alkotmánybíróság határozatai alapján hatáskörébe tartozik a személyes adatok védelméhez fűződő jog gyakorlásának és érvényesülésének garanciáit a vallási tárgyú adatkezelések vonatkozásában meghatározott korlátok között vizsgálni. A biztos e korlátokat tiszteletben tartotta, amint arra a kiadott állásfoglalás is utal: „*Az adatvédelmi vizsgálat a vallásszabadság tiszteletére és az állam tartózkodási kötelezettségére tekintettel nem terjedt ki olyan tartalmi kérdések vizsgálatára, amelyek a lelkiismereti meggyőződés és vallásos hit igazságtartalmára vonatkoznak, és amelyek az egyház önértelmezését érintik.*”

> A vizsgálat elsősorban az úgynevezett elektro-pszichometer, vagy e-méter néven ismert eszköz használatára irányult. Az eszközt az auditálási tevékenységgel összefüggésben használják. Az auditálás során a lelkész – vagy más néven auditor – olyan speciális kérdések sorát teszi fel a hívőknek, amely a lelki szenvedés egy meghatározott, a konkrét ülés alatt kezelendő területére vonatkoznak. Az

auditornak ehhez segítségére van egy különlegesen tervezett mérőműszer, az e-méter, amely az egyén állapotát vagy állapotváltozását méri, a kezében tartott elektródák segítségével.

A vizsgálat kiterjedt az érintettek által adott – korlátozásoktól mentes – hozzájárulás érvényességére is, különös tekintettel a tájékoztatás követelményére, valamint a tájékoztatáshoz való jogra.

Állásfoglalásában az adatvédelmi biztos felhívta az egyház vezető szerzetesének és titkárának figyelmét a jogszerű adatkezelés követelményeire, ezen belül a hozzájárulás érvényességének feltételeire és az érintett tájékoztatására vonatkozó kötelezettségre. Az állásfoglalás teljes terjedelmében a honlapon olvasható. *(732/A/2005)*

A vizsgálat során felmerült az e-méter hazugságvizsgálóként való alkalmazásának lehetősége is, melyre vonatkozóan a Nemzeti Nyomozó Iroda Bűnügyi Főosztálya adott szakvéleményt. Az egyház a szakvéleményt még a vizsgálat lezárása előtt kérte, kiadását azonban a biztos – az adatvédelmi törvény döntést megalapozó adatokra vonatkozó szabályai alapján – megtagadta. A szakvélemény – mint közérdekű adat – kiadása iránt az egyház keresetet nyújtott be a Fővárosi Bírósághoz. A bírósági eljárás részleteit és kimenetelét az adatvédelmi biztos pereiről szóló fejezet ismerteti.

További érdekes ügycsoportok

Az őszi zavargások kapcsán felmerült adatvédelmi kérdések

Megfigyelhető, hogy szinte minden, a közvéleményt foglalkoztató eseményhez, folyamathoz kapcsolódnak adatvédelmi kérdések. Bár ezt a kijelentést sokan kétségbe vonják, a szeptember-októberi fővárosi zavargások tökéletesen igazolják helytálló voltát.

A zavargásokról – melyek a Magyar Televízió székházának *„ostromával"* kezdődtek, és az október 23-i történésekben tetőztek – számos vélemény, értékelés látott napvilágot. Az adatvédelmi biztosnak azonban csak annyi lehet a feladata, hogy a felmerülő adatvédelmi kérdésekben állást foglaljon. Az ilyen események kapcsán ez azért nehéz, mert az egymással szemben álló vélemények olyan határozottan elkülönülnek, hogy bármilyen, valamelyik oldalt igazoló állásfoglalás –

még akkor is, ha az pusztán szakmai alapokon nyugszik – óhatatlanul politikai színezetet kap a közvélemény szemében. Hasonló a helyzet a választási kampányhoz kapcsolódó adatkezelésekkel is: ha valamelyik pártot a biztos elmarasztalja, azt a másik oldal saját igaza bizonyításának véli. A választások kapcsán azért egyszerű megelőzni azt, hogy bárki politikai elfogultsággal vádolja a biztost, mert a szemben álló pártok szinte mindegyike okot ad a fellépésre. A zavargások kapcsán felmerült adatvédelmi kérdések szintén mutatnak hasonló megoszlást: a biztosnak éppúgy fel kellett lépnie az állampolgárok, mint a rendőrök, bírák jogainak védelmében.

A legnagyobb nyilvánosságot kétségkívül a rendőrség által a kórházaknak küldött megkeresés kapta. A vizsgálat azzal indult, hogy a Budapesti Rendőr-főkapitányság több kórháznak elküldte azt a levelét, amelyben az *„október 23-ról 24-re virradó éjszaka folyamán, a Budapest területén történt zavargások során sérüléseket szenvedett”* személyek adatait kérte. Az első megkeresést két másik is követte, és az ügy nehezen jutott nyugvópontra.

> Az első megkeresést követően a biztos közleményt bocsátott ki, amelyben leszögezte: *„A […] rendőrségi levél sem a rendőrségi megkeresésekre vonatkozó formai, sem a tartalmi törvényes kritériumoknak nem felel meg, ezért ennek az adatszolgáltatásnak a kórház részéről történő teljesítése egyértelműen sértené a betegek személyes és különleges adatai védelméhez fűződő alkotmányos jogát”*. Ezt követően a rendőrség újabb megkeresést küldött, melyben megnevezték azt a bűncselekményt, amelyben a nyomozást folytatják, megjelölték az adatszolgáltatás jogalapját (Be. 71. §), valamint a kért adatokat (2006. október 23-án 00.00 óra és 2006. október 24-én 08.00 óra közötti időben ellátásra jelentkezett személyek neve, születési helye és ideje, anyja neve, lakcíme). Az adatkérésre nézve három törvény is tartalmaz szabályokat (az adatvédelmi törvény, az egészségügyi és a hozzájuk kapcsolódó személyes adatok kezeléséről és védelméről szóló 1997. évi XLVII. törvény, valamint a Be.), közös vonás azonban, hogy mindhárom jogszabály kiemelt jelentőséget tulajdonít annak, hogy a büntetőeljárással összefüggésben különleges adatok csak a célhoz kötöttség elvének szigorú betartásával kezelhetők.
>
> A második megkeresés a célt *„büntetőeljárásban való felhasználás”*-ként jelölte meg, amely túlságosan tág meghatározás. Nem fe-

lelt meg a megkeresés az adatminimum követelményének sem, mely szerint csak az elengedhetetlenül szükséges adatok kérhetők. Egyrészt túl hosszú a megjelölt időintervallum, másrészt nincsenek megkülönböztetve az ellátott betegek: a rendőrség valamennyi ellátásra jelentkezett személy adatait kérte, ide értve azon érintetteket is, akik semmilyen módon nem hozhatóak kapcsolatba a büntetőeljárás alapjául szolgáló bűncselekményekkel. Vagyis az adatszolgáltatás teljesítésével a rendőrség megkapta volna az otthoni sérüléssel, egyéb megbetegedéssel kezelt beteg adatait éppúgy, mint a gumilövedék okozta sérüléssel kezelt beteg adatait; de az érintetti kör kiterjedne a pár hónapos csecsemőre és a nyolcvan éves mozgáskorlátozott állampolgárra is.

A harmadik alkalommal elküldött megkeresés már megfelelt a vonatkozó törvényeknek, erről az adatvédelmi biztos tájékoztatta a kórházak vezetőit – akik a korábbi megkeresések alapján az adatszolgáltatást a betegek jogainak védelme érdekében megtagadták. Ezt követően is számos levél érkezett, melyekben a polgárok aggodalmukat fejezték ki. Ezek kapcsán a biztos leszögezte: ha olyan információ jut tudomására, amely szerint a rendőrség az átvett adatokat a megjelölt céltól (tanúk felkutatása) eltérően használja fel, és a tanúként beidézett személyek ellen sorozatban indít büntetőeljárást, fel fog lépni a polgárok jogainak védelmében. *(1734/A/2006)*

Szintén a rendőrség eljárását érintette egy másik vizsgálat, mely azokon a bejelentéseken, tájékoztatókon alapul, melyek szerint a rendőrség, illetve a büntetés-végrehajtás egyes intézményeiben működtetett kamerák felvételeiről az érintettek kérésre nem kaptak semmilyen tájékoztatást, számukra a betekintést megtagadták azzal az indokkal, hogy a kamerák a kérdéses intézményekben nem működtek. A kérdéses ügyekben az érintettek azért kérték a felvételeket, mert azokat bizonyítékként akarták felhasználni a rendőrség ellen indítandó eljárásokban – erre ugyanis az információs önrendelkezési jog alapján lehetőségük van. A vizsgálat során egyik fél igazát sem sikerült bizonyítani. Ennek oka részben az, hogy a térfigyelő rendszerekre vonatkozó szabályozás hiányos, a gyakorlat pedig nem minden esetben következetes *(1713/H/2006)*. E vizsgálat tapasztalatait is felhasználja az a hivatalból indított vizsgálat, amely a térfigyelő rendszerek hazai alkalmazására, annak jogi hátterére irányul.

Nagy nyilvánosságot kapott az az ügy is, amely a www.kuruc.info honlap adatkezelését érintette. A honlapon bírák, ügyészek neve, lakóhelye, otthoni telefonszáma, mobiltelefonszáma olvasható.

> A kérdéses adatok közül a bírák, ügyészek neve, beosztása, szolgálati helye nyilvános, bárki által megismerhető adat; az egyéb adatok azonban személyes adatnak minősülnek, így nyilvánosságra hozataluk – törvényi rendelkezés hiányában – csak az érintettek hozzájárulásával lett volna jogszerű. A jogellenes adatkezelés tényén az sem változtat, hogy egyes adatok más formában – például telefonkönyv vagy az egyik érintett esetében egy állatvédő szervezet honlapja útján – nyilvánosak. Ebben az esetben az adatok ugyanis nem a bíró, ügyész tevékenységével összefüggő adatok, és az újbóli nyilvánosságra hozatal vagy egyéb felhasználás csak az eredeti céllal megegyező cél esetében jogszerű. A honlap adatkezelésének a célja ettől nyilvánvalóan eltér, így ezen adatok jelen formában történő közzététele ugyancsak jogellenes.

A vizsgálat során azért nem sikerült eredményt elérni, mert a honlap nem hazai szerveren található, az impresszumban megadott adatok pedig nem valósak. A nyilvánosságra hozott adatok között szerepelt egy olyan állampolgáré is, aki semmilyen formában nem volt érintett, de neve megegyezett egy bíróéval. A panaszos emiatt számos zaklató hívást, fenyegetést kapott. Adatait a honlapról később eltávolították. *(1570/A/2006, 1578/K/2006, 1579/A/2006, 1580/A/2006, 1583/A/2006, 1675/A/2006)*

Végezetül említést kell tenni a Független Rendőr Szakszervezet által kezdeményezett konzultációról is. A szakszervezet azért kereste meg az adatvédelmi biztost, mert az őszi zavargások kapcsán egy kiállítást kívánt szervezni a Rendőrség-történeti Múzeumban. A kiállításhoz fel kívánták használni az egyes sajtótermékekben megjelent fényképeket is, melyek közül több azonosíthatóan mutatta a rendzavarókat, békés tüntetőket, rendőröket, mentősöket. A biztos munkatársai a szakszervezet munkatársaival közösen nézték át az összegyűjtött képeket, biztosítva azt, hogy a kiállítással senkinek ne sérüljön a személyes adatai, képmása védelméhez való joga. A kiállítás ezt követően *„A pajzs mögött”* címmel megnyílt az érdeklődők számára.

A választások kapcsán felmerült adatvédelmi kérdések

A választások adatvédelmi aspektusból is kiemelkedő jelentőségűek, hiszen a kampányidőszakban akár több millió választópolgár személyes adatai kerülhetnek a pártok, jelölő szervezetek és jelöltek birtokába. Az idei esztendőben megtartott országgyűlési és önkormányzati választások előtt, mintegy az esetleges jogsértéseket megelőzendő, az adatvédelmi biztos közleményben hívta fel a jelölő szervezetek és választópolgárok figyelmét a politikai kampány adatvédelmi kérdéseivel kapcsolatos fontosabb tudnivalókra. A közlemény aktualitását a közelgő választások mellett az adatvédelmi biztosok Montreux-ben (Svájc) 2005 szeptemberében a személyes adatok politikai célból történő felhasználása tárgyában elfogadott határozata adta.

A montreux-i határozat kidolgozásánál a biztosok abból a tényből indultak ki, hogy a kampányeszközök köre és módszerei világszerte sokat változtak. A politikai szervezetek különböző kommunikációs stratégiákat használnak azért, hogy minél több adatalannyal közvetlen és személyre szabott kapcsolatot alakítsanak ki.

> A montreux-i határozatban foglaltak szerint a személyes adatokat a pártok nagy mennyiségben – néha agresszív módon – folyamatosan gyűjtik különböző technikák alkalmazásával – közvéleménykutatás, software-kereső eszközön keresztül e-mail címek gyűjtése, városon belüli korteskedés vagy interaktív TV-n keresztül – ilymódon élve a politikai véleményformálás eszközével. Az adatok néha jogosulatlanul tartalmaznak valós (levelezési címek, telefonszámok, e-mail postafiókok, szakmai tevékenységgel kapcsolatos információk és családi kapcsolatok mellett) vagy feltételezett erkölcsi és politikai meggyőződésre utaló, illetve szavazási tevékenységre utaló különleges adatokat. A különböző személyekről tolakodó módszerek alkalmazásával olyan képet állítanak fel, melynek alapján őket – néha alaptalanul – szimpatizánsként, támogatóként, párttagként tüntetik fel, hogy saját politikai céljaik eléréséhez fokozni tudják az állampolgárokat megcélzó kommunikáció hatékonyságát. A határozat kimondja, hogy minden politikai kommunikációs tevékenység során – ideértve a választási kampányhoz nem kötődő tevékenységeket is –, mely együtt jár személyes adatok kezelésével, tiszteletben kell tartani az érdekelt személyek alapvető jogait és szabadságait, ideértve a személyes adatok védelméhez való jogot és az elfogadott adatvédelmi alapelveket.

A határozat nyomán született közleményben az adatvédelmi biztos kiemelten foglalkozott a telefonon, az e-mailen és az sms-ben folytatott kampány adatvédelmi kérdéseivel.

> A vonatkozó törvényi szabályok – Eht., Elkertv. – egyértelmű szabályokat tartalmaznak. Véletlenszerűen választott számok alapján bonyolított hívások csak abban az esetben megengedhetők, ha a szolgáltató olyan adatbázist használ a hívások alapjául, mely azon előfizetők adatait tartalmazza, akik a fentiek szerint hozzájárultak adataik ilyen célú felhasználásához. Egyéb módon közvetlen üzletszerzés vagy tájékoztatás célját szolgáló közlés – értve ez alatt a politikai kampány céljait szolgáló tájékoztatást is – telefonon vagy egyéb elektronikus hírközlési úton nem továbbítható annak az előfizetőnek, aki úgy nyilatkozott, hogy nem kíván ilyen közlést fogadni. Az Elkertv. és az adatvédelmi törvény rendelkezéseiből pedig az következik, hogy sms-ben vagy e-mailen csak akkor küldhető kampány célú üzenet, ha a címzett ahhoz előzetesen hozzájárult. A kommunikáció során az érintetteket az adatkezelésről tájékoztatni kell.

A választási eljárásról szóló 1997. évi C. törvény (Ve.) szabályozásából ered az állampolgárok beadványaiban visszatérően jelentkező, a központi nyilvántartásból a pártok által igényelhető személyes adatok letilthatatlanságával kapcsolatos probléma. A polgárok nem értik, hogy ha lehetőségük van adataik direkt marketing célú kiszolgáltatását megtiltani, miért nem tehetik meg ugyanezt a választási célú adatfelhasználás esetében. A biztos álláspontja szerint, melyről már több ízben tájékoztatta a politikai élet résztvevőit, indokolatlan, hogy a választási kampány esetén nem jár legalább ugyanaz a védelem a polgárok számára, mint amit a közvetlen üzletszerzést végző szervezetek tevékenységével szemben élvezhetnek. A változtatás által a törvényben biztosítani lehetne a személyes adataik kiadását korlátozó, illetve tiltó nyilatkozatot tett választópolgárok azon jogát, hogy adataikat ne szolgáltassák ki a választási kampány céljaira. Sokan úgy gondolják, a hatályos szabályozás elősegíti a polgárok aktívabb részvételét a politikai életben és az adatletiltás lehetővé tétele ellentétes azzal a méltányolható elvárással, hogy mind több polgár gyakorolja politikai jogait. A biztos megítélése szerint azonban a választópolgárok csak csekély hányada kérné adatai kiadásának korlátozását, és a kapcsolatfelvétel ilyen

módjának kizárása korántsem eredményezné azt, hogy e rétegek kirekesztődnének az egyébként kívánatos politikai párbeszédből.

Az igazságügyi és rendészeti miniszter arról tájékoztatta az adatvédelmi biztost, hogy a tárca a személyi adat- és lakcímnyilvántartásban szereplő adatoknak a pártok részére kampány céljából történő szolgáltatásának letiltására lehetőséget kíván biztosítani. E tárgyban a kormány T/237. számon benyújtotta törvényjavaslatát az Országgyűléshez. A törvényjavaslatot e beszámoló írásakor még nem fogadták el.

A pártok automatikus hívórendszerek igénybevételével bonyolított hívásai kapcsán érkezett a legtöbb panasz az Adatvédelmi Biztos Irodájához. Sokan zaklatásként élték meg a gyakori kéretlen telefonhívásokat, mások azt kifogásolták, hogy a hívásokat nem tudják megszakítani, és akadtak olyanok is, akiket titkos telefonszámukon kerestek fel a pártok. A panaszok kivizsgálása érdekében a biztos tájékoztatást kért a Fidesz–MPSZ és az MSZP illetékeseitől is.

> A pártok közlése szerint az automatikus tájékoztatás közben és azt követően személyhez kapcsolható adatokat, információkat nem rögzítettek, így tevékenységük személyes adatkezelést sem eredményezett. Emellett azonban a véletlenszerű számgenerálás útján megvalósuló kapcsolatfelvétel magában rejtette annak kockázatát, hogy titkos telefonszámokat is tárcsáz a központ. Amint a biztos a vizsgálatok összegzésében is kiemelte, bár a pártok eljárása kapcsán az adatvédelmi törvény rendelkezéseinek megsértését nem állapította meg, az automatikus hívórendszert alkalmazó adatkezelők eljárása az elektronikus hírközlésről szóló 2003. évi C. törvény 162. § (1) bekezdésének rendelkezésébe ütközhetett. E jogszabályhely szerint az emberi beavatkozás nélküli, automatizált hívórendszer az előfizető tekintetében csak akkor alkalmazható közvetlen üzletszerzési vagy tájékoztatási célra, ha ehhez az előfizető előzetesen hozzájárult. A kampány tapasztalatai sajnos azt mutatják, hogy e törvényi rendelkezés nem ad garanciális védelmet a polgároknak, más kérdések mellett e tevékenység részletes szabályozása is időszerű. *(15/A/2006, 19/A/2006, 405/A/2006, 632/A/2006)*

Egy állampolgári beadványra adott válaszában a biztos a választópolgárok lakhelyén történő adatfelvétel veszélyeire emlékeztetett. Az olyan eljárás ugyanis, melynek során a kérdőívek kitöltése a választópolgárok otthonában történik, adatvédelmi szempontból aggá-

lyos lehet, hiszen magában rejti a lakcímadatok feljegyzésének kockázatát, és így a vélemények személyhez társíthatóak. *(610/A/2006)*

Az idei választások sajnálatos fejleménye, hogy automatizált telefonhívásokkal és sms-üzenetekkel a kampánycsend időszakában is ostromolták a választópolgárokat. E problémával a választási bizottságok is szembesültek munkájuk során, a kifogások érdemi kivizsgálására azonban a hatályos jogszabályi rendelkezések alapján nem volt lehetőség, így a jogsértéseket sem szankcionálhatták. Az adatvédelmi biztos a választások tapasztalatait összefoglaló beszámolójában e jogszabályi anomáliát is részletesen ismertette, és szorgalmazta a vonatkozó jogszabályok módosítását.

B. Közérdekű adatok

2006-ban az információszabadságot érintő ügyek száma az előző évhez képest nem változott. A 197 ügyből 105 volt panasz, 78 az úgynevezett konzultációs kérdés, 5 esetben véleményeztünk szolgálati titokköri jegyzéket, 6 esetben indítottunk hivatalból eljárást és 3 alkalommal rendeztünk az információszabadság témakörében szakmai tanácskozást. A számok azt mutatják, hogy az idén mind az ügyek típusát, mind pedig az indítványozók összetételét illetően jelentős változás állt be. Míg a megelőző három évben a panaszbeadványokkal szemben a konzultációs ügyek voltak többségben, 2006-ban a helyzet megváltozott, ugyanakkor – szokatlanul – a panaszügyek mintegy negyedében az adatvédelmi biztos hatáskörének hiányát állapította meg. A másik fontos változás, hogy míg a korábbi években az állampolgárok a beadványozók mindössze negyedét, harmadát tették ki, 2006-ban arányuk megközelítette a 60 %-ot.

Az információszabadságot érintő ügyek indítványozók szerinti megoszlása az elmúlt három évben a következő volt:

	2006	**2005**	**2004**
Magánszemély	58%	32%	26%
Újságíró	5%	10%	16%
Maga az adatkezelő	21%	32%	31%
Civil szervezet	7%	10%	10%
Hivatalból indított eljárás	3%	2%	4%
Önkormányzati képviselő, polgármester	1,5%	6%	7%
Parlamenti képviselő	1,5 %	2%	3%
Ügyvéd (valamely szervezet képviseletében)	–	–	2%
Gazdasági társaság	1,5%	4%	1%
Egyéb	1,5%	2%	–

Nemzetközi kapcsolatok

Nemcsak az adatvédelem, hanem az információszabadság terén is örvendetesen növekszik a nemzetközi szakmai kapcsolatok szerepe. 2003-ban Berlinben 14 információs biztos (köztük a magyar adatvédelmi biztos) és ombudsman egy közösen kiadott nyilatkozattal létre-

hozta az együttműködés egy új nemzetközi keretét: az Információs Biztosok Nemzetközi Konferenciáját (International Conference of Information Commissioners – ICIC), melynek keretében az információs jogok biztosai és az e jogokat is védő ombudsmanok évente tartanak a világ különböző pontján tanácskozást. E konferenciák nemcsak a biztosok közötti szűk körű tapasztalatcserét szolgálják, hanem alkalmat adnak az információs jogok terén tevékenykedő civil szervezetek, közigazgatási szakemberek találkozójára is.

2005 novemberében ugyancsak Berlinben létrejött egy szűkebb körű, az európai kontinensre kiterjedő szervezeti forma: az Információs Biztosok Európai Konferenciája (European Conference of Information Conference – ECIC). Célja, hogy keretet adjon a folyamatos szakmai együttműködéshez az Unión belüli és kívüli európai országok jogi szabályozásának harmonizálása érdekében.

Ebben az évben – az információszabadság témakörében – az adatvédelmi biztos két nemzetközi tanácskozás rendezője volt. Szeptemberben Kínából fogadtuk azt a közigazgatási szakemberekből, kodifikációs szakértőkből álló delegációt, mely a kínai információszabadság-törvény előkészítése keretében az Európai Unió három országát: Magyarországot, Németországot és az Egyesült Királyságot kereste fel. A leendő kínai szabályozás részleteire is kiterjedő intenzív munkamegbeszélés során a kínai kollégák a közel másfél évtizedes magyar tapasztalatokra voltak kíváncsiak, különös tekintettel az adatvédelmi biztos szerepére.

Novemberben öt európai ország (Svédország, Norvégia, Szlovénia, Észtország és az Egyesült Királyság) információs biztosait, illetőleg szakértőit láttuk vendégül az európai információs biztosok együttműködése keretében. A tanácskozás célja az volt, hogy az információszabadság két izgalmas területével kapcsolatos tapasztalatokat kicseréljük. Az üzleti titok és a nyilvánosság, valamint az átláthatóbb párt- és kampányfinanszírozás kérdésének szabályozását valamennyi részt vevő országban viták kísérik, ezért rendkívül hasznosnak bizonyult a tapasztalatok, javaslatok, ötletek megosztása.

Közérdekű adatok az önkormányzatok kezelésében

Az ügyek közel egyharmada évek óta, így a 2006. évben is, az önkormányzatok működésének nyilvánosságával volt kapcsolatos. Változatlanul sokan fordulnak konzultációs kérdéssel az adatvédelmi biztoshoz, az állampolgárok mellett önkormányzati képviselők, polgármesterek, jegyzők is tájékoztatást kérnek az önkormányzatok üléseinek és dokumentumainak, illetve az önkormányzat által kötött szerződéseknek a nyilvánossága tárgyában.

A beadványokban feltett kérdések arra engednek következtetni, hogy a zárt ülések elrendelése, a zárt ülésen hozott döntések nyilvánossága még mindig gyakran okoz fejtörést az önkormányzat tisztségviselőinek. A biztos állásfoglalásaiban ismételten hangsúlyozta, hogy a jogalkalmazóknak különös gonddal kell vizsgálni, fennállnake egyáltalán a zárt ülés elrendelésének és ezáltal a nyilvánosság korlátozásának feltételei. A közérdekű adatok megismeréséhez való jog, az önkormányzatok demokratizmusa alapján mind az Avtv., mind az Ötv. szabályai az önkormányzati működés, a közpénzekkel, a vagyonnal való gazdálkodás nyilvánosságát, átláthatóságát kívánják garantálni, és az ezzel kapcsolatos adatok, információk nyilvánosságát deklarálják. Csak szűk körben, törvény által meghatározott esetekben van lehetőség a nyilvánosság korlátozására.

> Egy polgármester nem tudta eldönteni, hogy a zárt ülésen leadott szavazatokra vonatkozó információk – a szavazati arányokon túl – milyen részletességgel hozhatók nyilvánosságra. A biztos tájékoztató levelében kitért arra, hogy a zárt ülés tartásának indokaira figyelemmel a zárt ülés jegyzőkönyvére nem vonatkozik a betekintési jog. Amennyiben a zárt ülés jegyzőkönyvében egyébként nyilvános adat szerepel, úgy ezekről tájékoztatást kell adni. Ilyen adat maga a döntés vagy például az önkormányzati költségvetést érintő adatok. A biztos álláspontja szerint közérdekből nyilvános adatnak tekintendőek a zárt ülésen leadott képviselői szavazatok is, ha a szavazás nem titkos. *(1344/K/2006)*

Változatlanul gyakori, hogy az állampolgárok még azt megelőzően kérik a biztos véleményét, mielőtt az önkormányzati szervekhez fordulnának kérelmükkel. A biztos ilyenkor igyekszik segíteni abban, hogy az önkormányzathoz eljuttatott adatigénylés pontosabb legyen,

és hogy jogaikat megismerve az adatigénylők határozottabban lépjenek fel.

Egy állampolgár levelében az iránt érdeklődött, hogy közérdekből nyilvános adatnak tekinthető-e az önkormányzati képviselőjének egy önkormányzati tulajdonú cég vezető tisztségviselőjévé való jelölése, megválasztása, megválasztásának körülményei. A biztos válaszlevelében megerősítette, hogy a képviselő jelölése, illetve megválasztása egy önkormányzati cég vezetőjévé, közérdekből nyilvános adat. Állásfoglalásában ugyanakkor kitért arra is, hogy megválasztásának körülményei (indokai) azonban csak annyiban nyilvánosak, amennyiben az Ötv. 12. § (4) bekezdésének a) pontja szerinti feltételek fennállnak. E jogszabályhely alapján ugyanis a képviselő-testület zárt ülést tart választás, kinevezés, felmentés, vezetői megbízás adása, illetőleg visszavonása, fegyelmi eljárás megindítása, fegyelmi büntetés kiszabása és állásfoglalást igénylő személyi ügy tárgyalásakor, ha az érintett a nyilvános tárgyalásba nem egyezik bele.*(825/A/2006)*

Egy másik ügyben a beadványozó arról kért tájékoztatást, hogy az önkormányzati ingatlanra vonatkozó ingatlan-értékbecslés közérdekű adatnak minősül-e, illetve annak megismeréséhez az értékbecslő hozzájárulása szükséges-e. A biztos álláspontja szerint az ügy körülményeitől függően az önkormányzat által készíttetett értékbecslés minősülhet az Avtv. 19/A. §-a szerinti döntés-előkészítő adatnak, mely nem nyilvános, de a szerv vezetője a megismerést engedélyezheti. A döntés meghozatala után az adatigénylés nem utasítható el, kivéve, ha az adat megismerése a szerv működési rendjét vagy feladatellátását veszélyezteti. *(1410/K/2006)*

Előfordul, hogy az önkormányzatok kizárólag a hagyományosan (papír alapon) rögzített adatokat bocsátják a kérelmező rendelkezésére, a nyilvános ülésekről készített videó- vagy hangfelvételek másolati példányai átadásától elzárkóznak. A biztos számos alkalommal leszögezte, hogy az információszabadság szempontjából egyformán kezelendő a jegyzőkönyv, a hang- és képfelvétel, vagyis kérésre ezekről is tájékoztatást és másolatot kell adni. Bár az Ötv. 17. §-a csak az elhangzottak lényegét (jelenlévők neve, napirendi pontok, a tárgyalás lényege, szavazás, döntés) tartalmazó jegyzőkönyv készítését teszi kötelezővé, az önkormányzatok dönthetnek úgy, hogy szó szerinti jegyzőkönyvet készítenek, és egyéb adathordozó segítségével is rögzítik az elhangzottakat. Az Ötv. csak a minimálisan rögzítendő adatok körét határozza meg. A nyilvánosság

szempontjából nincs jelentősége annak, hogy a nem szó szerinti jegyzőkönyv és a felvételek adattartalma nem pontosan egyezik meg, mert mindegyik dokumentum nyilvános. A biztos állásfoglalásában hangsúlyozta, hogy az Avtv. fogalmi rendszere nem iratelven, hanem adatelven alapul, vagyis nem az adathordozó, hanem annak adattartalma a meghatározó. Az Ötv. csupán megnevez egy dokumentumfajtát, és deklarálja – az Avtv.-vel összhangban – a jegyzőkönyv teljes adattartalmának nyilvánosságát. Amennyiben fennáll valamely adat védelmének érdeke, a törvényben meghatározottak szerint zárt ülést kell/lehet elrendelni. *(87/K/2006)*

A nyilvánosság mellett foglalt állást a biztos abban az ügyben is, melyben az eldöntendő kérdés az volt, hogy megismerhetővé tehető-e, ha az érintett képviselő nem nyújtott be interpellációt. Egy önkormányzati képviselő interpellációjának ténye, illetve maga az interpelláció az Avtv. 19. § (4) bekezdése alá esik, mivel az önkormányzati képviselő képviselői minőségével, e minőségében végzett tevékenységével kétségtelenül összefügg. A biztosnak azt kellett tehát mérlegelnie, hogy mennyiben függ össze a képviselő *„feladatkörével”* az a tény, illetve tényállítás, hogy az érintett képviselő nem interpellált. A biztos álláspontja szerint e passzív megnyilvánulást sem lehet kizárni a képviselő *„feladatkörével összefüggő személyes adata”* köréből, ellenkező esetben ugyanis a közhatalmat gyakorló személyek esetében számos, a köztevékenységük és annak megítélése szempontjából jelentős adat maradhatna titokban. *(570/K/2006)*

A biztosnak ebben az évben is több alkalommal kellett közbenjárnia annak érdekében, hogy az önkormányzatok a közérdekű adatigényléseknek maradéktalanul és az Avtv.-ben előírt határidőben eleget tegyenek, az önkormányzat működésével kapcsolatos dokumentumokat a kérelmező rendelkezésére bocsássák *(231/A/2006, 79/A/2006, 998/A/2006)*. Az Avtv. 20 §-ában előírt 15 napos válaszadási határidő ugyan valóban akkor kezdődik, amikor a közérdekű adatok megismerése iránti igény a szerv tudomására jut, adódhat azonban olyan helyzet, amely e határidő számítását oly módon befolyásolja, hogy a kérelem beérkezése és az adatszolgáltatás teljesítése között jogszerűen hosszabb idő telik el.

A biztos nem találta jogsértőnek a jegyző eljárását, amikor az önkormányzati ülés jegyzőkönyvét csak 20 nap elteltével küldte meg a kérelmezőnek, mert az Ötv. 17. §-a értelmében a képviselő-testü-

leti ülés jegyzőkönyvének írásos változatát az ülést követő 15 napon belül kell elkészíteni, így az ülést követő napon, az igény beérkezésekor a kért dokumentum még nem állt az önkormányzat rendelkezésére. *(47/A/2006)*

Az egyik megyei jogú város polgármestere azt kifogásolta, hogy egy másik városi önkormányzat nem tett eleget közérdekű adatigénylésüknek. A polgármester egyben biztosi vizsgálatot is kezdeményezett a jogsértő önkormányzat ellen. A biztos érdemben nem foglalt állást. Hatásköre vizsgálatánál ugyanis nem hagyhatta figyelmen kívül azt a körülményt, hogy a közérdekű adatok megismerése a közhatalom és az egyén (illetve azok szervezetei) közötti kapcsolatban értelmezhető. A közszféra szervei egymás közötti adatforgalmára nem az Avtv. szabályait kell alkalmazni. Az önkormányzatok kapcsolatában (is) az Alkotmánybíróság egyik korai határozatában kifejtett elvnek kell érvényesülnie, mely szerint a jogállamiság elvéből következően a közhatalmi szerveknek az a kötelessége, hogy alkotmányos hatásköreiket jóhiszeműen, feladataik teljesítését egymást kölcsönösen segítve, együttműködve gyakorolják. *(614/A/2006)*

2006 decemberében az Önkormányzati és Területfejlesztési Minisztérium elkészített egy az önkormányzatok adatkezelésére vonatkozó és az önkormányzatoknak szánt szakmai útmutatót, melyet véleményezésre megküldött az adatvédelmi biztosnak. Tapasztalva az önkormányzati adatkezelés máig fennálló bizonytalanságait a biztos örömmel üdvözölte a kezdeményezést. *(2005/K/2006)*

Az elektronikus információszabadságról szóló törvény első éves tapasztalatai

A biztos tavalyi beszámolójában, miközben üdvözölte az elektronikus információszabadságról szóló 2005. évi XC. törvény (a továbbiakban: Eitv.) elfogadását, utalt a hatálybaléptetéssel kapcsolatos aggodalmaira is: a jogalkalmazók kellő időben való felkészítésének és az anyagi forrásoknak a hiányára. Kritizálta a törvény végrehajtási rendeleteinek késői közzétételét, hiszen a közérdekű adatok elektronikus közzétételére, az egységes közadatkereső rendszerre, valamint a központi jegyzék adattartalmára, az adatintegrációra vonatkozó részletes

szabályokról szóló 305/2005. (XII. 25.) Korm. rendeletet és a közzétételi listákon szereplő adatok közzétételéhez szükséges közzétételi mintákról szóló 18/2005. (XII. 27.) IHM rendeletet minden valószínűséggel már csak januárban, tehát az Eitv. hatálybalépését követően kézhez kapott Magyar Közlönyökből ismerhették meg az adatkezelők.

Az első év tapasztalatai részben igazolták a korábbi aggodalmakat. Az érintett szervek csak részlegesen tettek és tesznek eleget közzétételi kötelezettségeiknek. Nem alakult ki a közzététel egységes és az érdeklődők számára könnyen áttekinthető és használható formája. Az adatkezelők hiányosan teljesítik az Eitv.-ben szabályozott, általánosan közzéteendő adatok és a jogszabálytervezetek közlését. A végrehajtást késleltette a kormányzati rendszernek az országgyűlési választásokat követően történt átalakítása, emiatt egyes minisztériumok új honlapjainak kialakítása hónapokon át elhúzódott. A hiányosságok ellenére meglepő módon alig érkezett panasz az elektronikus közzétételi kötelezettségek elmulasztása miatt. Nem sokkal a törvény hatálybalépését követően egy újságíró-szervezet kifogásolta, hogy a törvény alapján közzétett Hatályos Jogszabályok Elektronikus Gyűjteménye a már elfogadott, de még hatályba nem lépett jogszabályokat nem tartalmazza, hátráltatva ezáltal a jogszabály alkalmazására való felkészülést. A biztos vizsgálatát hivatalból kiterjesztette a jogszabályok elektronikus közzétételének egész kérdéskörére, és megállapításait ajánlásban foglalta össze.

Az ajánlás leszögezi, hogy a jogalkotónak – amikor az Eitv. elfogadásakor úgy döntött, hogy elektronikus formában ingyenesen hozzáférhetővé teszi a jogszabályokat, illetőleg a hatályos joganyagot – számos megoldás közül volt módja választani. A törvény indokolása szerint *„elvárható az államtól, hogy a jogszabályok megismerhetőségét mindig a legmagasabb technikai színvonalon a lehető legtöbb ember számára a lehető legalacsonyabb költséggel biztosítsa*". Ilyen kívánalom különösen indokolt Magyarországon, ahol a rendszerváltás az egész hazai joganyag átalakítását követelte és követeli meg, ahol az elmúlt 16 év alatt közel kétezer törvény és törvénymódosítás, mintegy négyezer kormányrendelet, több tízezernyi miniszteri és önkormányzati rendelet született. A joganyagban való eligazodást tovább nehezítette Magyarország uniós csatlakozása a közvetlenül alkalmazandó uniós jogszabályok hatalmas mennyisége miatt.

Az idézett indokolásban megfogalmazott követelményt az Eitv. csak igen korlátozottan teljesíti. Ha az állam az internet segítségével a fel-

használó szempontjából a mindenkor legfejlettebbnek tekintett módon bárki számára hozzáférhetővé teszi a joganyagot, útmutatókkal segíti az abban való eligazodást, nem kegyet gyakorol. A XXI. században, az információs társadalom korában a tájékozódni akaró jogkereső állampolgár érdekeit az állami költségvetés fiskális szempontjai nem előzhetik meg. A jogszabályok dzsungelében való tájékozódás elősegítése az államnak is eminens érdeke, hiszen ezzel erősíthető a jogbiztonság. Az állam nemcsak a jogi kultúra javításához járul ezzel hozzá, hanem fontos lépést tesz annak érdekében, hogy a jogban való eligazodás ne kevesek kiváltsága legyen.

Az ajánlás – egyebek mellett – felkérte a Miniszterelnöki Hivatalt vezető minisztert, tegye meg a szükséges intézkedéseket annak érdekében, hogy a Hatályos Jogszabályok Elektronikus Gyűjteménye tartalmazza a már elfogadott, de még hatályba nem lépett jogszabályok szövegét is. Felkérte továbbá az igazságügy-minisztert és az informatikai és hírközlési minisztert, hogy kezdeményezzék az Eitv. módosítását annak érdekében, hogy az a lehető legmagasabb technikai színvonalon és a felhasználó számára a legelőnyösebb módon garantálja a Magyar Közlöny elektronikus változatának, valamint a hazai joganyag elektronikus gyűjteményének használatát. *(153/A/2006)*

A Miniszterelnöki Hivatalt vezető miniszter a Hatályos Jogszabályok Elektronikus Gyűjteményének kiegészítésére vonatkozó biztosi ajánlásra érdemben nem válaszolt. Az igazságügy-miniszter válaszában kifejtette, hogy a biztosi ajánlásban foglaltak szorosan összefüggnek a jogalkotás rendjével. Ezért álláspontja az, hogy a felvetett kérdéseket az újonnan beterjesztendő törvénynek kell rendeznie.

Az Eitv. első évi tapasztalatai alapján indokolt, hogy 2007-ben az adatvédelmi biztos hivatalból, átfogó vizsgálat keretében tekintse át a közzétételi kötelezettségek, valamint a törvényben és a végrehajtási rendeletekben foglalt egyéb kötelezettségek teljesítését.

Fogyasztóvédelem és nyilvánosság

A 2006-os esztendőnek az információszabadsággal összefüggő egyik legfontosabb közéleti ügye az élelmiszerbiztonság, a fogyasztóvédelem helyzete volt. Ezért az adatvédelmi biztos indokoltnak látta, hogy hivatalból vizsgálatot indítson a fogyasztóvédelmi ügyek nyilvánosságának javítása érdekében. A vizsgálatot 2006 márciusában egy

az Adatvédelmi Biztos Irodájában szervezett széleskörű szakmai tanácskozás előzte meg, melyen nemcsak az ügyben illetékes szervek munkatársai, hanem a sajtó és az érintett civil szervezetek képviselői is részt vettek.

A biztosi álláspont szerint a közérdekű adatok nyilvánossága hatékony eszköze lehet a fogyasztói jogok érvényesítésének, mivel az információk nyilvánossága elősegíti a fogyasztóvédelmi szabályok betartását, a fogyasztóvédelmi hatóságok tevékenységének átláthatóságát, csökkenti az emberek kiszolgáltatottságát. Nem lebecsülendő a nyilvánosság visszatartó ereje. A jogsértő esetek napvilágra kerülése pedig nemcsak a fogyasztók, de a piac jogkövető szereplői számára is fontos.

A vizsgálat feltárta, hogy fogyasztóvédelmi feladatokat ma tucatnyi szerv lát el, e hatóságok eljárásának nyilvánosságára vonatkozó szabályok azonban nem egységesek. A Gazdasági Versenyhivatal, a Pénzügyi Szervezetek Állami Felügyelete például rendszeresen, széles körben, elektronikusan közzéteszi fogyasztóvédelmi ügyekben hozott döntéseit, míg a fogyasztóvédelmi felügyelőségek, az állategészségügyi és élelmiszer-ellenőrző állomások határozatai szinte egyáltalán nem ismerhetőek meg a közvélemény által.

A fogyasztóvédelmet szabályozó egyes jogszabályok biztosítják a fogyasztók úgynevezett tájékoztatáshoz való jogát, mely egyrészt az áruk, szolgáltatások jellegzetességeire, árucímkén feltüntetendő adataira, másrészt meghatározott veszély, kockázat esetén a fogyasztók figyelmének felhívására vonatkozik. A biztos álláspontja szerint azonban az információszabadság hazai szabályai alapján e jog ennél sokkal szélesebb, beletartozik az is, hogy a fogyasztóvédelmi feladatokat ellátó hatóságoknál az eljárásuk során keletkezett adatok, információk is mint közérdekű adatok vagy közérdekből nyilvános adatok megismerhetőek.

A vizsgálat eredményeit a biztos ajánlásban összegezte, mely számos jogszabály módosítását kezdeményezte az illetékes minisztereknél.

> Az ajánlás – többek között – megállapította, hogy egyes fogyasztóvédelmi hatóságok szinte egyáltalán nem élnek a határozatok hozzáférhetővé tételének az Avtv. és a Ket. által biztosított lehetőségével, és csak kifejezett, egyértelmű jogszabályi előírás esetén közölnek információkat. Tartanak ugyanis attól, hogy üzleti titok sérel-

> me, a jóhírnév sérelme vagy károkozás miatt az elmarasztaló határozattal érintett ügyfél pert indít ellenük. A biztos álláspontja szerint azonban a vállalkozások jogszerű működésének ellenőrzésére hivatott hatóságok elmarasztaló határozata közérdekű adat. Az üzleti titok intézménye nem lehet menedék a piac jogsértő szereplői számára, a jogsértés titokban maradása nem tekinthető jogszerű érdeknek. A Ptk. jóhírnév védelméről szóló rendelkezése nem jelenti azt, hogy tilos volna mindennemű olyan tényállítás vagy adatközlés, amely a jogi személy társadalmi, piaci stb. megítélését hátrányosan befolyásolná, azaz ártana jóhírnevének. A közigazgatási szerv jogsértést megállapító, tárgyszerű határozatának közzététele nem jelenti a jóhírnév sérelmét, az ilyen határozat közzétételét lehetővé tevő vagy elrendelő jogszabály jogellenességet kizáró ok, illetve ilyen esetekben hiányzik a károkozás jogellenessége is. Az ajánlás kezdeményezte, hogy ismétlődő, súlyos, szándékos jogsértések esetén a hatóságoknak ne legyen mérlegelési joguk a közzétételt illetően, hanem jogszabály kötelezze őket a határozatok közzétételére, a lakosság tájékoztatására. A fogyasztók joggal igénylik a szélesebb körű tájékoztatást, mégpedig nemcsak a súlyosabb ügyekben, hanem a kisebb jogsértések esetén, vagy akár akkor is, ha egyszerűen a termék vagy a szolgáltatás minőségéről szeretnének többet tudni. *(363/H/2006)*

Az igazságügyi és rendészeti miniszternek az ajánlásra adott válasza szerint az új Ptk. előkészítése során hasznosítani fogják az ajánlásban felvetett szempontokat. Az egészségügyi miniszter is megteszi az ajánlásból következő intézkedéseket. A szociális és munkaügyi miniszter egyetértett azzal, hogy a fogyasztók érdekeit érintő ügyekben a nyilvánosság kiterjesztése indokolt, ezért az ajánlásban foglaltaknak megfelelően előkészítik a vonatkozó törvényi rendelkezések módosítását. A fogyasztóvédelemről szóló 1997. évi CLV. törvény módosítása – az ajánlás bizonyos pontjaihoz kapcsolódóan és annak megfelelően, bár elsősorban közösségi jogi kötelezettségek miatt – folyamatban van, az erről szóló javaslatot jelenleg tárgyalja az Országgyűlés *(1846J/J/2006)*. Az ajánlásban foglaltak megvalósítását, a szélesebb nyilvánosság érdekében megszülető intézkedéseket hivatalunk a későbbiekben is figyelemmel fogja kísérni.

Hatósági eljárás és információszabadság

Az adatvédelmi biztos tevékenységének kezdettől fogva az egyik fontos kérdése, hogy az egyedi hatósági ügyek dokumentumainak megismerhetőségét a közigazgatási hatósági eljárás vagy az Avtv. szabályai szerint kell megítélni.

A biztos álláspontja szerint valamely hatóságtól való adatkérés megítélésekor mindenekelőtt tisztázandó, hogy az adott esetben hatósági ügyről van-e szó, mert csak ebben az esetben alkalmazhatók az ügyféli jogokkal kapcsolatos szabályok. Amikor egy állampolgár vagy egy civil szervezet az Avtv.-re hivatkozva közérdekű adatokat kér, nem közigazgatási hatósági ügyről, nem egy eljárási jogról van szó, hanem az Alkotmány 61. § (1) bekezdésében foglalt jog érvényesítéséről: a közigazgatási szerv kezelésében (azaz birtokában) lévő közérdekű adatok megismeréséről. A közérdekű adatok megismeréséhez való jogot meg kell különböztetni az iratbetekintési jogtól. Nincs szükség az érdekeltség igazolására olyan adatok kérése esetén, amelyek közérdekű adatnak (például környezettel kapcsolatos adat, hatóság tevékenységére vonatkozó adat) vagy közérdekből nyilvános adatnak minősülnek. A közérdekű adatok megismerésének joga bárkit megillet, az nincs ügyféli pozícióhoz kötve. Ennek figyelembevételével kell eljárni a különféle hatósági döntések – például környezeti szakhatósági hozzájárulás, építési engedély, működési engedély, területfoglalási engedély, fakivágási engedély – megismerhetőségének vizsgálatakor. (*823/A/2006, 1359/A/2006)*

A közigazgatás szervei számára azonban az államigazgatási eljárásról szóló korábbi törvény és az Avtv. együttes alkalmazása sok ellentmondással járt. Ezek felszámolása érdekében az adatvédelmi biztos az elmúlt években számos javaslatot fogalmazott meg, melyek többségét a Ket. elfogadásakor a törvényhozó figyelembe vette. A 2005 végén hatályba lépett Ket. alkalmazásával kapcsolatos első tapasztalatok azonban vegyesek. Örvendetes, hogy a 69. § (6) bekezdésében megjelölt hatósági ügyekben a jogalkotó kinyitotta a nyilvánosság kapuit. Az adatvédelmi biztos elé került esetekből azonban kiderül, hogy a szövegezés nem kellő pontossága további kérdéseket vet fel.

Miként az Országos Munkaügyi és Munkabiztonsági Főfelügyelőség jelezte: miközben a Ket. nyilvánossá teszi a munkavállalók mun-

kavédelmi, munkabiztonsági jogait közvetlenül érintő ügyben hozott határozatokat, nem említi a munkajogi ügyekben hozott döntéseket, holott a főfelügyelőség szerint igencsak indokolt, hogy a munkajogi szabályok sérelmét megállapító határozatok nyilvánosak legyenek, megismerhető legyen a jogsértő cégek neve. A fogyasztóvédelmi ügyek nyilvánosságával kapcsolatban merült fel az a kérdés, hogy a Ket. 69. § (6) bekezdés d) pontjának alkalmazása során mikor állapítható meg a fogyasztók jogainak közvetlen érintettsége.

> Több jogszabályi rendelkezés is biztosítja a nyilvánosságot egy önkormányzati csatornaberuházás vagy például egy szeméttelep építési és működési engedélye tekintetében. Az Avtv. rendeli el azon adatok nyilvánosságát, melyek jogszabály vagy állami, illetőleg helyi önkormányzati szervvel kötött szerződés alapján kötelezően igénybe veendő vagy más módon ki nem elégíthető szolgáltatást nyújtó szervek vagy személyek kezelésében van, e tevékenységre vonatkozik. A Ket. 69. §-a (6) bekezdésének c) pontja szerint a hatóság bárki számára hozzáférhetővé teszi azokat a döntéseket, amelyeket az adott tevékenységgel összefüggésben a hatásterületen élő lakosság jelentős részét érintő ügyben hozott. Figyelembe kell venni továbbá a környezet védelmének általános szabályairól szóló 1995. évi LIII. tv. 12. §-át is, mely szerint közzé kell tenni az olyan jogerős hatósági határozatot, amelynek végrehajtása jelentős környezeti hatással jár. A környezethasználó köteles az általa okozott környezetterheléssel, környezet igénybevétellel, valamint környezetveszélyeztetéssel összefüggő adatokról kérelemre bárkinek tájékoztatást adni. *(431/K/2006, 1593/A/2006)*

A Ket. alkalmazása során felmerült további tapasztalat, hogy indokolt átgondolni a különféle hatósági nyilvántartások nyilvánosságának, közzétételének kérdéskörét. Célszerű az erre vonatkozó szakterületenkénti szabályozás felülvizsgálata. Sok esetben ugyanis semmilyen érdek nem fűződik egy-egy nyilvántartásnak a nyilvánosságtól való elzárásához. A biztos többször jelezte a jogalkotó szerveknek és a jogalkalmazóknak, indokoltnak tartja olyan jogi szabályozás kialakítását, mely a jelenleginél szélesebb körben biztosítja a hatósági nyilvántartások adatainak megismerhetőségét. Ennek érdekében szükség van megfelelő adatszolgáltatási szabályok kialakítására vagy közzétételi kötelezettség előírására.

Egy beadvány kapcsán kérdésként merült fel, hogy egy nyilvános szórakozóhely üzemeltetőjének adatairól köteles-e az illetékes hatóság tájékoztatást adni. A konkrét esetben egy civil szervezet egy kisebbségi diszkrimináció miatti jogvédelmi eljáráshoz kért tájékoztatást, azonban a hatóság megtagadta a nyilvántartás adatainak kiadását. A vizsgálat feltárta, hogy a jogi szabályozásból következően az üzlet működtetőjének neve, elérhetősége nem ismerhető meg, holott nincs olyan jog vagy érdek, mely ilyen adatok titkosságát indokolná. A biztos kezdeményezte a nyilvánosságot biztosító szabályok megalkotását. (*447/A/2006)*

A Ket. alkalmazásával kapcsolatos első tapasztalatok összegyűjtését az Önkormányzati és Területfejlesztési Minisztérium megkezdte, a szükségessé váló korrekciók érdekében az adatvédelmi biztos észrevételeit eljuttatta a tárcához. *(1866/J/2006)*

A két információs jog ütközése

Már az előző évről szóló beszámoló előrevetítette, hogy Avtv.-nek a közfeladatot ellátó személyek adatainak nyilvánosságáról rendelkező, 2005 júniusától hatályos új szabálya [a 19. § (4) bekezdése] megannyi értelmezési kérdést vet majd fel. E rendelkezés szerint: „*Ha törvény másként nem rendelkezik, közérdekből nyilvános adat az (1) bekezdésben meghatározott szervek feladat- és hatáskörében eljáró személy feladatkörével összefüggő személyes adata, továbbá egyéb, közfeladatot ellátó személy e feladatkörével összefüggő személyes adata. Ezen adatok megismerésére e törvénynek a közérdekű adatok megismerésére vonatkozó rendelkezéseit kell alkalmazni.*" A 2006-ban e tárgykörben érkezett beadványok az új rendelkezés szinte valamennyi elemét érintették. Az ügyek kapcsán igazolódott, hogy a biztos korábbi figyelmeztetése indokolt volt: az Avtv. módosítása a közfeladatot ellátó személyek jogviszonyát szabályozó törvények korrekciója nélkül az új szabály alkalmazását széles körben ellehetetleníti. Ezért hivatalból vizsgálatot indított annak tisztázására, hogy mely területeken szükséges a törvények összhangjának megteremtése.

A vizsgálat feltárta, hogy a két jog konfliktusának feloldása érdekében az Avtv. 2005. június 1-jén hatályba lépett módosítása immár valóban érdemi lépést tett. E változást azonban nem egészítette ki a

közszféra különböző területein foglalkoztatottak (így például a köztisztviselők, a közalkalmazottak, az ügyészek, a bírók, az igazságügyi alkalmazottak, a fegyveres szervek hivatásos állományú tagjai, a Magyar Honvédség hivatásos katonái) jogviszonyát szabályozó törvények módosítása. E törvények ma egymástól eltérően és meglehetősen szűk körben teszik lehetővé a közfeladatot ellátó szervek hatáskörében/feladatkörében eljáró személyek személyes adatainak nyilvánosságát. Ezen felül azonban más adatokra nézve – közvetve – a nyilvánosságra hozatal tilalmát tartalmazzák. Az Avtv. módosítása emiatt érdemi változást nem hozott, hiszen a korábbi korlátozó szabályok most már mint az Avtv. szabálya alóli kivételek élnek tovább. Ennek következtében fennáll a veszély, hogy az Avtv. 19. § (4) bekezdése a legtöbb érintett személy esetében gyakorlatilag ki is üresedik.

Az ajánlás az adatvédelmi biztos egész eddigi gyakorlatára alapozva összefoglalja az Avtv. új rendelkezésével kapcsolatos jogértelmezés lehetséges szempontjait: mely szervek tartoznak a közfeladatot ellátó szervek körébe, kik tekintendők közfeladatot ellátó személynek, mely adatok lehetnek kapcsolatosak a közfeladatot ellátó személy feladat- és hatáskörével. Az ajánlás részletesen áttekinti továbbá a közfeladatot ellátó személyek foglalkoztatásával összefüggő alapnyilvántartások jellemzőit. Ennek nyomán megállapítja, hogy az alapnyilvántartásokra vonatkozó jelenlegi szabályokat felül kell vizsgálni, mert mind a szabályozás logikája, mind pedig egyes rendelkezései ellentétesek az Avtv. 19. § (4) bekezdésével. A biztos ezért felkérte a Miniszterelnöki Hivatalt vezető minisztert, hogy a hatáskörrel rendelkező miniszterekkel együtt vizsgálja felül a közfeladatot ellátó személyek jogállását rendező törvényeket, és az Avtv.-vel való összhang megteremtése érdekében kezdeményezze a szükséges módosításokat. *(1234/H/2006)* A miniszter 2007 januárjában megküldött válaszában jelezte, hogy szakmai álláspontja *„gyökeresen eltér"* a biztosétól, ezért szakértői egyeztetést javasolt a kérdésben.

Ugyancsak az Avtv. 19. § (4) bekezdésének értelmezésével függ össze az az ügy, amely az Alkotmánybíróság egyik előadó bírájának megkeresése nyomán indult. A bíró egy alkotmányjogi panasz kapcsán kérte az adatvédelmi biztos szakmai véleményét. A Magyar Hivatalos Közlönykiadó Kft. azért fordult az Alkotmánybírósághoz, mert álláspontja szerint az Avtv. 2005. június 1-jén hatályba lépett 19. § (4) bekezdése nem zárja ki a visszamenőleges jogalkalmazás lehetőségét.

Emiatt pedig a Fővárosi Ítélőtábla jogerősen arra kötelezte a Közlönykiadót, hogy a szerkesztőbizottság tagjainak juttatásaival kapcsolatos adatokat a törvényhely hatálybalépését megelőző időszakra vonatkozóan is adja ki az azt igénylő civil szervezet számára. Az Alkotmánybíróság előtt fekvő alkotmányjogi panasz megalapozottságának elbírálása nem tartozik az adatvédelmi biztos hatáskörébe. Számára a vizsgálandó kérdés az volt, hogy az Avtv. szóban forgó rendelkezése, illetőleg annak hatálya hogyan értelmezendő.

A biztos állásfoglalásában hangsúlyozta, hogy az Avtv. 19. § (4) bekezdésében megtestesülő jogalkotói cél az volt, hogy a közszféra átláthatóságának biztosítása érdekében a közérdekű adatokon túl nyilvánossá tegye a közfeladatot ellátó személyek személyes adatainak bizonyos körét. Ez a szabály ugyanis a törvény megalkotása, azaz 1992 óta hiányzott az Avtv.-ből. Miközben a törvény egyfelől nemzetközi összehasonlításban is rendkívül erős garanciákat írt elő a személyes adatok védelme érdekében, másfelől hasonlóan radikálisan építette ki a közérdekű adatok megismerésének jogát – *„megfeledkezett”* a két jog konfliktusából eredő ellentmondások feloldásáról. A két információs jogot együttesen szabályozó hazai törvény terminológiai sajátossága, hogy szigorúan szétválasztja a közérdekű és a személyes adat fogalmát. A két halmaz között nincs átfedés. Ezért az új 19. § (4) bekezdésben megjelölt adatok törvény által nyilvánosnak minősített személyes adatok. Nyilvánossá tételük mögött ugyanaz a jogalkotói szándék áll, mint a közérdekű adatok esetében.

Ezért is mondja ki a 19. § (4) bekezdésének utolsó mondata, hogy *„ezen adatok megismerésére e törvénynek a közérdekű adatok megismerésére vonatkozó rendelkezéseit kell alkalmazni.”* 1992-ben az Avtv. elfogadásakor nem merült fel olyan javaslat, amely a törvény tárgyi hatályát csak a hatálybalépését követően született dokumentumokra kívánta volna kiterjeszteni. Az új 19. § (4) bekezdés szerint nyilvánossá tett adatkör esetében – az előbbiek alapján – tehát alappal vélelmezhető a jogalkotó hasonló szándéka. Ez pedig azt jelenti, hogy a közfeladatot ellátó személyek feladatkörével összefüggő adatok nyilvánosságát – miként a közérdekű adatok esetében – ezen adatok keletkezésének időpontjától függetlenül biztosítani kell – áll az adatvédelmi biztos állásfoglalásában. *(1437/K/2006)*

Még nem zárult le az ügy alkotmánybírósági vizsgálata, amikor a Közlönykiadó által a jogerős ítélet ellen benyújtott felülvizsgálati ké-

relem nyomán a Legfelsőbb Bíróság ítéletet (Pfv.IV.21.154/2006/5.) hozott. Ebben a testület úgy foglalt állást, hogy „*a jogbiztonság elvébe ütközne az Avtv. módosított 19. § (4) bekezdésének az az értelmezése, amely szerint a jogszabály hatálybalépését követően előterjesztett megismerési kérelem időpontjában hatályos rendelkezések szerint kell megítélni a korábban keletkezett nem nyilvános személyes adatok körét.*" A korábban keletkezett „*jogviszonyok során keletkezett személyes adatok utóbb nem tehetők nyilvánossá azon az alapon, hogy a későbbi jogszabálymódosítás ezeket a személyes adatokat (a jövőre nézve) közérdekből nyilvánossá minősíti és megismerésüket bárki számára lehetővé teszi.*"

Az ügy világosan jelzi, hogy Avtv. új 19. § (4) bekezdésének értelmezése az érintett jogalkalmazó szervek körében nem egységes, ezért az adatvédelmi biztos indokoltnak tartja, és 2007-ben kezdeményezni kívánja a felmerült kérdéseknek egy szakértői megbeszélés keretében történő megvitatását.

A közfeladatot ellátó személyek nyilvános személyes adatai közül az adatvédelmi biztos gyakorlatában immár évek óta visszatérő téma a vagyonnyilatkozatok kezelése és nyilvánossága. 2006-ban – ahogy ez választási években jellemző – megnőtt az ilyen ügyek száma.

> Egy beadvány kapcsán ismét felmerült az a kérdés, hogy a polgármesteri hivatal vezethet-e nyilvántartást azokról a személyekről, akik a vagyonnyilatkozatokba betekintettek, illetve köteles-e a betekinteni szándékozó magát igazolni. 2005 júniusa előtt erre a kérdésre az adatvédelmi biztos igennel válaszolt. Az Avtv. 19. §-a új (4) bekezdésének hatálybalépésével azonban a jogi szabályozás megváltozott, és a vagyonnyilatkozatban szereplő közérdekből nyilvános adatok megismerésére a közérdekű adatok megismerésére vonatkozó szabályokat kell alkalmazni. Ezért sem a személyazonosság igazolása, sem a betekintők adatainak rögzítése nem jogszerű. *(821/A/2006)*

> Egy másik ügyben az a kérdés merült fel, hogy az önkormányzati testület tagjainak vagyonnyilatkozatai közzétehetők-e a világhálón. A biztosi válasz szerint erre vonatkozó törvényi rendelkezés nincs, de tekintve, hogy az internetes közzététel az állampolgárok információs jogának érvényesítését szolgálja, és összhangban van a törvényhozói szándékkal, az ilyen nyilvánosságra hozatal jogszerű. *(1278/K/2006)*

Egy jegyző arról kért állásfoglalást, hogy az önkormányzati képviselő megbízatásának megszűnése után mi a teendő az érintett vagyonnyilatkozatával. A biztos álláspontja szerint amennyiben a képviselővel szemben vagyonnyilatkozati eljárás nem indult, úgy megbízatásának megszűnése után a vagyonnyilatkozatot vissza kell juttatni számára, vagy kérésére meg kell semmisíteni. *(1564/K/2006)*

Politikai kampány és információszabadság

A 2006-os esztendő választási kampányai és belpolitikai eseményei nemcsak a személyes adatok védelmével, hanem a közérdekű adatok nyilvánosságával kapcsolatos beadványokban is megjelentek.

Júliusban tizenöt panaszostól elektronikus levélben eljuttatott azonos tartalmú panasz érkezett az adatvédelmi biztoshoz azt kifogásolva, hogy a kormány az országgyűlési választásokat megelőzően közérdekű adatokat tartott vissza: eltitkolta az ország valós pénzügyi helyzetét, az adatokat csak közvetlenül a választások második fordulója után hozta nyilvánosságra. A biztos állásfoglalásában utalt arra, hogy az Avtv. kétféle adatszolgáltatást határoz meg: egy időpontokat, határidőt, adatfajtákat és szankciókat nem tartalmazó, úgynevezett általános tájékoztatási kötelezettséget és a konkrét adatigénylés alapján történő adatszolgáltatást, ezen kívül az államháztartással összefüggő adatok körében számos jogszabály ír elő kérelem nélküli közzétételi kötelezettséget. A panaszosok adatigényléssel nem fordultak a kormányzati szervekhez. A vizsgálat megállapította, hogy a Pénzügyminisztérium az adatigénylés nélküli közzétételi kötelezettségének az államháztartás működési rendjéről szóló 217/1998. (XII. 30.) Korm. rendeletben foglalt határidőket betartva a kampány során eleget tett. *(1018/A/2006, 1054/A/2006 -1068/A/2006, 1122/A/2006)*

Egy állampolgár abban kért állásfoglalást, hogy egy pártnak, egy egyesületnek, egy klubnak, egy vallási közösségnek vannak-e személyiségi jogai, hogy jogszerűen nyilvánosságra hozható-e mindaz, ami e szervezetek nem nyilvános összejövetelein elhangzik. A biztos leszögezte, hogy a felvetett kérdést illetően csak részben rendelkezik kompetenciával. Utalt arra, hogy az Avtv. szerint személyes adata csak természetes személyeknek van, e jog védelme tehát csak őket illeti meg. Amennyiben a felsorolt szervezetek nemnyilvános üléseiről a résztvevők hozzájárulása nélkül információk (például hang- vagy képfelvételek) kerülnek ki, ez felvetheti az ott

részt vevő személyek személyes adatainak sérelmét. Emiatt az érintettek bírósági eljárást kezdeményezhetnek, vagy panasszal fordulhatnak az adatvédelmi biztoshoz. Ugyanakkor a jogi személyeknek is vannak személyiségi jogaik. Ilyen a magántitokhoz való jog, mely az Alkotmány 59. § (1) bekezdése szerint egyben alkotmányos jog is. A magántitok sérelme esetén – jóllehet ez kétségtelenül határos a személyes adatok megsértésével – az adatvédelmi biztosnak nincs módja eljárni, de a hazai jogrendszerben van más megfelelő jogorvoslati lehetőség. A magántitok ugyanis polgári jogi és büntetőjogi védelem alatt áll. *(1054/K/2006)*

2006 szeptemberében az adatvédelmi biztos közleményt adott ki az információs jogok tiszteletben tartásának fontosságáról. Ebben hangsúlyozta: „*Az elmúlt hét politikai, közéleti eseményei kapcsán ismételten tapasztalnom kellett, hogy a politikusok, közéleti szereplők részéről egyre több fenyegetés éri az alkotmányos jogokat. Az adatvédelem és az információszabadság országgyűlési biztosaként elfogadhatatlannak tartom, hogy az információs jogok a politikai viták és konfliktusok áldozatává vagy harci fegyverévé legyenek. A szabad véleménynyilvánítás nem járhat mások jogainak sérelmével. A felfokozott politikai hangulat nem jelent felmentést az alól, hogy az adatok jogellenes gyűjtése, átadása, nyilvános közlése a személyes adatok védelméhez való jog megsértését jelenti, amely súlyosabb esetben büntetőjogi felelősségre vonást is eredményezhet. Nem hagyhatom szó nélkül, hogy a tüntetéseken, rendezvényeken, az azokról tudósító híradásokban szereplő személyek – politikusok, közéleti személyiségek, nyilvánossághoz jutó állampolgárok – másokról olyan tartalommal nyilatkoznak, amely túllép a szabad véleménynyilvánításhoz való jog gyakorlásán, és nem csupán az érintettek becsületét, jó hírnevét, de személyes adataik védelméhez való jogát is sérti. A magyar adatvédelmi szabályok szerint egyes személyes adatok – többek között az egészségi állapotra, faji eredetre, nemzeti és etnikai kisebbséghez tartozásra, vallásos meggyőződésre vonatkozó adatok – fokozott védelem alatt állnak. Az ilyen, különleges adatokkal kapcsolatban elkövetett visszaélés – például egyes személyek vallásos meggyőződésének nyilvánosságra hozatala – akár bűntettet is megvalósíthat, és három évig terjedő szabadságvesztést vonhat maga után. Nyomatékkal hangsúlyozom továbbá, hogy az információszabadság nem pártpolitikai harci eszköz, hanem a polgároknak a rendszerváltáskor született alkotmányos joga, hogy az államot ellenőrizzék.*” *(1459/H/2006)*

Egy állampolgár adatvédelmi biztosi vizsgálatot és intézkedéseket kezdeményezett a miniszterelnök szeptemberben nyilvánosságra

került beszédével kapcsolatban. A vizsgálat megállapította, hogy a panasz által felvetett ügyben az adatvédelmi biztosnak nincs hatásköre. Ugyanakkor általános jogi állásfoglalást adott arra vonatkozóan, hogy a miniszterelnököt milyen kötelezettségek terhelik a közérdekű adatok nyilvánosságának biztosításával kapcsolatban.

Az Alkotmány, az alkotmánybírósági határozatok, a hatályos jogszabályok és érvényes hazai és nemzetközi jogelvek alapján a biztos megállapította, hogy a miniszterelnök állami vezetőként köteles a pozíciójához kötődő feladatkörében a magyar társadalmat foglalkoztató kérdésekben a közvélemény rendszeres, pontos és tényszerű tájékoztatására. A tájékoztatási kötelezettség különösen kiterjed az állami költségvetéssel összefüggő közérthető információk és következtetések nyilvánosságra hozatalára. Az adatoknak pontosaknak és tényszerűeknek kell lenniük. A nyilvánvalóan hamis vagy meghamisított információk ugyanis az állampolgárok félrevezetését, az állam működésének átláthatatlanságát eredményezik, ezáltal a jogállamiság és a demokratikus alapelvek, valamint az alkotmányos jogok egyértelmű megsértésével járnak.

A biztos állásfoglalásában idézte az Alkotmánybíróság 34/1994. (VI. 24.) AB határozatát, mely szerint *„A nyílt, áttetsző és ellenőrizhető közhatalmi tevékenység, általában az állami szervek és a végrehajtó hatalom nyilvánosság előtti működése a demokratizmus egyik alapköve, a jogállami államberendezkedés garanciája.”*

Fontosnak tartotta azt is hangsúlyozni, hogy a jogi és erkölcsi kategóriák mesterséges szétválasztása beláthatatlan következményekkel és veszélyekkel járna. *(1443/A/2006)*

Sajtószabadság vagy információszabadság?

Ebben az esztendőben ismét felmerült a két jog együttes értelmezésének, illetve elhatárolásának kérdése. A biztos korábbi ügyek vizsgálata nyomán kialakított álláspontja, hogy az úgynevezett kommunikációs jogok (a sajtószabadság, a véleménynyilvánítás szabadsága, az információszabadság) rokon jogok, elhatárolásuk gyakran nem egyszerű, mégis látni kell a különbségeiket. Leszögezte, hogy felhatalmazása csak az információszabadsággal kapcsolatos ügyek kivizsgálására van.

Egy állampolgár a rádiózásról és televíziózásról szóló 1996. évi I. törvény (Rttv.) 49. § (1) bekezdése, valamint a közérdekű adatok

megismeréséhez való jog együttes értelmezésével kapcsolatos kérdésben kérte a biztos állásfoglalását. A beadványozó szerint valamennyi, az Rttv. hatálya alá tartozó műsorszolgáltatónak kötelessége, hogy az Alkotmány 61. §-a alapján az érintettek számára biztosítsa a közérdekű adatok megismeréséhez való jogosultságot. Ez nyilvánvalóan csak úgy lehetséges, ha valamennyi állampolgár számára biztosított annak lehetősége, hogy az idézett Rttv. paragrafushoz kapcsolódó esetekben álláspontja ismertetésre kerül. A biztos válaszában utalt arra, hogy az Avtv. definíciója szerint a közérdekű adatok az információk egy meghatározott körét: a közfeladatot ellátó szervek kezelésében lévő adatokat jelentik, és nem azonosak valamennyi közérdeklődésre számot tartó információval. A műsorszolgáltatóknak az az Rttv.-ből fakadó kötelezettsége, hogy betartsák a kiegyensúlyozott tájékoztatás követelményét, nincs összefüggésben a közérdekű adatok megismeréséhez fűződő joggal. A *„közfeladatot ellátó szerv kezelésében lévő adat”* kifejezés már létező, a szerv birtokában lévő adatot jelent. Az Rttv. szóban forgó rendelkezése viszont a kifejezés, a véleménynyilvánítás szabadságával és a kiegyensúlyozott tájékoztatás követelményével függ össze, melynek érvényesülését hatáskör hiányában a biztos nem vizsgálhatja. *(513/K/2006)*

Egy másik ügyben a panaszos a közfeladatot ellátó személyek tájékoztatási kötelezettségének megszegését kifogásolta. Arra hivatkozott, hogy a Hír Televízió híradója szerint az Egészségügyi Minisztérium államtitkára nem engedte meg a Hír Tv munkatársának, hogy egy nyilvános sajtótájékoztató után kérdést tegyen fel. Ugyancsak kifogásolta, hogy tudomása szerint a kormány egyetlen tagja sem fogadja el a Hír Televízió meghívását, mindez pedig sérti a közfeladatot ellátó személyeknek az Avtv.-ben foglalt tájékoztatási kötelezettségét. A biztos állásfoglalása szerint az Avtv. kétféle adatszolgáltatást határoz meg: egy időpontokat, határidőt, adatfajtákat és szankciókat nem tartalmazó, úgynevezett általános tájékoztatási kötelezettséget [19. § (1) bekezdése] és a konkrét adatigénylés alapján történő adatszolgáltatást (20. §). Az úgynevezett általános tájékoztatási kötelezettség formáját, tartalmát, gyakoriságát a törvény nem határozza meg. Az eddigi gyakorlat alapján e tájékoztatási kötelezettség teljesítéseként foghatók fel a közfeladatot ellátó személyek nyilvános szereplései: a parlamentben, a politikai rendezvényeken elmondott beszédek, a sajtótájékoztatók, a sajtó által készített interjúk, a közzétett publikációk. E tájékoztatási kötelezettség az Avtv. által definiálatlan, ezért ennek elmulasztása a biztos által csak akkor volna vizsgálható, ha a közfeladatot ellátó személyek az

előbbiekben felsorolt eszközökkel egyáltalán nem vagy csak nagyon ritkán élnének. A biztos hangsúlyozta, hogy az Avtv.-ben foglalt kötelezettségek nem csupán a kormány tagjaira, hanem valamennyi közfeladatot ellátó személyre vonatkoznak, így például valamennyi parlamenti vagy önkormányzati képviselőre, a polgármesterekre, stb. Az állásfoglalás szerint valóban jelentősen érintheti egyes médiumok tájékoztatási lehetőségeit, ha a közfeladatot ellátó személyek *„szelektív tájékoztatáspolitikát”* alkalmaznak. Hátráltathatja a médiatörvényben meghatározott tárgyilagos és kiegyensúlyozott tájékoztatást, ha a közfeladatot ellátó, választott vagy kinevezett tisztségviselők különbséget tesznek médiumok között. A minisztériumi sajtótájékoztatók rendje, a kormánytagok vagy kormányzati tisztviselők nyilatkozatadási gyakorlata azonban nincs összefüggésben a közérdekű adatok megismerésének az Avtv.-ben meghatározott szabályaival. Felvethetik a sajtószabadság sérelmét, ennek vizsgálatára azonban a biztosnak az adatvédelmi törvény alapján nincs hatásköre. *(2016/A/2006)*

C. Az adatvédelmi biztos jogalkotással kapcsolatos tevékenysége

Az adatvédelmi biztos nem rendelkezik jogalkotó hatáskörrel és nem tartozik a jogszabálytervezetek előkészítéséért felelős szervek közé sem, ezért általában a leendő jogszabály szabályozási tárgya szerint illetékes minisztériumi szakapparátus által előkészített tervezetről kell állást foglalnia. A biztos független a kormánytól, azonban a jogalkotással kapcsolatos tevékenységének nagymértékben igazodnia kell a kormányzati szabályozási előkészítő munka menetéhez, ütemezéséhez. A beszámolónak emiatt szükségképp ki kell térnie a kormányzati döntés-előkészítés azon részleteire, amelyek a biztos munkájára is kihatással voltak. A 2006. január 1-jén hatályba lépett az elektronikus információszabadságról szóló 2005. évi XC. törvény (Etiv.) egyértelművé teszi, hogy a jogszabályok előkészítése a közigazgatási egyeztetés kezdetétől fő szabályként nyilvános, következésképp a kormányzati jogszabály-előkészítés egyes 2006-os adatainak ismertetése nem indiszkréció.

Az idei beszámoló újdonsága a jogalkotással kapcsolatos tevékenységünk számszerű adatainak részletesebb elemzése. Ezt az az informatikai rendszer teszi lehetővé, amely támogatást nyújt az adatvédelmi biztos jogalkotással kapcsolatos tevékenységéhez. A nyilvántartó és ügyfeldolgozást segítő, integrált rendszer összekapcsolja az ügyek, a jogszabálytervezetek, a törvényjavaslatok és a jogszabályok nyilvántartását, egységes ügyviteli rendszerbe foglalva a biztos állásfoglalásainak előkészítését, valamint a törvényjavaslatok és a kihirdetett jogszabályok nyomon követését.

Az ügyek nagy száma miatt nem lehetséges tevékenységünk átfogó és részletes bemutatása. A korábbi évek gyakorlatának megfelelően idén is válogatunk az ügyek közül, azokat bemutatva, amelyek valamilyen szempontból jellegzetesek, fontosak, és ezért érdeklődésre tarthatnak számot. Idén az adatvédelmi biztos jogalkotással kapcsolatos feladatainak ismertetésébe ágyazva ismertetjük az állásfoglalásokat.

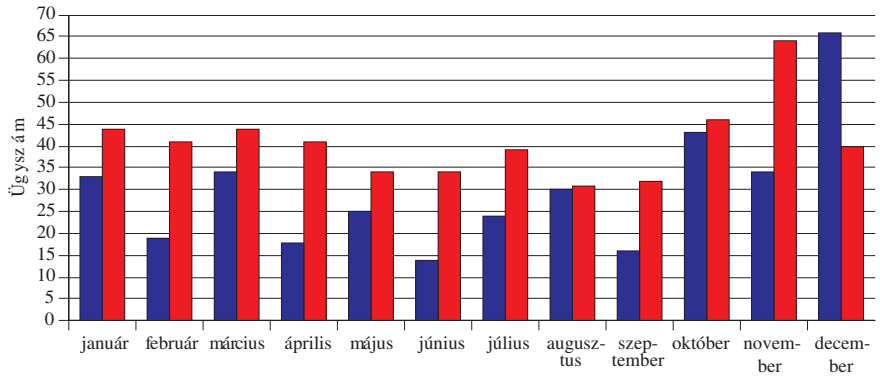
Az ügyek ismertetésében a kritika dominál. Nem azért, mintha lebecsülnénk a kormányzati jogszabály-előkészítő szakemberek munkáját, hanem azért, mert a beszámoló céljára tekintettel az elismerés kifejezésénél hasznosabb a problémákra, a még megoldandó feladatokra rávilágítani.

A véleményezett tervezetek száma

Az alábbi táblázat szemlélteti a véleményezett jogszabálytervezetek, valamint jogalkotással kapcsolatos egyéb tervezetek számának alakulását a korábbi két évhez viszonyítva:

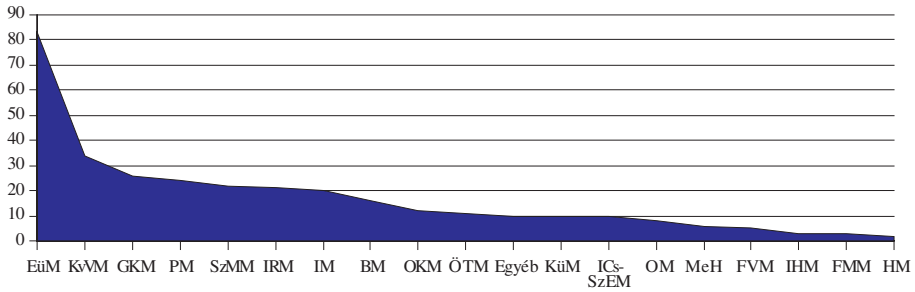
Év	**2004**	**2005**	**2006**
Törvény	83	130	48
Kormányrendelet	121	111	103
Miniszteri rendelet	179	158	127
Önkormányzati rendelet	0	0	0
Országgyűlési határozat	(Nincs adat)	(Nincs adat)	1
Kormányhatározat	58	43	21
Egyéb	34	46	26
Összesen	**475**	**488**	**326**

Szembetűnő a véleményezésre küldött tervezetek számának csökkenése, ami a törvénytervezetek esetében drasztikusnak mondható. Az összképen az a mintegy két tucat 2006-os adatvédelmi biztosi szabályozási kezdeményezés sem változtatna, amelyre a törvényjavaslatok és a kihirdetett jogszabályok monitorozása, illetve állampolgári beadványok vizsgálata nyomán, hivatalból került sor. Ugyancsak nem változtat a statisztikán az, hogy 30 esetben több fordulós egyeztetésre került sor, azaz az előterjesztő ismét véleményt kért az észrevételek nyomán átdolgozott jogszabálytervezetről. Érdekes ugyanakkor a véleményezésre érkezett tervezetek számának vizsgálata havonkénti bontásban az előző év adataihoz hasonítva.



A tervezetek száma december kivételével minden hónapban kevesebb volt a 2005. év megfelelő adatánál, és a korábbi évekénél nagyobb ingadozás tapasztalható a számokban. Az ügyszám februárban, áprilisban, júniusban és szeptemberben csökkent leginkább. A tavaszi visszaesés időben egybeesik az országgyűlési választásokkal és az új kormány megalakulásával. Valószínű, hogy a kormányzati apparátusokat ebben az időszakban a választási és a kormányváltással kapcsolatos feladatok kötötték le.

Figyelemreméltó, miként növekedett meg decemberben az ügyek száma. Az adatvédelmi biztos hivatalának fennállása óta még sosem fordult elő, hogy egy hónap alatt ennyi tervezetet küldjenek véleményezésre[1]. Az ismételten véleményezésre küldött tervezeteket is beleszámítva kevesebb mint három hét alatt 66 jogszabályról kellett állást foglalni, ami átmenetileg túlterhelte az adatvédelmi biztos munkaszervezetének szakértői kapacitását. A következő diagram a véleményezendő tervezetek beküldő minisztériumonkénti megoszlását szemlélteti.



Az adatok értelmezését némileg nehezíti, hogy év közben megváltozott a kormány felépítése, azonban megállapítható, hogy az Egészségügyi Minisztérium adatkezeléssel kapcsolatos szabályozási tevékenysége volt a legintenzívebb. A 83 jogszabálytervezet több mint a kétszerese a második helyezett Igazságügyi és Rendészeti Minisztériumból érkezett 41-nek (beleszámítva a jogelőd Igazságügyi Minisztérium adatát is.). Sorrendben a harmadik a Környezetvédelmi és Vízügyi Minisztérium 34 tervezettel, amelyek között azonban számos

1 Valójában nem is egy teljes hónap adatáról van szó, mert a december 20-a után érkezett tervezetek a 2007-es statisztikában fognak szerepelni.

olyan volt, amely nem tartalmazott a személyes adatok védelmével és a közérdekű adatok nyilvánosságával kapcsolatos rendelkezést.

> Például a rezervátumok létesítéséről szóló KvVM rendeleteknek legfeljebb annyi közük van az adatvédelmi biztos által oltalmazandó alapjogokhoz, hogy a rezervátumok területét, határait kijelölő felsorolások felfoghatók közérdekű adatként *(1273/J/2006, 1228/J/2006, 1115/J/2006)*. Ennek ellenére az adatvédelmi biztos nem kifogásolja a tervezetek megküldését, hiszen az adatkezelési szabályt nem tartalmazó tervezetek felesleges átnézése kisebb rossz, mintha egy az alapjogvédelem szempontjából fontos tervezet véleményezése elmarad.

A határidők

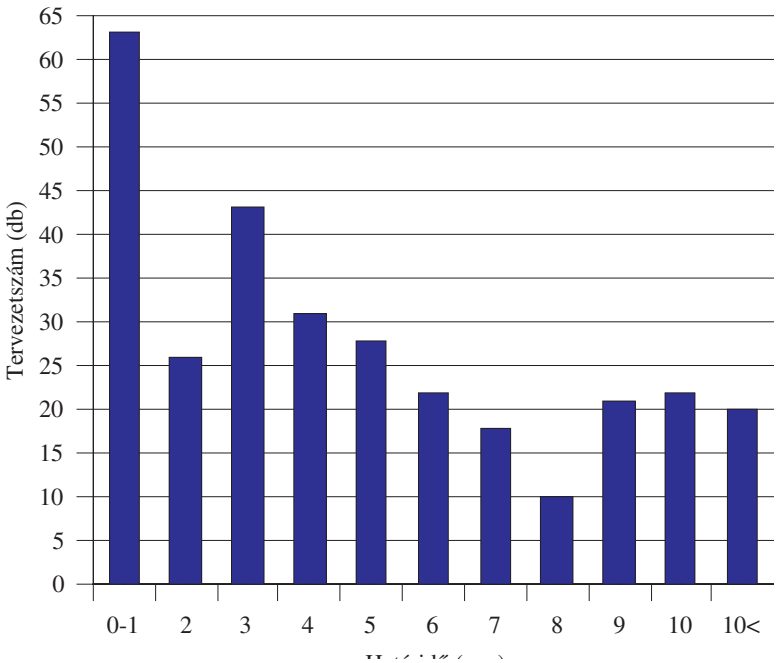
Egy demokratikus jogállamban a minőségi jogalkotáshoz az érdekeltek jogszabály-előkészítésbe való bevonása mellett az is hozzátartozik, hogy megfelelő idő álljon rendelkezésre a tervezet elemzésére, a véleményalkotásra, a különféle vélemények kifejtésére, közlésére, ütköztetésére, egyeztetésére és végül a szabályozási tervezet összeállítására. A Jat. arra kötelezi a jogszabály előkészítőjét, hogy a megalapozott véleményalkotáshoz szükséges időt biztosítsa a véleményezők számára.

A megalapozott véleményalkotáshoz szükséges időtartam függ a tervezet terjedelmétől és bonyolultságától, azonban általánosságban kijelenthető, hogy három munkanap, vagy annál rövidebb véleményezési határidő csak a rövid és egyszerű megítélésű tervezetek esetében fogadható el. (Az ügyvitel elektronizálása nélkül nem is lenne lehetséges ilyen rövid határidők megállapítása, mert három munkanap papír alapú ügyvitellel kevesebb, mint a postafordultához szükséges idő. 2006-ban például – a több fordulós egyeztetéseket is figyelembe véve – 315 előterjesztés érkezett elektronikus levélben, míg 41 hagyományos úton.)

A korábbi évek beszámolói elrettentésül mindig *„tollhegyre tűztek”* néhány olyan ügyet, amelynél azt kellett kifogásolni, hogy az előterjesztő túl rövid véleményezési határidőt határozott meg. Az egy munkanapos vagy annál rövidebb véleményezési határidő nem felel meg a jogalkotási törvény előírásainak. Szerencsére korábban ilyen extrém rövid határidejű ügyből legfeljebb ha másfél tucat fordult elő évente. E kétes dicsőségű ranglista első helyére 2006-ban egy olyan

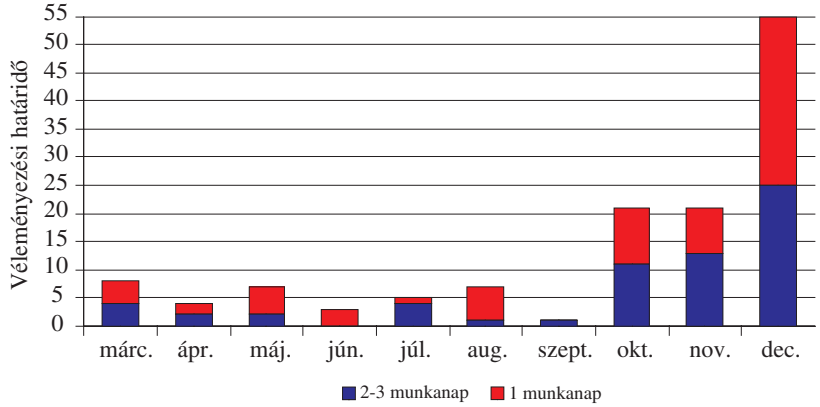
előterjesztés került, amely egyik nap délelőtt tizenegy órakor azzal az instrukcióval érkezett a hivatalunkhoz, hogy soron kívül várják hozzá az észrevételeket, amelyeket másnap délelőtt tíz órakor tartandó értekezleten kívánnak megvitatni. Az előterjesztés egyébként mintegy 150 oldal terjedelmű volt, és öt nem egyszerű megítélésű kormányrendelet-tervezet tartozott hozzá *(1726/J/2006)*.

Sajnos 2006-ban az ügyintézési határidőkkel kapcsolatban olyan változás következett be, amely részletes elemzést igényel. A 2006 március–december időszakban érkezett 304 tervezet közül 132 legfeljebb három napos véleményezési határidejű volt, egy munkanapos határidővel pedig 63 tervezet érkezett[2]. A következő ábra a tervezetek véleményezési határidő szerinti megoszlását mutatja.

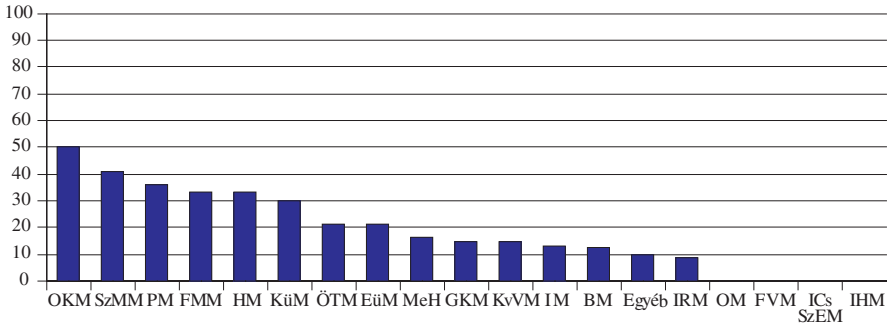


2 Márciustól állnak rendelkezésre statisztikai elemzésre alkalmas adatok.

Még tanulságosabb a rövid véleményezési határidejű tervezetek havonkénti megoszlásának bemutatása darabszám szerint:



Amint az ábra mutatja, az év első háromnegyed részében nagyjából a szokásos módon folyt a munka, majd októberben megugrott a rövid véleményezési határidejű tervezetek száma. Decemberben a 66 véleményezésre kapott tervezet mintegy 83 %-a legfeljebb 3 napos határidejű volt, míg 25 tervezet véleményezésére csak egy munkanap állt rendelkezésre. Sőt, decemberben az is többször előfordult, hogy az előterjesztő órákban határozott meg egy napnál rövidebb határidőt.



Az adatok arra utalnak, hogy 2006-ban a *„jogszabálygyár”* termelésének volumene a korábbiakhoz képest kisebb, azonban nagyobb időbeli ingadozást mutat. A kormányzati szabályozási döntés-előkészítés 2006 utolsó negyedében felgyorsult. Az egy napos, jelképes véleményezési határidejű tervezetek száma minden korábbit nagyság-

rendileg felülmúló volt. Ilyen körülmények között aligha lehet szó megalapozott, felelősségteljes véleményalkotásról. Tartani lehet attól, hogy az előkészítés túlzott felgyorsítása a jogi szabályozás minőségét hátrányosan fogja befolyásolni. Végül a következő diagram minisztériumonként mutatja be, hogy a véleményezendő tervezetek hány százalékát küldték kifogásolható véleményezési határidővel. A teljesíthetetlenül rövid véleményezési határidők tömeges előfordulása nehéz dilemma elé állítja azt, akinek törvényes feladatkörébe tartozik a tervezetek véleményezése: utasítsa vissza a véleményezésre vonatkozó felkérést, vagy vegyen részt a Jat. előírásainak nem megfelelő eljárásban, és adjon esetleg kiérleletlen, helytelen véleményt.

A jogszabálytervezetek véleményezése

A 2006-os jogalkotására kétségtelenül az nyomta rá leginkább a bélyegét, hogy nagyjából az év közepétől, a társadalom életére és az állam működésére jelentős hatást gyakorló reformok gyors előkészítése indult el. Ezek jellemzője, hogy a jogalkotói akarat akár több új, egymással összefüggő törvény megalkotásában és számos más törvény és más jogszabály módosításában nyilvánul meg. A több összefüggő jogszabály párhuzamos előkészítése mind az azért felelős kormányzati tisztviselőktől, mind a jogszabály-előkészítésben közreműködőktől koncentrált figyelmet igényel, és még így is nagy a tévedés veszélye. Nem könnyű több egymáshoz kapcsolódó törvény országgyűlési tárgyalását, valamint a törvények végrehajtási rendeleteinek párhuzamosan folyó előkészítését figyelemmel kísérni úgy, hogy a végrehajtási rendeletek tartalmát meghatározó törvényjavaslatok még képlékeny állapotban vannak. Az előterjesztő a jogszabály tervezetéhez előterjesztést és indokolást csatol ugyan, azonban rendszerint nem állnak a véleményező rendelkezésére azok a háttértanulmányok és hatásvizsgálatok, amelyek a tervezett szabályozás mélyebb összefüggéseinek és hosszabb távú hatásainak megismerését elősegítenék.

> Az egészségügyi reformmal összefüggő törvények előkészítése kapcsán az Egészségügyi Minisztérium szakállamtitkára által kezdeményezett megbeszélésen felmerült, hogy az állampolgárok egészségügyi életútjának nyomon követését lehetővé tevő központi adatbázis szükségességének és az információs önrendelkezési jog korlátozása arányosságának mérlegeléséhez ismerni kel-

lene a lehetséges informatikai-igazgatásszervezési alternatívákat és a minisztérium hosszabb távú fejlesztési terveit *(1600/J/2006, 1601/J/2006, 1614/J/2006)*

Az adatvédelmi biztos az egyes pénzügyi tárgyú törvények módosításáról szóló T/231. számú törvényjavaslattal kapcsolatban kiadott állásfoglalásában az elmúlt évek hasonló tárgyú törvénymódosításait áttekintve megállapítható, hogy a hatóságok közötti adatszolgáltatásra, adatátadásra vonatkozó változások rendszerint az információs önrendelkezési jog újabb és újabb korlátozásával, egyre több személyes adat hatóságok általi kezelésével járnak. A köztehervisélés és az állami bevételek biztosításának fontosságát elismerve némi aggodalomra ad okot ez a tendencia. Az állásfoglalás kifogásolja még azt, hogy a módosítások indokolása néhol semmitmondó, és nincs összhangban a tervezett intézkedésekkel. *(958/J/2006)*

A Miniszterelnöki Hivatal államtitkára felkérte az adatvédelmi biztost a köztisztviselői teljesítményértékelés és jutalmazás, valamint az azokkal összefüggő adatkezelés törvényi szabályozása céljából a köztisztviselők jogállásáról szóló 1992. évi XXIII. törvényhez (Ket.) benyújtandó módosító javaslat véleményezésére. A módosító javaslat a teljesítményértékeléssel összefüggő adatkezelés centralizálására vonatkozott. A biztos egyéb kifogásai mellett rámutatott, hogy a rendelkezésre álló dokumentumok – a módosító javaslat szövege és annak indokolása alapján – még arról sem lehet felelősséggel állást foglalni, hogy egyáltalában szükséges-e a központi nyilvántartás létrehozatala. A Ktv.-kiegészítés és a törvénymódosításhoz kapcsolódó végrehajtási rendeletalkotás időszaka átfedésben volt. Később az előterjesztő képviselője egyeztetést kezdeményezett, melynek során közösen sikerült megtalálni a személyes adatok védelme szempontjából megfelelő jogi szabályozási megoldásokat. *(2009/J/2006, 2020/J/2006)*

A folyamatban lévő reformok érintik az államszervezetet. Adatvédelmi szempontból nem mindegy, hogy a szabályozás változásai miképp befolyásolják az állami feladatok ellátáshoz szükséges személyes adatkezelést.

2006 szeptemberében az Igazságügyi és Rendészeti Minisztérium megküldte véleményezésre a Magyar Köztársaság minisztériumainak felsorolásáról szóló 2006. évi LV. törvénnyel és a központi államigazgatási szervekről, valamint a Kormány tagjai és az államtit-

károk jogállásáról szóló 2006. évi LVII. törvénnyel összefüggő egyes törvények módosításáról szóló törvény tervezetét. A nagy terjedelmű törvénytervezet célja a dereguláció és az egységes terminológia kialakítása mellett a közigazgatás ésszerűsítése és a kormány szervezetalakítási szabadságának érvényre juttatása az országos hatáskörű szerveket, központi hivatalokat és azok területi szerveit nevesítő rendelkezések olyan módosításával, hogy a törvényekben és a törvényerejű rendeletekben a hivatalok, szervek konkrét megnevezése helyett általános, a feladatkörre utaló megnevezések szerepeljenek. A szervezetalakítás kormánykompetenciába utalása érinti a közigazgatási szervezetekben történő adatkezelés szabályozását is. A tervezett változások következményeképp a közigazgatási szervezeten belüli adatkezelés, adatáramlás szabályozásának a jelenleginél nagyobb hányada kell, hogy végrehajtási rendeleti szintre kerüljön. Az Avtv. 3. §-ának (3) bekezdése szerint kötelező adatkezelés esetén az adatkezelés célját és feltételeit, a kezelendő adatok körét és megismerhetőségét, az adatkezelés időtartamát, valamint az adatkezelő személyét az adatkezelést elrendelő törvény vagy önkormányzati rendelet határozza meg. Az elfogadható, ha a törvény az adatkezelő személyét absztrakt módon, a feladataira utalva határozza meg, azonban olyan értelmezés nem lehetséges, amely szerint a közigazgatáson, illetve az állam szervezetein belüli adattovábbításokat törvénynél alacsonyabb szintű jogszabály rendelhetné el. A levél arra is felhívta a figyelmet, hogy ha az átszervezések folytán megváltozik az adatkezelő megnevezése, akkor a szabályozás tárgya szerint illetékes miniszter kötelessége bejelenteni az adatok megváltozását az adatvédelmi nyilvántartásba. *(1309/J/2006)*

A tervezett szervezet-összevonások következményeként azonos állami szervezet kezelésébe kerülhetnek jogelőd szervezeteknél különféle törvények alapján eltérő célból kezelt adatok. A szervezeti változás azonban kifejezett törvényi felhatalmazás hiányában nem járhat együtt az adatállományok összekapcsolásával vagy az eredetitől eltérő célú felhasználásával. *(958/J/2006, 1309/J/2006)*

Sajnos különösen az év utolsó negyedében nem lehetett nem észrevenni, hogy a véleményezendő tervezetek egy részében olyan hibák maradtak, amelyek arra utalnak, hogy nemcsak a közigazgatási egyeztetésre nem volt elég idő, de az azt megelőző szakmai és jogszabályszerkesztési előkészítésre sem.

Egy adatkezelő állami szervezetek összevonását célzó kormányrendelet véleményezésre kapott tervezetét többek között azért kellett kifogásolni, mert annak felépítése, szerkezete zavaros, ellentmondásos volt. A tervezet a személyiadat- és lakcímnyilvántartás részeként nevesítette a bűnügyi nyilvántartás résznyilvántartásait, az úti okmány nyilvántartást, a Magyar Igazolvány nyilvántartást, valamint további, közelebbről meg nem határozott nyilvántartásokat. A közúti közlekedésről szóló címe alatt kaptak helyet a közszolgálati és az idegenrendészeti nyilvántartással kapcsolatos adatfeldolgozói tevékenységek. Nem engedhető meg a különféle felhatalmazás alapján történő személyes adatkezelések ilyesféle összemosása. *(2004/J/2006).*

Az egyik, az Országgyűléshez benyújtott törvényjavaslat eredeti szövege *„legfeljebb 14 éves kiskorú”*-t és *„legalább 24 órás nyitvatartási idejű”* intézményt említ *(1601/J/2006).*

A már említett, a köztisztviselői teljesítményértékeléssel kapcsolatos adatkezelés részletes szabályait tartalmazó végrehajtási rendelet tervezete a szabályozás tartalmának megismerését zavaró jogszabályszerkesztési hibák miatt is kifogásolandó volt *(2009/J/2006).*

Az egyes pénzügyi tárgyú törvények módosításáról szóló törvénytervezet előkészítése során a Pénzügyminisztérium képviselőitől kapott szóbeli tájékoztatásából derült ki, hogy a taj-szám adóhatóság általi kezelésére vonatkozó, adatvédelmi szempontból erősen kifogásolt ideiglenes felhatalmazásra azért van szükség, mert későn derült ki számukra, hogy az adóhatóság informatikai fejlesztéseinek elmaradása miatt elháríthatatlan szabályozási szükséghelyzetbe kerültek. Az adatvédelmi biztos ezek után tudomásul vette a tájékoztatást, és néhány garanciális jellegű szabállyal javasolta kiegészíteni a törvénytervezetet. Később, a törvényjavaslat benyújtását követően országgyűlési bizottság előtt is beszámolt ezekről a történésekről *(1726/J/2006).*

Ugyancsak a jogszabály-előkészítési folyamat működési zavarára utal, hogy az adatvédelmi biztosnak 2006-ban számos alkalommal kellett szembesülnie azzal, hogy adatkezeléssel kapcsolatos jogszabálytervezeteket elmulasztották megküldeni hozzá véleményezésre. Erre részben a törvényalkotás nyomon követése, részben a kihirdetett jogszabályok hivatalból történő áttekintése során derült fény. A törvényalkotás nyomon követéséről később lesz szó, ezért most csak néhány, a 2006. évi 1-48. számú Magyar Közlönyökben kihirdetett jogszabályok rendszeres vizsgálatából származó adat következik.

A vizsgált időszakban 127, adatkezeléssel kapcsolatos jogszabályt hirdettek ki. Ezek nagyobb részét az adatvédelmi biztos korábban véleményezte, azonban 49 olyan is akadt, amely adatkezeléssel kapcsolatos rendelkezést tartalmazott, azonban elmulasztották véleményezésre megküldeni. Az igazsághoz az is hozzátartozik, hogy az utólagos elemzés többnyire azt állapította meg ezekről, hogy az adatkezelési szabályok tartalmilag nem kifogásolandók. Mindössze hat jogszabály tartalmazott olyan súlyú hibát, ami miatt a jogszabály módosítását kell javasolni. Ezek az ügyek még folyamatban vannak. *(1333/J/2006, 1436/J/2006, 1537/J/2006, 1551/J/2006, 1552/J/2006, 1824/J/2006)*

A problémát érzékelve a biztos 2006 júliusában levélben kereste meg a hivatalba lépett minisztereket, emlékeztetve őket törvényes egyeztetési kötelezettségükre. Az átiratra hat minisztertől érkezett válasz; ők kivétel nélkül az együttműködési készségüket hangsúlyozták *(1005/J/2006)*. Ennek ellenére továbbra is előfordult, hogy az adatvédelmi biztos csak utólag értesülhetett arról, hogy adatkezeléssel összefüggő törvény tervezetét az Országgyűlés elé terjesztették, illetve ilyen jogszabályt már ki is hirdettek. Hasonló megítélés alá esik az utólagos véleménykérés. Például az Egészségügyi Minisztérium a törvényjavaslatok Országgyűléshez történő benyújtását követően, tájékoztatásul küldte meg az úgynevezett egészségügyi reformcsomag néhány törvényét *(1600/J/2006, 1601/J/2006, 1614/J/2006)*. A minisztérium a T/1093. számú törvényjavaslatról még utólag sem kért állásfoglalást.

A törvényalkotás nyomon követése

Az adatvédelmi biztos 2006-ban a korábbinál nagyobb figyelmet fordított az Országgyűléshez benyújtott törvényjavaslatok sorsának figyelemmel kísérésére. Erre főként azért volt szükség, mert valamiképp *„nyakon kellett csípni"* azokat az adatkezeléssel kapcsolatos törvényjavaslatokat, amelyek tervezetét korábban, a közigazgatási koordináció időszakában elmulasztották megküldeni véleményezésre. Az is ösztönzőleg hatott, hogy a korábbi évek tapasztalatai szerint a törvényjavaslatokat tárgyaló országgyűlési bizottságok tagjai nyitottak az adatvédelmi biztos érveire. Végül a törvényalkotás munkájának figyelemmel kísérése azért is hasznos volt, mert 2006-ban többször előfordult, hogy országgyűlési bizottság vagy országgyűlési képviselő ál-

lásfoglalásra kérte fel az adatvédelmi biztost valamelyik éppen tárgyalt törvényjavaslattal, illetve módosító javaslattal kapcsolatban. Ilyen esetben értékes időnyereséggel járt, hogy a véleményezendő szöveg már nem volt ismeretlen az adatvédelmi biztos, illetve munkatársai számára, sőt esetleg előzetes elemzések is rendelkezésre álltak.

A sok törvényjavaslat és az azokhoz benyújtott nagyszámú módosító javaslat figyelemmel kísérésének informatikai feltételeit részben az Országgyűlés korszerű Parlamenti Információs Rendszere, részben az Adatvédelmi Biztos Irodájának ügyfeldolgozó rendszere biztosítja. Az új Országgyűlés hivatalba lépése óta 44, adatkezeléssel kapcsolatos törvényjavaslat sorsának alakulását követtük, követjük nyomon. Ezek listája a beszámoló függelékében található. Az informatikai rendszerben 74, adatkezeléssel összefüggő módosító javaslat adatait is regisztráltuk.

Hivatalból vizsgálta az adatvédelmi biztos az egyes pénzügyi tárgyú törvények módosításáról szóló T/231. számú törvényjavaslatot, amelyről már volt szó a beszámolóban. *(958/J/2006)*

Az államháztartásról szóló 1992. évi XXXI. törvény és egyes kapcsolódó törvények módosításáról szóló T/233. számú törvényjavaslat kapcsán az adatvédelmi biztos arra hívta fel az Országgyűlés Alkotmányügyi, igazságügyi és rendészeti bizottsága, valamint az emberi jogi, kisebbségi, civil- és vallásügyi bizottsága tagjainak figyelmét, hogy most, amikor az országnak lehetősége nyílik minden korábbinál jelentősebb európai uniós források felhasználására, indokolt lenne egyértelművé tenni, hogy az Áht.-ben meghatározott, a támogatások adatainak közzétételére vonatkozó kötelezettség az uniós forrásokból származó közpénzekre is vonatkozik. *(957/J/2006, 1830/J/2006)*

A pártok működéséről és gazdálkodásáról szóló 1989. évi XXXIII. törvény és a választási eljárásról szóló 1997. évi C. törvény, valamint ezzel összefüggésben egyes törvények módosításáról szóló T/237. számú törvényjavaslat a közérdekű adatok nyilvánossága szempontjából jelentős, üdvözlendő előrelépést irányoz elő a pártfinanszírozás átláthatóbbá tételével. A biztos emellett azt is jelezte, hogy a személyes adatok védelme szempontjából indokolt lenne az úgynevezett politikai marketinget oly módon is korlátozni, hogy a választópolgárok név- és lakcímadatait csak a kifejezett hozzájárulásuk esetén lehessen hozzáférhetővé tenni ilyen célra. Az állásfoglalás azt is megállapította, hogy a magánszemélyek által pártoknak

adott támogatások nyilvánossá tétele kifogásolható a személyes adatok védelme szempontjából, mert a különleges adatok kezelésének szabályozása nincs összhangban az adatvédelmi törvény előírásaival. *(1006/J/2006)*

A biztosítókról és a biztosítási tevékenységről szóló 2003. évi LX. törvény módosítására irányuló T/808. számú törvényjavaslat véleményezésére az Országgyűlés Gazdasági és informatikai bizottságának elnöke kérte fel a biztost, aki a törvényjavaslatot értékelve úgy válaszolt, hogy a törvényjavaslat olyan nyilvántartást és adattovábbítást kíván előírni, amelynek célja nem egyértelmű. A válasz kitért arra is, hogy noha a törvényjavaslatot korábban hivatalból megvizsgálta, a rendelkezésre álló részleges adatok birtokában a lehetséges jogsérelem súlyát mérlegelve nem kezdeményezte a törvényjavaslat módosítását. *(1494/J/2006)*

Ugyancsak országgyűlési bizottságtól érkezett felkérés az Európai Unió és az Amerikai Egyesült Államok között az utasnyilvántartási adatállomány (PNR) adatainak a légi fuvarozók általi feldolgozásáról és az Amerikai Egyesült Államok Belbiztonsági Minisztériuma részére történő továbbításáról szóló Megállapodás kihirdetéséről szóló T/1097. számú törvényjavaslattal kapcsolatban. A Külügyi és határon túli magyarok bizottságának elnöke kért tájékoztatást a biztos álláspontjáról. Az adatvédelmi biztos levelében ismertette a törvényjavaslat történeti előzményeit, így az Európai Tanács 2004. május 17-én elfogadott, ám az Európai Parlament kezdeményezésére az Európai Közösségek Bírósága által formai okból megsemmisített határozatának sorsát. A biztos fenntartásait hangoztatta amiatt, hogy az adattovábbítási felhatalmazások túl elnagyoltan, tágan vannak meghatározva a törvényjavaslatban. Arra is felhívta a figyelmet, hogy elmaradt a törvényjavaslat megfelelő előkészítése, és a tervezett törvény olyan részt is tartalmaz, amely nincs közvetlen összefüggésben a törvényjavaslat címével és fő szabályozási tárgyával. Amint az ismeretes, a törvényjavaslatot több országgyűlési bizottság sem tartotta általános vitára alkalmasnak és később a köztársasági elnök a már elfogadott törvényjavaslatot megfontolásra visszaküldte az Országgyűlésnek, éppen az adatvédelmi garanciák hiányossága miatt. *(1629/J/2006)*

A közérdekű adatok nyilvánossága érdekében kellett szót emelni a kormányzati szervezetalakítással összefüggő törvénymódosításokról szóló T/1202. számú törvényjavaslattal szemben. A törvényjavaslat tervezetét az Igazságügyi és Rendészeti Minisztérium korábban elküldte véleményezésre, azonban időközben mind a címe,

mind a tartalma módosult. A közigazgatási egyeztetést követően került bele az a rész is, amely a kormányülések mai dokumentálásának rendjét megváltoztatva megszüntetné a jegyzőkönyvezés kötelezettségét, az ülések dokumentálása helyett csupán egy úgynevezett összefoglaló készítését írva elő. A biztos emlékeztetett arra, hogy a tervezett változtatás ellentétes mindazzal, amit hivatali elődje és ő a kormányülések dokumentálásával, a dokumentumok megőrzésével és nyilvánosságával kapcsolatban korábban megfogalmazott. *(1329/J/2006)*

Az adatvédelmi biztosi ajánlás kiadására, közlemény vagy állásfoglalás közzétételére ügyeink kisebb részében kerül sor. Ezek általában olyan súlyú ügyek, amelyekről indokolt beszámolni.

Azért kellett sort keríteni a közfeladatot ellátó személyek feladatkörével összefüggő személyes adatai nyilvánosságára vonatkozó jogszabályok összhangjának megteremtéséről szóló ajánlás kiadására, mert az Avtv. 2005. június 1-jén hatályba lépett módosítását nem egészítette ki a közszféra különböző területein foglalkoztatottak jogviszonyát szabályozó törvények korrekciója. A biztos ajánlásában felkérte a Miniszterelnöki Hivatalt vezető minisztert, hogy a hatáskörrel rendelkező miniszterekkel együtt vizsgálja felül a közfeladatot ellátó személyek jogállására vonatkozó szabályokat, és szükség esetén kezdeményezze azoknak az Avtv.-vel összhangban álló módosítását. Az ajánlás részletes ismertetése az információszabadságról szóló fejezetben található. *(1234/H/2006)*

Hivatalból indított vizsgálat előzte meg a közgyógyellátás rendszerének adatvédelmi összefüggéseiről kiadott ajánlást, amely megállapította, hogy a közgyógyellátási jogosultságot megállapító jegyző nem ismerheti meg az érintett egészségügyi adatait – az egészségügyi rászorultság tényének kivételével –, ezt a jogszabálynak egyértelműen ki kell mondania. Az egészségbiztosítási szerv ugyanilyen indokok alapján nem jogosult a közigazgatási határozat azon részének megismerésére, melyen az érintett szociális helyzetére vonatkozó adatok szerepelnek. Végül az ajánlás leszögezi, hogy a gyógyszertár által a közgyógyellátási jogosultság ellenőrzése során kizárólag a törvényben meghatározott adatok rögzíthetőek, az OEP ezen túl adatrögzítést nem rendelhet el. *(1010/H/2006)*

2006 sajnálatos aktualitásai közé tartoznak a sorozatos élelmiszerbiztonsági botrányok, amelyek reflektorfénybe állították a fogyasztók tájékoztatási jogával kapcsolatos problémákat. Az ügyben foly-

tatott vizsgálat nyomán kiadott ajánlás kiindulópontja az, hogy az információszabadság révén a fogyasztók kiszolgáltatottsága csökkenthető. A nyilvánosság nemcsak a piaci helyzetükkel visszaélő termelőkkel és szolgáltatókkal szemben alkalmazható fegyver, de egyben érdeke a tisztességes piaci szereplőknek. A közérdekű adatok nyilvánossága hozzájárul a fogyasztói jogok érvényesüléséhez, mivel az információk nyilvánossága elősegíti a fogyasztóvédelmi szabályok érvényesülését, a fogyasztóvédelmi hatóságok tevékenységének átláthatóságát. Az ajánlás kezdeményezi egyebek mellett a fogyasztóvédelmi felügyelőségek eljárásának nyilvánosságát garantáló szabályok alkotását, valamint a közigazgatási eljárási és a szabálysértési normák harmonizálását. Az ügy utóéletéhez tartozik, hogy az adatvédelmi biztos a Ket. jogalkalmazási tapasztalatairól szóló jelentés tervezetéhez tett javaslatai között ismét sürgette olyan közigazgatási eljárási szabályok megalkotását, amelyek bizonyos feltételekkel lehetővé teszik a hatósági eljárás irataihoz való hozzáférést, ha az közérdekből szükséges. *(1866/J/2006)*

Évek óta újra és újra előkerül az úgynevezett *„pozitív adóslista”* létrehozatalának ötlete. 2006 elején számos hírforrás számolt be arról, hogy az állampolgári jogok országgyűlési biztosa által közzétett állásfoglalás nyomán *„elhárultak az alkotmányossági aggályok”*.

Az ezt követően kiadott adatvédelmi biztosi állásfoglalás leszögezte, hogy a személyes adatok védelmével kapcsolatos ügyekben elsősorban az adatvédelmi biztos jogköre állást foglalni. Az adatvédelmi biztosnak a pénzügyi szervezetek adatkezelését illetően tíz éves tapasztalata van, és az adósliták problematikáját is többször vizsgálta.

A most működő *„negatív”* adóslistával kapcsolatban korábban több ellenvetés hangzott el. Az adatvédelmi biztos és a Pénzügyi Szervezetek Állami Felügyelete is módosításokat javasolt a szabályozás előkészítéséért felelős Pénzügyminisztérium számára. Az adatvédelmi biztos részt vett azokon az egyeztetéseken, amelyek a mostani, adatvédelmi szempontból alapvetően elfogadható szabályozás megalkotásához vezettek.

A korábbi konzultációk folyamán a pozitív adóslista melletti legfőbb érv az volt, hogy a hitelezés kockázatának csökkenésével a hitelek kamata is csökkenhet. Az adatvédelmi biztos többször javasolta, hogy ezt az érvet támasszák alá olyan országokból származó adatokkal, ahol van pozitív adóslista. Erre mindeddig nem került sor, ezért a pozitív adóslista egyelőre csak egy kétes célú készletező adatgyűjtés lenne. Meglehet, hogy a pénzintézetek számára hasznos len-

ne, azonban az országgyűlési biztos feladata az állampolgárok jogainak védelme.

Érv az is, hogy a betétesek védelme, a tulajdonhoz való jog védelme szempontjából lenne előnyös a pozitív adóslista. Ezzel szemben a bankok csak kellő fedezet mellett, alapos hitelbírálat után nyújtanak hitelt, így a központi pozitív ügyféllista hiánya nem akadályozza a tevékenységüket.

Új érv a pozitív lista mellett a becsület és a jó hírnév védelme. Ez az érv igencsak kifacsart logikán alapul, hiszen a becsületet és a jó hírnevet nem hangoztatni kell, hanem védeni a támadások ellen.

A pozitív lista melletti érvek továbbra sem meggyőzőek, ezért az adatvédelmi biztos továbbra is fenntartja elutasító álláspontját, amelyen mindaddig nem változtat, amíg nem látja bizonyítottnak, hogy a pozitív lista olyan előnyökkel jár az állampolgárok számára, amely ellensúlyozza információs önrendelkezési joguk korlátozását. *(91/K/2006)*

Az elmúlt években az adatvédelmi biztos többször javasolt fokozottabb állami szerepvállalást a fogyatékos személyek részére nyújtott szolgáltatásokra vonatkozó információk nyilvánossága érdekében. Az egyes esélyegyenlőségi tárgyú törvények módosításáról szóló törvényjavaslat tervezetének véleményezésekor kezdeményezte a középületek akadálymentesítésének előrehaladására vonatkozó információk közzétételét, valamint javasolta az Eisztv. olyan kiegészítését, amely arra kötelezné a közfeladatot ellátó szerveket, hogy az interneten tegyék közzé azokat az információkat, melyek az általuk nyújtott nyilvános szolgáltatások akadálymentességére vonatkozik. Ezen információk nyilvánosságához kiemelkedő közérdek fűződik, hiszen az érintettek életminőségének javítása mellett ahhoz is hozzájárulnak, hogy a többiekkel azonos eséllyel vehessenek részt a társadalom életében. Az információk hasznosak lehetnek még azok számára is, akik a fogyatékos személyekhez hasonlóan akadályozva vannak. A biztos felhívta a figyelmet arra is, hogy a fogyatékosok esélyegyenlőségének elősegítése nem lehet kizárólag az állam, a közfeladatot ellátó szervek feladata, és elismerését fejezte ki azoknak, akik bárminemű törvényi kötelezettség nélkül is tettek, tesznek a fogyatékos személyek számára szükséges információk hozzáférhetővé tételéért. *(1820/J/2006)*

2006 októberében állampolgári panaszok alapján végzett vizsgálat lezárásaként nyilvános állásfoglalás született a társadalombiztosítási szervek által történő egyes adatkezelésekről. Az eljárás során

vizsgáltuk a háziorvosok kötelező és rendszeres havi adatszolgáltatását, az OEP-hez kerülő betegadatok körét, valamint a BNO-kód feltüntetését a vényköteles recepteken. Az adatvédelmi biztos hivatalból kiterjesztette a vizsgálatát az OEP-től kikerülő adatokra. A jogalkotási kezdeményezést is tartalmazó állásfoglalás részletes ismertetése a beszámoló egészségügyi adatkezelésről szóló részében található. *(1301/A/2006)*

Van a 2006-os ügyeinknek egy olyan része, amely makacsul ellenáll a rendszerezésre, csoportosításra, logikai összefüggések keresésére irányuló szerkesztői erőfeszítésnek, azonban ismertetésük nélkül nem lenne teljes a beszámoló.

Ajánlás kiadására nem került sor, de a közérdeklődésre tekintettel nyilvános az a levél, amelyben a lakosság energiafelhasználásának szociális támogatásáról szóló 231/2006. (XI. 22.) Korm. rendelettel kapcsolatos kifogásokat foglalja össze. Az állásfoglalás vitatja az adatkezelés jogalapját és az adatkezelés szabályozásának helyességét, kiváltképp az úgynevezett *„közreműködői feladatok"* meghatározásának tekintetében. Az ügy még folyamatban van. *(1824/J/2006)*

A Büntető Törvénykönyvről szóló 1978. évi IV. törvény és más büntetőjogi tárgyú törvények módosításáról szóló törvény véleményezése során tájékoztatta az adatvédelmi biztos az Igazságügyi és Rendészeti Minisztérium szakállamtitkárát arról, hogy vizsgálatainak tapasztalatai szerint a Btk. 177/A §-ában szabályozott *„visszaélés személyes adattal"* bűncselekmény tényállása nehezen alkalmazható, mert az alapesetének tényállási eleme a jelentős érdeksérelem. Fontos lenne, hogy akár a Btk., akár a szabálysértési jogszabályok módosítása útján biztosítva legyen a megfelelő szintű jogvédelem. *(1650/J/2006)*

Hivatalból indított vizsgálatunk azt állapította meg, hogy a hitelintézetek direkt marketing célú adatkezelési gyakorlata nem megfelelő és a hatályos jogszabályi rendelkezések sem egyértelműek. Gyakran előfordul, hogy az ügyfelek azért kénytelenek szerződéskötéskor aláírásukkal személyes adataik marketing célú kezeléséhez is hozzájárulni, mert erről külön nem nyilatkozhatnak. A szerződésbe foglalt hozzájárulás – különösen ebben a formában – azért megtévesztő, mert azt sejteti, hogy ezzel szemben nincs tiltakozási lehetőség. Az állásfoglalás olyan törvénymódosításra is javaslatot tett, amely csak az esetben tenné lehetővé direkt marketing célú megke-

resés elektronikus levélben történő továbbítását, ha ahhoz az érintett előzetesen kifejezetten hozzájárult. *(379/H/2006)*

Az országgyűlési választások adatvédelmi vizsgálatára szintén hivatalból került sor *(750/H/2006)*. A vizsgálat tapasztalatait és a jogi szabályozással kapcsolatos kezdeményezéseket a beszámoló választásokról szóló része tartalmazza.

A szolgálati titokköri jegyzékek

Az adatvédelmi biztos szolgálati titokkörökkel kapcsolatos véleményezési jogköre a személyes adatok védelméről és a közérdekű adatok nyilvánosságáról szóló 1992. évi LXIII. törvény (Avtv.) 25. §-ának (1) bekezdésével összhangban az államtitokról és a szolgálati titokról szóló 1995. évi LXV. törvény (Ttv.) 6. §-án alapul. A közleménnyel közzéteendő szolgálati titokköri jegyzéket bizonytalan jogforrási minősége is megkülönbözteti a véleményezendő jogszabályoktól, mégis célszerű azokkal együtt beszámolni a véleményezés céljából érkezett titokköri jegyzék tervezetekről. 2006 folyamán a következő szervek küldtek véleményezésre szolgálati titokköri jegyzék módosítására irányuló tervezetet:

- A Kormányzati Ellenőrzési Hivatal *(1000/T/2006)*
- A Magyar Kereskedelmi Engedélyezési Hivatal *(888/T/2006)*
- A Nemzeti Kutatási és Technológiai Hivatal *(439/J/2006)*
- A Rendvédelmi Szervek Védelmi szolgálata *(42/J/2006)*
- A Honvédelmi Minisztérium (A közigazgatás korszerűsítésével kapcsolatban egyes HM rendeletek módosításáról szóló HM rendelet részeként.) (*1822/J/2006*)

Örvendetes a Kormányzati Ellenőrzési Hivatal (KEHI) szolgálati titokkörének átdolgozása, amely számos adatvédelmi biztosi vizsgálat és az ügyben kiadott ajánlás után, a KEHI-ről szóló kormányrendelet módosításával együtt talán lezárhatja a KEHI minősített adatkezelésével kapcsolatos panaszok időszakát. A legutóbb véleményezésre küldött szolgálati titokköri jegyzék a közérdekű adatok nyilvánossága szempontjából kifogástalan.

A jogszabály-előkészítés nyilvánossága

2006. január 1-jén lépett hatályba az Eitv., amelynek 9. §-a néhány kivételtől eltekintve általános érvénnyel írja elő a jogszabályt előkészítő minisztérium vagy országos hatáskörű szerv számára az ott előkészített tervezetek honlapon történő közzétételét. A jogszabályok előkészítésének nyilvánossága az információszabadság szempontjából is fontos előrelépés, ezért helyénvaló a 2006-os év jogalkotásról szóló részében beszámolni az első tapasztalatokról.

Az Eitv. előkészítése során megfogalmazódott szkeptikus vélemény szerint hiába teszi nyilvánossá a törvény a jogszabályok közigazgatási előkészítését, nem győzheti le teljesen a hivatali szervezetekben meglévő titkolódzási hajlamot. Ha az kormányzati apparátusok ki akarják rekeszteni a nyilvánosságot az általuk valamilyen szempontból kényesnek vélt tervezet előkészítéséből, akkor úgyis meg fogják találni a törvényen a kiskapukat. Egyelőre nem találkoztunk olyan törekvéssel, amely az Eitv. kijátszására irányulna.

> Az Eisztv. hatálybalépését követően a MeH-nél létrehozott Szakmapolitikai Munkacsoport dönt a tervezet közigazgatási egyeztetésre bocsáthatóságáról. Amíg e testület nem rendelkezik a nyilvános közigazgatási egyeztetés funkciójával párhuzamos, illetve azzal konkuráló feladat- és jogkörrel, addig működése az adatvédelmi biztos álláspontja szerint nem ellentétes az Eitv. előírásaival. Az sem kifogásolandó, ha a közigazgatási egyeztetésre szánt tervezet elkészítését megelőzően valamely szakkérdést kivételesen előzetesen szűkebb szakmai körben megvitatnak. Indokolt esetben az adatvédelmi biztos sem zárkózik el ilyen felkéréstől. 2006-ban sor is került ilyen előzetes konzultációra, például a minősített adatok védelméről szóló törvény előkészítése kapcsán *(1717/J/2006)*. Nem lenne helyes azonban, ha általános gyakorlattá válna, hogy a szabályozásban érdekelt kormányzati szervek bizalmas tárgyalásokon megegyeznek a tervezetről, majd ezt követően puszta formalitásként bocsátanák azt nyílt egyeztetésre.

Az Eitv. 9. §-a értelmében – a törvényben meghatározott kivételektől eltekintve – a közigazgatási egyeztetésre bocsátott jogszabálytervezetek az előterjesztéssel és az indoklással együtt nyilvánosak, közzéteendők. Ezzel aligha egyeztethető össze, hogy a közigazgatási egyeztetésre bocsátott jogszabályt tartalmazó előterjesztést „*Nem*

nyilvános!" jelzéssel látják el. Mégis, 2006 folyamán számos alkalommal kellett felhívni a figyelmet a jelzés alkalmazásának indokolatlan voltára *(52/J/2206, 134/J/2006, 143/J/2006, 361/J/2006, 362/J/2006, 386/J/2006, 546/J/2006, 601/J/2006, 749/J/2006, 789/J/2006, 1129/J/2006, 1266/J/2006, 1458/J/2006, 1523/J/2006, 1615/J/2006, 1758/J/2006, 1791/J/2006, 1823/J/2006, 2005/J/2006, 2043/J/2006).* Feltételezhető, hogy a *„Nem nyilvános!"* jelzés helytelen alkalmazására egyszerűen figyelmetlenségből kerül sor. Erre több körülmény is utal, így például az, hogy az interneten egyébként szabályszerűen közzétett előterjesztés véleményezésre küldött szövegét jelölik nem nyilvánosként, vagy e jelzés jogalapjaként olyan joghelyre – Avtv. 19. §-ának (5) bekezdésére – utalnak, amelynek hatályos – módosított – szövege már semmilyen összefüggésben sincs a döntés-előkészítés céljára szolgáló közérdekű adatok nyilvánosságának korlátozásával.

Azzal az ellenvetéssel lehetne élni, hogy mit számít a közigazgatási egyeztetésre bocsátott tervezeten szereplő *„Nem nyilvános!"* jelzés, ha az iratokat elektronikus formában bárki számára hozzáférhetővé tették. Azt is figyelembe kell venni azonban, hogy az Eitv. 9. §-ának (6) bekezdése értelmében az elektronikus közzététel csak egy évig kötelező, ez után csak a közigazgatási egyeztetésre küldött iratokból ismerhető meg a tervezet tartalma.

Még nem alakult ki egységes joggyakorlat azt illetően, hogy milyen tervezetek tartoznak a nem nyilvános körbe.

> Az Eitv. szerint a jogszabálytervezeteken kívül a szabályozási koncepciókat is közzé kell tenni. Míg a jogszabálytervezetek előkészítésének, egyeztetésének rendje részletesen szabályozott, addig egy koncepció esetében nehéz eldönteni, hogy meddig tekintendő egy szűkebb tudományos vagy szakmai közösség belső munkaanyagának, és mikortól válik az Eitv. hatálya alá tartozó, közzéteendő koncepcióvá.
>
> Az Eitv. szerinti közzétételi kötelezettség nem terjed ki a szabályozási tervezetekkel, koncepciókkal kapcsolatos tervekre, így a minisztériumok jogalkotási tervére, azonban helyes lenne, hogy azt a minisztériumok törvényi kötelezettség nélkül is közzétennék, mint tette azt például a Belügyminisztérium. *(580/K/2006)*
>
> Az Eitv. a közzétételi kivételek felsorolásánál az Alkotmány 28/C. § (5) bekezdésére utal. Az ott felsoroltakra tekintettel a kivé-

telek közé tartoznak például a hatályos nemzetközi szerződésből eredő kötelezettségeket tartalmazó törvények tervezetei. E szabály értelmezési kereteinek kimunkálása szintén a jövő feladata, hiszen nem lenne helyes, ha a jogharmonizációs kötelezettség alapján megalkotandó – például európai irányelvet a magyar jogba átültető – jogszabályok tervezeteinek közzététele elmaradna.

Az Eitv. 9. §-ának (3) bekezdése szerint nem kell közzétenni az Alkotmány 28/C. § (5) bekezdése alapján országos népszavazásra nem bocsátható tartalmú, valamint a fizetési kötelezettségekről, az ármegállapításról, az állami támogatásról, valamint a szervezetalapításról szóló jogszabályok tervezeteit. Kérdéses, hogy mi a teendő, ha egy jogszabály kevert normatartalmú, azaz egyes rendelkezések a közzétételi kivételek körébe esnek, míg mások nem. Az adatvédelmi biztos szerint ilyen esetben kívánatos a tervezet közzététele, szükség szerint kihagyva belőle a kivétel alá eső részeket. A törlés tényét és helyét egyértelműen jelezni kell a részlegesen közzétett szövegben. Fontos ezúton is felhívni a jogszabály előkészítők figyelmet arra, hogy az Eitv. 9. § (3) bekezdésében meghatározott esetekben nem kötelezettség, hanem lehetőség a közzététel mellőzése.

Az adatvédelmi biztos november óta minden jogszabály-véleményezés során hivatalból vizsgálja, hogy ténylegesen megtörtént-e a jogszabálytervezetek Eitv. szerinti közzététele. Az első tapasztalatok vegyesek, de összességében inkább pozitívak.

Minden minisztérium létrehozta az internetes portálján a tervezetek közzétételére szolgáló lapot vagy lapokat, bár a Honvédelmi Minisztérium honlapján kezdetben gyakorlatilag megtalálhatatlanok voltak a véleményezésre bocsátott tervezetek. (A problémára felhívtuk a minisztérium szakértőinek figyelmét, akik gyorsan orvosolták a hiányosságot.) Néhány minisztériumi portálon nehezíti a keresett tervezetek megtalálását, hogy azok egy egységes lista helyett csak szakterületek szerinti csoportosításban vagy a közzététel időszaka szerinti bontásban, esetleg esztétikai okból több lapra tördelve hozzáférhetők.

Több kritika illeti a közzététel gyakorlatát. November óta számos esetben kellett felhívni az előterjesztők figyelmét a közzététel pótlására *(1726/J2006, 2004/J/2006, 2005/J/2006, 2006/J/2006, 1021/J/2006, 2039/J/2006, 2041/J/2006, 2044/J/2006, 2047/J/2006, 2050/J/2006,*

2062/J/2006, 2064/J/2006). Előfordult az is, hogy a közzétett és a véleményezésre bocsátott előterjesztés szövege nem egyezett meg teljesen *(2042/J/2006)*, vagy a jogharmonizációs tárgyú tervezet helyett csak annak jogharmonizációs javaslatát hozták nyilvánosságra. Örvendetes, hogy olyan dokumentumok – például kormányhatározat-tervezetek – nyilvánosságra hozatala is kezd gyakorlattá válni, melyek közzétételére az Eitv. nem kötelez.

Az Eitv. a jogszabály-előkészítés nyilvánossága mellett a jogalkotás nyilvánosságát is erősítette. A jogszabályok kötelező elektronikus közzétételével kapcsolatban 2006 márciusában született adatvédelmi biztosi ajánlás, amelyet a beszámoló információszabadságról szóló része ismertet.

Az adatvédelmi biztos a saját, jogalkotással kapcsolatos tevékenységét is legalább annyira átláthatóvá kívánja tenni, amennyire az a jogszabály-előkészítő minisztériumok számára kötelező, ezért az Eitv.-vel összhangban 2006. január 1-jétől rendszeresen nyilvánosságra hozza az általa véleményezett jogszabálytervezetek, valamint a jogalkotással kapcsolatos egyéb tervezetek (különféle határozatok, utasítások, koncepciók, jelentések stb.) listáját. A havonta frissülő jegyzék a http://abiweb.obh.hu/abi/index.php internetcímen érhető el. A rendszeres elektronikus közzétételre tekintettel az idei beszámolóhoz már nem szükséges csatolni a 2006-ban véleményezett tervezeteket felsoroló függeléket.

III. NEMZETKÖZI ÜGYEK

Konzultációk, panaszügyek

2006-ban jelentősen megemelkedett a nemzetközi ügyeink száma, az összes iktatott akta mintegy 10 %-át teszik ki. A külföldről érkező telefonos megkereséseket nem iktatjuk, csak a levélben, e-mailben érkező beadványokat.

Munkamegbeszélésen fogadtunk külföldi adatvédelmi biztosokat és munkatársaikat, így a román, a szlovén, a szlovák irodák képviselőit. A személyes megbeszéléseken túl írásban több tucatnyi – más tagállamok adatvédelmi hatóságaitól érkezett – megkeresésre válaszoltunk, így például a munkahelyen, pénzintézetben működtetett kamerákkal vagy a munkavállalók munkáltató általi földrajzi helymeghatározásával kapcsolatban *(936/I/2006, 1350/I/2006)*.

Nőtt a tengeren túlról küldött beadványok, kérdések száma, továbbra is első helyen szerepel a külföldre történő adattovábbítás lehetősége adatkezelés vagy adatfeldolgozás céljából, valamint a nyilvántartásunkba történő bejelentkezés *(300/I/2006, 804/I/206, 872/I/2006, 2115/I/2006)*. Új jelenség, hogy egyre többen érdeklődnek az Általános Szerződési Feltételek (Standard Contractual Clauses) magyar szabályozásáról, irodánk ezzel kapcsolatos gyakorlatáról *(1897/I/2006, 1909/I/2006, 2114/I/2006)*. E kérdésről – jelentőségére tekintettel – a panaszügyek ismertetését követően külön alfejezetben szólunk.

Az elhíresült *„PNR"*-ügy, a légi utasok adatainak kiküldése az USA-ba több uniós szervtől és nemzeti hatóságtól érkező megkeresésben szerepelt, erről bővebben a 29. cikk szerinti Munkacsoport anyagait ismertető alfejezetben írunk *(1009/I/2006)*, csakúgy, mint a szintén nagy vitákat kavaró SWIFT-ügyről *(1008/I/2006)*.

Az Európai Adatvédelmi Biztosok Tavaszi Konferenciájára Guernsey-ből Budapestre érkező egyik kolléga, az ottani helyettes adatvédelmi biztos beadvánnyal fordult hivatalunkhoz. Panasza szerint a Ferihegyi repülőtéren az útlevélkezelő hosszasan – egy speciális lámpa alatt, majd egy másik utas útlevelével összehasonlítva – megvizsgálta az útlevelét, majd azt az útlevélkezelő fülke ablakának nyomva megkért egy másik, brit útlevéllel rendelkező utast, hasonlít-

sa össze a két úti okmányt, s ezzel illetéktelen számára hozzáférhetővé tette a személyes adatait. Amikor kifogásolta az útlevélkezelő eljárását, azt a választ kapta, hogy a fénykép hátterével kapcsolatos problémát kellett tisztázni. A beadványozó véleménye szerint az eljárás nem volt jogszerű, ezért kérte az ügy kivizsgálását.

A Határőrség országos parancsnoka által lefolytatott belső vizsgálatról szóló tájékoztatás nem volt elég egyértelmű, ezért helyszíni adatvédelmi ellenőrzést folytattunk a Ferihegyi repülőtéren.

Az ellenőrzés eredményeként megállapítottuk, hogy az útlevélkezelők a kétéves kiképzést követően rendszeres továbbképzésben részesülnek, ahol – egyebek mellett – elsajátítják azokat az ismereteket, amelyek a hamis útlevelek kiszűréséhez szükségesek. Olyan határőr, aki az úti okmányok kezelésével kapcsolatos képzésben nem részesült, nem láthat el útlevélkezelői feladatokat. Minden szolgálatváltásba beosztanak egy olyan határőrt is, akit az alapképzésen túlmenően speciálisan, az okmányhamisítás jeleinek felismerésére és vizsgálatára képeztek ki, továbbá az ügyeleti helyiségben rendelkezésre áll egy okmányvizsgáló berendezés is. Amennyiben egy útlevél eredetiségével kapcsolatban kétség merül fel, az útlevélkezelő a további ellenőrzést átadja az erre szakosodott kollégájának, ő pedig folytatja a többi utas beléptetését.

Az általunk vizsgált esetben nem követték ezt az eljárási rendet, ezért felhívtuk a Határőrség országos parancsnokának figyelmét, hogy a hasonló esetek elkerülése érdekében a továbbiakban is a fentiekben ismertetett eljárási rendnek megfelelően végezzék a problémásnak tűnő úti okmányok ellenőrzését.

Az útlevélkezelő fülkéjének három oldalát olyan fóliával látták el, amely a kívülről betekintést megakadályozza, csak a negyedik, az utas felőli oldal átlátható mindkét irányba. A fülkén, jól látható helyen feltüntették, hogy panasz, probléma esetén kihez lehet fordulni a helyszínen.

A beadványozó ezzel a lehetőséggel nem élt a repülőtéren.

Az útlevélkezelő fülkéjében található számítógéppel a feladatok ellátásához szükséges adatbázisok elérhetők. Ezek egyike a Dokunet elnevezésű nyilvántartás, amely az egyes országok úti okmányainak mintáit és azok biztonsági jellemzőit tartalmazza. A nyilvántartás célja, hogy segítse az útlevélkezelők munkáját az úti okmányok eredetiségének vizsgálata során.

A panaszos úti okmányát egy brit koronafüggőségi terület (sziget, amely nem része sem az Egyesült Királyságnak, sem a gyarmatoknak; teljesen független, azonban a nemzetközi kapcsolatok és a védelem az Egyesült Királyság kormányának hatáskörébe tartoznak) állította ki. Az okmány általában a brit útlevél jellemzőivel rendelkezik, vannak azonban apró eltérések. Mivel a Dokunet nem tartalmazta e sziget úti okmányának mintáját és annak biztonsági jellemzőit, az útlevélkezelő azt hihette, hamisított brit útlevelet tart a kezében. Vizsgálatomat követően felkértem a Határőrség országos parancsnokát, hogy a jövőbeni problémák megelőzése érdekében intézkedjen az említett útlevélminta beszerzését illetően. A parancsnok értesítése szerint ez az intézkedés megtörtént.

A Határőrség jelenleg kétféle ellenőrzést végez a beléptetés során:

A kedvezményezett országok (kb. az EGT-tagállamok) állampolgárai és családtagjaik minimum-ellenőrzésben részesülnek, amely az útlevélben szereplő fénykép szerinti személyazonosítást és az úti okmány érvényességének ellenőrzését foglalja magába.

A harmadik országokból érkezőket alapellenőrzésben részesítik, amely a minimum-ellenőrzésen kívül a belépő személy adatainak a határregisztrációs rendszerben történő rögzítését, továbbá a különböző nyilvántartásokban (például körözési nyilvántartás) való, illetve a beutazás és tartózkodás feltételei (érvényes vízum, anyagi fedezet stb.) meglétének ellenőrzését foglalja magába.

A jogszabályok lehetőséget biztosítanak arra, hogy a kedvezményezett országokból érkezőket szúrópróbaszerűen alapellenőrzésben részesítsék.

A panaszos minimum-ellenőrzésben részesült.

Kértem annak megállapítását is, hogy az útlevelet kiállító sziget milyen „*státusszal*” rendelkezik a magyarországi beléptetés során, tekintettel arra, hogy nem tagja az Európai Uniónak, általában nem érvényesek a személyek, a szolgáltatások és a tőke szabad mozgására vonatkozó, illetve a bel- és igazságügyi együttműködés keretében megfogalmazott előírások, de a vámegyüttműködésben és néhány más területen a Nagy-Britannia által kötött megállapodásokban foglaltaknak megfelelően részt vesz. A Határőrség országos parancsnoka ezzel kapcsolatban arról tájékoztatott, hogy a hatályos jogszabályok alapján a sziget kedvezményezett országnak minősül, ezért a beléptetés során jogszerűen végeztek minimum-ellenőrzést.

A Határőrség hatáskörébe tartozik a személyi felelősség megállapítása, amelyet lehetővé tesz az öt évig őrzött szolgálatszervezési nyilvántartás, amely órára pontosan tartalmazza, hogy adott helyen és időben melyik munkatárs milyen feladatot látott el.

A Határőrség kiemelt figyelmet fordít a személyes adatok védelmével kapcsolatos előírások betartására és betartatására. Adatvédelmi oktatásban valamennyi munkatárs részesült, az új munkatársak képzése munkába állásukkor, illetve folyamatosan történik. Havonta egyszer oktatási napot tartanak, ahol az aktuális tudnivalók elsajátítására, az esetleges problémák megoldásainak ismertetésére kerül sor. Az oktatási napon a parancsnok is kap egy órát, amely az időszerű kérdések tisztázására szolgál.

Megkeresésünket követően e parancsnoki órán az esetet feldolgozták, illetve beépítették az adatvédelmi oktatás tananyagába. *(731/I/2006.)*

Az általános szerződési feltételek használata olyan harmadik országokba történő adattovábbítás esetén, ahol nem biztosított a személyes adatok megfelelő szintű védelme

2006-ban megszaporodtak az arra vonatkozó megkeresések, hogy a Bizottság által jóváhagyott általános szerződési feltételek (Standard Contractual Clauses) használata esetén be kell-e jelenteni az Adatvédelmi Biztos Irodájába az olyan harmadik országokba történő adattovábbítást, amelyekben nem biztosított a személyes adatok megfelelő szintű védelme. Továbbá felmerült az a kérdés is, hogy a bejelentés mellett irodánknál letétbe kell-e helyezni vagy be kell-e mutatni azt a szerződést, amely az általános szerződési feltételeket tartalmazza.

Az Európai Bizottság egy 2006-ban kelt munkadokumentumában (SEC(2006)95, elérhető: http://ec.europa.eu/justice_home/fsj/privacy/modelcontracts/index_en.htm) kritikával illeti azokat a tagállamokat, ahol nincs nyoma annak, ha az adatkezelők a Bizottság által jóváhagyott általános szerződési feltételeket használják a tagállamokon kívülre történő adattovábbításhoz. Ez a kritika Magyarországra is vonatkozik, ugyanis ha egy cég Magyarországról olyan országba küldi munkavállalóinak vagy ügyfeleinek adatait, ahol nem megfelelő a személyes adatok védelme, és a megfelelőséget a Bizottság által jóvá-

gyott általános szerződési feltételek alapján biztosítja, irodánk ugyan értesül az adattovábbításról, az általános szerződési feltételek alkalmazásáról azonban nem, mivel nem kötelezzük az adatkezelőket, hogy bejelentsék az általános szerződési feltételek alkalmazását.

Az Európai Bizottság munkadokumentuma a Bizottság azon két határozatának (2001/497/EC és 2002/16/EC) tagállami szinten történő végrehajtását értékeli, amelyek a harmadik országokba irányuló adattovábbítások alapjául szolgáló általános szerződési feltételekről szólnak. A Bizottság megállapítja, hogy a „*tagállamok nagyon kevés információval rendelkeznek mind az EU-n kívülre történő adattovábbítás alapjául szolgáló általános szerződési feltételek használatáról, mind pedig a külföldre irányuló adattovábbításokról általában, amely úgy tűnik, hogy a megfelelő ellenőrzés hiányának a következménye…A tíz új tagállam közül egyik sem értesítette még a Bizottságot szerződési feltételek vagy más megfelelő biztosítékok alkalmazásáról*". A Bizottság hangsúlyozza, hogy „*a tagállamok csak akkor tudják teljesíteni a 95/46/EK irányelvben előírt azon kötelezettségüket, hogy értesíteniük kell a Bizottságot és a többi tagállamot azokról az esetekről, amikor a külföldre történő adattovábbítást az adatkezelő által nyújtott megfelelő biztosítékok alapján hagyják jóvá, ha a tagállamok valamilyen módon ellenőrzik a külföldre irányuló adattovábbításokat*". A Bizottság kiemeli, hogy „*annak érdekében, hogy a jövőben eredményesebb értékelést végezhessen különösen az általános szerződési feltételek megfelelő működésének tárgyában, hasznos lenne, ha a tagállamok javítanának a külföldre irányuló adattovábbításokat ellenőrző rendszerükön és nyilvántartanák az olyan országokba irányuló adattovábbításokat, ahol nem biztosított a személyes adatok megfelelő védelme, valamint ezen adattovábbítások jogalapját, az általános szerződési feltételeket is beleértve. Értékes információt szolgáltatnának a nemzeti adatvédelmi hatóságok, ha éves beszámolójukba belefoglalnák ezeket az adatokat, amit a Bizottság fel tudna használni a jövőben értékeléseihez…Annak kapcsán, hogy a tagállamok nem rendelkeznek információval az általános szerződési feltételekről, felvetődik a kérdés, hogy megfelelően teljesítik-e azon kötelezettségüket, hogy ellenőrizzék a személyes adatoknak a nem megfelelő védelmet biztosító országokba történő továbbítását. Felmerül az a kérdés is, hogy vajon rendszeresen és kontroll nélkül történik-e ezekbe az országokba az adattovábbítás*".

Meg kell azonban jegyezni, hogy ha egy tagállam a Bizottság által jóváhagyott általános szerződési feltételek alapján járul hozzá egy harmadik országba történő adattovábbításhoz, akkor erről nem kell a Bizottságot értesítenie.

Annak ellenére, hogy a két tárgyalt bizottsági határozat nem kötelezte a tagállamokat, azoknak kb. a fele kötelezővé tette az általános szerződési feltételeket tartalmazó szerződések bemutatását, nyilvántartását. Felmerül a kérdés, hogy a Bizottság kritikája és felvetései alapján szükség van-e Magyarországon az általános szerződési feltételek nyilvántartására (bemutatására vagy letétbe helyezésére), ha az szolgál a harmadik országban megfelelő adatkezelés biztosításának igazolására. A nyilvántartás mellett szól az az érv, hogy várhatóan növekedni fog az általános szerződési feltételek használata az Avtv. 2004-es módosításának köszönhetően, hiszen a módosításig csak az érintett hozzájárulásával lehetett harmadik országba személyes adatot továbbítani. A várható növekedés másik oka az Európai Bizottság egy 2004 végén hozott határozata, amely egy új, a Nemzetközi Kereskedelmi Kamara által összeállított és a vállalatok szempontjait, észrevételeit jobban figyelembe vevő általános szerződési feltétel csomagot tartalmaz (2004/915/EC). A Kötelező Erejű Vállalati Szabályokkal (BCR) kapcsolatban kialakult gyakorlat a másik érv, amely a nyilvántartás mellett szól. A BCR-ek jóváhagyása irodánk feladata (erre már sor is került 2006-ban), tehát ha az adatkezelővel munkavállalói vagy ügyféli kapcsolatban lévő személyek adatait úgy továbbítják nem megfelelő védelmet biztosító harmadik országba, hogy BCR-t használnak a megfelelőség biztosítására, akkor irodánk erről értesül. Felmerül a kérdés, hogy nem lenne-e hasznos egységes gyakorlatot kialakítani a nem megfelelő védelmet biztosító harmadik országokba történő adattovábbításokkal kapcsolatban, a megfelelőség igazolásának nyomon követése terén. A Bizottság kritikája alapján indokolt lenne az ellenőrzést erre a területre is kiterjeszteni.

A fentiek alapján 2007 márciusában közleményt adunk ki arról, hogy az általános szerződési feltételek használatát jelentsék be az Adatvédelmi Biztos Irodájához.

Vízuminformációs rendszer

A 2004/512/EK (2004. június 8.) tanácsi határozat létrehozta a vízumadatok tagállamok közötti cseréjét kezelő Vízuminformációs Rendszert (a továbbiakban: VIS), amely a kijelölt hatóságok számára lehetővé teszi a vízumadatok rögzítését és frissítését, valamint az adatok elektronikus úton való megtekintését. A VIS egy központi információs rendszerből, a nemzeti rendszerekből, továbbá az ezek közötti kapcsolatot biztosító kommunikációs infrastruktúrából áll. A központi rendszer és a kommunikációs struktúra a Bizottság, a nemzeti rendszerek fejlesztése a tagállamok hatáskörébe tartozik.

A VIS jogi keretéről szóló COM(2004) 835 számú rendelet tervezete meghatározza a VIS célját, adattartalmát, a hozzáférő hatóságok körét és VIS-szel kapcsolatos feladatait, az adatkezelés, az adatfeldolgozás, az adatvédelem fő szabályait, illetve a felelősségi köröket. E rendelet tervezetéhez kapcsolódóan 2005-ben elkészült az a tanácsi határozattervezet, amely a tagállamok belső biztonságért felelős hatóságai és az Europol számára a terrorista cselekmények és más, súlyos bűncselekmények megelőzésének, felderítésének és nyomozásának céljából lehetővé teszi a VIS-hez való konzultációs hozzáférést, meghatározza annak jogalapját, valamint tartalmi és formai feltételeit.

Az adatvédelmi biztos ez utóbbi tervezetet a Tanács mellett működő Rendőrségi Együttműködési Munkacsoportban (Police Cooperation Working Party – PCWP) képviselendő magyar álláspont egyeztetésének koordinációja során, viszonylag későn, az egyeztetés többedik köre után kapta meg. A tervezetre tett tartalmi és formai észrevételeink többségét az akkori magyar tárgyalási álláspontba beillesztették, azonban a személyes adatok védelme szempontjából maradtak még nyitott kérdések. Itt jegyezzük meg: ez a határozattervezet tipikus példa arra, hogyan tervezik a bűnüldözési célt az adatvédelmi alapelvek háttérbe szorításával érvényesíteni, hogyan marad pusztába kiáltott szó az információs önrendelkezési jog tiszteletben tartása. E tervezet átgondolt kidolgozása azért bír még kiemelt fontossággal, mert precedensként fog szolgálni a további, nem bűnüldözési célú nyilvántartásokhoz (például Eurodac) bűnüldözési célból történő hozzáférés feltételeinek és eljárási rendjének megteremtéséhez.

Az egyik nyitott kérdés, hogy a belső biztonságért felelős hatóságok egy nemzeti központi vagy több kijelölt hatóságon keresztül fér-

hessenek hozzá a VIS-hez. A Bizottság, az Európai Parlament és az európai adatvédelmi biztos az előbbi megoldást támogatja, a Tanács (PCWP) az utóbbi mellett érvel azzal, hogy a hozzáférés szakmai indokoltságát az adott hatóság tudja megítélni, a központi lekérdező hatóság folyamatba illesztése megnehezíti (lassítja) a rendvédelmi szervek napi munkáját, továbbá a nemzeti jog szerint kijelölt hatóságok hozzáférésre felhatalmazott szervezeti egységeiről összeállított lista vezetésével, naprakészen tartásával biztosítható a lekérdezési lehetőség korlátozott igénybevétele. Észrevételeink között kifejtettük: a személyes adatok védelme szempontjából a lehető legkevesebb hozzáférési pont kialakítása támogatható. A legutóbbi tájékoztatás szerint valamennyi tagállam (a Tanács) a kijelölt hatóságok közvetlen és több ponton keresztül megvalósuló hozzáférését részesíti előnyben, az Európai Parlament viszont – helyesen – ragaszkodik azokhoz a szigorú biztosítékokhoz, amelyek a VIS-hez történő, bűnüldözési célú hozzáférést kivételként kezelik.

Vitatott a határozattervezet azon pontja is, amely a lekérdezési kulcsokról szól. A jelenlegi megfogalmazás szerint a felsorolt adattípusok (név, állampolgárság, úti okmány típusa és száma, úticél és a tartózkodás időtartama, utazás célja, érkezés és indulás időpontja, első belépés szerinti határ, lakóhely, ujjlenyomat, vízum típusa és vízumbélyeg száma) bármelyikére lehet keresni, és találat esetén a felsorolt adattípusok mindegyike megtekinthető. Véleményünk szerint e megfogalmazást pontosítani kellene, ugyanis annak megengedése, hogy például csak az állampolgárság vagy csak a határátkelőhely megadásával történhet lekérdezés, egyrészt „*kezelhetetlen*" mennyiségű adat megjelenítésével (átvételével), másrészt az adott ügy szempontjából érdektelen adatok tömegének megtekintésével járhat, s a meghatározott céltól eltérő adatfelhasználás kockázatát hordozza magában. Hozzáteszem: a határozattervezet következő bekezdése lehetővé teszi, hogy találat esetén részletesebb adatkörhöz is hozzájusson a lekérdező, tehát feleslegesnek tűnik e széles körű keresési kulcs megengedése. Mivel a határozattervezet jelenlegi szövege alapján eleve csak meghatározott, konkrét esetben és akkor lehet konzultációs célból a VIS-hez hozzáférni, ha az átvett adat jelentős mértékben hozzájárul az ügy feldolgozásához, feltételezhető, hogy egy adatnál több áll a belső biztonságért felelős hatóság rendelkezésére, így a feladatellátást nem akadályozza, ha két vagy több adatmező kötelező kitöltésé-

vel hajtják végre a lekérdezést. E módszer biztosítja az adott ügy szempontjából érdektelen adatok megtekintésének elkerülését, és a célhoz kötöttség elvének történő megfelelést. Az Európai Parlament és az európai adatvédelmi biztos szintén kifogásolta a keresési feltételek „*laza*" megfogalmazását, a Tanács azonban – a bűnüldözési feladatok ellátásához szükséges rugalmasság okán – ragaszkodik a jelenlegi szövegezéshez. Fenti észrevételünk a magyar tárgyalási álláspont koordinációja során is ellenkezést váltott ki.

Ugyan a Tanács és az Európai Parlament a határozattervezet szövege kapcsán több pontban ellentétes nézetet vall, a Tanács úgy számol, hogy 2007 első felében elfogadják a normát. Az erre való felkészülés jegyében a hazai koordinációban részt vevő hatóságok decemberben egyeztető értekezletet tartottak arról, hogy Magyarországon mely hatóságok, szervek számára biztosítsuk a VIS-hez történő hozzáférést a határozat hatálybalépése után. Az értekezleten az érdekelt hat szervezet képviselői (Rendőrség, Vám- és Pénzügyőrség, Határőrség, Legfőbb Ügyészség, Nemzetbiztonsági Hivatal, Információs Hivatal) úgy nyilatkoztak, hogy miután a leendő lista bármikor módosítható lesz, első körben hat (a Rendőrségnél kettő, a többi szervnél – a LÜ kivételével – egy-egy) hozzáférési pontra vonatkozó igényt nyújtson be Magyarország, s ha ezt valamilyen okból csökkenteni kell, akkor a Vám- és Pénzügyőrség, illetve a Határőrség a Rendőrség szervezetében lévő Nemzetközi Bűnügyi Együttműködési Központon keresztül kér majd adatot. Az adatvédelmi alapelvek érvényesítéséről, továbbá a hatóságokra vonatkozó jelenlegi hazai szabályozásról szóló figyelmeztetés ellenére egyedül a Legfőbb Ügyészség képviselője nyilatkozott úgy, hogy a feladatai ellátásához szükséges adatokat jelenleg is megfelelő hatékonysággal tudja beszerezni, ezért e lehetőséget nem fogják igénybe venni.

Az értekezlet után kértük a hozzáférő hatóságok körének újragondolását, mivel több problémát látunk a majdani hazai adaptálás vonatkozásában. Az egyik probléma az, hogy a nemzetbiztonsági szolgálatokról szóló 1995. évi CXXV. törvény rendelkezései alapján az Információs Hivatal feladatai között nincs olyan jellegű bűncselekmény-felsorolás, mint a Nemzetbiztonsági Hivatal esetében. E kérdésben az Igazságügyi és Rendészeti Minisztérium a Miniszterelnöki Hivatal Nemzetbiztonsági Iroda állásfoglalását fogja kérni.

Problémát okoz az is, hogy értelmezésünk szerint a nemzetbiztonsági szolgálatok valamilyen adatbázishoz történő közvetlen hozzáférése nem következik egyértelműen a jogszabály szövegéből, továbbá a nemzetbiztonsági szolgálatok adatkérése, adatbetekintése, adatszolgáltatása, valamint mindezek tartalma államtitkot képez. Ez utóbbi miatt nehezen lesz megvalósítható a határozattervezet azon előírása, amely szerint a VIS-hez történő konzultációs célú hozzáférés során rögzíteni (naplózni) kell a lekérdezés célját, a hozzáférés időpontját, a lekérdezett adatokat és azok típusát, a hozzáférő hatóság nevét, továbbá a hazai jogszabályoknak megfelelően a hozzáférő személy nevét és azonosító adatait. E két problémával kapcsolatos értelmezésünket az Igazságügyi és Rendészeti Minisztérium elfogadta.

Meghallgatásra talált az az észrevételünk is, amely a majdani adatvédelmi ellenőrzések végrehajthatóságára vonatkozott. A nemzetbiztonsági szolgálatokról, valamint az állampolgári jogok biztosáról szóló törvény előírásai alapján ugyanis az adatvédelmi biztos nem tekinthet bele – egyebek mellett – a számítástechnikai eszközök számával, elhelyezésével, működésével, illetve az alkalmazott szoftverekkel kapcsolatos dokumentumokba. Egy nyílt, a közösségi vízumpolitika eszközeként létrehozott adatbázis hozzáférési pontjának kialakítása szükségszerűen magába foglalja a számítástechnikai eszközök számának meghatározásával, valamint azok elhelyezésével, működésével és az alkalmazott szoftverekkel kapcsolatos dokumentumok készítését. A határozattervezet jelenlegi szövege által előírt adatvédelmi ellenőrzés nem valósítható meg kellő alapossággal e jogszabályi tilalom fennállása miatt. Megoldásként vagy a tilalom „*lazítása*" (például a VIS-hez történő hozzáférés kivételként való megfogalmazása) szolgálhat, vagy az, ha a nemzetbiztonsági szolgálat eláll attól a szándékától, hogy a VIS-ben tárolt adatokhoz közvetlenül férjen hozzá.

Miután mind uniós, mind hazai szinten vannak ellentétek a határozattervezet rendelkezéseit illetően, bízunk abban, hogy 2007-ben megszületik a mindenki számára megnyugtató megoldás.

Az iroda Magyarország schengeni térséghez történő csatlakozásával összefüggő tevékenysége

Belgium, Franciaország, Hollandia, Luxemburg és Németország 1985. június 14-én a hollandiai Schengenben aláírták a közös határai-

kon történő ellenőrzések fokozatos megszüntetéséről szóló megállapodást, 1990. június 19-én a végrehajtásról szóló megállapodást. Később a megállapodáshoz csatlakozott Ausztria, Dánia, Finnország, Görögország, Olaszország, Portugália, Spanyolország, Svédország, valamint Izland és Norvégia is.

Az egyezmény IV. címének rendelkezései értelmében létrehozták a Schengeni Információs Rendszert (SIS), mely az Európai Unió keretébe beillesztett schengeni vívmányokban (acquis) foglalt rendelkezések alkalmazásának alapvető eszköze. Az Európai Unióról szóló szerződéshez és az Európai Közösséget létrehozó szerződéshez csatolt jegyzőkönyv rendelkezik a schengeni vívmányoknak az Európai Unió keretébe történő beillesztéséről. A jegyzőkönyv 8. cikke alapján: „*Az új tagállamoknak az Európai Unióba történő felvételére vonatkozó tárgyalások során a schengeni vívmányokat és az intézmények által az ezek hatálya alá tartozó területen hozott további intézkedéseket olyan vívmányoknak kell tekinteni, amelyeket a tagjelölt országoknak teljes egészében el kell fogadniuk*". A csatlakozási szerződés 3. cikkének (2) bekezdésében került rögzítésre az az értékelési folyamat, amelynek végén a Tanács által hozott határozat alapján hazánk a schengeni térség teljes jogú tagjává válhat.

A SIS-t nem úgy tervezték, hogy fogadni tudja az Európai Unió megnövekedett számú tagállama, valamint a rendszerhez csatlakozni kívánó egyéb országok belépéséből származó megnövekedett igényeket, és a rendszerrel szemben megfogalmazott új követelményeket (terrorizmus elleni harc, határon átnyúló bűnözés stb.).

A fenti igények megjelenése, az információtechnológia legutóbbi fejlesztései nyújtotta előnyök kihasználása és az új funkciók bevezetésének lehetővé tétele érdekében 2001-ben döntést hoztak a Schengeni Információs Rendszer második generációjának (SIS II) kifejlesztéséről. Ez a munka azonban vontatottan haladt, melynek oka részben a közbeszerzési eljárások elhúzódása, részben a fejlesztési célkitűzések változása, új funkciók időközbeni beiktatása volt. Új funkciókat jelentett többek között a terrorizmus elleni harccal és a gépjárművekkel összefüggő eljárások SIS II-be történő illesztése.

A megváltozott körülményekre tekintettel a Tanács úgy határozott, hogy a rendszer fejlesztésének befejezését 2006. december 31-ről 2007. december 31-re halasztja.

A SIS II rendszernek biztosítania kell
(a) a határellenőrzésért,
(b) az országon belüli egyéb rendőrségi és vámellenőrzések végrehajtásáért és összehangolásáért,
(c) a vízumok és tartózkodási engedélyek kiadásáért, valamint a külföldiekkel kapcsolatos igazgatási ügyekért,
felelős hatóságok számára, hogy automatizált lekérdezési eljárás révén hozzáférjenek a személyekre, járművekre és tárgyakra vonatkozó figyelmeztető jelzésekhez.

A SIS két külön részből áll: az egyiket a központi rendszer (C.SIS) alkotja, a másikat a nemzeti rendszerek (N.SIS) összessége (országonként egy rendszer). A SIS azon elv alapján működik, hogy a nemzeti rendszerek egymás között nem tudják közvetlenül kicserélni a számítógépes adatokat, csak a központi rendszeren keresztül. Találat esetén a kiegészítő adatokat viszont két- és többoldalú alapon egymás között kell kicserélni.

Magyarország is tagja a SIS II rendszert alkalmazni kívánó országoknak, így a rendszerre vonatkozó előírásokat, eljárásokat alkalmaznia kell.

Magyarország teljes jogú schengeni tagságának előkészítéseként ez év márciusában az Európai Unió tagállamainak szakértőiből álló értékelő bizottság látogatott el az adatvédelmi biztos hivatalába. A jelenleg hatályos schengeni joganyag és a kidolgozás alatt álló SIS II létrehozására, működtetésére és használatára vonatkozó javaslatok egyaránt rendelkeznek arról, hogy a részes felek a Schengeni Információs Rendszer nemzeti része (N. SIS) adatállományának független felügyeletéért felelős ellenőrző hatóságot jelölnek ki. Magyarországon a Schengeni Információs Rendszer adatvédelmi ellenőrzéséért az adatvédelmi biztos lesz a felelős.

Az értékelő bizottság látogatását megelőzően egy kérdőívet kellett kitölteni, mely a szakértők felkészülését segítette. A szakértők látogatásuk során azt vizsgálták, hogy megvan-e az a szükséges jogszabályi felhatalmazás, amely alapján az adatvédelmi biztos ellenőrizheti az N.SIS adatállományát. Vizsgálták továbbá, hogy az adatvédelmi biztos rendelkezik-e a vizsgálatok elvégzéséhez szükséges megfelelő személyi és pénzügyi erőforrással, továbbá, hogy megvan-e az a kellő szakmai és gyakorlati tapasztalat, amely a schengeni ellenőrzések elvégzéséhez nélkülözhetetlen.

A szakértők jelentésükben megállapították, hogy Magyarország adatvédelmi szempontból megfelel a schengeni térséghez történő csatlakozáshoz szükséges kritériumoknak, ugyanakkor a jelentésben néhány ajánlást is megfogalmaztak.

A látogatás során az értékelő bizottságot nem sikerült meggyőzni afelől, hogy az adatvédelmi biztos hatásköre ki fog terjedni a schengeni rendszerre is. Annak ellenére, hogy többször felhívtuk a szakértők figyelmét arra, hogy az Avtv. hatálya a Magyar Köztársaság területén folytatott minden olyan adatkezelésre és adatfeldolgozásra kiterjed, amely természetes személy adataira vonatkozik, nem sikerült a szakértők kétségeit eloszlatni. Jelentésükben annak a reményüknek adnak hangot, hogy *„az adatvédelmi biztos hatásköre – összehasonlítva a jelenlegi jogosultságaival – a SIS és a SIRENE vonatkozásában nem fog csökkeni”*.

Javasolták, hogy a rendőrségnél létrehozott SIRENE irodánál az adatvédelmi biztos legkésőbb a schengeni rendszer bevezetése előtt végezzen helyszíni ellenőrzést. A szakértők szorgalmazták, hogy az adatvédelmi biztos kapjon tájékoztatást a Külügyminisztériumnál a vízumkérdésre vonatkozó munkáról. Továbbá üdvözölték az adatvédelmi biztos azon ígéretét, miszerint a schengeni felkészülés keretében a biztos felkeresi és ellenőrzi azokat a magyar konzulátusokat, amelyek a legtöbb vízumot adják ki. A szakértők példaértékűnek találták ezt a kezdeményezést. Az érintettek tájékoztatása érdekében emellett ismeretterjesztő kampány megszervezését javasolták. Mindezeknek az új feladatoknak az elvégzésére megfelelő költségvetési forrás biztosítását kérik az Európai Unió szakértői.

Októberben a Tanács illetékes munkacsoportjának megküldött úgynevezett nyomon követési jelentésben (follow-up report) adtunk számot arról, hogy a jelentésben megfogalmazott ajánlások közül mit sikerült időközben megvalósítani. Munkatársaim rendszeres munkakapcsolatban állnak a SIRENE iroda munkatársaival, szakmai tanácsokkal segítik az adatvédelmi vonatkozású kérdések megválaszolását.

Beszámoltunk a magyar konzulátusok adatvédelmi ellenőrzéséről is. Májusban a kijevi, szeptemberben az ungvári és beregszászi, októberben a belgrádi és szabadkai konzulátuson ellenőriztem a vízumkiadás során az adatvédelem gyakorlatát.

Hivatalunk a SIS II rendszer jelenlegi kialakítási fázisában a személyes adatok kezelésével összefüggő feladatok hazai megvalósítási

módjának előkészítését folyamatosan figyelemmel kíséri, az alkalmazók részéről a feladatok megoldása során felmerült kérdések megválaszolásában szakértői segítséget nyújt. Teszi ezt annak keretében, hogy az adatvédelmi biztos és az országos rendőrfőkapitány személyes találkozóján a rendőrség részéről erre vonatkozóan határozott igény merült fel.

Ez az iroda számára azért jelent új feladatot, mert a SIS II hazai bevezetésével összefüggésben 2003-ban a Belügyminisztérium keretén belül elkezdett előkészítő munkálatok kezdeti fázisában az adatvédelmi biztos jogosítványa nem terjedt ki a tevékenység felügyeletére.

A SIS II jogi és technikai feltételeinek hazai megteremtésében tevékenykedő munkacsoport tagjai vettek részt a hazai és a külföldön tartott egyeztető tárgyalásokon. A munkák során az idő előrehaladtával egyre inkább kiütköztek az egyes területeken tapasztalható rendezetlen viszonyokból adódó problémák.

Az egyes tagországok a SIS II központi rendszerében elhelyezik az úgynevezett „*figyelmeztető jelzés*”-t, ez a SIS II-be bevitt adatok halmaza, amely a hatáskörrel rendelkező hatóságok számára lehetővé teszi, hogy egy meghozandó egyedi intézkedésre tekintettel egy személyt vagy tárgyat azonosítsanak. Azonosítás estén a nemzeti hatóság által bevitt „*kiegészítő adat*” által tartalmazott információt veszik figyelembe, mely adat arra szolgál, hogy a figyelmeztető jelzést milyen okból helyezte el az adott ország hatósága a központi rendszerbe. Ezek az adatok minden ország rendelkezésére állnak, és a tagországok csak a központi rendszeren keresztül érhetik el azokat.

Amelyik ország hatóságainál a „*figyelmeztető jelzés*” alapján a rendszer találatot jelez, ott a hatóságnak kötelessége a jelzés alapján intézkedni. A szükséges intézkedést a „*kiegészítő információ*” tartalmazza, melyet a „*figyelmeztető jelzés*”-t a rendszerbe bevivő ország tárol, és közvetlen úton cserél ki annak a tagállamnak a hatóságával, ahol a találat volt.

A fentiek alapján látható, hogy a rendszer információáramlása két úton megy végbe, egyrészt a központi rendszeren keresztül, így a szükséges információk a tagállamok hatóságai számára közvetlenül elérhetők, másrészt adott ország hatóságai között közvetlenül, ahol erre szükség van.

Ez a megoldás az adott tagállamon belül szervezet meglétét írja elő, egyrészt az adatok pontosságáért, azok elhelyezésének jogosságá-

ért és naprakészségéért felelős szervezetet, másrészt a technikai hátteret biztosító számítógépes szolgálatot. Az előbbi szervezetet az adott ország SIRENE Irodája képezi, mely Magyarországon az ORFK NEBEK keretében működik. Ez az egység a EU által elfogadott SIRENE kézikönyv előírása alapján az egyedüli kapcsolattartó pont az adott tagállamban.

A technikai hátteret biztosító számítógépes szolgáltatást Magyarországon egy korábbi döntés értelmében a Központi Hivatal nyújtja, mely hivatal korábban a Belügyminisztériumhoz tartozott.

Az iroda munkatársai folyamatosan figyelemmel kísérik a schengeni csatlakozás feltételeinek teljesülését, és rendszeresen konzultálnak az ORFK munkatársaival az adatkezelésre vonatkozó rendeletek érvényesülése érdekében. A rendszer működésének kezdete után ellenőrizni fogják az előírások betartását a napi gyakorlat során.

Az iroda készen áll arra, hogy Magyarország schengeni térséghez történő csatlakozásától kezdődően ellenőrizze a SIS nemzeti részét. Reményeink szerint a belső határokon az ellenőrzés megszüntetésére vonatkozó politikai döntés nem várat magára sokáig, és talán a portugál javaslatot (SISone4all) elfogadva már 2007 végén ellenőrzés nélkül léphetjük át a határt.

A magyar konzulátusok vízumkiadásának adatvédelmi ellenőrzése

A személyes adatok védelméről és a közérdekű adatok nyilvánosságáról szóló 1992. évi LXIII. törvény és az állampolgári jogok országgyűlési biztosáról szóló 1993. évi LIX. törvény felhatalmazása alapján, továbbá Magyarország teljes jogú schengeni csatlakozására tekintettel az adatvédelmi biztos munkatársaival 2006-ban három alkalommal folytatott helyszíni ellenőrzést határainkon kívül:

Május 29-30 között a Magyar Köztársaság kijevi konzulátusán,
Szeptember 19-20 között Ungváron és Beregszászon,
Október 24-25-én Belgrádban és Szabadkán.

A vizsgálatok a vízumkiadás adatvédelmi vonatkozásait érintették, a klasszikus konzuli ügyeket nem.

Az adatvédelmi biztos most ellenőrizte először magyar konzulátusok vízumkiadását.

A kijevi ellenőrzés

2005-ben Ukrajnában a magyar konzulátusokon 210 625 vízumot adtak ki, ebből Kijevben 54 562-öt. A vízumkiadás ilyen jelentős forgalma miatt döntött úgy az adatvédelmi biztos, hogy először az ukrajnai magyar konzulátusokon végez ellenőrzést. Az ungvári konzulátus májusi költözése miatt az ottani ellenőrzést őszre halasztottuk.

A vízumügyintézés és a klasszikus konzuli ügyek intézése a Konzuli Információs Rendszeren (KIR) keresztül történik. A vízumügyintézés során az egyes adminisztratív fázisok (vízumkérelmek átvétele, adatbevitel, döntéshozatal, vízumbélyeg nyomtatás) jól elkülönülnek egymástól. A konzulátuson ez az elkülönülés fizikailag is jól megoldott.

A konzulátuson dolgozók a KIR azon részéhez férnek hozzá, melyre munkájuk ellátásához jogosultságuk kiterjed. A rendszer minden módosítást naplóz.

A vízumkérelmek leadásakor a kérelmezők leadják útlevelüket, az útlevél adatlapjának fénymásolatát, a kitöltött vízumkérelmet és egyéb szükséges dokumentumot (meghívólevél, szálláshely visszaigazolás stb.). A vízumkérelmek átvételét követően az útlevél adatait útlevél leolvasó segítségével felviszik a rendszerbe. Ha a beolvasás nem tökéletes, akkor manuálisan rögzítik az adatokat. A vízumkérelem elbírálásához szükséges további, az útlevélben nem szereplő adatokat szintén manuálisan rögzítik, például a balesetbiztosítás időtartama. Az adatbevitelt követően a vízumkérelem a konzulhoz kerül. A kérelem elbírálásának megkezdésekor a konzulok egy, a képernyőn megjelenő ablakban tájékoztatást kapnak arról, hogy a vízumkérelmező adatai szerepelnek-e a tiltónévjegyzékben és az elveszett úti okmányok adatbázisában. A tiltónévjegyzékhez és az elveszett úti okmányok adatbázishoz hozzáférési jogosultsága kizárólag a konzuloknak van. A tiltónévjegyzékben és az elveszett úti okmányok adatbázisában keresni nem lehet, egy-egy ügyhöz kapcsolódóan jelez találatot a rendszer, vagy jelzi, hogy az adott személy nem szerepel az adatbázisban.

A KIR a vízumkérelmezők adatait a Külügyminisztériumon (KÜM) keresztül a Bevándorlási és Állampolgársági Hivatalba (BÁH) továbbítja. A klasszikus konzuli ügyek adatai a Külügyminisztériumnál maradnak. A jogszabályban meghatározott esetekben a vízumké-

relem ügyében nem a konzulátuson születik döntés, hanem a rendszerben továbbított adatok alapján a BÁH dönt a kérelem ügyében.

A külföldiek beutazásáról és tartózkodásáról szóló 2001. évi XXXIX. törvény (Idtv.) 79. § (2) bekezdése értelmében a vízumkérelmek és a kiadott vízumok alapján a külföldi adatait a központi adatkezelő szerv (BÁH) a vízum érvényességi idejének lejártát követő öt évig, az illetékes idegenrendészeti hatóság (konzulátus) a vízum érvényességi idejének lejártát követő egy évig kezeli. Ezt a rendelkezést a papíralapú iratok esetén betartják, mivel a konzulátuson a vízumkérelmeket és a vízumkérelem elbírálásához szükséges további iratokat évente selejtezik. A KIR-ben azonban az adatok törlése nem megoldott, a rendszer minden adatot megőriz, mivel nincs (automatikus) törlési funkciója.

A KÜM tájékoztatása alapján a közeljövőben kezdeményezni fogják az Idtv.-nek az adatmegőrzés határidejére vonatkozó rendelkezéseinek módosítását. Jelenleg ez ellen a módosítás ellen nincs kifogásom, hiszen a Vízuminformációs Rendszerre vonatkozó uniós jogszabálytervezetek is a vízumkérelmek ötéves megőrzését írják elő. Ugyanakkor fenntartom a jogot arra nézve, hogy a jogszabály módosítása során erre a kérdésre még visszatérjek, figyelembe véve az Európai Unió akkor hatályos vonatkozó normáit és a többi tagállam szabályozását.

A papír alapú iratok tekintetében az irattározás rendje áttekinthető, a pincében elhelyezett, zárt irattárban őrzik az iratokat. A vízumkérelmeket egy évig őrzik, kivéve azokat a vízumokat, amelyeknél a vízum érvényességi ideje hosszabb, mint egy év. Az elutasított kérelmeket öt évig őrzik. Mivel az Idtv. nem rendelkezik az elutasított vízumkérelmek esetén a kérelemben szereplő adatok kezelésének időtartamáról, e tekintetben a jogszabály módosítása szükséges.

A vízumkérelmezők tájékoztatása megfelelő. Az interneten kétnyelvű honlapon található információ a Magyarországra történő utazáshoz szükséges feltételekről. Természetesen a szükséges információt a konzulátuson is meg lehet kapni.

A helyi konzuli együttműködés keretében az Európai Unió néhány tagállama megküldte azon kérelmezők listáját, akiknek a vízumkérelmét elutasították. A kapott tájékoztatás alapján a kérelmezőkkel kapcsolatos személyes adatok átadása más állomáshelyeken ugyanakkor jelenleg is folytatott gyakorlat, így szükségesnek tartom megteremteni az ilyen módon szerzett adatok kezelésének jogalapját.

Összegzés

A vizsgálat megállapította, hogy a Magyar Köztársaság kijevi konzulátusán a vízumkiadás során az adatkezelés, adatvédelem megfelel a jogszabályi előírásoknak.

A már több alkalommal továbbfejlesztett KIR, amelynek adattartalma megfelel a jogszabályban előírtaknak, megfelelő számítástechnikai hátteret biztosít. Jelenleg azonban nem biztosított az adatoknak a rendszerből történő törlése. Az erre irányuló szoftverfejlesztést, amely figyelembe veszi az Idtv. vonatkozó, esetleges módosítását, minél hamarabb el kell végezni.

Az úti okmányok adatoldalának fénymásolása szükségtelen, hiszen az úti okmány a vízum kiadásáig ott marad a konzulátuson, azaz ellenőrizni lehet, hogy a vízumkérelemben szereplő adatok azonosak-e az útlevél adataival. A vízumkérelem elbírálásához az útlevél adatait vagy útlevél-leolvasó segítségével, vagy manuálisan rögzítik a KIR-ben, tehát az útlevélben megtalálható adatok a számítástechnikai rendszerbe is bekerülnek. Emellett szükségtelen az úti okmány fénymásolása és a fénymásolat őrzése. Ilyen irányú kötelezettséget az Idtv. sem ír elő.

Megismerve a konzulátuson folyó munkát, amelynek a szakmai munka mellett nagyon sok adatvédelmi vonatkozása van, javasoltuk, hogy a konzulátusokon nevezzenek ki adatvédelmi felelőst. Az adatvédelmi felelős lenne megbízva az adatkezeléssel összefüggő kérdések meghozataláért, az érintettek jogainak biztosításáért és az adatvédelmi jogszabályi rendelkezések és belső utasítások maradéktalan betartásáért. Figyelembe véve ugyanakkor azt a tényt, hogy nem minden konzulátuson azonos a munkateher, megoldási javaslatként merülhet fel adatvédelmi tárgyú továbbképzések megszervezése a konzuli munkatársak részére a Külügyminisztérium keretén belül.

Az ungvári főkonzulátus és a beregszászi ügyfélszolgálati iroda ellenőrzése

A vizsgálat megállapította, hogy a Magyar Köztársaság ungvári főkonzulátusán és a főkonzulátus beregszászi ügyfélszolgálati irodáján a vízumkiadás során az adatkezelés, adatvédelem a következő ajánlások figyelembevételével megfelel a jogszabályi előírásoknak.

Szükségtelennek és adatvédelmi szempontból kifogásolhatónak találtuk, hogy a konzuli adminisztrátorok képernyőjén megjelenő ab-

lak a kérelmező adatainak tiltónévjegyzéken történő esetleges előfordulására enged következtetni. A tiltónévjegyzék megismerése kizárólag a konzuli tevékenységhez kapcsolódhat.

Beregszászon az útlevelek kiadása úgy történik, hogy a konzulátus udvarán állók közül név szerint szólítják az útlevél tulajdonosát. Javasoltuk, hogy a szólítás ne név szerint, hanem sorszám alapján történjen. A kérelmezők a kérelem benyújtásakor két példányban kapnak sorszámot. Ezek közül az egyik a kérelmezőnél marad, a másikat a benyújtott dokumentumokhoz tűzik. A sorszám kiadás ilyen módszere mellett nem látjuk akadályát a sorszám alapján történő szólításnak.

A vizsgálat során a konzulok részéről két adatvédelmet érintő kérdés fogalmazódott meg. Az egyik a meghívó fél adatainak kezelésére vonatkozik. A Magyar Köztársaság Kormánya és Ukrajna Miniszteri Kabinetje között az állampolgárok utazásának feltételeiről szóló, Kijevben 2003. október 9-én elfogadott megállapodás [199/2003. (XII.10.) Korm. rendelet] értelmében és az annak alapján kialakult gyakorlat során az ukrán állampolgároknak meghívólevelet csak a tartózkodási, D típusú vízumkérelemhez kell bemutatni, a C típusú vízumhoz nem. Ezek után esetenként felmerül a kérdés, hogy a Vízumkérelem a Magyar Köztársaságba történő beutazáshoz elnevezésű nyomtatvány 34. pontjában szereplő meghívó személy személyes adatai a valóságnak megfelelnek-e, és hogy a meghívóként megjelölt személy valójában biztosít-e szállást a beutazónak, gondoskodik-e eltartásáról. A Külügyminisztérium tájékoztatása alapján a rovat kitöltése mindenképpen szükséges, ezért a vízumkiadásakor a szúrópróbaszerű ellenőrzést javaslom, így bizonyosodva meg afelől, hogy a vízumkérelemben szereplő természetes személy adatai valósak, és valóban ő a meghívó fél.

Bár adatvédelmi kérdést csak közvetve érint, kértem a Külügyminisztériumot, vizsgálja meg, hogy a megállapodás kormányrendeletben történt kihirdetése megfelel-e a magyar jogalkotási előírásoknak.

Egy másik kérdés az akkreditált utazási irodák által szervezett utazáson Magyarországra látogatók Ukrajnába történő visszatérésére vonatkozik, abból a célból, hogy a konzulátus ki tudja szűrni azokat az irodákat, melyekkel az utazók egy része nem tér vissza hazájába. A Határőrségtől történő tájékoztatás kérése helyett célszerűbb lenne az akkreditációs feltételek között szerepeltetni egy olyan feltételt, hogy az utazási irodának a csoport visszatérését követően a vízumot

kiadó konzulátusra el kell juttatnia egy statisztikát arról, hogy hányan utaztak el a csoporttal, és ebből hány utas tért vissza Ukrajnába/maradt Magyarországon. A Határőrség bűnüldözési, bűnmegelőzési, rendészeti, honvédelmi és államigazgatási célból folytat adatkezelést. A fent említett adatkérés célja pedig az utazási iroda működésének vizsgálata lenne.

Ahogy azt már a kijevi konzulátus ellenőrzéséről szóló megállapításaimban is tettem, ebben az esetben is hangsúlyozni szeretném az Idtv. módosításának és ezzel párhuzamosan a KIR fejlesztésének szükségességét. A KIR-ben az adatok törlése nem megoldott. A korábbiakban a KüM arra tett ígéretet, hogy a SIS II bevezetésekor orvosolják a KIR hiányosságait. A SIS II bevezetésének már több ízben történő elhalasztása azonban felveti azt a kérdést, hogy a SIS II bevezetéséig elodázhatóak-e ezek a fejlesztések.

A Magyar Köztársaság belgrádi nagykövetsége konzuli osztályának és szabadkai főkonzulátusának adatvédelmi ellenőrzése

A 2005-ös adatok szerint Szerbiában adják ki a magyar vízumok 30 %-át, 12 %-ot Belgrádban, 18%-ot Szabadkán.

A vízumügyintézés és a klasszikus konzuli ügyek intézése a Konzuli Információs Rendszeren keresztül történik. A vízumügyintézés során az egyes adminisztratív fázisok – a kárpátaljai tapasztalatainkkal megegyezően – jól elkülönülnek egymástól. Az adatbiztonságot szolgálja, hogy az érdemi ügyintézést (kérelem elbírálása, vízumbélyeg nyomtatása) konzulok, illetve vízumadminisztrátori beosztásban dolgozó magyar kiküldöttek végzik, míg a helyi alkalmazottak csupán az adminisztrációban (kérelmek átvétele) vesznek részt. A belgrádi konzulátuson az adatok rögzítését is vízumadminisztrátori beosztásban dolgozó magyar kiküldöttek végzik.

A konzulátuson dolgozók itt is csak a KIR azon részéhez férnek hozzá, melyre munkájuk ellátása érdekében jogosultságuk kiterjed. A rendszer minden módosítást naplóz.

Szerbiában akkreditált utazási irodák mellett, az úgynevezett Concordia Minoritatis Hungaricae (CMH) hat helyi kirendeltsége is gyűjti a vízumkérelmeket az erre vonatkozó megállapodásnak megfelelően.

A vízumkérelmek átvételét követően az útlevél adatait manuálisan rögzítik a KIR-ben, mivel a Szerbiában kiállított útlevelek gépi le-

olvasásra nem alkalmasak. A vízumkérelem elbírálásához szükséges további, az útlevélben nem szereplő adatokat szintén rögzítik, például a balesetbiztosítás időtartamát. Az adatok bevitelét követően a konzuli adminisztrátorok képernyőjén – attól függően, hogy a kérelmező szerepel a tiltó névjegyzékben vagy nem – egy ablak jelenik meg a következő információval: „*A kérelmező nagy valószínűséggel szerepel a kiutasítási listán vagy az elveszett útiokmányok listáján.*" vagy „*A kérelmező adatai nem szerepelnek sem a tiltó névjegyzékben, sem az elveszett útiokmányok adatbázisában.*"

Az adatbevitelt követően a vízumkérelem a konzulhoz kerül. A kérelem elbírálásának megkezdésekor a konzulok egy, a képernyőn megjelenő ablakban tájékoztatást kapnak arról, hogy a vízumkérelmező adatai szerepelnek-e a tiltó névjegyzékben és az elveszett úti okmányok adatbázisában.

A vízum kiadásakor a vízumbélyeggel ellátott útlevél visszakerül az útlevél tulajdonosához, a vízumkérelem adatlapját irattárban őrzik. Elutasított vízumkérelem esetén az útlevélben látható a kérelem átvételét jelző pecsét, amely jelzi, hogy a kérelmet elutasították. Elutasított D vízumoknál a kérelmező írásban egy formanyomtatványon kap tájékoztatást kérelme elutasításának okáról.

A KIR a vízumkérelmezők adatait a Külügyminisztériumon keresztül a Bevándorlási és Állampolgársági Hivatalba továbbítja. A jogszabályban meghatározott esetekben a vízumkérelem ügyében nem a konzulátuson születik döntés, hanem a rendszerben továbbított adatok alapján a BÁH vagy a Külügyminisztérium dönt a kérelemről.

A papír alapú iratok tekintetében az irattározás rendje mind a konzulátuson, mind a főkonzulátuson áttekinthető, zárt irattárban őrzik az iratokat.

Az irattárba csak konzul léphet be, vagy az ügyintézők konzul kíséretében. A vízumkérelmeket a vízum érvényességének lejártát követően egy évig őrzik, kivéve azokat a vízumokat, amelyeknél a vízum érvényességi ideje hosszabb, mint egy év. Az elutasított kérelmeket öt évig őrzik.

A vízumkérelmezők tájékoztatása céljából a konzulátuson és a főkonzulátuson két nyelven olvasható információ a Magyarországra történő utazáshoz szükséges feltételekről.

A vizsgálatról szóló jelentésünk összegzése megállapította, hogy a Magyar Köztársaság belgrádi nagykövetségének konzuli osztályán és

szabadkai főkonzulátusán a vízumkiadás során az adatkezelés, adatvédelem a következő ajánlások figyelembevételével megfelel a jogszabályi előírásoknak.

A zárt rendszerű biztonsági kamerákról az ügyfeleket már az épületbe/udvarra való belépéskor jól látható módon tájékoztatni kell.

A szabadkai főkonzulátus honlapja csak magyar nyelven érhető el. Az ügyfelek tájékoztatását egy többnyelvű (magyar és szerb) honlap szolgálná megfelelően. Elfogadható megoldást jelenthetne, ha a honlapról link mutatna a belgrádi nagykövetség szerb nyelvű oldalára, ahol a szükséges információk szerb nyelven megtalálhatóak.

A szabadkai főkonzulátuson többször előfordult, hogy a vízumigénylő adatai annak ellenére szerepeltek a tiltó névjegyzékben, hogy már nem állt beutazási és tartózkodási tilalom alatt. Az ügy tisztázásának érdekében levélben kerestem meg a Bevándorlási és Állampolgársági Hivatalt, a tiltó névjegyzék adatkezelőjét.

Megkeresésemre a BÁH főigazgatója arról tájékoztatott, hogy a BÁH beutazási és tartózkodási tilalom adatbázis változásait naponta, illetve a teljes adatbázist hetente elektronikus úton továbbítja a Külügyminisztérium illetékes szervéhez, amely gondoskodik a külképviseleteken lévő adatbázis frissítéséről. Vélhetően az adatbázis frissítés részben vagy egészben történő meghiúsulása okozhatja a problémát. A BÁH és a KüM informatikai szakemberei egy új, jelenleg tesztelés alatt álló informatikai megoldást dolgoztak ki, mellyel elkerülhetők az ilyen problémák.

A szabadkai főkonzulátuson bemutatták annak a felmérésnek az eredményét, melyet az ügyfelek körében végeztek a főkonzulátus munkájának értékeléséről. Az ilyen felmérés eredménye közérdekű adatnak minősül, és az Avtv. 19. §, valamint az elektronikus információszabadságról szóló 2005. évi XC. törvény az ilyen adat közzétételét írja elő. Meggyőződésem, hogy a felmérés eredményének közzététele az ügyfelekkel való hatékony együttműködést is elősegíti.

Váminformációs rendszer

A vámügyi együttműködés fejlesztése során az információcsere elősegítése érdekében a tagállamok és a Bizottság által egyformán hozzáférhető automatizált Váminformációs Rendszer (CIS) kialakításáról döntöttek, amelynek első és harmadik pilléres jogi alapját az

515/97/EK rendelet és az 1995. június 26-i Egyezmény teremtette meg. Ez utóbbit Magyarországon a 2005. évi XCIX. törvény hirdette ki. A Bizottság által kifejlesztett CIS célja a vámügyekkel, a mezőgazdasággal és a kábítószerek prekurzor anyagaival kapcsolatos szabálytalanságok és csalások feltárásának elősegítése.

A CIS egyik legfőbb jellemzője, hogy a tagállam által kijelölt illetékes nemzeti hatóság (a 2005. évi XCIX törvény 3. §-a alapján a Vám- és Pénzügyőrség) közvetlen adatbeviteli lehetőséggel rendelkezik. A nemzeti adatbázisban szereplő adatok központi rendszerbe történő rögzítését csak *„jóváhagyó"* (*„authorizer"*) jogosultsággal rendelkező végezheti, aki a rögzítés során vizsgálja az adatok jogszerűségét és az adatvédelmi szabályok érvényesülését. A bevitt adatokat bármelyik regisztrált felhasználó lekérdezheti. A felhasználói jogosultság megadása a *„jóváhagyó"* által aláírt formanyomtatvány alapján az OLAF-nál történik. A felhasználói jogosultság beállításáról és egyéb kapcsolódó információkról a *„jóváhagyó"*-t értesítik; a felhasználónak az első belépés során kötelező a jelszót megváltoztatni.

A lekérdezések 1%-át automatikusan rögzítik annak ellenőrzése céljából, hogy a lekérdezés jogszerű volt-e, illetve az arra felhatalmazott felhasználó hajtotta-e végre azt. Ezt a nyilvántartást hat hónap múlva törlik.

Az információk tárolása az OLAF[3]-nál található központi adatbázisban történik. A tárolt adatokat évente felülvizsgálják. Azon adatokat, amelyek a CIS céljainak eléréséhez már nem szükségesek, áthelyezik az úgynevezett korlátozott területre (*„grey zone"*). Ez a terület kizárólag adatvédelmi ellenőrzés céljából hozzáférhető; az adatokat innen egy év múlva törlik.

A tagállami hatóságok közvetlenül, az AFIS[4] levelező rendszerén keresztül is cserélhetnek információt.

Az OLAF által kidolgozott és a tagállamok által alkalmazandó Műveleti Eljárások Kézikönyve tartalmazza a CIS céljait, jogi hátterét, a képzésre vonatkozó előírásokat, az adatbiztonsági alapelveket és mi-

3 Csaláselleni Hivatal, amelynek fő feladata az Európai Unió pénzügyi érdekeinek védelme. Az ellenőrzéseket közigazgatási eljárás keretében végzik, szükség esetén a tagállami kapcsolattartó pont segítségével indítanak büntetőeljárást.

4 Antifraud Information System, amely egyebek mellett a CIS-t is magában foglalja.

nimum-követelményeket, továbbá a személyes adatok védelmére vonatkozó szabályokat.

A CIS adatvédelmi felügyelete többrétű:

– az első pillérbe tartozó ügyek esetében a tagállami adatbázist a nemzeti adatvédelmi ellenőrző hatóság, az OLAF-nál lévő központi adatbázist az európai adatvédelmi felügyelő és az OLAF adatvédelmi felelőse ellenőrizheti; közös és egységes megoldást kívánó problémák megtárgyalására a 505/97/EK rendelet 43. cikk (5) bekezdésében hivatkozott ad-hoc bizottság keretében van lehetőség;

– a harmadik pillérbe tartozó ügyek esetében a tagállami adatbázist a nemzeti adatvédelmi ellenőrző hatóság, európai szinten pedig a közös adatvédelmi ellenőrző hatóság (Customs Joint Supervisory Authority – Customs JSA) felügyeli. Az adatvédelmi biztos 2006 nyara óta tagja a közös adatvédelmi ellenőrző hatóságnak.

Statisztikai adatok:

A CIS-ben 375 harmadik pillér hatálya alá tartozó *„élő"* ügy volt (a rögzített ügyek száma 470) 2006. április 30-ig.

A CIS harmadik pillér hatálya alá tartozó részében 1.311 felhasználót regisztráltak, s 4.915 lekérdezést hajtottak végre 2006. április 30-ig.

Magyar adatok:	**1. pillér**	**3. pillér**
Aktív ügyek száma:	8	0
Élő ügyek száma:	11	0
Regisztrált felhasználók:	328	305
Lekérdezések száma:	86	5

2006. júniusban a Customs JSA úgy döntött, hogy valamennyi tagállamban egységes adatvédelmi ellenőrzést kell tartani a CIS vonatkozásában. Az e célból, a Tanács Adatvédelmi Titkárság által összeállított kérdőív az OLAF-nál tett látogatás megállapításain alapul, s főleg adatbiztonsági kérdéseket (eljárási rend és kötelezettségek, képzés, felhasználói jogosultság törlése, fizikai és környezeti biztonság, jelszóhasználat, a rendszerhasználat felügyelete és ellenőrzése, stb.) tartalmaz.

A Customs JSA a konkrét kérdések megválaszolásán kívül az alábbiak vizsgálatát is javasolta:

– az OLAF által kiadott különböző technikai és szervezési intézkedéseket tartalmazó dokumentumok adaptálása megtörtént-e, hatékonyan alkalmazhatók-e, beleértve az esetleges problémák feltárását is;

– az OLAF meglátása szerint sok az olyan regisztrált felhasználó, aki sosem használta a rendszert.

Az említett kérdőív megválaszolása érdekében felkerestük a Vám- és Pénzügyőrség Országos Parancsnokságát, ahol ízelítőt kaptunk a CIS felépítéséről és működéséről.

A látogatás alapján megállapítottuk, hogy Magyarországon a CIS adta lehetőségek kihasználása nem teljes mértékű. A munkatársak meglátása szerint a tagországok nem töltik fel a rendszert naprakész adatokkal, mondván, úgysem sokan használják. Akik nem veszik igénybe a szolgáltatást, arra hivatkoznak, hogy a rendszer tartalma nem naprakész, s például sürgős esetben a faxon történő adatcsere gyorsabb, mint a CIS használata. Ennek ellenére a Vám- és Pénzügyőrség a munkatársak folyamatos oktatásával és tájékoztatással igyekszik a lehetőség jobb kiaknázását megteremteni.

Az adatbázis első pilléres részét azok a magyar szervek, amelyeknek a jogszabályi háttér lehetővé tenné a hozzáférést, nem veszik igénybe, inkább a Vám- és Pénzügyőrségtől kérnek adatszolgáltatást.

A Vám- és Pénzügyőrség véleménye szerint a CIS használatának hatékonyságát *„rontja”*, hogy az egyes modulokhoz külön jelszóval lehet hozzáférni, ami egy-egy munkatárs esetében azt jelenti, hogy az általa igénybe vett adatbázisok miatt 8-10-15 jelszót is meg kell jegyeznie.

Adatvédelmi ellenőrzési problémát jelent, hogy a CIS használatával kapcsolatos valamennyi (első és harmadik pilléres) naplóadatot az OLAF kezeli és tárolja, így a jogszabályok alapján a nemzeti rendszer igénybevétele jogszerűségének vizsgálatára felhatalmazott adatvédelmi biztosnak az OLAF-tól kell kérnie az ellenőrzés alapját képező naplóadatokat. Ezen az sem segítene, ha az adatvédelmi biztos a CIS-hez közvetlenül hozzáférne, mivel a legmagasabb jogosultsági szint sem terjed ki a naplóadatokba történő betekintésre.

Az adatbiztonsági előírások az OLAF előírásainak figyelembevételével készültek, helyenként azonban a szigorúbb magyar szabályokat alkalmazzák.

Europol, NEBEK

2006-ban új feladatként jelentkezett, hogy a nemzetközi bűnügyi információcsere, ezen belül az Európai Rendőrségi Hivatallal (Europol) folytatott együttműködés adatvédelmi felügyelete az adatvédelmi biztoshoz került. Az uniós csatlakozási tárgyalások során, a bel- és igazságügyi fejezet keretében jelent meg feltételként az úgynevezett *„egyablakos elv"* jogi és szervezeti keretének megteremtése. Az *„egyablakos elv"* azt jelenti, hogy meghatározott feladatokat egy kijelölt központi hatóság lát el a tagállamban, amely a hazai koordináció mellett az uniós szervezettel való kapcsolattartásért is felelős, az-az közvetítő szerepet tölt be a hazai szervezetek és az uniós szervezet között.

E működési elvet tartalmazza az Európai Rendőrségi Hivatal létrehozásáról szóló, 1995. július 26-án aláírt Egyezmény (Europol Egyezmény) is, amely szerint a hágai székhelyű Europol két vagy több tagállamot érintő súlyos, nevesített bűncselekmények (terrorizmus, kábítószer- vagy embercsempészet, pénzmosás stb.) esetén – egyebek mellett – elemzési segítséget nyújt a tagoknak. Az elemzéshez szükséges adatokat és információkat a tagállamokban kijelölt nemzeti egységek gyűjtik össze a hazai nyomozó hatóságoktól, és továbbítják a kihelyezett összekötőknek. Az összekötők feladata az információk Europolnak történő átadása, illetve az Europol-elemzéshez (szakmai) segítség nyújtása. Az összekötők feladata az is, hogy az Europoltól vagy más tagországtól érkező adatkérést a nemzeti egységnek megküldjék.

Az *„egyablakos elv"*-nek való megfelelés céljából az Európai Unió bűnüldözési információs rendszere és a Nemzetközi Bűnügyi Rendőrség Szervezete keretében megvalósuló együttműködésről és információcseréről szóló 1999. évi LIV. törvény hozta létre az Országos Rendőr-főkapitányság szervezetében a Nemzetközi Bűnügyi Együttműködési Központot (NEBEK). A törvény hatálya kiterjed az Europollal, az Interpollal, a Schengeni Információs Rendszerben (SIS), az Európai Csalásellenes Hivatallal (OLAF), valamint a két- és többoldalú nemzetközi szerződések keretében vagy az európai közösségi jogi normák alapján megvalósuló bűnügyi együttműködésre és információcserére, továbbá meghatározza a NEBEK feladatait és az adat- és információcsere hazai szereplőkre vonatkozó szabályait. A NEBEK a törvényben meghatározott teljes hatáskörű működését csak 2002. januárban kezdte meg.

A törvény eredetileg tartalmazta a NEBEK adatkezelése és adattovábbítása tekintetében a független adatvédelmi ellenőrzés „*intézményrendszerét*" is, amelyet a Belügyminisztériumban 2002. áprilisi hatállyal létrehozott önálló osztály testesített meg. Később, 2001. december 25-i hatállyal, a Magyar Köztársaság és az Európai Rendőrségi Hivatal között Budapesten, 2001. október 4-én aláírt Együttműködési Megállapodás kihirdetéséről szóló 2001. évi LXXXIX. törvény csak az Europollal folytatott adatcserére korlátozta az adatvédelmi ellenőrzést úgy, hogy az előbb említett önálló osztályt még létre sem hozták.

Ezt követően a 2006. február 16-án kihirdetett, az Európai Unióról szóló Szerződés K.3. cikkén alapuló, az Európai Rendőrségi Hivatal létrehozásáról szóló, 1995. július 26-án kelt Egyezmény (Europol Egyezmény) és Jegyzőkönyveinek kihirdetéséről, valamint a Rendőrségről szóló 1994. évi XXXIV. törvény módosításáról szóló 2006. évi XIV. törvény hatályon kívül helyezte a NEBEK adatvédelmi felelősére vonatkozó rendelkezéseket, s az adatvédelmi biztost jelölte meg az Europol Egyezmény 23. cikke szerinti önálló nemzeti adatvédelmi felügyelő hatóságként, valamint a 24. cikk szerinti Közös Adatvédelmi Ellenőrző Hatóság (Europol Joint Supervisory Body – Europol JSB) tagjaként.

2006 májusára valósultak meg az új feladat személyi és technikai feltételei, s az országos rendőrfőkapitánnyal folytatott megbeszélés után megkezdődtek az adatvédelmi ellenőrzések. 2006 második felében a NEBEK-nél tartott három ellenőrzés során 14 ügyet, a hágai összekötő irodában tartott vizsgálat alatt 12 ügyet tanulmányoztunk.

A NEBEK igazgatója az adatvédelmi biztos véleményét kérte arról, hogy az elektronikus iktatórendszerük eleget tesz-e az adattovábbítási nyilvántartás követelményeinek. Arról is tájékoztatott, hogy – a schengeni csatlakozás előkészítése keretében – új elektronikus ügyfeldolgozó rendszer fejlesztésén dolgoznak, amelynél az adattovábbítási nyilvántartással kapcsolatban – válaszomtól függően – alkalmaznák a jelenlegi rendszer megoldásait. A vélemény elkészítéséhez munkatársaink az első ellenőrzés során elvégezték a mostani iktatóprogram adattovábbítási nyilvántartási szempontú vizsgálatát.

A NEBEK 2004. május 1-jétől vezette be az elektronikus iktatórendszert, amelynek célja a „*papírmentes iroda*" („*paperless office*") megteremtése volt. Az iktatórendszer a hagyományos adatokon (ikta-

tószám, tárgy, küldő szerv, dátum stb.) kívül tartalmazza a rendszer bevezetését követően keletkezett iratok elektronikus változatait is. A NEBEK működésének 2002. januári indulásáig visszamenőleg csak az ügyek főbb paramétereit (iktatószám, tárgy, küldő, ügyintéző, stb.) rögzítették, az iratok beszkennelését utólag nem végezték el, ezért előfordul, hogy például egy 2004 áprilisában érkezett adatkérést nem, míg az arra adott májusi válasz elektronikus iratát tartalmazza a rendszer.

A NEBEK vezetői és munkatársai eltérő jogosultsági szinttel rendelkeznek: előbbiek – beosztástól függően – szélesebb adattartalomhoz férnek hozzá (például betekinthetnek az irányításuk alatt álló ügyintézőnél lévő ügybe), ügyintéző-kijelölési, kiadmányozási stb. joguk van, míg a munkatársak hozzáférése csak a saját ügyeikre és néhány kereső funkció használatára terjed ki. Az iratok beszkennelése az iktatást végző szervezeti egység feladata. Tekintettel arra, hogy technikailag nem megoldható a csak olvasási jogosultság beállítása, az adatvédelmi ellenőrzést végző munkatársaim *„ügyintézői"* jogosultságot kaptak az elektronikus iktatórendszerhez feladataik ellátása céljából. A rendszer a hozzáféréseket és műveleteket naplózza.

A többféle lekérdezési menüpont tesztelése alapján megállapítottuk, hogy a jelenlegi elektronikus iktatórendszer kisebb-nagyobb nehézségek árán, csak átmeneti jelleggel használható adattovábbítási nyilvántartásként. Tájékoztattuk az igazgatót arról is, hogy az adattovábbítási nyilvántartás vezetésétől általában eltekinteni nem lehet, s adott esetben az is probléma, ha egy rendszer túl bonyolultan képes betölteni ezt a funkciót. Felhívtuk a figyelmét, hogy az adattovábbítási nyilvántartás funkcióját és tartalmát tekintve nem azonos az iratnyilvántartással, s kértük, hogy az adattovábbítási nyilvántartás vonatkozásában erre legyenek figyelemmel az új ügyfeldolgozó rendszer kialakítása során.

Az adatvédelmi ellenőrzések során a fentiekben már említett, összesen 26 átvizsgált ügy alapján több hibát azonosítottunk, amelyek többsége nagyobb odafigyeléssel, pontosabb adminisztrálással elkerülhető lett volna.

Az egyik hiba, hogy az elektronikus iktatórendszerben nem tételesen, hanem csoportosítva szerepelnek azok az adatbázisok, amelyekből a törvény alapján a NEBEK közvetlen adatátvételre jogosult, s

csak a lekérdezés tényét jelölik az adatbázis-csoport neve melletti rovatban[5]. Emiatt (a vizsgáltak közül 6 ügyben) nem volt egyértelműen megállapítható, hogy ki, melyik adatbázisból, milyen adatokat kérdezett le; ráadásul gyakran csak akkor rögzítik (például az összekötőnek küldött átiratban) a keresés eredményét, ha valamelyik nyilvántartásban találat volt.

Mivel *„[…]a büntetőeljárás során vagy azt megelőzően a bűncselekménnyel vagy a büntetőeljárással összefüggésben, a büntetőeljárás lefolytatására, illetőleg a bűncselekmények felderítésére jogosult szerveknél, továbbá a büntetés-végrehajtás szervezeténél keletkezett, az érintettel kapcsolatba hozható, valamint a büntetett előéletre vonatkozó személyes adat"* különleges adatnak minősül (Avtv. 2. § 2-3. pont), ezért különösen fontos, hogy pontosan nyomon követhető legyen: ki, milyen célból, melyik adatbázisból, milyen adatot vett át, tekintett meg vagy továbbított.

Jelentős probléma (a vizsgáltak közül 3 ügyben fordult elő), hogy az adatokat CD-n vagy mágneslemezen továbbítják úgy, hogy azokról másodpéldány a NEBEK-nél nem áll rendelkezésre, ezért megállapíthatatlan, hogy milyen személyes adatok átadására került sor. Ez a *„megoldás"* oda vezet, hogy amennyiben egy állampolgár a személyes adatai kezeléséről érdeklődik, valótlan vagy pontatlan lesz a tájékoztatás, s ezzel sérül alkotmányos jogának gyakorlása. Ilyen esetekben nem állapítható meg az sem, hogy a személyes adatok kezelése megfelel-e az Avtv. 7. §-ában előírtaknak: felvételük és kezelésük tisztességes és törvényes volt-e, a személyes adatok pontosak, teljesek és időszerűek voltak-e stb.

---

5 A *„PRIO"* elnevezésű rovat például az alábbi adattárakat tartalmazza:
- bűntettesek nyilvántartása
- modus operandi nyilvántartás
- büntetőeljárás alatt állók nyilvántartása
- kényszerintézkedés alatt álló külföldiek nyilvántartása
- kényszerintézkedés alatt állók nyilvántartása
- külföldre utazásban korlátozott személyek nyilvántartása
- beutazási, tartózkodási tilalom alá eső külföldiek nyilvántartása
- DNS-profilok nyilvántartása
- tartózkodási, bevándorlási engedéllyel rendelkező külföldiek nyilvántartása
- külföldi állampolgárok elvesztett úti okmányainak nyilvántartása

Egy olyan esetet is találtunk, amikor a személyes adatok továbbításának célja nem volt megállapítható, ezért kértük a személyes adatok törlését. Ebben az ügyben az adatkérő nyomozó hatóság leírta, hogy kikkel kapcsolatban, milyen célból és milyen adatokra lenne szüksége, egyúttal tájékoztatást kért az adatkérés teljesítésének feltételeiről. A válaszból kiderült, hogy nem a megfelelő helyen érdeklődött, emiatt a személyes adatok továbbítása céltalanul történt.

Figyelembe véve az Avtv. 5. § (1) és (2) bekezdésében[6] írtakat, amennyiben az adatkérő tájékoztatást kér a szükséges információk beszerzésének feltételeiről, a személyes adatok feltüntetése szükségtelen a megkeresésben. Ha azonban az adatkérő tudja, hogy milyen adatokra van szüksége, akkor azzal is tisztában kell(ene) lennie, hogy kitől és milyen feltételek mellett szerezheti be azokat.

Több esetben előfordult az, hogy egy adatkérés néhány nap eltéréssel megérkezett az Interpoltól és az Europoltól is. Mivel ugyanazon eseménnyel vagy személlyel kapcsolatos adatkérésről volt szó, a NEBEK illetékes szervezeti egysége egy iktatószámon vette nyilvántartásba az ügyet. Ennek logikája – bizonyos szempontból – érthető, ugyanakkor adatkezelési szempontból nem felel meg a vonatkozó jogszabályi előírásoknak. A két nemzetközi szervezet hatásköre, illetékessége és tevékenysége, valamint jogi háttere eltérő, ezért ugyanazon személyes adat kezelésének (továbbításának) konkrét célja is eltérő. Az Interpol hatásköre kiterjed valamennyi olyan bűncselekményre, amely nem politikai, hadi (katonai), vallási vagy faji indíttatású, ezzel szemben az Europol az Europol Egyezmény mellékletében

6 *„5. § (1) Személyes adatot kezelni csak meghatározott célból, jog gyakorlása és kötelezettség teljesítése érdekében lehet. Az adatkezelésnek minden szakaszában meg kell felelnie e célnak.*
(2) Csak olyan személyes adat kezelhető, amely az adatkezelés céljának megvalósulásához elengedhetetlen, a cél elérésére alkalmas, csak a cél megvalósulásához szükséges mértékben és ideig.”

felsorolt bűncselekmények[7] felderítéséhez és nyomozásához nyújt elemzési vagy technikai segítséget. További – a jövő évre tervezett – vizsgálatot igényel az a tény, hogy az Interpol egy 186 tagú *„világszervezet"*, s a tagok között találunk olyan harmadik országot is, amelyben a személyes adatok megfelelő szintű védelmének vizsgálatára szükség lehet.

Az Europolhoz kihelyezett összekötőnél tartott vizsgálatot a Központi Adatfeldolgozó, Nyilvántartó és Választási Hivataltól bekért, véletlenszerűen kiválasztott időszakok alatt végzett lekérdezések naplóadatai alapján végeztük el. Az ellenőrzés során tájékozódtunk az összekötő munkavégzésének körülményeiről is.

Az összekötő irodájába telepített számítástechnikai eszközök lehetővé teszik az Europol adatbázisaihoz való hozzáférést, az Europol szakértőivel és a többi tagország összekötő tisztjeivel folytatott, hálózaton belüli információcserét, valamint a NEBEK-kel való kapcsolattartást. Az adatbiztonsági követelmények miatt ezekre a számítógépekre külső adatbeviteli egység nem csatlakoztatható, és az internet elérésére sincs lehetőség.

A szoftverek karbantartását, fejlesztését az Europol szakemberei végzik, illetve ők állítják be vagy módosítják az adatbázisokhoz való hozzáférési jogosultságokat. Az Europol által el nem fogadott vagy jóvá nem hagyott program nem telepíthető ezekre a számítógépekre.

---

7 emberölés, testi sértés, emberi test tiltott felhasználása, kényszerítés, személyi szabadság megsértése, emberrablás, nemzeti, etnikai, faji vagy vallási csoport tagjai elleni erőszak, közösség elleni izgatás, apartheid, bűnszövetségben vagy üzletszerűen elkövetett lopás, orgazdaság, visszaélés kulturális javakkal, csalás, zsarolás, szerzői vagy szerzői joghoz kapcsolódó jogok védelmét biztosító műszaki intézkedés kijátszása, jogkezelési adat meghamisítása, iparjogvédelmi jogok megsértése, közokirat-hamisítás, pénzhamisítás, készpénz-helyettesítő fizetési eszközzel visszaélés, számítástechnikai rendszer és adatok elleni bűncselekmény, számítástechnikai rendszer védelmét biztosító intézkedés kijátszása, veszтegetés, vesztegetés nemzetközi kapcsolatban, visszaélés robbanóanyaggal vagy robbanószerrel, természetkárosítás, környezetkárosítás, környezetre veszélyes hulladék jogellenes elhelyezése, terrorcselekmény, emberkereskedelem, embercsempészet, visszaélés kábítószerrel, visszaélés robbanóanyaggal vagy robbanószerrel, visszaélés lőfegyverrel vagy lőszerrel, fegyvercsempészet, visszaélés radioaktív anyaggal, pénzmosás

Amennyiben az összekötő a küldő ország valamelyik adatbázisát kívánja elérni, csak külön számítógéppel tudja megtenni. A magyar összekötő tiszt is ilyen, az Europol hálózatától független, vonali titkosító berendezéssel ellátott kommunikációs csatornán keresztül kérdez le a hazai adatbázisokból. E módszer miatt a megjelenő adatok nem kerülhetnek közvetlenül az Europol nyilvántartásaiba, szükség esetén az összekötő manuálisan rögzíti azokat. A számítógép és a vonali titkosító Magyarország tulajdonát képezi.

Az összekötő által az Europol számítógépes rendszerei közül az információcserére szolgáló InfoEx, az Index Rendszer és az Információs Rendszer (IS) érhetők el[8]:

A: Az InfoEx egy olyan levelezőrendszer, amely egyúttal naprakész adatbázisként is szolgál. Az előzmények vagy kapcsolódó elektronikus iratok kereshetők címzett, tárgy (bűncselekmény-kategóriák) és dátum szerint; lekérdezhetők például a meg nem válaszolt üzenetek (ottjártunkkor 172 ilyen volt).

B: Az Index Rendszer az elemzési munkafájlokban (AWF) található adatok tárgymutatóját foglalja magában, amely nem naprakész, mert az előírások szerint az Europol szakértőinek 6 hónap áll rendelkezésre, hogy egy adott információról eldöntsék, felveszik-e az adatbázisba, vagy sem. (Egyik aktuális kérdés, hogy ez alatt a hat hónap alatt ki a felelős az információért: az Europol, amely még *„gondolkodik”* vagy a küldő ország, amelynek már kikerült az adat a *„kezéből”*? A megoldást tartalmazó jegyzőkönyv-tervezetet még tárgyalják.)

8 Az elemzési munkafájlokat (*„analytical working file”* – AWF) tartalmazó számítógépes adatbázishoz az azt koordináló és feldolgozó Europol-elemzők, illetve az érintett tagállam összekötői vagy szakértői férnek hozzá.
Az Europol Egyezmény 10. cikke alapján az AWF-ekben végzik el a bűncselekménnyel, elkövetési formával vagy bűnözői csoporttal kapcsolatos, a tagállamoktól beérkező információk elemzését. Egy AWF-ben való ügyfeldolgozást megelőzően úgynevezett nyitási utasítást készítenek, amelyet az igazgatótanács hagy jóvá, s véleményezésre meg kell küldeni a Közös Adatvédelmi Ellenőrzési Hatóságnak. Az Europol jelenleg 17 AWF-en dolgozik, amelyből 11-ben Magyarország is részt vesz. Az Europol Egyezmény alapján lehetőség van arra is, hogy egy AWF-ben található információtömegből kiemeljenek például egy személyt vagy egy bűnözői csoportot, s erre vonatkozóan külön, célzottabban gyűjtsenek és elemezzenek különböző adatokat. Ebben a munkában általában csak a konkrétan érdekelt tagállamok vesznek részt (ami szűkebb kört jelent, mint az AWF-ben), s a kiemelést *„célcsoport”*-nak (target group) nevezik.

Az Index Rendszerben személyre, kommunikációs formára (telefonszám, e-mail cím stb.), közlekedési eszközre, helyszínre, szervezetre lehet keresni.

C: Az Információs Rendszer (IS) „*referencia adatbázis*"-ként működik, amelybe többnyire a közelmúltban befejezett ügyek adatai kerülnek. Mivel a rendszer üzembe állítására tavaly került sor, az adatfeltöltés folyamatosan zajlik; ottjártunkkor 62697 rekordot és 9890 személyre vonatkozó rekordot tartalmazott. Az adatok rendszerből történő törlésének határidejét az Europol figyeli, s három hónappal a lejáratot megelőzően értesíti a tagországot. A tagországok egy részénél az összekötő, más részénél a nemzeti egység munkatársa törli – az esetleges további tárolásra vonatkozó egyeztetés után – a lejárt határidejű adatokat.

A december elején tartott ellenőrzés idején az InfoEx-ben 1850 beérkező és 1482 kimenő üzenet (összesen 3332) volt, amelybe a konkrét személyes adatok cseréjéről szóló iratokon kívül beleértendők a különböző tájékoztatók, elemzői jelentések stb. is. (Az összekötő tájékoztatása szerint 2005-ben összesen 3250 információcsere történt kb. 985 ügyben; 135 megkeresés érkezett célzottan Magyarországnak, amelyből 71 a kétoldalú, 64 pedig a többoldalú – ezen belül az Europollal folytatott – együttműködés keretébe tartozott.)

A hágai ellenőrzés során megállapítottuk, hogy az összekötői munka gyakorlata többé-kevésbé a hatályos előírásoknak megfelelően alakult ki, azonban hiányosságként állapítottuk meg, hogy a hazai adatbázisokból történő lekérdezések adminisztrációja pontatlan, s a vizsgált 12 ügyből – a NEBEK-nél folytatott későbbi egyeztetés alapján – 4-et az összekötő saját hatáskörben intézett el. Tekintettel arra, hogy az Europol Egyezmény értelmében az Europol és a tagállami illetékes hatóságok közötti egyetlen összekötő szerv a NEBEK, ezekről az ügyekről legalább utólag értesíteni kellett volna.

További észrevételünk, hogy a Magyarországról érkező adatkérések, illetve a külföldi megkeresésekre adott válaszok gyakran nem elég részletesek/pontosak, sokszor hiányoznak a kezelési kódok[9] és

9 H-1, ha az információ bizonyítékként történő felhasználására igazságszolgáltatási (bírósági) eljárásban csak a küldővel történt egyeztetést követően kerülhet sor; H-2, ha a küldővel történő egyeztetés kötelező az információ felhasználása, továbbítása előtt; H-3, ha a mellékletben meghatározott valamely továbbítási cél, illetőleg különleges továbbítási engedély vagy korlátozás megjelölése szükséges.

egyéb megjegyzések (például az információ besorolásának úgynevezett 4x4-es rendszere[10] szerinti jelölés)[11].

Itt jegyezzük meg, hogy az úgynevezett rutinszerű lekérdezés jelei láthatók némelyik ügyiratban: például egy cseh megkeresésben bankkártya-csalás miatti nyomozáshoz kérték a megadott adatok ellenőrzését a modus operandi nyilvántartásban, ennek ellenére 9 adatbázisban hajtották végre a keresést. Az okokra vonatkozó információkat nem találtunk az iratokban, s az ellenőrzött munkatárs sem adott kielégítő magyarázatot.

Ellenőrzési tapasztalataink alapján a jogszabályi háttér felülvizsgálata és a napi gyakorlathoz történő igazítása, a NEBEK Adatvédelmi és Biztonsági Kézikönyvének elkészítése[12], annak elérése, hogy a rendőrségi adatokat tartalmazó adatbázisok adatkezelője a rendőrség legyen, az Europol tevékenységének a hazai nyomozó szervekkel történő jobb megismertetése, a nemzetközi információcsere elveinek következetesebb érvényesítése hozzájárulna ahhoz, hogy a meglévő szervezési és szakmai hiányosságok ne adatvédelmi problémaként jelenjenek meg.

---

10 Az információforrás megbízhatóságának jelölése: „A", ha a forrás hitelessége, megbízhatósága és illetékessége nem kétséges, vagy az információ olyan forrástól származik, aki a múltban minden esetben megbízhatónak bizonyult; „B", ha az információ olyan forrástól származik, akitől a kapott információ a legtöbb esetben megbízhatónak bizonyult; „C", ha az információ olyan forrástól származik, akitől a kapott információ a legtöbb esetben megbízhatatlannak bizonyult; „D", ha a forrás megbízhatósága nem értékelhető.
Az információ megbízhatóságának jelölése: „1" az olyan információ esetén, amelynek pontossága nem kétséges; „2" az olyan információ esetén, amelyet a forrás személyesen észlelt, de amelyet a továbbító tisztviselő személyesen nem észlelt; „3" az olyan információ esetén, amelyet a forrás nem személyesen észlelt, de amelyet más, korábban rögzített információ megerősít; „4" az olyan információ esetén, amelyet a forrás nem személyesen észlelt, és az nem is erősíthető meg.

11 A kezelési kódokat és az úgynevezett 4x4-es rendszer szerinti jelöléseket az 1/2002. (BK 5.) BM-PM együttes utasítás tartalmazza.

12 Az Adatvédelmi és Biztonsági Kézikönyv elkészítését a 4/2002. BM-PM együttes rendelet írja elő, de annak összeállításával és hatálybaléptetésével ötödik éve adós a NEBEK. Tekintettel arra, hogy a NEBEK a nemzetközi bűnügyi információcsere iránya, tartalma, sebessége szempontjából meghatározó szereplő, szükséges lenne az ORFK belső rendelkezéseitől eltérő vagy azokat kiegészítő szabályok összefoglalására.

Az EURODAC vizsgálat

Az Európai Közösség tagállamainak egyikében benyújtott menedékjog iránti kérelem megvizsgálására illetékes állam meghatározása érdekében 1990. június 15-én Dublinban aláírták az erről szóló egyezményt (a továbbiakban: a dublini egyezmény). Az egyezmény előírásai értelmében meg kell állapítani a menedékjogot kérelmező személyek és a Közösség külső határainak jogellenes átlépése miatt letartóztatott személyek azonosságát, valamint lehetővé kell tenni annak ellenőrzését, hogy az adott tagállam területén illegálisan tartózkodó külföldiek kértek-e menedékjogot valamely másik tagállamban.

A személyek pontos azonosításának céljára a Európai Közösség tagállamai az ujjnyomatok összehasonlítását választották. Az erre szolgáló rendszer EURODAC néven került kialakításra. Az EURODAC létrehozása a Tanács 2725/2000/EK rendelete alapján történt. Az itt meghatározott EURODAC rendszer egy központi egységből áll, amely az ujjlenyomatadatok számítógépes központi adatbázisaként működik, és a tagállamok, valamint a központi adatbázis közötti elektronikus adatátvitelt szolgálja.

Az EURODAC rendszer tehát egyrészt a menedékjogot kérelmező személyek azonosítására, másrészt a menedékjog elbírálásában eljáró ország meghatározására szolgál. A rendszer alkalmazása ennek megfelelően bonyolult jogi és eljárási feladatokat lát el. A rendszer 2003. december 15-én kezdte meg hivatalosan a működését.

A személyek azonosítását végző rendszer két részből áll. Egyrészt a központi egységből, másrészt a hozzá távközlési vonalakon keresztül kapcsolódó, a tagállamok területén működő nemzeti rendszerekből. Az európai adatvédelmi biztos 2006 folyamán elrendelte az EURODAC rendszerre vonatkozó adatvédelmi előírások betartásának ellenőrzését. Az ellenőrzések végrehajtása során az EURODAC központi egységénél az Európai Adatvédelmi Biztos Hivatalának munkatársai végezték az ellenőrzést, míg a tagállamoknál a nemzeti adatvédelmi hatóság, Magyarországon az Adatvédelmi Biztos Irodájának munkatársai hajtották végre az ellenőrzést.

A rendszer működésének egységes és összehasonlítható ellenőrzése érdekében a tagállamok hatóságai az európai adatvédelmi biztos által a tagországoknak átadott kérdőív alapján végezték az ellenőrzést. Magyarországon a kérdőívet a vizsgálat elvégzésének kezdetekor átad-

tuk az ujjnyomatok kezelését végző Bűnügyi Szakértői és Kutatóintézet, valamit a menedékkérők ügyeinek intézését is végző IRM Bevándorlási és Állampolgársági Hivatal vizsgálatban illetékes munkatársainak. Ezt követően az Adatvédelmi Biztos Irodájának munkatársai konzultációt folytattak a kérdőív kérdései alapján a szóban forgó szervezetek munkatársaival, és ennek alapján összeállították a rendszer adatvédelmi eljárására vonatkozó kérdőív egyes kérdéseire a választ.

Az EURODAC EU adatvédelmi biztosa által elrendelt vizsgálatának kérdései és az azokra adott válaszok a következők voltak:

1. Hogyan biztosítják, hogy csak harmadik ország állampolgárairól gyűjtsenek adatot és az EU állampolgárairól nem?
   Ha EU állampolgár jelentkezik bevándorlóként, a magyar hatóságok sohasem továbbítják az ujjnyomatukat az EURODAC-ba.
2. Milyen intézkedést tesz a tagállam, hogy javítsa az ujjnyomatok minőségét?
   A Daktiloszkópiai Osztály két munkatársa figyelemmel kíséri az összes beérkezet ujjnyomat minőségét, és rendszeres helyszíni segítségnyújtással, tanácsadással és gyakorlati oktatással segíti az ujjnyomatok minőségének javítását.
3. Milyen szabályokat és eljárásokat alakított ki a Nemzeti Elérési Pont, ha a kérelemért folyamodó személy kiskorú? Ezek a szabályok megfelelnek-e az Egyesült Nemzetek Szervezete Gyermekjogi Egyezményének?
   Minden menedékkérővel ismertetik a kérelem benyújtásának kritériumait, így a 14 éven aluliakra vonatkozó ujjnyomatvételt tiltót is. Az erről szóló anyagot több nyelven elkészíttette a hatóság, és a menekültkérők megkapják azt. Ezenkívül az ismertetésnél tolmács van jelen, aki szükség esetén elmagyarázza a leírtakat. Az eljárás során, ha a kiskorú kísérővel érkezik (szülő vagy rokon) akkor ez a személy, ha kísérő nélkül érkezik, akkor a kinevezett ügygondnok van jelen az adatok felvételénél. Ha a kiskorúnak nincs semmilyen okmánya, akkor a kísérő által bemondott születési időt veszik alapul az ujjnyomat vételénél.
4. Alkalmaz-e a tagállam olyan eljárást, amelynek során az állampolgárságot megszerző kérelmezők listáját állítják össze?
   Igen. Az Állampolgársági Főosztály értesítése alapján az elismert menekültek adatait zárolják, az állampolgárságot szerzettekét törlik.

5. Milyen adminisztratív intézkedéseket alkalmaznak a három kategória kezelésére?
   Nem történik intézkedés, ha más tagállamban kap tartózkodási engedélyt a kérelmező, vagy más tagállamon keresztül hagyja el az országot, vagy más tagállamban kap állampolgárságot.
6. Hasznos volna tudni, hogy milyen szabályok – eltekintve az EURODAC szabályzat 11. cikkében szereplő három esettől – határozzák meg, hogy a külföldi állampolgárok adatait mikor továbbítják a központi egységbe?
   Az a hatóság határozza meg, hogy 3. kategóriába[13] tartozik-e az illető menekült, amelyik az ujjnyomatot leveszi. Ebben az esetben a központi egységhez csak ellenőrzésre továbbítják az adatokat.
7. Van-e tudomása az adatvédelmi hatóságnak arról, hogy valaki azzal a kéréssel keresse meg a hatóságot, hogy személyes adatai szerepelnek-e az EURODAC rendszerben? Ha az egyéni megkeresések száma nem egyezik a különleges keresések aktuális számával, hogy magyarázza az ellentmondást?
   Nem volt ilyen kérés. A kérelmezőket tájékoztatja a magyar hatóság, hogy hol kérhetnek különleges keresést[14].
8. A jogszerűtlen adatfelhasználásnak milyen szankciói vannak az EURODAC szabályzat 25. cikke alapján?
   A jogosulatlan adattovábbítást a magyar büntető törvénykönyv szankcionálja.
9. Milyen intézkedést tesznek, hogy a többszörös adatbevitelről tájékoztassák az érintettet?
   Tájékoztatjuk, hogy adatai tekintetében több találatot jelzett a rendszer.
10. Az EURODAC szabályzat 18. cikkében foglaltak nem rónak-e aránytalan terhet a hatóságra?
    Az eddigi gyakorlat alapján ez nem jelentett aránytalan megterhelést.

---

13 1. kategória: menedékjogot kérelmező személy;
2. kategória: a külső határok jogellenes átlépése miatt elfogott külföldiek;
3. kategória: valamely tagállam területén illegálisan tartózkodó külföldiek;

14 különleges keresés: „*az érintettnek jogában áll megismerni a központi adatbázisban nyilvántartott, rá vonatkozó adatokat, valamint hogy azokat mely tagállam továbbította a központi egységhez.*"
(2725/2000/EK tanácsi rendelet)

11. Van-e a nemzeti hatóságnak biztonsági auditja?
    Nincs.
12. Van-e naprakész listája a hatóságnak azokról a személyekről, akik hozzáférnek az EURODAC-hoz?
    Igen.
13. Milyen szabályai vannak a Dublinettel történő adatcserének?
    A Dublinethez három főnek van hozzáférési jogosultsága. Az adatcsere titkosított pdf formátumban történik. Az alkalmazott adatcsere szabályai megfelelnek a 1560/2003/EK rendeletben leírtaknak.
14. A személyes adatok cseréje alkalmával milyen adatvédelmi intézkedést biztosítanak?
    Jelszó, jelszócsere, a hozzáférés és a végzett műveletek naplózása, titkosító eljárás alkalmazása.

A fenti kérdések és a rájuk adott válaszok áttekintik az EURODAC előírásokat és azok gyakorlati alkalmazásának összhangjára hivatkozva az egyes intézkedések EU-s jogalapjait.

A Prümi Szerződéshez való csatlakozás előkészületei során tett észrevételek

Belgium, Németország, Spanyolország, Franciaország, Luxemburg, Hollandia és Ausztria 2005. május 27-én írták alá a határon átnyúló együttműködés fokozásáról szóló szerződést különösen a terrorizmus, a határon átnyúló bűnözés és az illegális migráció leküzdése érdekében (Prümi Szerződés, a továbbiakban PSZ, illetve Szerződés). Ezt a szerződést a sajtó és közvélemény Schengen III. néven is említette, noha sem jogilag, sem intézményileg nem kötődik a korábbi schengeni egyezményekhez, de filozófiájában és intézményeiben azonban kétségtelenül épít a schengeni vívmányok egyes elemeire.

A PSZ létrehozásának ötletét Otto Schily, korábbi német szövetségi belügyminiszter vetette fel 2003-ban, és kezdetben Németország, Ausztria és a Benelux államok vettek részt az egyezmény szövegének kidolgozásában. A PSZ-ben lefektetett elvek összhangban álltak a közben kibővült Unió bel- és igazságügyi együttműködése ötéves fejlesztési célkitűzésének keretében elfogadott Hágai Program előírásaival, ezért mintegy pilot projektben való részvételként Franciaország és Spanyolország is csatlakozott a Szerződéshez.

A Hágai Program egyik alapvető újdonsága az, hogy alapvető célként határozza meg a *„hozzáférhetőség elvét”*. Ennek keretében célul tűzték ki, hogy 2008. január 1-től a bűnüldözési információk határokon átnyúló cseréje érdekében a hozzáférhetőség elvét kell alkalmazni az Unió egész területén. Amennyiben egy bűnüldözési tisztviselőnek az egyik tagállamban feladatainak végrehajtásához információra van szüksége, megkaphatja azt egy másik tagállamból, és a másik tagállam azon bűnüldözési ügynöksége, amelynek a szóban forgó információ birtokában van, a kérvényezett célra rendelkezésre fogja azt bocsátani, figyelembe véve az adott államban zajló vizsgálatok követelményeit. Az információcsere alkalmával előírták, hogy milyen feltételeket kell betartani.

A Hágai Program végrehajtása során a hozzáférhetőség elvének betartása terén napjainkig nem sikerült kézzelfogható eredményt elérni. 2005 folyamán olyan döntés született, hogy hat adatfajta (DNS-profilok, ujjlenyomatok, ballisztikai adatok, gépjármű-nyilvántartási információk, telefonszámok és egyéb hírközlési adatok, személyi és lakcímadatok) tekintetében egyenként, fokozatosan kell kidolgozni a megvalósítás módozatait. Az előkészítő munka azonban lassan, vontatottan halad.

A PSZ tagállamai a szerződés céljainak technikai végrehajtása során olyan előrehaladást értek el, hogy kijelentették, részükről nem teszik kívánatossá uniós szinten, hogy más jogi és technikai megoldások épüljenek ki.

Ezzel olyan helyzet állt elő, hogy a Hágai Program elvének megvalósítását egy attól független szerződés keretében teljesítik az abban részt vevő országok. Ebben a tekintetben a PSZ DNS, daktiloszkópiai és gépjárműadatok cseréjére szolgáló rendelkezései kiemelkedő jelentőségűek.

A PSZ-t aláíró államokban a szerződés 2007 folyamán hatályba lép. Négy további uniós tagállam (Portugália, Olaszország, Szlovénia és Finnország) jelezte csatlakozási szándékát a szerződéshez. A Hágai Program megvalósításának késedelme miatt a német kormány úgy döntött, hogy kezdeményezi a PSZ uniós jogi keretbe emelését.

A DNS, a daktiloszkópiai és a gépjármű adatbázisból történő adattovábbítás eltérő mértékben rendelkezik személyes adatokkal. Ezekből az adatbázisokból történő közvetlen lekérdezésnél azzal kalkulálnak, hogy a rendszer fokozatosan lesz technikailag működőké-

pes, 2007 nyarára utolsóként a gépjárműadatok is hozzáférhetőek lesznek.

A PSZ a személyes adatok kezelése miatt több adatvédelmi előírást tartalmaz. Ezek alapján az adatok kezelésének meg kell felelni az európa tanácsi rendelkezéseknek.

A személyes adatok átadása a Szerződés alapján nem kezdődhet meg, amíg a PSZ. 7. fejezete (adatvédelmi rendelkezések) hatályba nem lépett az átadásban érintett szerződő felek területén. A feltételek teljesülését a Miniszteri Bizottság határozatban állapítja meg. Fontos szerepet kap a célhoz kötöttség elvének betartása is. Ez a gépjármű-nyilvántartás terén az egyes országokban eltérően jelentkezik. Van, ahol az adatszolgáltatás céljaként szabálysértési kategóriát jelölnek meg, míg máshol bűncselekmények esetén tartják indokoltnak az adatszolgáltatást.

A Prümi Szerződéshez történő magyar csatlakozás lehetőségének vizsgálata során tett észrevételek

2006 folyamán felmerült a PSZ-hez való csatlakozás lehetőségének és szükségességének vizsgálata. A csatlakozás adatvédelmi kérdéseinek tisztázása végett előbb az országos rendőrfőkapitány, később az Igazságügyi és Rendvédelmi Minisztérium kérte fel az adatvédelmi biztost, hogy tegye meg észrevételét a csatlakozással, illetve az előkészítő anyaggal kapcsolatban. A kérésnek megfelelően a biztos a következőkben fejtette ki véleményét:

„A Prümi Szerződés célja, hogy az abban részt vevő országok fokozzák a határon átnyúló együttműködésüket a terrorizmus elleni harc, a határon átnyúló bűnözés és az illegális migráció területén, különös tekintettel a kölcsönös információcserére. Ennek fő területeit a DNS-profil, az ujjnyomat és a gépkocsi-nyilvántartás adatainak kölcsönös cseréjében határozzák meg, hangsúlyozva, hogy az adatok cseréjénél az egyes országok nemzeti joganyagának előírásait kell figyelembe venni, és az adatok cseréjét a nemzeti kapcsolattartó egységen (national contact point) keresztül kell végrehajtani.

Ismereteink szerint mind a DNS, mind az ujjnyomat-nyilvántartás két részből áll, mely egy szakértői és egy személyes adat nyilvántartást tartalmaz. Az azonosítás elvégzéséhez mindkét esetben szakértői közreműködés szükséges, és csak a vizsgálat eredménye alapján lehet megállapítani vagy elvetni az illető személyazonosságát. Ennek megfelelő-

en lehet a személy adatait kezelni. Mivel a biometrikus azonosítás elvégzését többféle eljárással lehet megvalósítani, ezért az egyes államok más és más eljárást alkalmaznak, így az ezekből kialakított szakértői adatbázis adatai is különfélék lesznek az egyes országokban.

A szóban forgó adatbázisokkal kapcsolatban előbb kifejtett gondolat azért fontos, mert a Prümi Szerződés egyik célkitűzése hosszabb távon az, hogy az egyes nemzeti adatbázisok adatait külső, az egyezményt aláíró másik állam hatóságai adott esetben közvetlenül is elérjék. Álláspontom szerint ezek a törekvések nem támogathatók sem adatvédelmi, sem adatbiztonsági, sem szakértői szempontból.

A Prümi Szerződés célkitűzéseivel egyetértek, de annak megvalósítását a nemzeti kapcsolattartó ponton keresztül tartom elképzelhetőnek. Ez az egység alkalmas kell, hogy legyen a szakértői szervezetek gyors elérésére és az általuk adott szakvélemény soron kívüli továbbítására, illetve az azonosítás eredményeként ismertté vált személyes adatok kezelésére. A nemzeti kapcsolattartó pont feladatai között célszerű szerepeltetni – a vonatkozó adatvédelmi, adatbiztonsági szabályok betartása mellett – az egyezményben szereplő gépjármű regisztrációs adatok kezelését is.

A nemzeti kapcsolattartó pont működésének kialakításakor figyelembe kell venni (célszerűnek tartom figyelembe venni) az adatbázisokhoz való hozzáférés jogosultsági kérdéseinek tisztázását, az adatvédelmi és adatbiztonsági előírások figyelembevételével.

A bűnüldözési célú adatbázisok adatkezelője a jelenlegi törvényi szabályozás szerint nem a rendőrség. Amennyiben Magyarország csatlakozni kívánna a Prümi Szerződéshez, a csatlakozás előtt meg kellene vizsgálni a szóban forgó adatbázisok rendőrség által történő adatkezelésének szükségességét és az ehhez szükséges törvényi újraszabályozás lehetőségét, valamint csatlakozás feltételeiből származó kötelezettségeket is. Ez adott esetben körültekintő elemző munka elvégzését jelenti."

„A Prümi Szerződés (PSZ) és a Hágai Program (HP) egymáshoz való viszonyát elemezve megállapítható, hogy a HP-ban meghatározott hozzáférhetőség elvét az eltelt időszakban nem sikerült a gyakorlatban megvalósítani, melynek egyik fő oka, hogy az elvek megvalósítása során túl sok adatfajtát vettek figyelembe, és az eljárás adatvédelmi követelményeinek teljesítése hosszas egyeztetést tett szükségessé. A PSZ a fenti problémák gyakorlatias megoldását tette lehetővé az abban részt vevő országok számára. Ebben a fázisban még nem EU-s elő-

írásként, hanem a részt vevő országok saját elhatározásból származó eljárásaként jelenik meg. Komoly erőfeszítés történik a részt vevő országok számának növelése érdekében, majd a végzett munkára és a befektetett anyagi eszközökre is hivatkozva kezdeményezik az eljárás EU-s jogba való emelését.

Mivel a HP-ban meghatározott adatkörre vonatkozóan a hozzáférhetőség elvének alkalmazása a kitűzött határidőre nem látszik teljesíthetőnek, ezért a PSZ célként – ez nem az előterjesztésből, hanem a PSZ angol nyelvű változatából derül ki – a szervezett bűnözés elleni harcot, a határon átnyúló bűnözés kezelését és az illegális migráció visszaszorítását tűzte ki. Ezt azért tartjuk lényegesnek rögzíteni, mert a célhoz kötöttség elvét a PSZ keretei között is be kell tartani, bár a PSZ adatvédelmi kérdései még nem kellően megoldottak.

A célhoz kötöttség elvét a PSZ-ben történő lekérdezések során is be kell tartani, mert adatvédelmi szempontból csak így támogatható a lekérdezés.

A PSZ alkalmazása kapcsán felmerülhet az a kérdés is: amennyiben a PSZ joganyaga eltér az EU-s gyakorlattól, és nem lesz az EU joganyag része, akkor az itteni eljárást adott esetben meg lehet-e támadni a bíróságnál, amely a közösségi jog alapján dönt.

A PSZ-hez való csatlakozás melletti érvek áttekintése mellett talán érdemes lenne összegyűjteni a csatlakozás ellen szóló érveket is, így együtt lehetne látni az előnyt–hátrányt és a megoldandó feladatok körét is.

A PSZ keretében on-line elérni kívánt három adatbázis: a DNS, a daktiloszkópiai és a gépjármű-nyilvántartás. A három adatbázis alapvetően különbözik egymástól. A DNS és a daktiloszkópiai adatbázisok szakértői adatbázisok, ami a mi esetünkben azt jelenti, hogy a lekérdezés során személyes adatok kezelésére nem kerül sor, mert azt külön kezelik, és ennek megfelelően az előterjesztésben szereplő referencia adatbázis nem is tartalmaz személyes adatokat. A gépjármű-nyilvántartásból történő lekérdezésénél viszont személyes adatok kezelésére is sor kerül. Ez okozza a különböző adattárak on-line lekérdezésének eltérő megítélését.

A DNS és a daktiloszkópiai referencia adattárak kezelését szakértők végzik. Csak ők alkalmasak az adatok bevitelére, lekérdezésére, a kapott adatok összehasonlítására, az eredmény minősítésére. A szakértők munkája az on-line lekérdezés során is megkerülhetetlen. Ez az oka

annak, hogy a lekérdezés a nemzeti összekötő ponton keresztül történik. Nem feladatunk az ehhez tartozó szakmai tevékenység megítélése, de az előterjesztés nem tér ki arra, hogy az eltérő nyelvi és technikai feltételek milyen feladatok elvégzését követelik meg ahhoz, hogy például Spanyolországból le lehessen kérdezni a magyar adatokat, és mit kell tennie a magyar szakértőnek ahhoz, hogy holland adatbázist le tudjon kérdezni. Az adatbázisok szöveges része általában az adott ország saját nyelvén kérdez. Ehhez lehet, hogy az adott szakértői rendszereket is át kellene alakítani.

A PSZ-hez való csatlakozással összefüggésben az IRM által készített előterjesztés tartalmazza a BSZKI helye és szerepe meghatározásának fontosságát. Javasoljuk, hogy az IRM kezdeményezze a kérdés mielőbbi megoldását, mert az adattárak helyzete az új minisztériumi struktúrában jelenleg nem megoldott, egy sor kérdésről az adattárak adatvédelmi helyzetének tisztázása miatt is intézkedni kell. (rendőrség, BSZKI, AH egymáshoz való viszonya)

A gépjármű-nyilvántartásból történő adatszolgáltatás leírása a szóban forgó anyagban számunkra elnagyolt. A három szóban forgó adatbázis közül adatvédelmileg ez a legérzékenyebb. A „4. Gépjármű-nyilvántartási adatok automatizált keresése" című részben leírtak adatvédelmi szempontból nem megnyugtatóak. A lekérdezés célja csak a PSZ céljaként említett ok (a szervezett bűnözés elleni harc, a határon átnyúló bűnözés kezelése és az illegális migráció visszaszorítása) lehet, ezzel szemben az előterjesztés szabálysértés esetén történő adatszolgáltatást is említ. Ez nem a PSZ célja, ebben az esetben a célhoz kötöttség nem áll meg. A gépjármű adatbázis adatainak on-line lekérdezése adatvédelmi szempontból problémát jelent, mert a lekérdezés jogosságának, célhoz kötöttségének ellenőrzése ebben az esetben nem megnyugtatóan megoldott. Ebben az esetben az adatszolgáltató ország adatvédelmi hatóságának nincs lehetősége a lekérdezés célhoz kötöttségét ellenőrizni. A gépjármű-nyilvántartás személyes adatainak relevanciája külföldön történt szabálysértési ügyekben nem minden esetben áll meg. Hasonlóan a közrend és közbiztonság érdekében történő lekérdezések sem tartoznak a PSZ által meghatározott célok körébe, ezért az ilyen esetekben történő lekérdezés is aggályos.

Az előterjesztésben ismertetett, a gépjármű-nyilvántartásból történő automatikus lekérdezésre vonatkozó lehetőségek és esetek körét adatvédelmi szempontból aggályosnak tartjuk, és a jelenlegi törvényi szabá-

lyozással ellentétesnek találjuk. A csatlakozási folyamat során ennek az on-line lekérdezési lehetőségnek a törvényi hátterét tisztázni kell."

A 29-es Adatvédelmi Munkacsoport tevékenysége

A Munkacsoportban a tagállamok független nemzeti hatóságainak biztosai dolgoznak közösen az európai adatvédelemért. A tagállamok adatvédelmi szervei, az európai adatvédelmi biztos és az Európai Bizottság közös munkájának köszönhetően a Munkacsoport alkalmas fórum az európai adatvédelem kihívásainak megoldására.

A Munkacsoport gondos mérlegelés útján dönt arról, hogy a számos adatvédelmi probléma közül melyeket vegyen fel munkaprogramjába. A kiválasztásban a következő szempontokat vizsgálják: (1) fennáll-e az adott probléma egynél több tagállamban; (2) van-e olyan politikai ok, ami miatt a probléma sürgős; (3) hány embert érint a probléma; (4) van-e esélye annak, hogy a problémára a Munkacsoport konkrét megoldásokat tud találni. Az előbbiek figyelembevételével a 2006/2007-es munkaprogram főbb pontjaiként a Munkacsoport a következőket jelölte meg: az adatvédelmi irányelv, új technológiák, nemzetközi adattovábbítás EU-n kívüli országokba, külső kommunikáció.

A Munkacsoport feladatainak egyik jelentős területe az EU adatvédelmi irányelvéhez kapcsolódik. Tanácsot ad az Európai Bizottságnak vagy az Európai Parlamentnek az irányelv módosításával kapcsolatban és biztosítja, hogy az irányelvet a személyes adatok védelmének szempontjából kedvezően és Európa-szerte egységesen értelmezzék. Ezen törekvések jegyében, például a rádiófrekvenciás azonosító chipekhez kapcsolódóan, a Munkacsoport meg fogja vizsgálni a személyes adatok definícióját, azt követően pedig az adatmegőrzés, valamint az egészségügyi adatok feldolgozásának kérdését tárgyalja. Az értelmezés mellett az irányelv végrehajtása is hangsúlyos szerepet kap a Munkacsoport programjában. A Munkacsoport szervezésében az Ügykezelési Munkafórum rendszeresen találkozik, és tevékenységével, gyakorlati esetek megoldásával elősegíti a különböző európai adatvédelmi jogszabályok harmonizációját. A Munkacsoportnak az irányelv végrehajtásáért felelős alcsoportja pedig egy átfogó vizsgálatba kezdett még 2005-ben: a tagállamok magán egészségbiztosító társaságainak adatkezelési gyakorlatát tekintette át. A vizsgálat eredményének értékelése a közeljövőben várható.

A Munkacsoport tevékenységének egy másik hangsúlyos területét az új technológiák jelentik (például rádiófrekvenciás azonosítás, e-kormányzat, biometrikus azonosítás, az e-egészségügy betegekre vonatkozó információi). A Munkacsoport fontosnak tartja, hogy az új technológiák adatvédelmi vonatkozásait a lehető leghamarabb feltárja és elemezze, még mielőtt a nagyobb jelentőségű alkalmazásokra sor kerülne. Ennek a gyakorlatnak az a célja, hogy az új technológiákat úgy vezessék be a gyakorlatba, hogy az megfeleljen az EU adatvédelmi irányelvének.

Harmadik fontos területként az Európai Unión kívüli országokba történő adattovábbítás említhető. A Munkacsoport számos munkadokumentumot készített azzal a céllal, hogy segítséget nyújtson a multinacionális cégek adattovábbítással kapcsolatos problémáinak megoldásához. A nemzetközi cégcsoportok tagjai közötti adattovábbítást rendező Kötelező Érvényű Vállalati Szabályok jelentik az egyik megoldást arra, ahogy a cégek bizonyíthatják adatkezelési gyakorlatuk megfelelőségét adatvédelmi szempontból. A Munkacsoport azonban egyéb olyan megoldások alkalmazásához is nyújt iránymutatást, mint például a Bizottság által jóváhagyott Általános Szerződési Feltételek.

Az elmúlt években a Munkacsoport tevékenységét erősen befolyásolták az európai és más kormányok azon intézkedései, amelyeket a nemzetközi terrorizmus elleni harc jegyében hoztak, mivel ezek az intézkedések általában konfliktusban állnak a személyes adatok védelméhez fűződő joggal. Ezt a konfliktust a mai napig sem sikerült feloldani, ezért az EU harmadik pillérével kapcsolatos adatvédelem egyre fontosabb szerepet játszik a tagállamok adatvédelmi hatóságainak munkájában. Különösen az Európai Unió és az Egyesült Államok közötti, a PNR adatoknak (utasnyilvántartási adatállomány) a légi szállítók általi feldolgozásáról és az Egyesült Államok Belbiztonsági Minisztériuma Vámügyi és Határvédelmi Irodájának történő továbbításáról szóló megállapodás (PNR megállapodás) jelentett az elmúlt években nagy kihívást a Munkacsoport számára. A Munkacsoport több véleményében is kifejezte kétségeit a megállapodás által lehetővé váló adatfeldolgozásban a személyes adatok védelmét illetően. 2006-ban több fejlemény is történt a PNR adatok továbbításával kapcsolatban. Többek között az Európai Parlament kérelmére az Európai Közösség Bírósága 2006. május 30-án megsemmisítette az Egyesült Államok Vámügyi és Határvédelmi Irodájának rendelkezésére bocsá-

tott, a légiutasok utasnyilvántartási adatállományában tárolt személyes adatok megfelelő védelméről szóló bizottsági határozatot és a PNR megállapodást. A bíróság indoklásában kifejtette: igaz ugyan, hogy a PNR adatok gyűjtését a légitársaságok a közösségi jog hatálya alá tartozó tevékenységük keretében végzik (jegyeladás), így ez az adatfeldolgozás az EU adatvédelmi irányelvének hatálya alá tartozik. Azonban a megfelelőségi határozat és a PNR megállapodás arra az adatfeldolgozásra vonatkozik, melynek keretében a légitársaságok továbbítják a PNR adatokat az USA-ba. Ez az adattovábbítás a közbiztonsággal és a büntetőjog területén végzett állami tevékenységekkel kapcsolatos adatfeldolgozásnak minősül, így nem tartozik az adatvédelmi irányelv hatálya alá. Ezért az Európai Közösségnek hiányzott a hatásköre a megfelelőségi határozat meghozatalára és a PNR megállapodás megkötésére.

Az első és a harmadik pillérre vonatkozó adatvédelem mesterséges szétválasztása joghézagot eredményez az uniós állampolgárok magánéletének védelmében. Ezért fontos lenne a belső piacra vonatkozó, valamint a rendőrségi és bűnüldözési együttműködésre vonatkozó adatvédelmi szabályozás következetessége. A harmadik pillérre vonatkozó adatvédelmi szabályozás alapját is a 95/46/EK adatvédelmi irányelvnek kellene képeznie. A Munkacsoport azonban bármilyen, az Uniót érintő adatvédelmi kérdéssel foglalkozhat és állásfoglalást bocsáthat ki.

A Munkacsoport 2006-ban is több véleményt és munkadokumentumot tett közzé, melyek rövid összefoglalását az alábbiakban ismertetem.

● Vélemény az uniós adatvédelmi szabályoknak a számvitel, belső számviteli ellenőrzés, könyvvizsgálati kérdések, korrupció, banki és pénzügyi bűnözés elleni küzdelem terén létrehozott belső visszaélés-jelentési rendszerekre történő alkalmazásáról (WP 117):

A belső visszaélés-jelentési rendszereket (whistleblowing schemes) a vállalatok azzal a céllal hozzák létre, hogy az alkalmazottak a vállalaton belül egy speciális csatornán keresztül jelenthessék a csalást és kötelességszegéseket a számvitel, belső számviteli ellenőrzés, könyvvizsgálati kérdések és jelentéstétel terén. A rendszerek meghirdetett célja a nemzetközi pénzügyi piacok pénzügyi biztonságának

garantálása, valamint a korrupció, a banki és pénzügyi bűnözés, valamint a bennfentes kereskedelem elleni küzdelem.

A belső visszaélés-jelentési rendszerek kialakítását az Amerikai Egyesült Államok Kongresszusa tette kötelezővé 2002-ben a Sarbanes-Oxley törvénnyel (SOX) a vállalati pénzügyi botrányok gyakorisága miatt. Több amerikai vállalat tevékenysége folytán a SOX mellett az uniós adatvédelmi szabályok hatálya alá is tartozik. Ezért a Munkacsoport véleményével iránymutatást nyújt számukra ahhoz, hogy miként működtethetők a belső visszaélés-jelentési rendszerek az adatvédelmi irányelvvel összhangban. A Munkacsoport megjegyzi, hogy a jelenlegi rendelkezések különleges védelmet biztosítanak a visszaélést jelentő alkalmazottak számára, de nem tesznek külön említést a megvádolt személy védelméről, annak ellenére, hogy az adatvédelmi irányelv és a nemzeti jog adatvédelmi szabályai által biztosított jogokhoz a megvádolt személynek is joga van. Komoly a veszélye annak, hogy a megvádolt személyt már azelőtt megbélyegzik, mielőtt tudomást szerezne az ellene felhozott vádról, vagy az állítások indokoltságát megállapították volna. Az adatvédelmi szabályok megfelelő alkalmazása hozzájárul az említett veszélyek csökkentéséhez.

Az adatvédelmi szabályok visszaélés-jelentési rendszerekre történő alkalmazásakor a Munkacsoport először a rendszerek törvényességének kérdését vizsgálja. Mivel a SOX az USA törvénye, rendelkezései nem tekinthetők törvényes alapnak az adatkezeléshez. Az adatkezelés törvényességét a vállalatok következő jogszerű érdekei biztosítják: a csalás és kötelességszegések megelőzése a számvitel, belső számviteli ellenőrzés, könyvvizsgálati kérdések és jelentéstétel terén, valamint a nemzetközi pézügyi piacok pénzügyi biztonságának garantálása, a korrupció, a banki és pénzügyi bűnözés, valamint a bennfentes kereskedelem elleni küzdelem. Mindazonáltal a Munkacsoport hangsúlyozza, hogy egyensúlyt kell teremteni a vállalatok jogszerű érdeke és az adatfeldolgozással érintettek alapvető jogai között. Figyelembe kell venni a jelenthető feltételezett bűncselekmények súlyosságát, valamint a következményeket az érintettekre nézve. Biztosítani kell azt is, hogy az érintettek lényeges jogos érdekből bármikor tiltakozhassanak a rájuk vonatkozó adatok kezelése ellen.

Az adatminőség és az arányosság elveinek alkalmazásakor a Munkacsoport tárgyalta a nevesített és névtelen jelentések kérdését, a

gyűjtött és feldolgozott adatok arányosságának és pontosságának problémáját és az adatmegőrzési időszakokat. A Munkacsoport úgy gondolja, hogy a jelentések névtelensége számos okból nem jó megoldás a visszaélést jelentő személy vagy a szervezet számára, például a névtelenség nem akadályozza meg, hogy mások kitalálják, ki emelt panaszt, vagy kialakulhat a rosszindulatú névtelen jelentések gyakorlata. Továbbá a névtelenség ellen szól az az alapelv is, hogy személyes adatok csak tisztességesen gyűjthetők. Csak kivételes esetben fogadható el a névtelenség. A rendszereket úgy kell kialakítani, hogy ne ösztönözzék a névtelen jelentéseket, ezért az első kapcsolatfelvételkor tájékoztatni kell a jelentést tevő személyt, hogy személyazonosságát a folyamat valamennyi szakaszában bizalmasan kezelik, azt nem fedik fel harmadik félnek, a megvádolt személynek, sem pedig feletteseinek. Azonban fel kell hívni a figyelmet arra, hogy a személyazonosság felfedésére sor kerülhet a vizsgálat eredményeként megindított további vizsgálatokban vagy későbbi bírósági eljárásokban.

Az adatok arányosságával és pontosságával kapcsolatban a Munkacsoport kiemelte, hogy csak olyan adatok dolgozhatók fel a rendszerben, amelyek a vádak igazolásához feltétlenül és objektív módon szükségesek. A rendszer szempontjából közömbös adatok közlése esetén azokat csak abban az esetben lehet továbbítani a vállalat megfelelő tisztviselőjéhez, ha az érintett személy alapvető érdekei vagy az alkalmazottak erkölcsi integritása forog kockán, vagy ha a bűnüldözési vagy államháztartási szervek számára jogi kötelezettség alapján kell továbbítani az információt.

Az adatmegőrzéssel kapcsolatban a Munkacsoport megjegyzi, hogy a személyes adatokat a vizsgálat befejezését követő két hónapon belül törölni kell. Ha eljárás indul a megvádolt személy vagy a hamis vagy becsületsértő kijelentést tevő, visszaélést jelentő személlyel szemben, akkor az adatokat az eljárása lezárásáig vagy a fellebbezésre rendelkezésre álló időszak végéig kell megőrizni. Haladéktalanul törölni kell azonban a megalapozatlannak talált jelentéshez kapcsolódó személyes adatokat.

A bejelentett személyek jogaival kapcsolatban a Munkacsoport kiemelte, hogy a rendszerért felelős személy köteles a megvádolt személyt az őt érintő adatok rögzítését követően a lehető leggyorsabban tájékoztatni, különösen az alábbiakról: mivel vádolták meg, ki felelős

a rendszerért, kik kaphatják meg a jelentést, hogyan gyakorolhatja hozzáférési és helyesbítési jogát. Azonban az értesítés elhalasztható, amíg fennáll annak a kockázata, hogy a megvádolt személy megsemmisítené vagy módosítaná a bizonyítékokat. Továbbá biztosítani kell az érintettek hozzáférési, helyesbítési és törlési jogát, azzal a korlátozással, hogy a megvádolt személy nem tudhatja meg a jelentést tevő személyazonosságát, csak akkor, ha az rosszhiszemű, hamis kijelentést tett.

A visszaélés-jelentési rendszerek irányítása tekintetében a Munkacsoport úgy véli, hogy a rendszer belső kezelését kell előnyben részesíteni, de a vállaltok igénybe vehetnek külső szolgáltatót is. Belső kezelés esetén különálló szervezetet kell létrehozni a vállalaton belül a jelentések kezelésére és a vizsgálatok vezetésére. A kijelölt szervezetnek korlátozott számú, speciálisan képzett és erre kijelölt személyzetből kell állnia, akiket különleges titoktartási kötelezettségek szerződésben kötelezneknek. Külső szolgáltató igénybevétele esetén is a vállalat marad a felelős az adatfeldolgozásért. A külső szolgáltatóra is szigorú titoktartási kötelezettségnek kell vonatkoznia, és kötelezettségeik teljesítését a vállalatnak ellenőriznie kell. Továbbá a Munkacsoport szerint a vállalatcsoportoknak néhány kivételtől eltekintve helyi szinten, az Unión belül kell kezelniük a jelentéseket. Ha az adattovábbítás harmadik országba történik, és az nem biztosít adatvédelmi szempontból megfelelő szintű védelmet, az adatokat csak akkor lehet továbbítani, ha a címzett tagja a Safe Harbor rendszernek, vagy vele adattovábbítási szerződést kötöttek, vagy ha kötelező érvényű vállalati szabályok vannak érvényben a címzettnél.

A Munkacsoport végül hangsúlyozta a világos és teljes körű tájékoztatási kötelezettséget a rendszerrel kapcsolatban. Kiemelte az adatfeldolgozás biztonságának jelentőségét, valamint a nemzeti adatvédelmi hatóságok előzetes ellenőrzésének vagy az általuk előírt bejelentési kötelezettségnek való megfelelés kötelezettségét is.

● Vélemény az e-mailek átvilágítására vonatkozó szolgáltatásokról (WP 118):

Az internetszolgáltatók és e-mail szolgáltatók többsége szűrőket használ a spamek és a vírusok kiküszöbölésére, valamint ellenőrzi az üzeneteket, például az előre meghatározott tartalom észlelése, keresés

és helyesírás-ellenőrzés, sürgős üzenetek megjelölése, a bejövő e-mailek mobiltelefonos szöveges üzenetté alakítása érdekében. A Munkacsoport úgy véli, hogy a szűrők használata nem mindig felel meg a hatályos adatvédelmi jogszabályoknak.

A Munkacsoport úgy találta, hogy az e-mailek vírusok kiszűrése céljából történő ellenőrzése nem jogsértő. Az ellenőrzés azért jogszerű, mert az EU elektronikus hírközlési adatvédelmi irányelve (a továbbiakban ePrivacy irányelv) előírja, hogy az e-mail szolgáltatónak megfelelő műszaki és szervezeti intézkedéseket kell tennie szolgáltatásai biztonságának érdekében. Továbbá a szűrőrendszerek létrehozásával az e-mail szolgáltatók biztosítják az ügyfelekkel kötött szolgáltatói szerződés teljesítését. Azonban az e-mail szolgáltatóknak be kell tartaniuk a következőket: (1) az e-mailek és csatolt mellékletek tartalmát titokban kell tartani, és csak a címzettek előtt szabad feltárni, (2) amennyiben vírust találnak, a telepített szoftvernek biztosítania kell a titkosságot, (3) vírusellenőrzéskor az e-mailek tartalmát nem ellenőrizhetik más célból, (4) az átvilágításról tájékoztatást kell nyújtani.

A spamek akadályozhatják az internetes forgalmat, és súlyosan károsíthatják az e-mail szolgáltatások általános megbízhatóságát és hatékonyságát. Ezért a spamek szűrése szükséges az érintettel kötött szerződés teljesítéséhez. Ugyanakkor aggodalomra ad okot, hogy a szűrés néha összekeveri a spameket a tényleges e-mailekkel, melyeket meg szeretne kapni a fogadó. A tévesen spamnek ítélt e-mailek kiszűrése sérti a szólásszabadságot, és a magáncélú közlésekbe történő beavatkozásnak minősül. Ezért a Munkacsoport szorgalmazza, hogy az e-mailek fogadói rendelkezhessenek a nekik címzett üzenetekkel, például ellenőrizhessék, hogy mely e-maileket minősítették spamnek. Továbbá a vélemény hangsúlyozza, hogy az e-mail szolgáltatóknak világosan és egyértelműen tájékoztatniuk kell az előfizetőket a spamekkel kapcsolatos politikájukról, és biztosítaniuk kell a megszűrt e-mailek titkosságát, valamint azt, hogy a kiszűrt e-mailek ne legyenek más célra felhasználhatók.

A Munkacsoport véleménye szerint az e-mailek átvilágítása előre meghatározott tartalom észlelése érdekében még az illegálisnak ítélt anyag esetén sem tekinthető olyan intézkedésnek, amely szükséges az e-mail szolgáltatások biztonságához. Az e-mail tartalma nem fenyegeti az e-mail szolgáltatót károsodással és a kommunikáció leállásával,

így az ellenőrzést nem legitimálja a szolgáltatás biztonságának megőrzésére irányuló törekvés. A Munkacsoport aggályosnak találja, hogy a szűréssel az e-mail szolgáltatók cenzúrázzák a magánjellegű e-mail közléseket, ami a szólás- és véleményszabadság, illetve a tájékozódáshoz való jog alapvető kérdéseit veti fel. Az e-mail szolgáltatók tehát az érintett felhasználók hozzájárulása nélkül nem szűrhetik, tárolhatják és nem tarthatják vissza a közléseket és az azokra vonatkozó forgalmi adatokat az előre meghatározott tartalom észlelése céljából. A Munkacsoport szerint megfelelő az e-mail szolgáltatók gyakorlata, ha a vírusok és a spamek szűréséről a szolgáltatás szerződéses feltételeinek részeként tájékoztatják az előfizetőket.

Az e-mailekhez kapcsolódó egyéb szolgáltatások tekintetében a Munkacsoport az e-mailek megnyitását nyomonkövető *„Elolvasták"* szolgáltatást vizsgálta meg. A Munkacsoport erősen ellenzi ezt az adatkezelést, mert a címzettek viselkedésével kapcsolatos személyes adatokat az érintett címzett egyértelmű hozzájárulása nélkül rögzítik és továbbítják. Annak megállapításához, hogy az e-mail címzettje elolvasta-e az e-mailt, ha igen, mikor, és továbbította-e harmadik félnek, a címzett hozzájárulására van szükség.

● Vélemény a nyilvánosan elérhető elektronikus hírközlési szolgáltatások nyújtása, illetve a nyilvános hírközlő hálózatok szolgáltatása keretében előállított vagy feldolgozott adatok megőrzéséről (WP 119):

Véleményében a Munkacsoport fenntartásait fejezte ki a 2006/24/EK irányelvvel kapcsolatban. Megállapította, hogy a hírközlési adatok súlyos bűncselekmények elleni harc céljából történő megőrzésének messzemenő következményei lesznek minden európai polgár magánéletére vonatkozóan. A Munkacsoport az irányelv hírközlési adatok megőrzésére vonatkozó rendelkezéseit példa nélkül álló, történelmi léptékű döntésnek nevezi. Ezért elengedhetetlennek tartja olyan intézkedések alkalmazását, amelyek korlátozzák az irányelv magánéletre való hatását.

Annak érdekében, hogy a tagállamok az adatmegőrzési irányelvet egységes módon ültessék át nemzeti jogaikba, és az átültetés megfeleljen az adatvédelmi követelményeknek, a Munkacsoport számos biztosíték bevezetését javasolta véleményében. Elsőként arra hívta fel a figyelmet, hogy az adatokat kizárólag meghatározott célból szabad

megőrizni, és minden további feldolgozást ki kell zárni. A *„súlyos bűncselekmény"* kifejezést ezért pontosabban kell meghatározni. Továbbá fontos, hogy az adatok kizárólag egyedileg meghatározott bűnüldöző szervek számára legyenek hozzáférhetőek. A kijelölt szervek jegyzékét a nyilvánosság számára, az adatlekérések nyilvántartását pedig a felügyelő hatóságok részére hozzáférhetővé kell tenni. Az adatmegőrzés nem vezethet nagymértékű adatbányászathoz a bűnüldöző hatóságok által nem gyanúsított személyek utazási és kommunikációs szokásaira vonatkozóan. Az adatokhoz való hozzáférést az igazságügyi hatóságnak eseti alapon kell engedélyeznie, és az engedélyben pontosan részletezni kell az esethez szükséges, engedélyezett adatokat. Fontos a közrend célját szolgáló adattárolási rendszerek elkülönítése az üzleti célú rendszerektől. Végül meg kell határozni a műszaki és szervezeti biztonságra vonatkozó minimális követelményeket.

A Munkacsoport felszólítja a tagállamokat, hogy hangolják össze az adatmegőrzési irányelv nemzeti jogba történő átültetését annak érdekében, hogy azt az Európai Unióban egységesen alkalmazzák, és biztosítsák az adatvédelmi követelmények betartását.

● Vélemény az utasokra vonatkozó adatok légi és tengeri utasszállítók általi, a fertőző betegségek ellenőrzése céljából történő gyűjtéséről szóló új amerikai jogszabálytervezetről (WP 121):

Az amerikai javaslattervezet személyes adatok gyűjtésére kötelezne minden olyan nemzetközi légi és tengeri utasszállító társaságot, amelyik az USA-ba szállít utasokat. Az adatkezelés célja azon utasok fellelhetőségének biztosítása lenne, akik gyaníthatóan fertőző betegségnek voltak kitéve, így biztosítva a fertőző betegség terjedésének megelőzését. Az utasszállító társaságoknak a következő adatokat kellene összegyűjteniük, megőrizniük 60 napig és kérelem esetén eljuttatniuk az USA Betegségmegelőzési és Járványvédelmi Központja (CDC) igazgatójának: teljes név; betegség, vagy baleset esetén értesítendő személyek elérhetősége; e-mail cím; állandó lakcím; útlevél vagy utazási okmány száma, a kibocsátó ország vagy szervezet neve; utastársak vagy csoportos utazás esetén a csoport neve; a repülési útra vagy az útba ejtett kikötőkre vonatkozó információk; a visszarepülésre vonatkozó adatok (az indulás időpontja, a repülőgép száma és a járat száma), vagy a visszatérés során útba ejtett kikötőkre vonatkozó

adatok; valamint telefonszám. A CDC igazgatója további, előre meg nem határozott adatokat kérhetne a fertőző betegségek bejutásának vagy terjedésének megakadályozása céljából. A Munkacsoport véleménye szerint az amerikai törvénytervezet jelenlegi formájában ellentétes az EU adatvédelmi irányelvének rendelkezéseivel és a WHO Nemzetközi Egészségügyi Szabályzatával.

Az összes javasolt adat feldolgozása nem szükséges a tervezet céljainak eléréséhez. A javaslat nem számol azokkal a személyes adatokkal, amelyekhez az amerikai hatóságok jelenleg is hozzáférhetnek (például PNR adatok), és azt sem veszi figyelembe, hogy léteznek az utasinformációk begyűjtésének más, nemzetközileg elismert formái is, mint például az utasok közegészségügyi célból szükséges fellelhetőségét biztosító kártyák (public health passenger locator cards).

További probléma, hogy az adatgyűjtés anélkül történne, hogy egy konkrét közegészségügyi veszély fennállna, vagy annak bekövetkezése fenyegetne. Az EU adatvédelmi irányelvében felsorolt jogalapok nem alkalmazhatók erre az adatgyűjtésre, mivel az nem szükséges olyan jogi kötelezettség teljesítéséhez, melyet egy közösségi vagy tagállami jogszabály ír elő az adatkezelő (utasszállító) számára, nem szükségszerű az érintett személy létfontosságú érdekei védelme céljából (olyan esetekre is vonatkozik az adatgyűjtés, amikor nem áll fenn jelentős közegészségügyi veszély), és nem szükséges az EU egyik tagállamának közérdekből végrehajtott feladatához sem (egyedül az USA érdeke). Az adatok feldolgozására jogalap lehet, ha az az adatkezelő jogos érdekéből történt. Viszont szükséges, hogy a jogos érdeknél ne legyenek magasabb rendűek az érintett személy érdekei az alapvető jogok és szabadságok tekintetében. Az érintett személyeknek azonban meg kell adni a lehetőséget, hogy bármikor tiltakozhassanak a rájuk vonatkozó adatok feldolgozása ellen.

Az amerikai javaslat szerint a személyes adatokat a betegség lappangási idejére és fertőzőképességére tekintet nélkül egységesen 60 napig kellene megőrizni. Mivel a javaslat nem nevezi meg a fertőző betegségeket, ezért nem lehet megállapítani, hogy a megőrzésre előírt időtartam megfelelő-e, ha a betegség jellegzetességeit figyelembe vesszük. További probléma, hogy a CDC előre meg nem határozott személyes adatokat kérhet. Ez ellentétes a Nemzetközi Egészségügyi Szabályzat azon rendelkezésével, mely meghatározza az adatoknak azt a körét, amelyeket az illetékes egészségügyi szervek gyűjthetnek.

Végül a Munkacsoport hangsúlyozta, hogy nemcsak az adatgyűjtésnek, hanem az adatok Európai Unióból az USA-ba történő továbbításának is hiányzik a jogalapja, mivel az USA-ra nem vonatkozik az a megállapítás, hogy megfelelő szinten biztosítja a személyes adatok védelmét. Továbbá az adatok szóban forgó körére nem vonatkozik az a két megállapodás, melyek alapján jelenleg adatokat lehet továbbítani az EU-ból az USA-ba (a Safe Harbour és a PNR megállapodások). Az adattovábbítás így csak az érintett személy beleegyezésével történhet, amiről viszont az amerikai javaslat nem rendelkezik.

● Vélemények az Európai Bíróság ítéletéről az utasnyilvántartások Egyesült Államokba történő átadásával kapcsolatban és egy mielőbbi új megállapodás szükségességéről (WP 122, WP 124):

2006-ban a Munkacsoport két véleményben is foglalkozott az utasokkal kapcsolatos adatok (PNR adatok) továbbításának kérdésével. Mindkét vélemény a PNR adatok továbbításáról szóló megállapodás megsemmisítésével keletkezett joghézag problémáját elemezte.

Az Európai Bíróság 2006. május 30-i ítéletében kötelezte a közösségi intézményeket, hogy legkésőbb 2006. szeptember 30-ig mondják fel az Egyesült Államokkal kötött, PNR adatok továbbításáról szóló megállapodást. A Munkacsoport az ítélettel kapcsolatos véleményében felhívja a figyelmet arra, hogy a joghézag elkerülése végett és az utasok jogainak védelme érdekében alapvető fontosságú egy új EU-szintű megállapodás időben történő megkötése az USA-val. A Munkacsoport szerint a leendő megállapodásnak meg kell őriznie az USA által már eddig vállalt adatvédelmi szintet, integrálnia kell a Munkacsoport kritikai észrevételeit (például az adatok számának csökkentéséről), biztosítania kell, hogy a légitársaságok maguk válogathassák a továbbítandó adatokat, és ne az amerikai hatóságok tegyék ezt, korlátoznia kell a továbbított PNR adatok további felhasználását. A megállapodás csak 2007 novemberéig lehet érvényben.

A Munkacsoport következő PNR adatokkal kapcsolatos véleményében kifejezte rendkívüli aggodalmát amiatt, hogy az USA és az EU még mindig nem kötött új megállapodást, annak ellenére, hogy 2006. október 1-jén lejár a PNR adatok továbbítására vonatkozó megállapodás. Felhívta a Tanácsot, a Bizottságot és az EU tagállamait annak garantálására, hogy az utasok magánéletét a megállapodás hiányában is

megfelelően tartsák tiszteletben. A Munkacsoport szerint abban az esetben, ha nem jönne létre megállapodás, a tagállamok hatóságainak meg kell előzniük, hogy a PNR nyilvántartásokban található személyes adatokat az USA hatóságai felé továbbítsák vagy a Munkacsoport által megfelelőnek ítélt 19 adattételen felül egyéb adatokat továbbítsanak.

Az EU és az Amerikai Egyesült Államok 2006. október 6-án ideiglenes megállapodást kötött a PNR adatok továbbításával kapcsolatosan. Ennek köszönhetően folytatódhat a PNR adatok továbbítása az USA-ba az USA korábbi kötelezettségvállalásainak betartása mellett.

● Vélemény a tartással kapcsolatos ügyekben a joghatóságról, az alkalmazandó jogról, a határozatok elismeréséről és végrehajtásáról, valamint az e területen folytatott együttműködésről szóló tanácsi rendeletre irányuló javaslatról (WP 123):

Az Európai Bizottság e véleményben tárgyalt javaslatának az a célja, hogy az Európai Unión belül felszámolja a tartási követelések behajtásának akadályait. A javaslat lehetővé tenné, hogy a tagállamok központi hatóságai összegyűjtsék a tartásra jogosult és kötelezett helyzetével kapcsolatos, számos adatkezelő által különböző célokra feldolgozott információkat (például a munkáltatók, adó- vagy társadalombiztosítási hatóságok által), valamint ezen információk tagállamok közötti cseréjét. A központi hatóságok által összegyűjtött személyes adatokat egybegyűjtenék, és közölnék a tartási követeléssel foglalkozó bírósággal, majd a bíróság a tartási kötelezettségekről hozott határozatok végrehajtásának biztosítása céljából feldolgozza az adatokat.

A Munkacsoport elégedetten jegyezte meg, hogy a javaslat számos olyan elemet tartalmaz, amelyek célja annak biztosítása, hogy az adatfeldolgozási műveletek az adatvédelmi irányelvben foglalt elveknek és szabályoknak megfeleljenek. Így például a javaslat szerint az, hogy milyen adat közölhető, attól függ, hogy a tartási kötelezettségre vonatkozó eljárás mely szakaszában jár. A kötelezett tartózkodási helyének megállapításához szükséges személyes adatok némelyikét az eljárás elején kérhetik és továbbíthatják bármely tartásdíjat követelő személy kérésére. Azonban a kötelezett tartásdíjfizető képességének felméréséhez szükséges adatokat (például bankszámlák, fizetések) csak akkor lehet kiadni, ha a tartásdíj-fizetési kötelezettséget a bíró-

ság megállapította. További adatvédelmi garancia a rendszerbe beépített bírói szűrő: a bíróság dönt a tartási kérelem megalapozottságáról és arról, hogy a központi hatóságtól igényelt adatok valóban szükségesek-e. A kötelezettek személyes adatainak védelmét szolgálja az is, hogy tilos egy egységes nyilvántartás kialakítása az eredetileg különálló nyilvántartásokban szereplő különféle kategóriájú információkból. További garanciák, hogy az információkat csak a megkeresett hatóság továbbíthatja a megkereső hatóság számára, és a megkereső hatóság ezután csak a tartási követeléssel foglalkozó bíróság vagy hatóság számára továbbíthatja az információkat. Az információt nem lehet továbbítani a jogosult vagy harmadik fél számára, és amint a megkeresett vagy a megkereső hatóság közölte az információkat, azokat kötelesek törölni. A javaslat azt is előírja, hogy az információkat csak a tartási követeléssel foglalkozó bíróság tárolhatja és csak addig, amíg az szükséges a tartási követelés behajtásának megkönnyítéséhez, de legfeljebb egy évig.

A Munkacsoport azonban a pozitívumok kiemelése mellett számos olyan javaslatot is tett, amelyek azért szükségesek, hogy az adatvédelmi irányelv rendelkezései teljes mértékben megvalósuljanak. Így például az adatok biztonságát megfelelő technikai és szervezési intézkedésekkel kellene garantálni. A Munkacsoport arra is felhívta a figyelmet, hogy a javaslat túl széleskörűen határozta meg az információkhoz való hozzáférés célját. A hozzáférés célját korlátozni kellene a kötelezett tartózkodási helyének meghatározására és vagyonának megállapítására. A kötelezett munkáltatójának vagy bankszámlájának beazonosítása csak akkor releváns, ha a fizetés vagy a bankszámlán elhelyezett összeg a kötelezett vagyonának nagyon jelentős elemét képezi. A Munkacsoport azt is rendkívül fontosnak tartja, hogy a bíróságokon belül meghatározzák azt az illetékes testületet, amely elrendeli a magánéletet érintő intézkedéseket.

Az adatok tárolásával kapcsolatban is számos észrevételt tett a Munkacsoport. A megkereső központi hatóság köteles a bíróságnak történő megküldés után azonnal megsemmisíteni az adatokat. A bíróságok csak addig dolgozhatják föl az adatokat, amíg az szükséges az adott tartási követelés behajtásának megkönnyítéséhez. Végül, a kötelezettet azonnal értesíteni kell adatai közléséről, és tájékoztatni a feldolgozás céljáról.

● Munkadokumentum az eSegélyhívó-kezdeményezés adatvédelmi és a magánélet tiszteletben tartását érintő vonatkozásairól (WP 125):

A munkadokumentum egy páneurópai, járműbe építhető segélyhívó („*eSegélyhívó*") szolgálat tervezett bevezetésének adatvédelmi és magánéleti vonatkozásait elemzi. A Munkacsoport elismerte, hogy az eSegélyhívó szolgálat bevezetése számos társadalmi-gazdasági előnnyel járna, ugyanakkor kiemelte, hogy a kezdeményezés adatvédelmi és magánéleti hatásait is hangsúlyozni és kezelni kell.

Az eSegélyhívó működése

A járműbe épített eSegélyhívó egy olyan segélyhívó, amelyet vagy manuálisan a járműben tartózkodók, vagy automatikusan a járműbe épített érzékelők hoznak működésbe baleset esetén. A segélyhívást a 112-es hívószámú, megfelelő közbiztonsági válaszponthoz (KBVP) továbbítja a rendszer. A segélyhívás a 112-es számra történő telefonhívás hanganyagából és a minimális mennyiségű adatból (MMA) tevődik össze. A mobiltelefon-hálózat üzemeltetője azonosítja a hívó vonalat, és megállapítja a hívás lehető legpontosabb helyét. Ezután továbbítja a 112-es híváshoz tartozó hangot, a hívásazonosítót, a hívó lehető legpontosabban meghatározott helyzetét és a híváshoz tartozó minimális mennyiségű adatot a megfelelő KBVP-hez. Fontos megjegyezni, hogy a jelenlegi javaslat szerint kívülálló harmadik személy a járműben elhelyezett rendszert nem fogja folyamatosan követni, mivel a rendszer nem lesz állandó jelleggel a mobilkommunikációs hálózathoz kapcsolva, csak akkor, ha baleset esetén aktiválódik vagy manuálisan aktiválják a jármű utasai.

A minimális mennyiségű adat a következőkből áll: (1) a baleset időpontja, (2) a baleset pontos helye és az odavezető útvonal, (3) jármű azonosítás, (4) a segélyhívás minősítése, amely megadja a baleset súlyossági fokát, (5) egy lehetséges szolgáltatóra vonatkozó információ.

Kötelező vagy önkéntes eSegélyhívó

Ha az eSegélyhívó önkéntes jelleggel kerül bevezetésre, ugyan minden jármű rendelkezni fog az eSegélyhívó rendszerrel, de a jármű utasai döntenek arról, hogy aktiválják-e azt. Ezért biztosítani kell, hogy a rendszer bármiféle technikai vagy anyagi nehézség nélkül ak-

tiválható és kikapcsolható legyen. Az EU adatvédelmi irányelve szerint az adatkezelés jogszerűségéhez szükséges az adatalany egyértelmű és önkéntes beleegyezése személyes adatainak kezeléséhez. A Munkacsoport hangsúlyozta, hogy a beleegyezés nem önkéntes, ha az adatalanynak el kell fogadnia olyan szerződési feltételeket, amelyek nem képezhetik megállapodás tárgyát (ahogyan az a jármű-adásvételi szerződéseknél szokásos). Továbbá a Munkacsoport jogellenesnek tartja azt, ha a biztosító társaságok vagy autóbérléssel foglalkozó cégek nyomást gyakorolnak annak érdekében, hogy az eSegélyhívó rendszert folyamatosan aktiválva tartsák ügyfeleik. Az is jogellenes, ha a munkavállalókat közvetve vagy közvetlenül kényszerítik az eSegélyhívó rendszer használatára a céges autókban. A Munkacsoport felhívta a figyelmet arra is, hogy ugyan az adatfeldolgozás sok esetben az érintettek létfontosságú érdekében történik, az is előfordulhat, hogy az eSegélyhívó automatikusan aktiválódik egy baleset után, annak ellenére, hogy arra szükség volna..

Ha az eSegélyhívó rendszer alkalmazása kötelező lesz, azt minden járműbe beszerelik, és aktiválása kötelező lesz. Ezt az esetet azonban egy uniós rendeletnek kell majd szabályoznia, melyben az arányosság elvét kiemelten kell kezelni. Olyan biztosítékokat kell kialakítani, amelyek megakadályozzák, hogy a rendszer által megfigyelhessék az embereket.

A Munkacsoport az önkéntes bevezetést tartja megfelelőbbnek. Kötelező alkalmazás esetén megfelelő adatvédelmi biztosítékokat kell bevezetni.

Kétszintű szolgáltatás

A kezdeményezés lehetővé tenné, hogy a minimális mennyiségű adaton felül további adatokat is továbbítson a rendszer, mint például biztosítótársaságok, ügyvédek, autóklubok által tárolt adatokat. Különböző szolgáltatók a balesettel vagy az utasokkal kapcsolatos adatokat kaphatnának annak érdekében, hogy például autóklub-szolgáltatást vagy nyelvi segítséget nyújtsanak, ha a járműtulajdonos és a szolgáltató erre nézve szerződést kötött. A Munkacsoport nem ellenzi az eSegélyhívó szolgáltatás második szintjét, de felhívta a figyelmet arra, hogy ez a megoldás adatvédelmi szempontból összetettebb, ezért alapos értékelést igényel. Különösen az adatbiztonságra vonatkozó

rendelkezéseket kell szigorúan betartani, tekintettel arra, hogy különleges adatokat is feldolgoznak ebben a rendszerben. A külső szolgáltatóknak különösen a következőkre kell figyelniük: (1) a járműtulajdonos/használó és a szolgáltató közötti szerződésben egyértelműen le kell fektetni az adatkezelés célját és az adatok pontos körét; továbbá azt is rögzíteni kell, hogy a külső szolgáltató az adatkezelő, ezáltal mind az adatvédelmi irányelv, mind pedig a nemzeti jogszabályok rendelkezéseit be kell tartania, (2) csak a szükséges és releváns adatokat lehet továbbítani, tehát biztosítani kell, hogy a külső szolgáltató csak azokat az adatokat kapja meg, amelyek a szerződés céljának megvalósításához szükségesek, (3) ha a továbbítandó adatok különleges adatokat is tartalmaznak, a járműtulajdonos beleegyezése is szükséges az adattovábbításhoz.

Egyéb kérdések

Adatvédelmi szempontból problémát jelenthetnek azok az adatbázisok, melyeket a rendszerrel való visszaélések megelőzésére hoznának létre azáltal, hogy az eSegélyhívó SIM-kártyájához kötnének járműtulajdonost. A Munkacsoport egyik fő problémája a harmadik személyek esetleges hozzáférése az adatbázishoz, ezért hangsúlyozta, hogy az adatok másodlagos felhasználása (például a közlekedéssel kapcsolatos végrehajtási eljárásokban) az adatvédelmi irányelvvel ellentétes lenne.

Az arányosság elvének érvényesülésével kapcsolatban a Munkacsoport két megjegyzést tett. Véleményük szerint a járműazonosító számot nem kellene a minimális mennyiségű adatok közé felvenni, mivel az nem szükséges a célok megvalósításához. Továbbá az eSegélyhívó rendszer egészének szükségessége megkérdőjelezhető, mivel számos tagállamban már jól működő segélyhívó rendszerek léteznek.

Az adatok megőrzésének megfelelő időtartamát meg kell határozni az eSegélyhívó szolgáltatás minden egyes láncszemére tekintettel, és a nemzeti hatóságoknak ezt ellenőrizniük kell.

● Az elektronikus hírközlési adatvédelmi irányelvvel kapcsolatos vélemény (WP 126):

Az Európai Bizottság 2006-ban felülvizsgálta az elektronikus hírközlő hálózatokra és az elektronikus hírközlési szolgáltatásokra vo-

natkozó európai uniós szabályokat. A 29-es Munkacsoport ebben a véleményben a felülvizsgálat eredményéről készült bizottsági jelentéshez tesz észrevételeket, különösen az elektronikus hírközlési adatvédelmi irányelv (a továbbiakban ePrivacy irányelv) tekintetében.

A Munkacsoport általános javaslatként fogalmazza meg a biztonsági intézkedések fejlesztését, és felhívja a figyelmet arra, hogy a biztonsági infrastruktúra fejlesztésekor komoly hangsúlyt kell helyezni a felhasználók védelmére és az elektronikus kommunikáció iránti bizalom kialakítására. A vélemény szerint olyan on-line alkalmazásokkal kapcsolatos kérdésekkel is foglalkozni kellene, mint például az üzemeltetők felelőssége és jogi helyzete, és az adatkezelőkkel kapcsolatos kérdések tisztázása. A Munkacsoport hangsúlyozta: nem támogatja azt, hogy a biztonsági intézkedések fejlesztése olyan eszközökkel valósuljon meg, melyek nagyobb fokú megfigyelést vagy több internetes oldal tartalmának zárolását eredményeznék.

A Munkacsoport véleménye szerint az ePrivacy irányelv hatályának nemcsak a nyilvános hírközlő hálózatokra, hanem a magánhálózatokra is ki kellene terjednie, mivel azok egyre nagyobb szerepet töltenek be mindennapi életünkben, így egyre nagyobb kockázatot hordoznak, különösen annak következtében, hogy egyre specifikusabbak (például a munkavállalók viselkedésének ellenőrzése a forgalmi adatok segítségével).

A Bizottság megvizsgálta az ePrivacy irányelv végrehajtási mechanizmusait, valamint a végrehajtásért felelős hatóságok részére biztosított hatásköröket, és azok kiigazítását javasolta. Az ePrivacy irányelv végrehajtásával kapcsolatban a Munkacsoport megjegyezte, hogy néhány tagállamban az adatvédelmi hatóságok korlátozott vizsgálati jogkörrel rendelkeznek, melynek alapján nem férhetnek hozzá olyan adatokhoz, melyek szükségesek lennének az irányelv megsértésének bizonyításához. Számos tagállamban a végrehajtáshoz jelenleg biztosított hatáskörök nem teszik lehetővé a gyors beavatkozást. Egy további probléma a végrehajtás szempontjából, hogy sok spammer a tagállamokon kívül működik. A Munkacsoport szerint ezeket a problémákat kezelni kellene.

A Bizottság az ePrivacy irányelv biztonsági rendelkezéseinek kiegészítését és szigorítását javasolja. A Munkacsoport ezzel egyetért, azonban javasolja, hogy a biztonság általános fogalmán belül olyan

specifikus problémákat is célozzon meg a Bizottság, mint például a hitelesség megállapítására irányuló eljárások és a személyazonossággal való visszaélés. A Munkacsoport azonban hangsúlyozza, hogy a hitelesség megállapítására szolgáló eljárások tárgyalásakor nem szabad figyelmen kívül hagyni, hogy a nyilvánosan elérhető elektronikus hírközlési szolgáltatásokat a személyazonosság felfedése nélkül is tudniuk kell az embereknek használni.

A bizottsági munkadokumentum szerint a jelenlegi szabályozás túl nagy mozgásteret biztosít a szolgáltatóknak saját biztonsági intézkedéseik értékelése terén. A Bizottság a szolgáltatókat terhelő új kötelezettségek meghatározását javasolja a biztonsági intézkedések terén. A Munkacsoport úgy véli, hogy a biztonsági intézkedéseket és az irányelv biztonsággal kapcsolatos fogalmait nem az adatvédelmi hatóságoknak kellene meghatározni és tisztázni, hanem szektorspecifikus biztonsági szakértőknek. Továbbá el kell kerülni a túlzott mértékű szabályalkotást is.

A Munkacsoport egyetért a Bizottság azon javaslatával, hogy a rendszer biztonságának sérelméről a hálózatüzemeltetőknek és internetszolgáltatóknak értesíteni kell a sérelmet szenvedő ügyfeleket, a biztonság súlyos sérelme esetén pedig minden ügyfelet. Azonban felhívja a figyelmet, hogy a közelmúltban történt biztonsági rendszerek feltörései nem az internetszolgáltatókat érintették, ezért meg kellene fontolni, hogy a bankokat, adatbrókereket és egyéb on-line szolgáltatókat is terhelje értesítési kötelezettség.

● Vélemény a fuvarozóknak az utasokkal kapcsolatos adatok közlésére vonatkozó kötelezettségéről szóló tanácsi irányelvről (WP 127):

2004. április 29-én a Tanács elfogadta a fuvarozóknak az utasokkal kapcsolatos, az EU külső határait ellenőrző hatóságok által kért adatok közlésére vonatkozó kötelezettségéről szóló irányelvet. Az EU tagállamainak 2006. szeptember 5-ig kellett nemzeti jogukba átültetni az irányelvet. Számos állam azonban elmulasztotta ezt a határidőt, és még mindig tárgyalja az átültetést megvalósító jogszabályt. A Munkacsoport arra törekszik, hogy az irányelv átültetése a lehető legharmonizáltabb és legkövetkezetesebb módon történjen, a 95/46/EK irányelvben foglalt adatvédelmi elvek figyelembevételével. A Munkacsoport már korábban is kifejezte azon véleményét, hogy közép- és

hosszútávon egy következetesebb megközelítés kialakítása szükséges az utasinformációk cseréjével kapcsolatban annak érdekében, hogy a légi közlekedés biztonsága, az illegális bevándorlás elleni küzdelem és az emberi jogok tiszteletben tartása globális szinten biztosítva legyen. Ezen okoknál fogva a Munkacsoport ebben a véleményében néhány értelmező és az irányelv végrehajtására vonatkozó iránymutatást fogalmazott meg.

Az iránymutatások első csoportja az adatok célhoz kötöttségének követelményével kapcsolatos. Az adatgyűjtésnek az irányelvben rögzített céljai a határellenőrzés javítása és az illegális bevándorlás elleni küzdelem. A nemzeti jogszabályoknak egyértelműen rendelkezniük kell az adatfeldolgozás céljairól, melyek nem léphetik túl az irányelvben lefektetett célokat. Az irányelvben meghatározott céloktól eltérni csak bűnüldözési céllal lehet, a tagállamok nemzeti jogszabályainak rendelkezései szerint és összhangban az adatvédelmi irányelv rendelkezéseivel. A Munkacsoport fontosnak tartja, hogy a tagállamok az eltérésre vonatkozó rendelkezéseket megszorítóan alkalmazzák, így pontosan határozzák meg, hogy mely esetekben lehet a kérdéses adatokat bűnüldözés céljából felhasználni. A Munkacsoport szerint ilyen célú felhasználás csak súlyos bűncselekmények felderítése érdekében történhet, meghatározott esetekben és meghatározott adatvédelmi biztosítékok fennállása esetén. Elengedhetetlen az adatvédelemhez fűződő jogok biztosítása, amikor nem azok a hatóságok használják fel az adatokat, amelyeknek elsődlegesen szánták őket. A Munkacsoport azt is kiemelte, hogy az irányelv csak azokra a járatokra vonatkozik, amelyek célállomása egy EU tagállam, és nem jogosítja fel a tagállamokat arra, hogy kötelezhessék a légifuvarozókat az EU-n belüli repülésekkel kapcsolatos adatok gyűjtésére és továbbítására.

Az iránymutatások második csoportja a gyűjtendő adatok körére vonatkozik. Az irányelv egyértelműen meghatározza azoknak az adatoknak a körét, melyeket a légifuvarozók továbbíthatnak az illetékes hatóságoknak. A Munkacsoport hangsúlyozza, hogy ezeket az adatokat az irányelvben meghatározott célok megvalósításához szükségesnek és elégségesnek kell tekinteni. Az irányelv ugyanakkor lehetővé teszi a tagállamoknak, hogy nemzeti jogszabályaikban engedélyezzék, hogy a fuvarozók kérelemre a meghatározott adatkörön felüli, további adatcsoportokat továbbítsanak. A Munkacsoport álláspontja sze-

rint további adatok gyűjtése, mint például a visszaútra vonatkozó adatoké, nem szükséges a célok megvalósításához; a biometrikus adatok felhasználása azonban még aggályosabb lenne az adatgyűjtésre és feldolgozásra vonatkozó, egyértelmű előírások hiányában. Azoknak a biometrikus jellemzőknek a körét is feltétlenül meg kell határozni, amelyek az irányelv céljainak megvalósításához szükségesek és a célokkal arányosak. A Munkacsoport azt is kiemelte, hogy a tagállamok megsértenék a 95/46/EK adatvédelmi irányelvet, ha az összes olyan adatot követelnék, amely az utasnyilvántartási adatállományban (PNR) vagy a légifuvarozók indulás-ellenőrzési listáján szerepel, mivel ezek az adatok jelentősen túllépik a jelen iránymutatásokban és egyéb nemzetközi szabványokban szereplő adatok körét. Továbbá azt is hangsúlyozni kell, hogy a PNR adatok nem szükségesek az irányelv egyik célja, a határellenőrzés megvalósításához.

Az iránymutatások harmadik csoportja az adatok megőrzésére vonatkozik. Fő szabály szerint a határellenőrző hatóságok az adatokat 24 órán túl csak jogszabályban előírt feladataik teljesítése érdekében őrizhetik meg. Az irányelv azonban nem szabályozza, hogy a bűnüldöző hatóságok mennyi ideig őrizhetik meg a részükre továbbított adatokat. A Munkacsoport hangsúlyozza, hogy 24 óránál tovább csak különleges esetekben lehet az adatokat megőrizni, mint például amikor nem állapítható meg az utasok személyazonossága, vagy nem rendelkeznek megfelelő úti okmányokkal. A Munkacsoport véleménye szerint a tagállamoknak biztosítaniuk kell, hogy az adatokat ne lehessen hosszabb ideig megőrizni, mint ameddig feltétlenül szükséges a különleges célok tekintetében.

Az iránymutatások utolsó csoportja az érintettek tájékoztatására vonatkozik. A Munkacsoport az adatvédelmi irányelvben és két korábbi véleményben foglaltakat ajánlja a tagállamok figyelmébe. Továbbá felszólítja őket, hogy írják elő nemzeti jogszabályukban az utasok tájékoztatásának kötelezettségét arra az esetre is, ha adataikat továbbítják a bűnüldöző hatóságoknak.

Kötelező Erejű Vállalati Szabályok

Az Európai Unióban széleskörű támogatást élveznek a nemzetközi adattovábbításra vonatkozó Kötelező Érvényű Vállalati Szabályok (Binding Corporate Rules, a továbbiakban BCR). A BCR-t multinacio-

nális vállalatok alakítják ki és alkalmazzák a cégcsoport különböző országokban (EU-n kívül is) elhelyezkedő tagjai közötti adatcsere szabályozására. A BCR-eket – így az azokban található, személyes adatok védelmére vonatkozó szabályokat is – a nemzeti adatvédelmi hatóságok hagyják jóvá, és kötelező erővel bírnak a cégcsoport minden tagjára nézve. A BCR-ekkel a cégek azt igazolják – Magyarországon az Avtv. 9. § (2) bekezdés c) pont alapján – hogy az adatkezelés vagy adatfeldolgozás során megfelelő szinten biztosítják a személyes adatok védelmét, az érintettek jogait és azok érvényesítését.

A BCR-ek alkalmazása esetén a munkavállalók személyes adatai vélhetően magasabb fokú védelemben részesülnek. A BCR-ekben a vállalatok az EU adatvédelmi irányelvét és az adatcserével érintett országok nemzeti adatvédelmi szabályait saját szervezetükre, a vállalatnál folyó adatcsere-folyamatokra képezik le, ami konkrétabb, az adatfeldolgozást végző munkavállalók számára könnyebben érthető szabályokat eredményez. A nemzeti adatvédelmi hatóságok a BCR-ek jóváhagyásakor vizsgálják, hogy a szabályok ne csak elméletben, hanem gyakorlatban is kötelező erővel rendelkezzenek, például a BCR tartalmazza, hogy a vállalat belső fegyelmi szankciókat alkalmaz, ha munkavállalói azt megszegik; a vállalat oktatást szervezzen a BCR alkalmazásáról az adatfeldolgozást végző munkavállalóinak. A BCR-eknek tartalmazniuk kell, hogy az a munkavállaló, akinek személyes adatait külföldre továbbítják (érintett), panaszt tehet a nemzeti adatvédelmi hatóságnál, és igényét a bíróságon is érvényesítheti, ha személyes adatainak kezelésével kapcsolatban jogsérelem érte. A szabályoknak biztosítaniuk kell, hogy az érintett legalább ugyanolyan jogokkal rendelkezzen a jogsértő adatkezelést végző vállalattal szemben, mint amit az EU adatvédelmi irányelve vagy a nemzeti jog biztosít. Ha a nemzeti jog szigorúbb adatvédelmi szabályokkal rendelkezik, akkor azokat kell alkalmazni. A BCR-nek tartalmaznia kell azt a fontos kötelezettségvállalást is, hogy a cégcsoport EU-n kívüli tagjainak cselekményeiért vagy a vállalat EU-ban található székhelyű központja vagy a cégcsoport egy európai tagja átvállalja a felelősséget és szükség esetén kártérítést fizet. A BCR betartását belső és külső audittal is ellenőriztetnie kell a vállalatnak. A cégcsoportnak együttesen és tagjainak külön is kötelezettséget kell vállalniuk, hogy az illetékes adatvédelmi hatóságokkal együttműködnek, és ezen hatóságoknak a BCR értelmezésével és alkalmazásával kapcsolatos javaslatait alkalmazzák. Az adat-

védelmi hatóságok a BCR jóváhagyását visszavonhatják, ha a cégcsoport nem tanúsít kellő együttműködést. Végezetül fontos kiemelni, hogy a BCR-ek az érintettekről és az adatvédelmi hatóságokról a vállalatokra helyezik át annak a terhét, hogy biztosítsák az adatvédelmi jogszabályoknak való megfelelést.

A multinacionális cégcsoportok számára különösen azért előnyös a BCR, mivel egyetlen szabályzat rendezi a cégcsoport tagjai közötti adatcserét. Így a vállalatok sok időt és pénzt takarítanak meg a bonyolult és állandó jelleggel módosításra szoruló, az EU-n kívülre történő adattovábbítást szabályzó szerződések mellőzésével. Továbbá nagyobb védelmet tudnak biztosítani munkavállalóik személyes adatainak, mivel a számos nemzeti és uniós jogszabály egy átláthatóbb és könnyebben betartható rendszert alkot a BCR-ekben.

A 29-es Adatvédelmi Munkacsoport már több lépést tett a BCR-ek alkalmazásának megkönnyítése és ösztönzése érdekében. A Munkacsoportnak eddig három munkaanyaga foglalkozott a BCR-ekkel. Az első munkaanyag egy általános elemzést és útmutatást nyújtott, a következő dokumentum pedig a nemzeti adatvédelmi hatóságok együttműködési eljárását vázolta fel a BCR-ek jóváhagyására. A nemzeti adatvédelmi hatóságok együttműködése azért fontos, mert egy vállalatcsoport BCR-jét minden olyan országban jóvá kell hagyni, ahonnan adatot továbbítanak az EU-n kívülre. Ez egy rendkívül hosszú eljáráshoz vezetne, ha a hatóságok munkája nem lenne összehangolva. A legutóbbi munkaanyag pedig egy listát tartalmazott azokról a kérdésekről, amelyeket a vállalatoknak egy BCR-ben feltétlenül tisztázniuk kell. 2006-ban is folytatódott a párbeszéd a multinacionális cégcsoportok, a Munkacsoport és a nemzeti adatvédelmi hatóságok között. Jelenleg a Munkacsoport BCR-alcsoportja egy standard, BCR-jóváhagyásra irányuló kérelem összeállításán dolgozik, melynek végleges formába öntése hamarosan várható. Ezt a kezdeményezést a Nemzetközi Kereskedelmi Kamara (ICC) indította, majd az ICC által összeállított standard jelentkezést a Munkacsoport továbbfejlesztette a tagállamok észrevételeivel kiegészítve. A standard jelentkezési formanyomtatvány több szempontból is előnyös lesz: (1) felhasználóbarát, standard szöveg áll majd a vállalatok rendelkezésére, (2) leegyszerűsíti a nemzeti adatvédelmi hatóságok munkáját, és (3) a BCR-eljárást egyszerűbbé és hatékonyabbá teszi.

A BCR-ek azonban nemcsak elméletben, hanem már a gyakorlatban is léteznek. Számos BCR-t (például a General Electric, a Deutsche Telekom, a Bank Austria Creditanstalt, a Daimler-Chrysler kérelmezők részére) hagytak már jóvá az EU tagállamainak nemzeti adatvédelmi hatóságai, köztük a magyar adatvédelmi biztos is. Magyarországról azonban a munkavállalók személyes adatai harmadik országbeli adatkezelő részére csak akkor továbbíthatók, ha az érintett ahhoz hozzájárult vagy törvény azt lehetővé teszi, és a harmadik országban az átadott adatok kezelése, illetőleg feldolgozása során biztosított a személyes adatok megfelelő szintű védelme. Így a BCR-ek a munkavállalók adatainak továbbítására csak hozzájárulásuk esetén alkalmazhatók vagy akkor, ha az adattovábbítást törvény lehetővé teszi [Avtv. 9. § (1)(b)]. A munkavállalók hozzájárulásának önkéntessége azonban egzisztenciális kiszolgáltatottságuk miatt megkérdőjelezhető. Azon esetek száma pedig, amikor a BCR-eket az Avtv. 9. § (1)(b) pont alapján lehet alkalmazni, eléggé korlátozott. Ezért célszerű lenne, ha a Munka Törvénykönyve (MT.) lehetőséget adna arra, hogy a munkavállalók személyes adatainak vállalatcsoporton belüli továbbítása lehetséges legyen kötelező belső szabályzatok alapján, akár Unión kívüli államok viszonylatában is, ezzel szélesebb körben lehetővé téve a BCR-ek alkalmazását. Ennek érdekében a közelmúltban kezdeményeztem a szociális és munkaügyi miniszternél, hogy tegye meg a szükséges lépéseket az MT. következő módosításánál.

A Munkacsoport által kezdeményezett tagállami vizsgálatok

2006-ban a 29-es cikkely Adatvédelmi Munkacsoportjának megbízásából sor került egy átfogó vizsgálatra, mely a magán egészségbiztosítók adatkezelését vizsgálta. Magyarországon jelenleg az egészségügyi ellátásokat – az OEP-en keresztül – közvetlenül az állami költségvetésből finanszírozzák, de hozzáteszem, hogy az egészségügyi és finanszírozási rendszer napjainkban zajló átalakulása miatt a jövőben a magánbiztosítók is nagyobb szerephez juthatnak. A vizsgálat során több biztosítótársaságot megkerestünk azzal, hogy töltsék ki az egységes kérdőívet (például milyen tájékoztatást adnak ügyfeleiknek az adatkezelésre vonatkozóan, milyen egészségügyi adatokat kezelnek, mi az adatkezelés jogalapja stb.), majd a válaszokat kiértékeltük. Mivel a nemzetközi vizsgálat eredményeinek feldolgozására még nem

került sor, erről valószínűleg a jövő évi Beszámolóban tudunk csak bővebben hírt adni.

Szintén a 29-es Munkacsoport megbízásából a magyar Adatvédelmi Biztos Irodája vállalta az előkészítés szerepét a *„Levéltári és tudományos kutatás adatvédelmi összefüggései"* témakörben. A német, olasz, litván, szlovák, cseh, román, norvég és francia hozzászólásokat felhasználva elkészült egy 15 oldalas szakértői anyag, mely az általános levéltárak és a diktatúrák összeomlását követően a titkosszolgálati eszközökkel összegyűjtött anyagokat őrző speciális levéltárak helyzetét elemzi, és több konkrét javaslatot is megfogalmaz (például az állampolgársághoz kötött joggyakorlás korlátjának feloldása, válogatott listák tisztességtelen, politikai célból történő nyilvánosságra hozatala elleni szigorúbb fellépés stb.). Az eddigi munkát a Munkacsoport 57. ülésén röviden bemutattuk, és felkérést kaptunk a téma további *„gondozására"*.

Az Európai Adatvédelmi Biztosok Tavaszi Konferenciája

Az Európai Adatvédelmi Biztosok Tavaszi Konferenciája az Európai Unió tagállamai adatvédelmi felügyelő hatóságainak egyik legfontosabb éves találkozója. Az első ilyen konferenciát 1991-ben Hágában rendezték meg. Az 1993-ban Párizsban szervezett konferenciát követően született döntés arról, hogy minden évben tavasszal rendezzék meg az Európai Adatvédelmi Biztosok Tavaszi Konferenciáját. Minden egyes konferenciát az adatvédelem különböző európai kérdéseinek szentelnek, így különösen az adatvédelmi irányelv rendelkezései érvényesítésének és az országok saját megfigyeléseinek, tapasztalatainak. A tárgyalási témák között szerepelnek a rendőrséggel folytatott együttműködés céljából történő adatkezelések, valamint a bíróságokkal büntetőjogi vagy polgári jogi esetekben történő együttműködés kérdései is.

2006. április 24-25-én a magyar adatvédelmi biztos adott otthont a Tavaszi Konferenciának. A konferenciát a köztársasági elnök úr levélben köszöntötte, amelyben többek között arra is rámutatott, hogy *„Az adatvédelem mindig példával szolgál a nagyközönségnek arra, hogy semmiféle – bármilyen jogos – politikai igény sem hagyhatja figyelmen kívül a szabadságjogokban rejlő korlátokat... Napjainkban arra kell figyelmeztetni, hogy a terrorizmus elleni harc sem szolgálhat feltétel nél-*

küli indokul az információs önrendelkezés korlátozására. Ehelyett egy új, gondosan előállított egyensúly kidolgozásáról lehet szó."

A konferencia nyitóbeszédét Dr. Baka András, az Európai Emberi Jogi Bíróság bírája tartotta, kiemelve az adatvédelemnek emberi jogi bírói gyakorlatban betöltött fontos szerepét. A konferencia programja a továbbiakban a legaktuálisabb adatvédelmi témákat érintette. Az előadók a harmadik pillér adatvédelme, a földrajzi helymeghatározás, a munkáltatói információs ellenőrző rendszer, a történeti és tudományos kutatás során az adatvédelem, az adatvédelmi hatóságok működésének hatékonysága, a nemzeti egészségügyi adatbázisok és a genetikai adatok terén a legújabb fejleményeket, a tagállami szabályozásokat és rendszereket mutatták be.

A konferencia nyilatkozatot fogadott el, amely a harmadik pillérbeli, a bel- és igazságügyi együttműködést érintő intenzív jogszabályalkotás során felhívja a figyelmet az adatvédelmi elvek megfelelő szintű figyelembevételére, továbbá magas szintű és harmonizált adatvédelmi standardok kialakítására e területen. Ez a Hágai Program logikus következménye, mely szerint a szabadság, biztonság és igazságosság biztosítása az Európai Unió mint egész feladatának oszthatatlan eleme, valamint olyan területeken, mint a Vízuminformációs Rendszer (VIS), a Schengeni Információs Rendszer II (SIS II) vagy az igazság- és belügy terén az európai adatbázisok közötti kölcsönös átjárhatóság, nemrégiben EU-szinten tett lépések következménye. Csak ilyen standard kialakításával lehet majd elérni az EU bűnüldözési hatóságai között az információcsere létező és jövőbeli formái közötti megfelelő egyensúlyt, és egyrészt az EU-ban élő állampolgárok biztonságának, másrészt a szabadság, biztonság és igazságosság területén a polgári szabadságjogok biztosításakor eleget tenni az arányossági alapelvnek.

Az Adatvédelmi Biztosok 28. Nemzetközi Konferenciája

Évente rendezik az Adatvédelmi Biztosok Nemzetközi Konferenciáját, melynek 2006. november 2-án és 3-án London volt a helyszíne. A konferencia egyetlen központi témaként a „*megfigyelt társadalom*" hatásaival foglalkozott. Az előadások foglalkoztak többek között a megfigyelés jövőjével, a jogainkra leselkedő veszélyekkel és kockázatokkal, a múltbéli tapasztalatokkal, a jogérvényesítéssel, a magánszfé-

ra és a bűnözés kapcsolatával, az állam információfelhasználásával, a fogyasztói és üzleti érdekek szembeállításával. Dr. Baka András, az Európai Emberi Jogi Bíróság bírája az emberi jogok viszonyait a megfigyelt társadalomban vizsgálta meg és adta elő prezentációjában.

A résztvevők által elfogadott záró közleményben a biztosok kiemelték, hogy a mindennapjainkban is jelenlévő megfigyelési tevékenységek jelentős kockázattal járnak az emberek magánszférájának korlátozása terén. A konferencia megállapította, hogy a megfigyelés törvényességének fontos biztosítéka az adatvédelmi szabályozás. Kiemelkedő jelentősége van annak, hogy az emberek bízzanak a megfigyelési tevékenységekben, illetve abban, hogy a magánéletükbe történő bármiféle beavatkozás szükséges célból történik és arányosan. Habár a megfigyelt társadalom kérdése meghaladja az adatvédelem területét, az adatvédelmi hatóságok szerepe nélkülözhetetlen. A biztosok elkötelezettek, és komoly erőfeszítéseket tesznek a jövőben is annak érdekében, hogy a modern információs társadalomban nélkülözhetetlen adatvédelmi biztosítékokat és szabályozó eszközöket a kihívásoknak megfelelve időszerűen fenntartsák.

Az európai adatvédelmi hatóságok nyilatkozatot fogadtak el a londoni konferencia keretén belül, különös figyelemmel a rendvédelmi célból történő, határon átnyúló információáramlásra. Az európai adatvédelmi hatóságok felhívják a tagállamokat, hogy tartsák tiszteletben és erősítsék meg az EU állampolgárainak polgári szabadságjogait úgy, hogy biztosítják a rendvédelmi célokat szolgáló adatkezelésekre vonatkozó adatvédelem magas szintű és harmonizált színvonalát, és megfelelő adatvédelmi rendszert alakítanak ki, mely nemcsak a tagállamok közötti adatcsere esetén alkalmazandó, hanem minden, a rendvédelem céljából kezelt személyes adat esetén is. A védelem magas szintjét kell biztosítani a harmadik országokba és nemzetközi szervezetekhez irányuló adattovábbítások esetében, amelyeknek közös európai standardokon alapuló megfelelőségen kell nyugodniuk.

Rendőrségi munkacsoport

A rendőrségi munkacsoport az európai adatvédelmi biztosok konferenciája által felállított munkacsoport, amely a biztosok konferenciája elé kerülő, különösen a büntetőügyekben folytatott rendőrségi és igazságügyi együttműködésre vonatkozó dokumentumok előké-

szítő szerve. A rendőrségi munkacsoport jelenlegi elnöke a magyar adatvédelmi biztos. Budapesten megrendezett konferenciájukon az európai adatvédelmi biztosok felkérték a rendőrségi munkacsoportot, hogy néhány aktuális témakört részletesen dolgozzon ki, és megállapításairól a biztosok következő találkozóján adjon tájékoztatást. A megvizsgálandó témakörök a hozzáférhetőség elve, az ellenőrzés/felügyelet kérdésköre, biometria, az adatok felhasználásának nagyobb átláthatósága és az adatmegőrzés. A munkacsoport megkezdte a munkaanyagok kidolgozását.

A munkacsoport októberi ülésén beszámolót hallgatott meg a büntetőügyekben folytatott, a rendőrségi és igazságügyi együttműködés keretében feldolgozott személyes adatok védelméről szóló kerethatározat tervezetnek a Tanácsnál folyó előkészítéséről. A tervezet kidolgozása során az egyik legvitatottabb kérdés a tervezet hatálya. Egyes elképzelések szerint a kerethatározatot csak a határon átnyúló adatcsere esetén kell alkalmazni, más vélemények szerint a kerethatározat hatályának ki kell terjednie azon nemzeti adatkezelésekre is, amelyek a rendvédelem célját szolgálják. A rendőrségi munkacsoport által összeállított dokumentum alapján az európai adatvédelmi hatóságok vezetői 2006. november 2-i nyilatkozatukban felhívják a figyelmet arra, hogy az adatvédelem elveit az szolgálja leginkább, ha a kerethatározat tervezet hatálya a szélesebb körű megoldásra terjed ki. Ez a megoldás a rendőrségi és igazságügyi együttműködés hatékonyságát is elősegíti.

A munkacsoport decemberi ülésén a rendvédelem terén a hozzáférhetőség elvének alkalmazásáról szóló munkaanyag előző ülésen már megkezdett részletes kidolgozását folytatta.

Részvétel Ikerintézményi Fejlesztési Programban

Az Adatvédelmi Biztos Irodája 2006 elején Bulgária Adatvédelmi Bizottsága adminisztratív megerősítésére kiírt Ikerintézményi Fejlesztési Programban (Twinning) vett részt. A projekt célja a bolgár intézmény adminisztratív kapacitásának növelése mellett a személyes adatok védelmére vonatkozó jogszabályok implementálásához, érvényesítéséhez szükséges feltételek nyújtása volt.

Az Európai Unió Bizottságának benyújtott írásbeli pályázatunk részletesen, alapvető periodikus struktúrában határozta meg a fejlesz-

tési tervet. A magyar delegáció által készített előterjesztés a bolgár Adatvédelmi Bizottság minden strukturális részlege számára történő segítségnyújtást célozta. Ez magában foglalta a lehető legjobb és leghasznosabb gyakorlati megoldásokat az adatvédelmi szabályok hatékony és eredményes implementálása céljából úgy, hogy a lehető legtöbbet lehessen kihozni az ámbár különböző, mégis hatékony szervezeti működésre alapozott gyakorlatból és a tapasztalatokból, melyek átadására az Adatvédelmi Biztos Irodája egyébként is nyitott.

A Twinning projektre vonatkozó magyar előterjesztés felépítése a megvalósítandó célokhoz és részfeladatokhoz igazodik, ezért rövid, közép és hosszú távú modulokba rendeztük a programokat. A modulok magukban foglalták az intézmény fejlesztését, kapacitásának növelését, a szakképzést az eredményesebb működés elérése céljából. A szakmai képzésbe tartozott az Európai Unió elvárásainak, követelményeinek megfelelő, adatvédelemmel kapcsolatos jogszabályi, gyakorlati (panaszügyintézés, hivatalból vagy beadvány alapján indított vizsgálatok), technikai és informatikai ismeretek átadása.

A szóbeli meghallgatásra és prezentációra Szófiában került sor, ahol mind a bolgár Adatvédelmi Bizottságnak, mind az Európai Unió Bizottságának a munkatársai további lényegretörő tájékoztatást kaptak az intézmény fejlesztését célzó, a magas szintű és hatékony működést, illetve az Európai Unió által elfogadott és érvényesített legjobb gyakorlatát szem előtt tartó javaslatunkból.

Az Ikerintézményi Fejlesztési Programban való részvétel kapcsán szerzett tapasztalatok jelentős fontossággal bírnak, a jövőben eredménnyel lehet azokat kamatoztatni.

Nemzeti szakértők az európai uniós intézményekben

Örömmel számolhatok be arról, hogy az Adatvédelmi Biztos Irodája 2006-ban a nemzetközi, európai uniós színtéren, az uniós intézményekben is képviseltette magát, mivel két munkatársamnak is sikerült nemzeti szakértőként (úgynevezett Seconded National Expert) tapasztalatot szerezni. Dr. Szabó Endre, az adatvédelmi főosztály munkatársa 2006 februárjában kezdte meg a nemzeti szakértői kiküldetést Brüsszelben az Európai Adatvédelmi Biztos Hivatalánál. Kiküldetése 2007. július 30-ig tart. A nemzetközi főosztálytól Dr. Halmos György az Európai Unió Igazságügyi Együttműködési Egységénél

(Eurojust) Hágában helyettesítette 2006 májusától fél éves időtartamban az Eurojust adatvédelmi tisztviselőjét.

A nemzeti szakértői állásokra jellemzően a tagállamok közigazgatási intézményeiben foglalkoztatott köztisztviselők jelentkezhetnek. A státusz kettős szerepet tölt be: egyrészt hasznos a fogadó és a küldő intézmény közötti tapasztalatcsere, másrészt a későbbi együttműködés szempontjából. A fogadó intézmény szempontjából azért előnyös, mert a szakértő az adott szakterületen kiírt állásnak, feladatnak megfelelő speciális szakterület ismerettel rendelkezik, amely alapvetően az intézményi sajátosságokra tekintet nélkül a fogadó intézményben is alkalmazható. A küldő intézmény szempontjából pedig hasznos, hogy a szakértő a szakterülthez kapcsolódóan gyakorlati tapasztalatot szerez speciálisan az Unió, az uniós intézmény(ek) működésére, az uniós joganyag konkrét alkalmazására vonatkozólag, bővítve ezzel a hazai tudásbázist.

Alább az Eurojust adatvédelmi tisztviselőjének tevékenységét foglaljuk össze.

I. Az Eurojust rövid bemutatása

a) Az Eurojust felállítása

Az Eurojust felállításáról az Európai Tanács 1999 októberében a finnországi Tamperében tartott csúcsértekezletén született döntés. Az Eurojustot a 2003. június 18-i 2003/659/IB tanácsi határozattal módosított, 2002. február 28-i európai tanácsi határozat az „*Eurojust létrehozásáról a súlyos bűncselekmények elleni közös fellépés érdekében*", (a továbbiakban Eurojust-határozat) hozta létre. A szervezet 2001. március 1-jétől ideiglenesen Brüsszelben működött, majd 2002 decemberében Hágába költözött. Az Eurojust jogi személy.

b) Az Eurojust küldetése

Az Eurojust az Európai Unió büntetőügyekben folytatott rendőrségi és igazságügyi együttműködési ügynökségei[15] közé tartozó új szerv, amelyet a célból hoztak létre, hogy Európa-szerte erősítse az

15 Ezen ügynökségek az Európai Rendőrségi Hivatal (EUROPOL) és az Európa Rendőrakadémia (CEPOL).

együttműködést a büntető igazságszolgáltatás területére tartozó ügyekben, valamint azért, hogy növelje a tagállamok illetékes hatóságainak hatékonyságát, amennyiben azok a súlyos, határokon átnyúló és szervezett bűnözéssel kapcsolatban nyomozást, vádeljárást folytatnak.

c) Az Eurojust szerepe

Az Eurojust az igazságügyi hatóságok világon elsőként folyamatosan működő hálózata. A szervezet előmozdítja és javítja a nyomozások és a vádemelések összehangolását, ugyanakkor támogatást nyújt a tagállamoknak a nyomozások és vádemelések eredményesebbé tételében is. Ennek érdekében megszervezi az ügyészek és nyomozók részére azokat a megbeszéléseket, amelyek során megtárgyalják az egyes, valamint a stratégia szintű ügyeket és meghatározott bűncselekménytípusokat. Az Eurojust kulcsfontosságú partnere az olyan európai intézményeknek, mint a Parlament, a Tanács és a Bizottság.

d) Az Eurojust szervezeti felépítése, összetétele

Az Eurojust 25 nemzeti tagot számláló Testületből, valamint a Testület munkáját segítő adminisztratív apparátusból áll. A Testületbe az Unió minden egyes tagállama egy tagot delegál. A nemzeti tagok tapasztalt, magas beosztású ügyészek, bírák vagy rendőrtisztek; munkájukat helyettesek és segítők támogatják.

e) Az Eurojust hatásköre

Az Eurojust hatáskörébe tartoznak mindazok a bűncselekmények, amelyekre vonatkozólag az Europol hatásköre az Europol Egyezmény szerint megállapítható, továbbá a számítógépes bűnözés, a csalás, a korrupció és bármely egyéb bűncselekmény, amely az Európai Unió pénzügyi érdekeit hátrányosan befolyásolja, a pénzmosás, a környezeti bűncselekmények, a bűnszervezetben való részvétel, és egyéb bűncselekmények, amelyeket az előbb említett bűncselekményekkel együttesen követnek el.

f) In Concreto[16]: A *„Spanish Guardia Civil"* egy speciális szoftvert fejlesztett ki azon számítógépek azonosítására, amelyeket gyermek-

16 Az esettanulmány angol nyelven megtalálható az Eurojust sajtóközleményei között, az alábbi elérhetőségen:
http://www.eurojust.europa.eu/press_releases/2006/22-02-2006.htm

pornográfia Interneten való terjesztésére használnak fel. A szoftver segítségével a különféle országokban azonosíthatóvá váltak a számítógépek IP címei, a tartalom terjesztői, valamint lakhelyük. Az Eurojust megbeszélést hívott össze az egyidejű akciók koordinálása érdekében. Az akcióterv két lépésből állt: elsőként azonosítani kellett a gyanúsítottak lakóhelyét, ahol a számítógépeket tárolják, második lépésként házkutatást kellett tartani ugyanazon a napon, órában valamennyi országban az azonosított lakóhelyeken. Az ilyen akciók megszervezésének nehézsége, hogy a művelet során számtalan ügyésznek, rendőrnek kell együttműködni. A házkutatásokat 2006 február 21-én hajtották végre, melynek eredményeképpen több tucat számítógépet foglaltak le a bizonyítékok beszerzése érdekében, 17 országban számos személyt tartóztattak le. Az eredményes akció egyértelmű jelzés volt, hogy ezek a fajta bűncselekmények sikerrel nyomozhatók világszerte, amennyiben a különféle országok ügyészi és rendőri hatóságai együttműködnek. A gyermekpornográfiát Interneten terjesztőknek tudomásul kell venniük, hogy többé nincsenek biztonságban".

II. Az Eurojust információs, adatvédelmi jogi környezete

Fontos kiindulópont, hogy mivel az Eurojust az Európai Unió harmadik pillérében a *„Rendőrségi és bűnügyi együttműködés"* területén fejti ki tevékenységét, ezért az adatvédelemi jogi környezetét – a harmadik pillér adatvédelmét szabályozó kerethatározat hatálybalépéséig – elsősorban az Eurojustra vonatkozó jogi normák jelentik. Az olyan általánosan ismert alapnormák, mint az *„Európai Parlament és a Tanács 1995. október 24-i 95/46/EK Irányelve a személyes adatok feldolgozása vonatkozásában az egyének védelméről és az ilyen adatok szabad áramlásáról"*, valamint az *„Európai Parlament és a Tanács 2000. december 18-i 45/2001/EK Rendelete a személyes adatok közösségi intézmények és szervek által történő feldolgozása tekintetében az egyének védelméről, valamint az ilyen adatok szabad áramlásáról"*, az Eurojust esetében nem alkalmazandók, hiszen ezek hatályukat tekintve az Unió első pillérében folytatott adatvédelemi tevékenységre vonatkoznak.

Függetlenül attól, hogy az Irányelv, mint az első pillér centrális jogszabálya nem alkalmazandó, azonban az általa megfogalmazott adatvédelmi alapelvek, fogalommeghatározások, annak logikája, szelleme az Eurojust adatvédelmi jogszabályi környezetének megalkotá-

sakor iránytűként játszott(ak) szerepet. Az elvek és a fogalommeghatározások például teljes egészükben adaptálásra kerültek.

1.) A jogi normák között elsőként említendő a fentebb már hivatkozott „*Tanács 2002. február 28-i Határozata az Eurojust létrehozásáról a súlyos bűncselekmények elleni közös fellépés érdekében*"[17], mely részletes adatvédelmi szabályokat tartalmaz a 14-27. cikkekben. Lényegében az Eurojust-határozat hatalmazza fel az Eurojustot a személyes adatok kezelésére, rendelkezik az adatvédelmi tisztviselő kinevezésének kötelezettségéről, annak feladatairól, az adatalanyok hozzáférési jogáról, a helyesbítés és törlés jogáról, az adatbiztonságról, a tárolási határidőről, a partnerekkel, harmadik személyekkel történő adatcsere feltételeiről, a jogellenes adatkezelés esetén fennálló felelősségről, az automatizált ügykezelési rendszerről stb. Kiemelném az Eurojust-határozat 15. cikkét, a személyes adatkezelés „*megszorításait*", amely konkrétan, taxatív felsorolással nevesíti, hogy az Eurojust, mely személyes adatok kezelésére jogosult az adatalanyokra vonatkozólag, valamint azt, hogy ezen adatokon kívül milyen feltételek teljesülése esetén kezelhet további személyes és különleges adatokat.

2.) Másodsorban említendő az „*Eurojust személyes adatok védelmére és feldolgozására vonatkozó eljárási szabályzata*"[18] (az Eurojust Testületének 2004. október 21-i ülésén egyhangúlag elfogadott és a Tanács által 2005. február 24-én jóváhagyott szövege) (a továbbiakban Eljárási Szabályzat), amely tartalmazza az adatvédelmi fogalommeghatározásokat, az Eurojustra alkalmazandó általános elveket, az ügyhöz kapcsolódó, valamint az ügyhöz nem kapcsolódó adatkezelésre vonatkozó szabályokat.

Az Eljárási Szabályzat tagolása szerint az Eurojust által kezelt személyes adatokat két alapkategóriába sorolhatjuk. Az egyik csoportba tartoznak az Eurojust nemzeti tagjai által kezelt, az ügyekhez, a nyomozások koordinálásához kapcsolódó személyes adatok, azaz konk-

17 http://www.eurojust.europa.eu/official_documents/Eurojust_Decision/l_06320020306en00010013.pdf

18 http://www.eurojust.europa.eu/official_documents/Data_Protection_Rules/c_06820050319hu00010010.pdf

rétan a nyomozás védeljárás alatt lévő bűncselekmény elkövetőinek, az áldozatok és a tanúk személyes adatai. Ezeket a személyes adatokat a nemzeti tag részére vagy a küldő tagállam hatósága, vagy másik, az ügyben érintett nemzeti tag továbbítja. A személyes adatok másik csoportját az ügyekhez nem kapcsolódó, az intézmény adminisztratív tevékenysége során az adminisztráció adatkezelői által kezelt személyes adatok képezik.

Az Eljárási Szabályzat 43. cikke szerint *„szükség esetén az Eurojust ügyhöz nem kapcsolódó műveletek esetében a személyes adatok feldolgozására vonatkozó további szabályokat dolgoz ki […]"*. A Testület *„Az Eljárási Szabályzathoz kapcsolódó további szabályokat"* 2006-ban alkotta meg, mely részletes szabályokat tartalmaz az adatvédelmi tisztviselő feladataira, az adatkezelők és adatfeldolgozók kötelezettségeire, jogaira, valamint az adatalanyok hozzáférési jogának gyakorlására, valamint a feltételezett jogellenes adatkezelés esetén követendő eljárás szabályaira vonatkozólag.

3.) Természetesen az Eurojust esetében is érvényesül az információszabadság. Az információhoz való szabad hozzáférés jogának gyakorlására vonatkozó eljárási rendelkezéseket a *„Hozzáférés az Eurojust dokumentumaihoz"*[19] című jogszabály tartalmazza.

4.) Az Eurojust adatvédelmi tevékenységének rendszeres felülvizsgálatát a Közös Ellenőrző Szerv, a *„Közös Ellenőrző Szervre vonatkozó törvény"*[20] rendelkezései szerint végzi. A jogszabály rendelkezései közül kiemelendők azok az eljárási szabályok, amelyek az adatalanyok hozzáférési jogához kapcsolódó fellebbezési jog gyakorlására, valamint a Közös Ellenőrző Szerv dokumentumaihoz való hozzáférésre vonatkoznak.

19 http://www.eurojust.europa.eu/official_documents/Access_to_Documents/Access_to_Documents.pdf

20 http://www.eurojust.europa.eu/official_documents/Joint_Supervisory_Body_ACT/c_08620040406en00010007.pd

5.) Egyéb uniós jogszabályok

Az alábbi uniós jogszabályok jelentős viszonyítási pontok az Eurojust esetében is.

a) Szerződés az Európai Unióról (Maastrichti Szerződés) 6. cikke:

„Az Unió a szabadság, a demokrácia, az emberi jogok és az alapvető szabadságok tiszteletben tartása és a jogállamiság elvein alapul, amely alapelvek közösek a tagállamokban.

Az Unió a közösségi jog általános elveiként tartja tiszteletben az alapvető jogokat, ahogyan azokat az emberi jogok és alapvető szabadságok védelméről szóló, 1950. november 4-én Rómában aláírt európai egyezmény biztosítja, továbbá ahogyan azok a tagállamok közös alkotmányos hagyományaiból erednek."

b) Az emberi jogok és alapvető szabadságok védelméről szóló egyezmény 8. cikke a

„Magán- és családi élet tiszteletben tartásához való jogról".

c) Az Európa Tanács 1981. január 28-i egyezménye a személyes adatok gépi feldolgozása során az egyének védelméről.

d) Az Alapvető Jogok Európai Chartája 7-8. cikkei a *„Magán- és családi élet tiszteltben tartásáról, valamint a személyes adatok védelméről".*

6.) A harmadik pilléres adatvédelemre vonatkozó kerethatározat

A büntetőügyekben folytatott rendőrségi és igazságügyi együttműködés keretében feldolgozott személyes adatok védelméről szóló tanácsi kerethatározat javaslat – mely többször nem került elfogadásra a jogalkotók által – az a jogszabálytervezet, amely a harmadik pillérben folytatott adatvédelmi szabályokat hivatott lefektetni. A jogszabálytervezet jelenlegi formájában külön megjelöli az Eurojustra vonatkozó eltérő szabályokat.

III. Az adatvédelmi tisztviselő

Tudható általában, hogy az uniós intézmények kötelezettek adatvédelmi tisztviselőt[21] kinevezni az általuk kezelt személyes adatok vé-

21 Az egyes intézményekben kinevezett adatvédelmi tisztviselők elérhetősége az Európai Adatvédelmi Biztos honlapján megtalálhatók: (http://www.edps.europa.eu/05_en_reseau_dpo.htm)

delme érdekében. Az Unió I. pillérében működő intézmények adatvédelmi tisztviselőire az Európai Parlament és Tanács 2000. december 18-i 45/2001/EK. Rendelete a személyes adatok közösségi intézmények és szervek által történő feldolgozása tekintetében az egyének védelméről, valamint az ilyen adatok szabad áramlásáról[22] vonatkozik. Ebben a tekintetben kivételt képez az Eurojust adatvédelmi tisztviselője, mivel tevékenységét nem az előbbi jogszabály, hanem az Eurojust-határozat és az Eljárási Szabályzat határozza meg.

Az Eurojust adatvédelmi tisztviselőjére vonatkozó szabályozás centruma az Eurojust-határozat 17. cikke[23], mely szerint:

(1) Az Eurojust külön kijelöl egy adatvédelmi tisztviselőt, aki az Eurojust személyzetének tagja. A tisztviselő ebben a tekintetben a testületnek közvetlenül alárendelt. Az ebben a cikkben előírt feladatainak ellátása során utasításokat senkitől nem fogadhat el.

(2) Az adatvédelmi tisztviselő feladatai különösen a következők:

a) függetlenül eljárva gondoskodik a személyes adatok kezelésének jogszerűségéről és a személyes adatok kezelésére vonatkozóan ebben a határozatban előírt rendelkezések betartásáról;

b) biztosítja, hogy az eljárási szabályzatban meghatározandó rendelkezésekkel összhangban, a 22. cikkben előírt biztonsági feltételek szerint – különösen a 19. cikk (3) bekezdésének alkalmazásában – írásban rögzítsék a személyes adatok átadását és átvételét;

c) gondoskodik arról, hogy az érintettek az ebben a határozatban biztosított jogaikról kérelemre tájékoztatást kapjanak.

(3) Feladatainak ellátása során a tisztviselő az Eurojust által kezelt adatokhoz hozzáférhet, és az Eurojust összes helyiségébe beléphet.

(4) Amennyiben azt állapítja meg, hogy az adatkezelés nem felelt meg e határozat rendelkezéseinek, a tisztviselő:

a) tájékoztatja erről a testületet, amely igazolja a tájékoztatás kézhezvételét;

b) amennyiben a testület az adatkezelés szabálytalanságának tárgyában ésszerű határidőn belül nem dönt, a Közös Ellenőrző Szerv elé terjeszti az ügyet.

---

22 http://www.edps.europa.eu/legislation/Reg_45-2001/Reg_45-2001_hu.pdf

23 Forrás: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2002:063:0001:01:HU:HTML

A fenti rendelkezések, valamint az Eurojust szervezeti ábrájának tanulmányozása alapján is levonható az a következtetés, hogy az adatvédelmi tisztviselő egy szervezetbe integrált, ugyanakkor *„függetlenséggel"* felruházott *„belső"* kontroll funkciót ellátó tisztség. Az adatvédelmi tisztviselő tevékenyégének különösen fontos jellemzője a *„függetlenség"*, pontosabban a független véleményformálási, döntési, cselekvési mód, a kezelt adatokhoz való korlátlan hozzáférés.

Az európai adatvédelmi biztos

Beszámolóinkban immáron rendszeresen említést teszünk az európai adatvédelmi biztosról. Ez indokolt több szempontból is. Az európai adatvédelmi biztos (angol elnevezésének rövidítése: EDPS) egyrészt olyan meghatározó szereplője az európai adatvédelemnek, amely szükségessé teszi, hogy a magyar adatvédelmi biztos beszámolójában szerepeljen. Másrészt a magyar adatvédelmi biztos – többi európai uniós kollégájához hasonlóan – közvetlenül is együttműködik az EDPS-szel, a gyakori konzultációkon túl a 29-es Munkacsoportban is. Ezen túl sikeres pályázatunkat követően egyik kollégánk jelenleg nemzeti szakértőként dolgozik az EDPS hivatalában. Az ő tevékenységéről lentebb beszámolunk.

Ahogyan a magyar adatvédelmi törvény, úgy a közösségi intézmények adatkezelésére vonatkozó rendelet is ismeri az előzetes ellenőrzés intézményét. Az EDPS ezen a téren jelentős tapasztalatokat gyűjtött, ezért érdemes kitérni joggyakorlatára. Minden európai uniós szerv és egyéb intézmény köteles adatvédelmi felelőst kinevezni. Az adatvédelmi felelősök kulcsszerepet töltenek be az adatvédelmi szabályok adott szerven belüli végrehajtásában, illetve az adatvédelmi követelmények érvényesítésében. Szerepükből eredően az EDPS számára fontos szereplők, akik gyakran egy kisebb stáb segítségével látják el feladataikat. Az adatvédelmi felelősök belső nyilvántartást vezetnek minden olyan adatkezelésről, amelyet az őket kinevező szerv végez. Ezek közül azokat, amelyek a személyes adatok közösségi intézmények által történő feldolgozása tekintetében az egyének védelméről, valamint az ilyen adatok szabad áramlásáról szóló (45/2001/EK) rendelet szerint különös kockázatokat rejtenek, kötelesek előzetes ellenőrzés céljából az EDPS-hez bejelenteni. Ilyen különös kockázatot je-

lent például az egészségre vonatkozó adatok, bűnügyi adatok kezelése, vagy ha az adatkezelés egyének magatartásának értékeléséhez kapcsolódik.

A bejelentést követően két hónap áll az EDPS rendelkezésére, hogy a bejelentett adatkezelést megvizsgálja, és formális véleményben megfogalmazott állásfoglalást adjon ki. Az előzetes ellenőrzés során kiadott véleményben az EDPS részletesen elemzi az adatkezelés szempontjából lényeges tényeket, elemzi az adatmegőrzés, adatminőség követelményének feltételeit, megvizsgálja az érintett jogainak érvényesülését, azok esetleges korlátozásának jogszerűségét. Véleményének zárásaként összszefoglalja ajánlásait az adatkezeléssel összefüggésben, amelyeket az adatkezelőnek, illetve adatfeldolgozónak be kell építenie az adatkezelésébe. Ha ezeket az ajánlásokat az adatkezelő megvalósítja, abban az esetben az EDPS jogszerűnek ismeri el a bejelentett adatkezelést.

A kibocsátott vélemények túlnyomó többsége már megkezdett adatkezelési műveleteket vizsgál, ilyen értelemben ezek az ellenőrzések már nem előzetesek. Ez abból ered, hogy az európai adatvédelmi biztost csak 2003-ban választották meg, tényleges működését pedig 2004 elején kezdte meg. Az előzetesen ellenőrzendő adatkezelések pedig ekkor már folyamatban voltak, értelemszerűen „*előzetesen*" már nem lehetett elvégezni az ellenőrzéseket. Ez azonban nem jár azzal, hogy az EDPS ajánlásait az adatkezelők és adatfeldolgozók ne lennének kötelesek végrehajtani. A kibocsátott vélemények egyébként szinte kivétel nélkül érdemi garanciák beépítését, belső szabályok kiegészítését, esetleg megalkotását írják elő, amellyel az EDPS mintegy „*feltételekkel jóváhagyja*" az adatkezelést. 2006-ban azonban megszületett az első olyan európai adatvédelmi biztosi vélemény, amely az adatkezelést kiegészítő esetleges járulékos garanciák esetén sem látja jogszerűnek, ezért annak átfogó átalakítását tartja szükségesnek. Ez a vélemény az Európai Bizottság belső informatikai ügyfélszolgálatának gyakorlatát érintette, mely szerint minden telefonbeszélgetést rögzítenek. A válogatás nélküli rögzítés nem fogadható el adatvédelmi szempontból, ezért a rögzítés céljára tekintettel csupán egy szűk körű és rövid határidőre szóló rögzítés fogadható el.

Mint minden jogszabály, úgy adott esetben az Európai Unió jogszabályai is értelmezésre szorulnak. Leginkább akkor, ha a jogszabá-

lyokat egy különösen összetett kontextusban kell alkalmazni. Az EDPS azzal a céllal, hogy segítse a közösségi szervek munkáját, felvállalja, hogy egy-egy személyes adatok védelmével érintkező, kiemelt területre vonatkozó jogszabály rendelkezéseit a jogalkalmazás eredményeit is figyelembe véve elemzi. Ezek nem tekinthetők jogi iránymutatásoknak, hanem inkább az adatkezelők munkáját megkönnyítő, az értelmezésben támpontokat nyújtó elemzéseknek. Ilyen háttérdokumentumot adott ki az EDPS a közösségi szervek által kezelt dokumentumokhoz való hozzáférésről. Ezen túl előkészítés alatt áll több, a közeli jövőben kibocsátandó dokumentum is.

Az adatvédelmi vonatkozású uniós jogszabályok tervezetei kötelezően elküldendők az EDPS-hez véleményezésre. A véleményezett jogszabályok száma meghaladta a tízet, ezek közül az alábbiak külön is kiemelendők:

- A Vízuminformációs Rendszerhez (VIS) a tagállamok belső biztonságért felelős hatóságai, valamint az Europol számára a terrorcselekmények és egyéb súlyos bűncselekmények megelőzése, felderítése és kivizsgálása érdekében, konzultációs céllal történő hozzáférésről szóló tanácsi határozati javaslathoz kapcsolódó vélemény;
- A hozzáférhetőség elve alapján történő információcseréről szóló tanácsi kerethatározati javaslathoz kapcsolódó vélemény;
- A bűnügyi nyilvántartásból származó információk tagállamok közötti cseréjének megszervezéséről és azok tartalmáról szóló tanácsi kerethatározati javaslathoz kapcsolódó vélemény;
- A tartással kapcsolatos ügyekben a joghatóságról, az alkalmazandó jogról, a határozatok elismeréséről és végrehajtásáról, valamint az e területen folytatott együttműködésről szóló tanácsi rendeletre irányuló javaslathoz kapcsolódó vélemény;
- A harmadik államok polgárai részére kiadott tartózkodási engedélyek egységes formáját meghatározó tanácsi rendelet módosítására irányuló javaslathoz fűzött vélemény;
- A rendőrségi és igazságügyi együttműködés keretében kezelt adatok védelméről szóló tanácsi kerethatározati javaslathoz kapcsolódó vélemény.

A légi utasok adatainak Egyesült Államokba történő továbbításával kapcsolatos európai kifogások régóta megoldást sürgetnek, előrelépésről azonban annak ellenére nem lehet beszámolni, hogy 2006-ban a meglévő megállapodást az Európai Közösség Bíróságának azt megsemmisítő ítélete után újra kellett tárgyalni. Az EDPS csalódottságának adott hangot a Bíróság légi utasok adatainak Egyesült Államokba történő továbbítása ügyében hozott határozatával kapcsolatban. A luxemburgi bíróság előtt lefolytatott eljárásba az EDPS a felperes oldalán beavatkozott és szintén az Egyesült Államok és az Európai Unió között létrejött megállapodás hatályon kívül helyezése mellett érvelt. A Bíróság pusztán formális hiányosságokra (nem megfelelő jogalap) hivatkozással helyezte hatályon kívül a szóban forgó megállapodást. Ennek következményeként a légi utasok adatainak védelmét érdemben érintő kérdéseket nem részletezte az ítélet. Ez végeredményben pedig oda vezetett, hogy a megállapodás újratárgyalása során az utasok adatai védelmének szintjét illetően nem sikerült áttörést elérni (az ügy magyar vonatkozásával összefüggésben bővebben az adatvédelmi biztos jogalkotással kapcsolatos tevékenységéről szóló fejezetben olvashatnak).

Aktív szerepet játszott az EDPS az európai bankok nemzetközi elszámolásait intéző belga székhelyű cég, a Swift vitatott adatkezelésének ügyében is. A Swift nyilvántartási rendszere úgy épül fel, hogy az európai központtal párhuzamosan működik egy annak tökéletes tükörképét alkotó adatbázis az Egyesült Államokban is. A 2001. szeptember 11-i terrorista támadások után a terrorizmus elleni harc keretében arra utasították az amerikai hatóságok a Swiftet, hogy az európai nemzetközi tranzakciókat is tartalmazó amerikai adatbázist adják át nekik. Ezt a kérést a Swift kénytelen volt teljesíteni, elmulasztotta azonban ezt a tényt közölni az európai adatvédelmi hatóságokkal. Bár az Európai Központi Bank már évekkel korábban tudomást szerzett az adatátadásról, a tények csupán 2006 tavaszán váltak ismertté a közvélemény számára. Az EDPS támogatta a 29-es Munkacsoport Swifttel kapcsolatos véleményét, amely a saját állásfoglalásával lényegében megegyező megállapításokat tartalmaz. Ennek megfelelően mind az EDPS, mind a 29-es Munkacsoport elvárja a Swifttől és minden érintett szereplőtől, így a bankoktól is, hogy haladéktalanul olyan eljárásokat alakítsanak ki, amelyek segítségével az európai tranzakciókhoz

kötődő személyes adatok megfelelő védelemben részesülnek, és az európai adatvédelmi normákat súlyosan sértő adattovábbításra többé ne kerülhessen sor.

Amint arról már tavalyi beszámolónkban is említést tettünk, a magyar adatvédelmi hatóság munkatársa az első nemzeti szakértő, akit az EDPS foglalkoztat. A nemzeti szakértői program célja kettős. A nemzeti szakértő egyrészt segíti az EDPS munkáját a nemzeti hatóságnál szerzett tapasztalataival, másrészt pedig az EDPS mellett szerzett tapasztalatok a szakértő hazatérése után a magyar adatvédelmi biztos stábjának tudását gazdagítják. A 2007 júliusáig az EDPS mellett dolgozó szakértőnk feladata a felügyeleti tevékenységben való részvétel. Ez magában foglalja panaszügyek intézését, valamint az úgynevezett előzetes ellenőrzéseket, melyekre fentebb kitértünk.

EDPS honlapcíme: www.edps.europa.eu

IV. AZ ADATVÉDELMI NYILVÁNTARTÁS; A SZEMÉLYES ADATOK KEZELÉSÉVEL KAPCSOLATOS ELUTASÍTOTT KÉRELMEK ÉS A KÖZÉRDEKŰ ADATOK MEGISMERÉSÉRE IRÁNYULÓ ELUTASÍTOTT KÉRELMEK NYILVÁNTARTÁSA

A. Az adatvédelmi nyilvántartás

Az adatvédelmi biztos, összhangban a 95/46/EC Irányelvvel, a személyes adatok védelméről és a közérdekű adatok nyilvánosságáról szóló 1992. évi LXIII. törvény (a továbbiakban: Avtv.) 24. §-ának c) pontja alapján adatvédelmi nyilvántartást vezet.

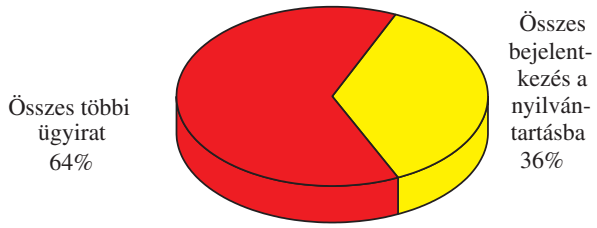
Az adatvédelmi nyilvántartás a személyes adatok kezelését végző szerveket (természetes és jogi személyeket, illetve jogi személyiség nélküli gazdasági társaságokat, szervezeteket) tartja nyilván. A nyilvántartás információt nyújt a Magyar Köztársaság területén személyes adattal végzett adatkezelésekről, arról, hogy ki, milyen célból, milyen személyes adatokat, mennyi ideig kezel, illetve arról is, hogy az általa kezelt személyes adatokat milyen forrásból gyűjtötte, illetve továbbítja-e más szerv vagy személy részére.

A nyilvántartás egyrészt az adatkezelések jogszerűségének ellenőrzésére szolgál, másrészt az érintettnek ad lehetőséget arra, hogy adatai kezeléséről tudomást szerezzen, különösen abban az esetben, ha információs önrendelkezési jogát közvetlenül nem gyakorolhatja.

Az adatvédelmi nyilvántartás deklaratív hatályú, adatai az adatkezelőt kötelezik. Az adatvédelmi biztos – bár a nyilvántartásba vételt nem tagadhatja meg – már a bejelentéssel egyidőben felléphet, ha a bejelentett adatkezelés nem felel meg a törvényes előírásoknak.

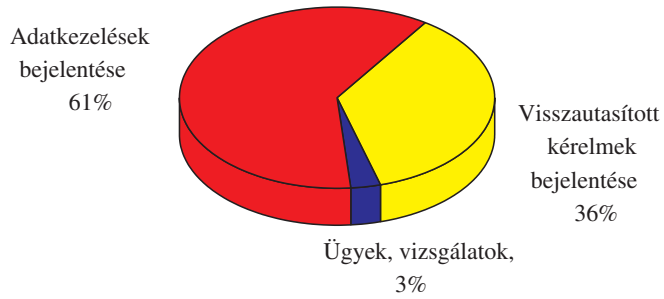
Az Avtv. 28. § (1) bekezdése rendelkezik az adatvédelmi nyilvántartásról. Az ebben a szakaszban meghatározott adatokat kell az adatkezelőnek, az adatkezelés megkezdése előtt – az Avtv. 30. §-ában meghatározott adatkezelések kivételével – bejelentenie.

Az ABI tevékenységi körében az adatvédelmi nyilvántartás helyzete
2006 (%)



Az adatvédelmi nyilvántartásba bárki betekinthet. A nyilvántartás a honlapunkról is elérhető.

Az ABI nyilvántartási tevékenységének megoszlása a beérkezett nyilvántartási ügyek alapján
2006 (%)



Az adatvédelmi nyilvántartásba történő bejelentések 2006. évi tapasztalatai

Az adatkezelők az adatvédelmi nyilvántartásba történő bejelentéseiket továbbra is elsősorban a honlapunkról letölthető adatlapon tették meg. Azon bejelentések esetében, amikor sokféle személyes adatnak bonyolult rendszerben történő kezeléséről van szó, célszerű az

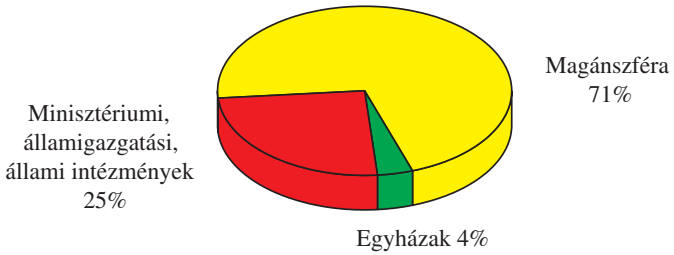
Avtv. 28. §-ában megjelölt adatoknak az adatlapon való bejelentése mellett még egy bővebb, az adatkezelés folyamatát is leíró magyarázatot mellékelni.

Bár az adatvédelmi biztosnak az Avtv. a nyilvántartásba vétel megtagadására nem ad jogszabályi felhatalmazást, azon bejelentések esetében, melyek hiányosak, felhívja az adatkezelőt a bejelentés kiegészítésére, módosítására. A bejelentés célja, hogy az érintettek tájékozódhassanak az egyes adatkezelések során kezelt személyes adataik útjáról, ami akkor lehetséges, ha a bejelentésből pontosan nyomon követhető, hogy mely természetes személyek, milyen személyes adatait konkrétan milyen szerv vagy személy, milyen célból és mennyi ideig kezeli. Tekintettel az adatkezelések sokféleségére az adatlap nem minden esetben nyújt a bejelentett adatkezelésről elegendő információt. A bejelentést ilyen esetekben az adatkezelés folyamatának leírásával, az adatvédelmi biztosnak címzett levélben is meg lehet tenni. Természetesen, ha egy adatkezelés nyilvánvalóan jogellenes, ennek megszüntetésére az adatkezelőt az adatvédelmi biztos haladéktalanul felhívhatja, így a nyilvántartásba bejegyzés mintegy *„okafogyottá válik”*.

Az adatvédelmi nyilvántartásba történő bejelentés egy jognyilatkozat, melyet az adatkezelő szerv vagy személy köteles megtenni, a jognyilatkozatra vonatkozó formai kritériumok megtartásával. A bejelentések feldolgozása során tapasztaljuk, hogy sok esetben nem az adatkezelő, hanem az adatfeldolgozással megbízott adatfeldolgozó végzi az adatkezelő részére a bejelentéssel kapcsolatos adminisztratív feladatokat. Ilyen esetben szükséges a bejelentéshez csatolni a Polgári Törvénykönyv, illetve a gazdasági társaságokról szóló törvény képviseletre vonatkozó szabályainak megfelelően a képviseleti jogosultságot igazoló okiratot (meghatalmazás, megbízás). Az adatvédelmi nyilvántartásba bejelentést – tekintve, hogy jognyilatkozatról van szó – az adatkezelő aláírásával kell ellátni. Bár az adatlapon erre vonatkozóan külön rubrika nincs megjelölve, az adatlap minden oldalának, illetve a kísérőlevélnek aláírásával kell a bejelentést hitelesíteni.

A bejelentést továbbra is – tekintettel arra, hogy az elektronikus aláírás fogadására a hivatalnak nincs módja – csak postai úton, vagy személyesen lehet megtenni.

Főbb adatkezelői kategóriák
(önkormányzatok nélkül) 2006 (%)



2006-ban az adatvédelmi nyilvántartásba bejelentést tevők száma és összetétele a korábbi évekhez hasonlóan alakult. Továbbra is elsősorban a marketing tevékenységet végző szervek éltek bejelentéssel a hivatalhoz, akár saját, akár megbízójuk nevében.

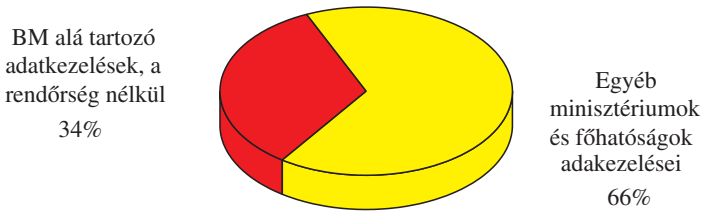
Az elmúlt évek tendenciájának megfelelően nőtt az interneten történő adatgyűjtések száma. Ez elsősorban az egyes weboldalakon történő regisztrációval, másrészt a különféle webáruházak elterjedésével, a vásárlási célú adatkezeléssel valósul meg.

Nem történt változás az adatvédelmi nyilvántartásba bejelentést tevők összetételében a tekintetben sem, hogy tovább csökkent az állami szférából érkező bejelentések száma. Az Avtv. 28. §-ának (2) bekezdése szerint a jogszabályban elrendelt adatkezeléseket a szabályozás tárgya szerint illetékes miniszter, országos hatáskörű szerv vezetője, illetőleg polgármester, főpolgármester, a megyei közgyűlés elnöke köteles bejelenteni a jogszabály hatálybalépését követő 15 napon belül.

Az elmúlt években a minisztériumok és az országos hatáskörű szervek kevés bejelentést teljesítettek annak ellenére, hogy jelentős adatkezelést is érintő jogszabály-módosítások történtek. Kivételt képez az adatvédelmi nyilvántartásba bejelentő állami szervek sorában a rendőrség, illetve a határőrség, melyek mind a központi szervekre, mind a helyi szervekre vonatkozó adatkezeléseket, illetve az adatkezelésekben bekövetkezett változásokat rendre bejelentik. E két fegyveres testületen kívül 2006-ban bejelentést tett még a Vám- és Pénzügyőrség Országos Parancsnoksága, a BM Rendvédelmi Szervek Védelmi Szolgálata, illetve az Állami Számvevőszék és az Országos Gyógyszerészeti Intézet. Láthatjuk, hogy a bejelentések mennyisége nem ará-

nyos a közszféra által végzett adatkezelések mennyiségével. Az időközben bekövetkezett jogszabályváltozások szükségessé tennék az adatvédelmi nyilvántartásnak az adatkezelők bejelentése alapján történő aktualizálását, frissítését, ami azonban a bejelentések elmulasztása miatt elmarad.

Minisztériumok és főhatóságok adatkezeléseinek megoszlása
2006 (%)



Tekintettel arra, hogy a közelmúltban, illetve előreláthatóan a közeljövőben is jelentős változások történnek a közszférában, szükségesnek látjuk felhívni a minisztériumok és az országos hatáskörű szervek vezetőinek figyelmét az Avtv. 28. §-ának (2) bekezdésében szabályozott bejelentési kötelezettségre. Az adatvédelmi nyilvántartásba be kell jelenteni a jogszabályváltozások következtében létrejövő új adatkezeléseket, valamint az egyes adatkezelések esetében az adatkezelő személyében történő változást, illetve természetesen azt is, ha az adatkezelő megnevezése megváltozik. Az Avtv. 29. §-ának (2) bekezdése alapján be kell jelenteni az adatvédelmi nyilvántartásba az adatkezelésben bekövetkezett minden olyan változást, amely a bejelentésben meghatározott adatkört érint. Így be kell jelenteni az adatkezelés céljában, a kezelt adatok fajtájában, az érintettek körében, az igénybevett adatfeldolgozó személyében történt változást, be kell jelenteni továbbá azt is, ha az adatkezelés alapjául szolgáló jogszabály, így az adatkezelés jogalapja változik meg.

A Magyar Köztársaság minisztériumainak felsorolásáról szóló törvénnyel és a központi államigazgatási szervekről, valamint a kormány tagjai és az államtitkárok jogállásáról szóló törvénnyel összefüggő egyes törvények módosításáról szóló törvény véleményezése során a igazságügyi és rendészeti miniszternek megküldött válaszle-

velünkben leírtuk, hogy az átszervezéseket követően a közigazgatási szervek működése nem lehet ellentétes az Avtv. szabályaival. Ezzel összhangban is felhívtuk a figyelmet közszféra átalakításából adódó bejelentési kötelezettségre.

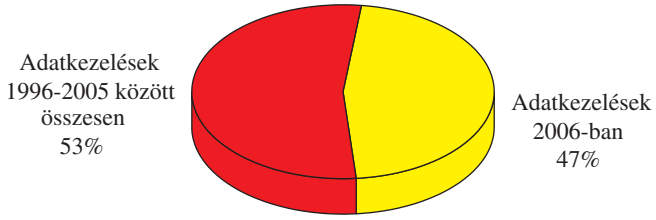
Aláírásgyűjtés célú adatkezelések bejelentése

A 2006-os év második felében az előző évekhez képest tovább növekedett az aláírásgyűjtések száma. A népszavazás, népi kezdeményezés célú aláírásgyűjtések esetében az Országos Választási Bizottság még az aláírásgyűjtő ívek hitelesítése előtt felhívja a népszavazás, népi kezdeményezés szervezőit az adatkezelés adatvédelmi nyilvántartásba történő bejelentésére. Ennek ellenére még mindig sok olyan petíciós célú aláírásgyűjtésről szerzünk tudomást, melynek adatvédelmi nyilvántartásba történő bejelentését az adatkezelő elmulasztotta.

Az aláírásgyűjtés során személyes adatok kezelése történik, melynek alapja az Alkotmányban meghatározott petíciós jog, illetve az országos népszavazásról és népi kezdeményezésről szóló 1998. évi III. törvény, valamint a helyi önkormányzatokról szóló 1990. évi LXV. törvényben szabályozott helyi népszavazás, népi kezdeményezés mint a népakarat kifejezésének közvetlen formája. Az aláírásgyűjtő ívek aláírása, illetve egyéb személyes adatok megadása önkéntes, így az adatkezelés jogalapja az érintett hozzájárulása.

Az aláírásgyűjtés során az aláírásgyűjtés kezdeményezői az aláírásgyűjtő ívet aláíró személyek személyes adatai tekintetében adatkezelőkké válnak. Népszavazás, népi kezdeményezés esetében az aláírásgyűjtés időszakában az adatkezelőt terhelő törvényi kötelezettségek teljesesítéséért az a természetes vagy jogi személy felel, aki vagy amely az Országos Választási Bizottságnál kezdeményezte a kérdés, illetve az aláírásgyűjtő ív hitelesítését. Felelőssége mindazon személyekért fennáll, akik az aláírásgyűjtés szervezésében részt vesznek, a kitöltött aláírásgyűjtő íveket birtokolják, tárolják.

Aláírásgyűjtéssel kapcsolatos adatkezelések száma
(%)



Az aláírásgyűjtés célú adatkezelést – függetlenül attól, hogy népszavazásról, népi kezdeményezésről, vagy petícióról van-e szó – az adatvédelmi nyilvántartásba be kell jelenteni. A bejelentés során meg kell jelölni, hogy ki az adatkezelő/aláírásokat gyűjtő szerv vagy személy, mi az adatkezelés/aláírásgyűjtés célja, milyen körben történik az aláírásgyűjtés/adtakezelés, mely szerv vagy személy részére történik az aláírásgyűjtő ívek továbbítása, illetve azt, hogy mennyi ideig történik az aláírások gyűjtése. A népszavazási kezdeményezéshez, népi kezdeményezés támogatásához kapcsolódó aláírásgyűjtés esetén a bejelentési kötelezettséget az Országos Választási Bizottság, illetve a helyi/területi választási iroda vezetője hitelesítő döntését követően – a jogorvoslatra nyitva álló 15 napos határidő kezdetén – célszerű teljesíteni. Ez esetben az aláírásgyűjtő ív hitelesítő záradékkal történő ellátása idejére az adatvédelmi nyilvántartási azonosító – a hitelesítő záradékkal való elláthatóságtól függő hatállyal – kiadható a kezdeményezők részére. Egyéb aláírásgyűjtés esetén az adatvédelmi nyilvántartásba történő bejelentkezést követően kezdhető meg ez a tevékenység.

Az adatvédelmi biztos álláspontja alapján az adatvédelmi nyilvántartási számot az aláírásgyűjtés helyszínén is jól látható formában megtekinthetővé kell tenni.

Interneten keresztül megvalósuló adatkezelések bejelentése

Modern világunkban az elektronikus háló egyre nagyobb szerephez jut az emberek mindennapi életében. Míg alig néhány évvel ezelőtt az internet használata elsősorban információszerzésre irányult, ma már interneten keresztül kommunikálunk, vásárolunk, ismerkedünk. Minél több időt töltünk a világhálón, minél több szolgáltatást

veszünk igénybe elektronikus úton, annál több személyes adatunk kerül fel a hálóra.

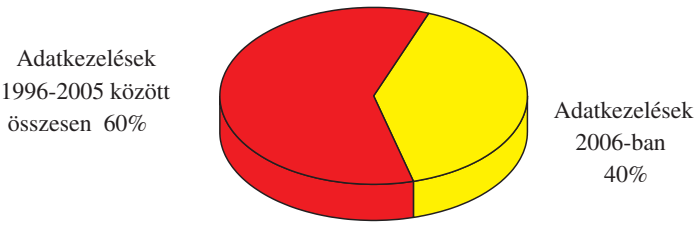
Ha az internetfelhasználóhoz kapcsolódó adatok (IP-cím, a felhasználó neve, e-mail címe stb.) természetes személlyel összekapcsolhatóak, illetve kapcsolatuk a természetes személlyel helyreállítható, akkor személyes adatnak minősülnek. Ezen személyes adatok kezelése adatkezelésnek minősül. Az interneten történő adatkezelés esetében mind a szerver üzemeltetője, mind a tartalom szolgáltatója adatkezelővé válhat. A személyes adatoknak a szerveren történő tárolása esetén az adatkezelő a szerver üzemeltetője. Ha azonban a felhasználó regisztrálja magát a weboldalon, a személyes adatok kezelője a tartalomszolgáltató.

Az internetes oldalakon történő regisztráció önkéntes. Az adatkezelés jogszerűségének feltétele azonban, hogy az adatkezelő a regisztráció helyén megfelelő tájékoztatást nyújtson arról, hogy kik, milyen célból, mennyi ideig kezelik a regisztrált személyes adatait. Az adatkezelőnek biztosítania kell továbbá, hogy az érintett bármikor, legalább olyan egyszerűen, mint ahogy a regisztrációra is sor került, „*leregisztrálhasson*", vagyis kérje személyes adatainak az adott oldalról történő törlését.

Felhívjuk az adatvédelmi nyilvántartásba bejelentést tevő internetes adatkezelők figyelmét az elektronikus kereskedelmi szolgáltatások, valamint az információs társadalommal összefüggő szolgáltatások egyes kérdéseiről szóló 2001. évi CVIII. törvény rendelkezéseire is, mely szerint kizárólag az igénybe vevő egyértelmű, előzetes hozzájárulásával küldhető elektronikus úton, levelezés során elektronikus hirdetés. Az elektronikus hirdető, az elektronikus hirdetési szolgáltató és az elektronikus hirdetés közzétevője köteles nyilvántartást vezetni azokról, akik számára bejelentették, hogy kívánnak elektronikus hirdetést kapni; nem küldhető elektronikus hirdetés annak, aki nem szerepel ebben a nyilvántartásban.

Az interneten keresztül – ahogy a bármilyen más módon – végzett adatgyűjtéseket, adatkezeléseket az adatvédelmi nyilvántartásba be kell jelenteni.

Internettel kapcsolatos adatkezelések száma
(%)



Az utóbbi időben megnövekedett a különféle közösségi portálok száma. Ezen közösségi portálok bejelentése során felhívtuk az üzemeltetők figyelmét arra, hogy tekintettel a portálon kezelt személyes adatok mennyiségére, különös figyelmet kell fordítani az érintettek egyértelmű és részletes tájékoztatására.

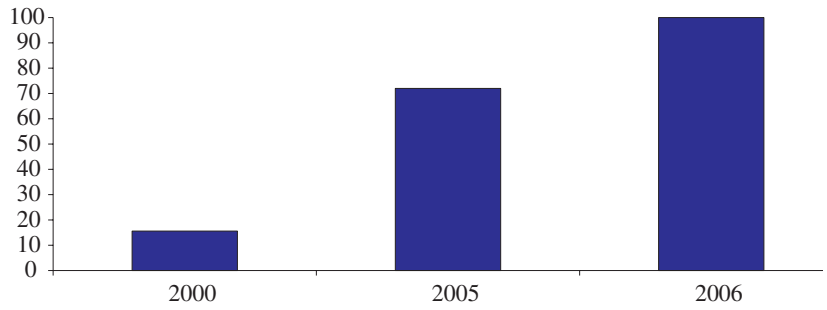
Továbbra is sok bejelentés érkezik az internetes áruházakat üzemeltető adatkezelők részéről. Webáruház üzemeltetése egyfajta szolgáltatás nyújtása az interneten, mely során személyes adatok gyűjtése, tárolása is történik. Az internetes áruházban történő vásárlással *„szokványos”*, a kereskedelmi forgalomban megvalósuló adásvétel jön létre. Ha a személyes adatok felhasználása csak a konkrét vásárlással összefüggésben történik, úgy mint például számlázás, az adatkezelést nem kell az adatvédelmi nyilvántartásba bejelenteni, mivel az az Avtv. 30. §-ának a) pontjában szabályozott ügyfélkapcsolatnak minősül. A szolgáltatás nyújtásához szükségszerűen nem kapcsolódó adatkezelést (például adatok tárolása reklámanyag továbbítása céljából), illetve az egyéb célú adatkezelést (például fórum) azonban az adatvédelmi nyilvántartásba be kell jelenteni.

Marketing, direkt marketing célból megvalósuló adatkezelések bejelentése

Több éve tapasztaljuk, hogy a reklám célú adatgyűjtéseket nagyrészt a piacon jelen lévő marketing tevékenységgel foglalkozó cégek végzik, többségében megbízási szerződés keretében. Ezek a cégek rengeteg promóciós adatgyűjtést, nyereményjátékot szerveznek a különböző termékeket és szolgáltatásokat megrendelő, használó személyek körének megkeresése érdekében. A marketinggel foglalkozó cégek – a

bejelentések nagy számára tekintettel – nagy gyakorlatot szereztek már az adatvédelmi nyilvántartás kérdésében, bejelentéseik nagy számban és rendszeresen érkeznek.

Bejelentkezett magánszféra (adatkezelők)
2000-2006 (%)



Az adatvédelmi nyilvántartásba bejelentési kötelezettsége az adatkezelőnek van. Mivel a megbízó – az a szerv, amely a reklámcéget azzal bízza meg, hogy részére akár promóciós, akár más céllal személyes adatokat gyűjtsön, rendszerezzen, kezeljen – határozza meg az adatkezelés célját, a célhoz kötöttség elvének értelmében adatkezelőnek minősül. Adatfeldolgozó ebben az esetben a megbízott szerv. A megbízott adatfeldolgozó a bejelentés ügyében csak az adatkezelő cég képviseletében, az adatkezelő által adott meghatalmazás, esetleg ilyen tárgyú megbízás birtokában járhat el.

Abban az esetben, ha a megbízás a promóció teljes lebonyolítására, az adatkezelés egészére vonatkozik, és a megbízó az adatokhoz nem fér hozzá, azokat semmilyen céllal nem kezeli, akkor a megbízó a szűken értelmezett adatkezelésben nem vesz részt. Ez esetben a megbízott adatkezelővé válik, az Avtv. 28. §-ának (1) bekezdése szerint ő lesz köteles az adatkezelést az adatvédelmi nyilvántartásba bejelenteni.

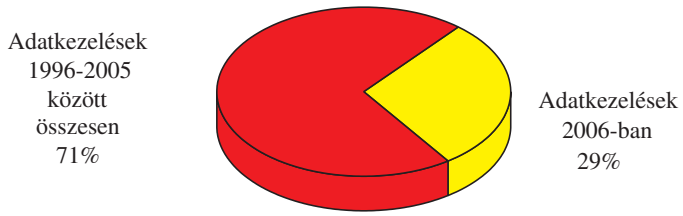
Továbbra is problémát okoz a kiskorú gyermekek személyes adatainak, illetve a direkt marketing levelekben megszólított személyek hozzátartozói, családtagjai személyes adatainak kezelése. Személyes adatával mindenki saját maga rendelkezhet érvényesen, a családtagok

személyes adatainak jogszerű kezeléséhez minden egyes családtag hozzájárulása szükséges. Az érintett adatkezeléshez való hozzájárulása egy jognyilatkozat, melyre a Polgári Törvénykönyvről szóló 1959. évi IV. törvény (a továbbiakban: Ptk.) rendelkezései irányadóak. A Ptk. szerint tizennegyedik életévét be nem töltött kiskorú (cselekvőképtelen) nevében a törvényes képviselője jár el, tizennegyedik életévét betöltött kiskorú (korlátozottan cselekvőképes) esetében pedig a kiskorú nyilatkozatának érvényességéhez – ha jogszabály kivételt nem tesz – törvényes képviselőjének beleegyezése vagy utólagos jóváhagyása szükséges. Bár a korlátozottan cselekvőképes kiskorú törvényes képviselőjének közreműködése nélkül is megkötheti a mindennapi élet szokásos szükségleteinek fedezése körébe tartozó kisebb jelentőségű szerződéseket, tehet jognyilatkozatot, mégis előfordulhatnak olyan visszás helyzetek, amikor a kiskorú olyan ügylethez adja személyes adatainak (például képmás) kezeléséhez való hozzájárulását, amely a mindennapi élet szokásos jogügyletein túlmutat. Az adatkezelő felelőssége, hogy jogszerűen kezelje a kiskorúak személyes adatit. Ez különösen az interneten keresztül történő adatkezelések során okoz nehézséget, mégis úgy gondoljuk, hogy a kiskorúak érdekeinek védelme érdekében az adatkezelő köteles – akár külön technikai módszer alkalmazásával is – biztosítani a személyes adatok kezeléséhez való hozzájárulás törvényességét.

Munkavállalók személyes adatai kezelésének bejelentése

Az adatkezelővel munkaviszonyban álló személyek adatait tartalmazó adatkezelést, az Avtv. 30. §-ának a) pontja alapján az adatvédelmi nyilvántartásba nem kell bejelenteni. A munkavállalók személyes adatainak kezelésével kapcsolatos kérdések elsősorban arra irányulnak, hogy szüksége-e az adatvédelmi biztosnak bejelentést tenni az esetben, ha a munkavállalók adatait a munkáltató más szervhez vagy külföldre továbbítja.

Munkavégzéssel kapcsolatos adatkezelések száma
(%)



A munkavállalók személyes adatainak továbbítását, mivel az adattovábbítás címzettje az adatok tekintetében adatkezelővé válik, az adatvédelmi nyilvántartásba be kell jelenteni. Szintén bejelentési kötelezettség alá esik a munkaviszonnyal közvetlenül össze nem függő adatgyűjtés, így például a külföldi munkavállalók vízumügyintézése, külföldi anyavállalathoz történő továbbítása vagy munkavállalói részvényprogramhoz kapcsolódó adatkezelés.

Kivételek az adatvédelemi nyilvántartásba történő bejelentési kötelezettség alól

A bejelentési kötelezettség alá nem eső adatkezelések – a jogalkotó szándéka szerint – azért mentesülnek ezen kötelezettség alól, mivel az adatkezelés célja egyrészt az érintett számára ismert, és az adatfelvétel közvetlenül tőle történik, másrészt célja az érintett személyes érdekén túlmutat, vagy ki sem kerül a személyes szférából. Egyes esetekben az adatkezelés szorosan kötődik a jogi személyek működéséhez, és a személyes adatok kezelése az érintettel fennálló jogviszonyhoz vagy szolgáltatáshoz kapcsolódik, más esetekben a személyes adatok kezelése közérdeket szolgál, vagy a cél teljesüléséhez a személyes jelleg megőrzésére csak az adatkezelés meghatározott szakaszában van szükség. A törvényi kivételek között említett esetekben is be kell jelenteni az adatkezelést az adatvédelmi nyilvántartásba, ha az adatokat az adatkezelő más személy vagy szerv részére hozzáférhetővé teszi, nyilvánosságra hozza, vagy egyébként az eredetitől eltérő célra használja fel.

Nem kell bejelenteni az adatvédelmi nyilvántartásba azt az adatkezelést, amely az adatkezelővel

- munkaviszonyban,
- tagsági,
- tanulói viszonyban,
- ügyfélkapcsolatban álló személyek személyes adatait tartalmazza.

Az a) pontban felsorolt kivételek esetében az adatkezelő és az érintett között valamilyen, többségében szerződéses jogiszony áll fenn. Ezekben az esetekben a felek a szerződésben, illetve a jogviszonyra vonatkozó jogszabályban (például közoktatás) a jogviszony jellegéből fakadó elemek mellett a kezelt adatok körét is meghatározzák. Nincs szükség az adatkezelés bejelentésére, mivel az érintett önként, szerződési szabadságával élve maga kezdeményezi az adatkezelővel létrehozandó jogviszonyt.

Az iroda gyakorlata szerint az ügyfélkapcsolat – mint a bejelentési kötelezettség alóli kivétel – akkor áll fenn, ha az adatkezelés az adatkezelő és az érintett között fennálló jogviszony szükségszerű eleme. Tipikusan ilyen például a biztosító és a biztosított, a bank és „*ügyfele*" közti viszony. Ügyfélkapcsolatnak minősülhet az olyan jogviszony is, amely – bár tényleg adásvételt jelent – nem testesül meg egy klasszikus értelemben vett szerződés formájában. Ilyen például az internetes áruházakban történő vásárláshoz kapcsolódó adatkezelés. A szolgáltatás nyújtásához szükségszerűen nem kapcsolódó adatkezelést (például adatok tárolása reklámanyag továbbítása céljából), illetve az egyéb célú adatkezelést (például fórum) azonban az adatvédelmi nyilvántartásba be kell jelenteni.

Kérdés merült fel az Avtv. 30. §-ának b) pontjában szabályozott kivétellel kapcsolatban is. Nem kell bejelenteni az adatvédelmi nyilvántartásba azt az adatkezelést, amely egyház, vallásfelekezet, vallási közösség belső szabályai szerint történik. Nem kell tehát bejelenteni az olyan adatkezeléseket, amelyet az egyház, vallásfelekezet például tagjairól, a tagok által az egyházban betöltött funkcióiról vezet. Mivel nem az egyház belső szabályait érinti, be kell azonban jelenteni a támogatókról, adományozókról vezetett nyilvántartást.

Az adatvédelmi nyilvántartásba történő bejelentés alól mentesülő adatkezelések közül még problémát okoz az Avtv. 30. §-ának j) pontjában szabályozott, a természetes személy saját célját szolgáló adatkezelés értelmezése. E tekintetben megszorítóan kell értelmezni a törvényt. Csak olyan adatkezelés minősül a természetes személy saját

célját szolgáló adatkezelésnek, amely során az érintettek tudtával kerülnek személyes adatok az adatot kezelő birtokába, azokat az adatbirtokos csak magáncélra kezelheti.

Belső adatvédelmi felelősök bejelentése

Az Avtv. 2004. január 1-jén hatályba lépett módosítását követően a *„nagy"* adatkezelők jórészt eleget tettek törvényi kötelezettségüknek, és kijelölték az adatvédelmi feladatok koordinálásával, ellenőrzésével megbízott adatvédelmi felelősöket. Ezek az adatkezelők az adatvédelmi felelősöket az adatvédelmi nyilvántartásba is bejelentették. A kezdeti dömpinget követően már kevés szerv jelentette belső adatvédelmi felelős kinevezését, a korábban bejelentést tevő szervek azonban rendszeresen bejelentik az adatvédelmi felelős személyében bekövetkező változásokat. Tekintettel azonban arra, hogy nincs adatunk arról, hány olyan szerv működik Magyarországon, melyben az adatvédelmi felelős kinevezése kötelező, arra nézve sincs pontos adatunk, hogy mely szervek mulasztották el bejelentési kötelezettségüket.

Az adatvédelmi nyilvántartás tartalmi összetétele

Minisztériumi, államigazgatási, állami intézmények mint adatkezelők:	415
adatkezeléseik:	1.309
A magánszférába tartozó adatkezelők:	1.176
adatkezeléseik:	2.840
Önkormányzatok mint adatkezelők:	3.161
Egyházak mint adatkezelők:	63
adatkezeléseik:	72

Az Adatvédelmi Biztos Irodája informatikai rendszerének állapota és fejlesztése

Az adatvédelmi biztos megújított honlapja

Az elkészített és jóváhagyott rendszerterv és programtervek alapján a 2005. év végére a fejlesztési, programtechnológiai munkák befejeződtek, és 2006. január 2-ával egy megújult multimédiás honlap jelentkezett a http://abiweb.obh.hu/abi/ címen mint az adatvédelmi biztos honlapja.

A honlap előző megjelenési formájában 2004. március 1-jétől került bevezetésre és üzemeltetésre.

Ebben a formájában 2005. december 31-ig 70.390 látogatót fogadott.

A honlapon található adatvédelmi és közérdekű információs tartalmat tekintve eleget tett a vele szemben támasztott követelményeknek. Megjelenése azonban már nem tükrözte az egyre népszerűbb, napjainkra gyakorlatilag elvárt multimédiás megjelenítési formákat.

A régi honlapon a hangsúly egyértelműen a megjelenített írásos anyagok tartalmi relevanciáján volt és nem az egyes oldalak vizuális megjelenítésén.

Az elektronikus információs kultúra terjedése és változása, ahhoz vezetett, hogy a tervezők próbálják jobban érthetőbbé, látványosabbá és áttekinthetőbbé tenni honlapjuk mondanivalóját vizuális hatások segítségével.

Az új honlap rendszertervének kidolgozása során a Nyilvántartási Főosztály informatikai fejlesztő munkatársai nagy figyelmet szenteltek a rendszerrel szemben támasztott felhasználói elvárások összegzésének, hiszen a honlap iránt érdeklődők széles társadalmi körből kerülhetnek ki, mivel a biztoshoz minden olyan magán- vagy jogi személy fordulhat, aki Magyarország területén tartózkodik. Törekedtünk arra, hogy az olvasható információkat, ahol csak lehet, egészítsék ki vizuális (grafikus és/vagy animációs) elemek.

Úgy gondoljuk, sikerült elérni, hogy a honlap navigációja egyértelmű, megjelenése egységes legyen, ezt segítse az animációs elemekből épülő menüs megjelenés.

Lehetővé tettük, hogy a honlap egyes főbb fejezeteiben és a főmenü pontjaiban részenkénti, valamint az egészében összetett keresést is lehessen végezni.

Az új multimédiás honlap szerkezetében is alkalmazkodik a társadalom egyes rétegeiben a személyes adatok védelme, valamint a közérdekű adatok nyilvánossága iránt megnyilvánuló különböző mélységű érdeklődés eltérő szintű kiváltásának lehetőségéhez.

Az új multimédiás honlap bejelentkező (főoldal) oldalát az alábbi ábra mutatja:


Adatvédelmi Biztos
English Site
Főoldal | Aktuális információk | Tájékoztató | GYIK | Adatvédelmi nyilvántartás | Nemzetközi kitekintés | Sajtófigyelő |
Éves parlamenti beszámolók | Törvények, jogszabályok | Linkek | Rendezvények | Publikációk | Elektronikus információszabadság oldalak |
Visszatérő jelenségekkel kapcsolatos álláspont:
Egészségügy - Kórházlista, betegazonosító, HIV szűrés
Ügynökügy
Kamerázás
Választás, aláírásgyűjtés
Köztisztviselők, önkormányzati tisztségviselők személyes adatai
Internet
Igazolvány másolás
Munkaügy
A biztos ügyforgalmára vonatkozó adatok:
a) adatvédelmi ügyek
b) információ szabadság ügyek
c) nemzetközi ügyek
d) adatvédelmi nyilvántartás ügyek
e) jogszabály véleményezés
f) a biztos vezetői tevékenységével kapcsolatos ügyek
Véleményezett jogszabály tervezetek listája
Részletek...
Az Adatvédelmi Nyilvántartás jellemzői
Részletek...
A nemzetközi adatvédelmi együttműködés adatai
Részletek...
TÍZÉVES AZ OMBUDSMANTÖRVÉNY
Az adatvédelmi biztos köszönti
a honlap látogatóit.
Leállítás
Elérhetőségeink
Magunkról
Gyakran Intézett Kérdések
1992. évi LXIII. tv
Ismerkedés az adatvédelemmel
Közérdekű információk
Hol tarthatják Önt nyilván?
Ajánlások, állásfoglalások, közlemények:
Az adatvédelmi biztos ajánlása a közfeladatot ellátó személyek feladatkörével összefüggő személyes adatai nyilvánosságára vonatkozó jogszabályok összhangjának megteremtéséről
2006-10-30
Nagy érdeklődést keltő ügyek:
Keresés
Keresendő kifejezés:
Keresés helye:
Teljes honlap
Keresés
Súgó
Hírek
Gregorik László zavargásokról
feldolgozva
IWIW, a legnagyobb internetes közösségi hálózat, egyben "önkéntes kémprogram" is
személyes adat
IWIW, a legnagyobb internetes közösségi
AZ OMBUDSMANOK TÍZ ÉVE
TEN YEARS OF THE OMBUDSMEN
1995-2005
MAGYAR KÖZLÖNY
1997/106. szám Az Adatvédelmi Biztos közleménye
2005/1 . szám Az Adatvédelmi Biztos közlemé-

A honlap középső részét animált menüs választás lehetősége tölti ki, amely az átlagos állampolgár érdeklődését kívánja felkelteni a személyes adatok védelméhez, valamint a közérdekű adatok nyilvánosságához fűződő alkotmányos alapjogok érvényesülése terén.

A grafikus menü az alábbi ábrán található:

Ez az animált menüs rész látványos, animációs és multiplikációs módon segíti a nem professzionális adatvédelmi szakembereket abban, hogyan fordulhat az adatvédelmi biztoshoz személyesen, levélben, telefonon, faxon, e-mail-ben (Elérhetőségeink, Magunkról).

Érdekes multiplikációs effektusokkal világítja meg a biztoshoz leggyakrabban intézett kérdésekre adott válaszokat (Gyakran Intézett Kérdések).

Kedves, animációs kvízjátékkal segíti az érdeklődőket tájékozottságuk ellenőrzésében a személyes adatok védelme, valamint a közérdekű adatok nyilvánossága által felvetett kérdéskörökben (Ismerkedés az adatvédelemmel).

Felvilágosítást ad az érdeklődőknek a közérdekű adatok megismerésére irányuló igények teljesítésének rendjéről az Adatvédelmi Biztos Irodáján (Közérdekű információk).

Kalauzolja a polgárokat a személyes nyilvántartások világába, amiről az adatvédelmi nyilvántartás nyújt képet (Hol tarthatják Önt nyilván?).

A honlap horizontális főmenüje – amelyet a következő ábra mutat – már inkább a professzionálisabb tájékozottsággal bíró látogatók érdeklődésére számíthat.

Néhányat kiemelnénk a széleskörű választékból:

A látogató rendkívül hasznos információkhoz juthat az adatvédelmi biztos ajánlásaiból, állásfoglalásaiból, közleményeiből, valamint a vizsgált és a honlapra kihelyezett nagy érdeklődést keltő ügyekből (Aktuális információk).

Részletesen áttekintheti az adatvédelmi biztosok eddigi tevékenységét, amiről ők a parlamentben számoltak be (Éves parlamenti beszámolók).

A biztos nemzetközi együttműködés keretében végzett tevékenységéről, a 29-es Adatvédelmi Munkacsoportról, az uniós adatvédelemről, a schengeni csatlakozásból a biztosra háruló feladatokról, a nemzetközi jogalkotásról a (Nemzetközi kitekintés) menüpont ad tájékoztatót.

Az adatvédelem kérdéseinek, az adatvédelmi biztos tevékenységének a médiában történő tükröződéséről a (Sajtófigyelő) és ennek archívuma ad számot, napjainktól 2004. március 1-ig.

Az 1992. évi LXIII. törvény (Avtv.) 24. § c) pontja szerint az adatvédelmi biztos gondoskodik az adatvédelmi nyilvántartás vezetéséről.

Ezt tükrözi az (Adatvédelmi nyilvántartás) főmenüpont, amely az érdeklődő és/vagy érintett állampolgárok részére ad felvilágosítást arról, hogy milyen adatkezelők, mely személyes adatukat, milyen célból kezelik. A bejelentésre kötelezetteknek pedig útmutatókkal, segédletekkel nyújt támaszt kötelezettségük teljesítéséhez.

Az elektronikus információszabadságról szóló 2005. évi XC. törvény (a továbbiakban: Eitv.) támasztotta követelményeknek való megfeleltetés során az új honlapon új főmenüpont került bevezetésre, az (Elektronikus információszabadság oldalak).

Ez a pont további almenükre bomlik: Általános közzétételi lista, Egyedi közzétételi lista, Közérdekű adat igénylése, Szabályzat a közérdekű adat igénylés teljesítéséről megnevezéssel.

Az Eitv. végrehajtásának előkészítési munkálatai során a Nyilvántartási Főosztály szakértői az új honlapon lehívható, interaktív kitöltést biztosító közérdekű adat igénylő űrlapot fejlesztettek ki. Ezen az elektronikus űrlapon a közérdekű adat iránti igény az Adatvédelmi Biztos Irodája honlapján keresztül (http://abiweb.obh.hu/abi/, www.obh.hu – Adatvédelmi Biztos) benyújtható.

Az Adatvédelmi Biztos Irodáján a közérdekű adatok megismerésére irányuló igények teljesítésének rendjét előíró szabályzatban foglalt rendelkezések alapján a Nyilvántartási Főosztály továbbra is gondoskodik az Adatvédelmi Biztos Irodája szervezeti egységeitől kapott összes közzéteendő adatnak a honlapon történő megjelentetéséről, az adatigénylések fogadásáról és ennek folytonosságáról, a főosztályt érintő adatigénylésekre adandó válaszok előkészítéséről. Ezután is biztosítja közérdekű adatigénylésekről a statisztikai adatgyűjtést, jelentések és a parlamenti beszámolóhoz szükséges kimutatások készítését, az egyedi közzétételi listán szereplő, a főosztály feladatkörébe sorolt adatok előállítását, közzétételre előkészítését, valamint lehetővé teszi a közérdekű adat igénylésnek minősülő beadványoknak az intranetes iktatási rendszerbe történő regisztrációját.

A külföldről érdeklődő, a magyar nyelvet nem beszélő személyek a honlap angol változatát látogathatják, amelynek más a megjelenési formája, és tartalmi összetevői sem egyeznek meg a magyar változat oldalaival.

Az új honlap látogatottsága 2006-ban

Az elektronikus ügyintézés mind nagyobb és szélesebb körű szerepet tölt be a magyar államigazgatási ügyintézésben, így az Adatvédelmi Biztos Irodájának honlapja is egyre fontosabb szerephez jut úgy az érdeklődők, mint az adatkezelések érintettjei információs önrendelkezési jogainak védelmében és érvényesítésében.

Az adatkezelők adatvédelmi nyilvántartási bejelentkezési kötelezettségeinek teljesítése érdekében is a biztos honlapját használják mind a letölthető útmutató anyagok, mind a kitöltendő űrlapok lehívása tekintetében.

Ez megmutatkozik a honlap látogatottságában is. Míg az előző megjelenésű honlap iránt 2004. március 1. és 2005. december 31. közötti 22 hónap alatt 70.390 alkalommal érdeklődtek, addig az új tervezésű adatvédelmi biztosi honlapot a 2006. év folyamán, 12 hónap alatt 80.440-en látogatták meg.

Informatikai korszerűsítések

Az elhasználódott számítástechnikai eszközök cseréjének szükségességére, arra, hogy ez az elkerülhetetlen beruházás az adatvédelmi nyilvántartás, illetve az iktatási rendszer szolgáltatása biztonságának érdekében halaszthatatlanná vált, már előző évi beszámolókban felhívtuk a figyelmet.

Annak ellenére, hogy a szükséges berendezések nagyobb része beszerzésre került, a megújulást biztosító, az új hardware-re és operációs rendszerre való áttérést lehetővé tevő adatbázis-kezelő szoftver beszerzése 2006 végéig anyagi eszközök hiányában meghiúsult. 2006 végén a szükséges programrendszer megrendelésre került, beérkezése 2007 első félévében várható.

A beérkezés után lehetséges csak a szoftvermigrációs fejlesztések végzése, így ennek következtében továbbra is a 10 éve üzembe helyezett MicroVAX szerverről történik az adatvédelmi nyilvántartás szolgáltatása.

B. A személyes adatok kezelésével kapcsolatos elutasított kérelmek és a közérdekű adatok megismerésére irányuló elutasított kérelmek bejelentése

Az adatvédelmi biztos 2006-ban a Magyar Közlöny 158. számában megjelent felhívásában hívta fel az adatkezelők figyelmét a személyes adatok kezelésével kapcsolatos elutasított kérelmek és a közérdekű adatok megismerésére irányuló elutasított kérelmek bejelentésére.

Az érintett az adatkezelőtől tájékoztatást kérhet személyes adatai kezeléséről. A tájékoztatást az adatkezelő köteles a kérelem benyújtásától számított legrövidebb idő alatt, legfeljebb azonban 30 napon belül írásban megadni. Az érintett tájékoztatását az adatkezelő csak a törvényben szabályozott esetekben tagadhatja meg. A tájékoztatás megtagadás esetén az adatkezelő köteles az adatvédelmi biztost – évente – az elutasítás tényéről és az elutasítás indokáról tájékoztatni.

Közérdekű adat megismerése iránt bárki igényt nyújthat be. A közérdekű adat megismerésére irányuló igénynek az igény tudomására jutását követő legrövidebb idő alatt, legfeljebb azonban 15 napon belül kell eleget tennie az adatkezelőnek. Az igény teljesítésének megtagadásáról, annak indokaival együtt, 8 napon belül értesíteni kell az igénylőt. A közérdekű adatot kezelő szerv ezen kívül köteles az elutasított igényekről évente értesíteni az adatvédelmi biztost.

Személyes adat iránti kérelmek elutasítását minden adatkezelőnek, közérdekű adat iránti kérelmek elutasítását pedig a közfeladatot ellátó szerveknek kell bejelenteniük. A korábbi felhívásokban is felkértük az adatkezelőket – annak ellenére, hogy a törvény ilyen kötelezést nem tartalmaz –, hogy a teljesített kérelmekről is adjanak tájékoztatást, hiszen ennek ismeretében kísérhető figyelemmel az információszabadság alkotmányos jogának érvényesülése. A személyes adatok kezelésével kapcsolatos elutasított kérelmek esetében a törvény csak az érintett felé ír elő indoklási kötelezettséget, az adatvédelmi biztos felé nem. A közérdekű adatokra vonatkozó kérelmek elutasítása esetében ezzel szemben a törvény előírja, hogy az érintett írásbeli tájékoztatásán túl az adatkezelő köteles az éves jelentésében az adatvédelmi biztost értesíteni az elutasított kérelmekről és annak in-

dokairól. A részben teljesített kérelmek esetében is fennáll a jelentési kötelezettség a részben elutasított kérelemre, illetve annak indokára nézve.

Az elutasított kérelmek bejelentésére külön formanyomtatvány nincs. Az Avtv. rendelkezéseinek értelmében statisztikai adatokat kell az adatvédelmi biztosnak jelenteni, vagyis azt, hogy az elmúlt évben hány személyes adat iránti kérelem érkezett az adott adatkezelőhöz, és ebből mennyit utasítottak el; illetve, hogy hány közérdekű adat iránti kérelem érkezett az adott szervhez, és ebből mennyit utasítottak el, illetve mi volt az elutasítás indoka. Sajnos az évről évre ismétlődő felhívások ellenére még mindig kevés és azon belül is sok pontatlan jelentés érkezik.

Személyes adatok kezelésével kapcsolatos elutasított kérelmek nyilvántartása

2006-ban összesen 212.871 személyes adat iránti kérelmet nyújtottak be 446 különböző adatkezelőhöz, ebből 422 személyes adat iránti kérelmet utasítottak el.

	2004	2005	2006
Jelentést küldők száma	496	498	446
Személyes adat iránti kérelem	276.612	315.818	212.871
Elutasított kérelmek	435	168	422

2006-ban 221 önkormányzati szervhez összesen 49.925 személyes adat iránti kérelmet nyújtottak be, ebből 143 kérelmet utasítottak el.

198 különböző állami szervhez 2006-ban összesen 150.814 személyes adatok iránti kérelmet nyújtottak be, ebből 276 kérelmet utasítottak el.

2006-ban a privát szférából 27 társaság jelentett adatkérést az adatvédelmi biztos számára, összesen 12.132 személyes adat iránti kérelmet, ebből 3 kérelmet utasítottak el.

Nem növekedett a bejelentést tevők száma az idei évben sem. Összesen 27 magán adatkezelő tett jelentést személyes adat kezelésével kapcsolatos kérelemről. Látjuk, hogy ez az adat, tekintve a civil szférában megvalósuló adatkezeléseket, még mindig nagyon kevés. Tovább növekedett azonban az állami adatkezelők részéről érkező bejelentések száma.

A személyes adatok kezelésével kapcsolatos kérelmek elutasításának leggyakoribb indoka az illetékesség hiánya. Sok elutasítás történt azért, mert nem jogosulttól származott a kérelem, illetve mert az adat a megkeresett adatkezelőnél nem található. Néhány szerv esetében továbbra is elutasítási indokként szerepel a nemzetbiztonsági ok, illetve a bűnüldözési ok.

Közérdekű adatok megismerésére irányuló elutasított kérelmek nyilvántartása

2006-ban összesen 183.959 közérdekű adat megismerésére irányuló kérelmet jelentett be 442 adatkezelő, ebből 466 kérelmet utasítottak el.

	2004	2005	2006
Jelentést küldők száma	495	498	442
Közérdekű adatok megismerésére irányuló kérelmek	50.271	129.984	183.959
Elutasított kérelmek	41	25	466

218 önkormányzati szervhez 2006-ban összesen 6.573 közérdekű adat megismerésére irányuló kérelmet nyújtottak be, ebből 218 kérelmet utasítottak el.

197 különböző állami szervhez 2006-ban összesen 177.144 közérdekű adat megismerésére irányuló kérelmet nyújtottak be, ebből 248 kérelmet utasítottak el.

Nem növekedett a közérdekű adatok megismerésére irányuló kérelmek jelentőinek száma sem. Emellett azonban tovább növekedett a közérdekű adat iránti kérelmet beterjesztők száma, ami az állampolgárok információs önrendelkezési jogának tudatosulását jelzi, azonban a tavalyi évhez képest az elutasítások száma is nőtt.

Közérdekű adat iránti kérelmek tekintetében elutasítási indokként szerepelt, hogy a kért adat üzleti titok; egy esetben történt személyes adatra való hivatkozás. Több elutasítás történt azért, mivel a kért adat belső használatra készült, vagy döntés-előkészítéssel összefüggő adat.

Az elutasított kérelmek bejelentésére vonatkozó kötelezettségnek – az évről évre megismétlődő felhívások ellenére is – csak az adatkezelők egy része, jellemzően ugyanazon része tesz eleget. Még mindig

nagyon kevés jelentés érkezik a magán adatkezelőktől, annak ellenére, hogy a személyes adatok védelmével kapcsolatos, illetve a közérdekű adatok nyilvánosságával kapcsolatos tájékozottság – tapasztalataink szerint – egyre szélesebb körű. Bízunk benne, hogy a bejelentések elmulasztása ellenére az állampolgárok a legtöbb adatkezelő szervnél ma már kimerítő tájékoztatást kapnak személyes adataik, illetve a közérdekű adatok kezeléséről.

V. AZ ADATVÉDELMI BIZTOS IRODÁJA

Az állampolgárok adatvédelemmel és információszabadsággal kapcsolatos ismereteinek növelése

Az adatvédelmi biztos ebben az évben is élt azzal a lehetőséggel, hogy munkatársaival megjelenjen a Sziget Fesztivál Civil Szigetén, ahol kifejthette tájékoztató, ismeretterjesztő, figyelemfelhívó tevékenységét, illetve a nagy érdeklődést kiváltó ügyek ismertetése mellett hivatalának elérhetőségei is széles körben nyilvánosságot kaptak. A program megszervezésére és eredményes megvalósítására idén is annak köszönhetően került sor, hogy a Sziget Szervező Irodája benyújtott pályázatunkat pozitív elbírálásban részesítette.

Az elmúlt évek gyakorlatának megfelelően az adatvédelmi biztos a további három országgyűlési biztossal együtt jelent meg a Sziget Fesztiválon 2006. augusztus 9-15. között. A közösen megvalósított programok gerincét az előadások, beszélgetések, fórumok adták, ahol részt vettek az adott napi téma jeles képviselői, szakemberei is. Beszélgetéseket az alábbi témákban tartottunk: Adatok a hálóban, azaz a személyes adatok védelme az interneten; Elismertség, siker – roma fiatalként; A vallásgyakorlás szabadsága az országgyűlési biztosok gyakorlatában; A bűncselekmények áldozatainak védelme egy jogász és egy lélekgyógyász szemével; „*Zenész a pályán*" – beszélgetés Földes László „*Hobo*"-val. Igyekeztünk olyan témaköröket választani, amelyek szélesebb érdeklődésre tarthattak igényt, illetve amelyek a Szigetlakókat érinthették.

Állandó programként kínáltuk az érdeklődők számára a változatos adatvédelmi, emberi jogi, kisebbségi jogi totók kitöltését, melyet szerény anyagi lehetőségeinkhez mérten megpróbáltunk ajándékkal jutalmazni. A totók elsődleges célja a kérdésekből és a válaszokból szerzett ismeretek növelése, illetve a tájékoztatás volt. A Civil Szigeten részt vett valamennyi munkatársunk több idegen nyelven tudott segíteni az érdeklődő külföldieknek, részükre a totók angol nyelvű verzióját ajánlottuk.

Tájékoztatást nyújtottunk tevékenységünkről, az állampolgárok alkotmányos jogairól, jogérvényesítésük lehetőségeiről, módjáról. Az

érintetteknek lehetőségük volt a helyszínen panasz benyújtására és személyes konzultációra.

Az OBH sátrában a Sziget-lakók nyitástól zárásig folyamatosan érdeklődtek. A kitöltött (természetesen anonim) tesztek mennyiségéből és az informatív beszélgetésekből arra lehet következtetni, hogy a résztvevők alkotmányos jogaikkal többé-kevésbé tisztában vannak, a gyakorlati megoldások kapcsán sokszor részletesebb információt kértek, illetve jelentékeny számban előfordultak olyanok, akik például az adatvédelemről itt a Szigeten hallottak először. Az adatvédelmi biztos és munkatársai Civil Szigeten való részvételét és tájékoztató tevékenységét sikeresnek ítélem.

A 2005. évi beszámoló parlamenti fogadtatása

Az adatvédelmi biztos 2005. évi tevékenységéről szóló beszámolót a Magyar Köztársaság Országgyűlése 2006. december 18-ai ülésnapján 355 igen, 2 nem szavazattal, 1 tartózkodás mellett elfogadta.

Az iroda szervezete és gazdálkodása

Az Adatvédelmi Biztos Irodájánál – a 2006. december 31-i állapot szerint – 45 főállású és 2 mellékfoglalkozású munkatárs dolgozik. Betöltetlen álláshely nincs. Az alábbiakban a 2006. év kiadásait mutatjuk be a hivatal egészére vonatkozó beruházási kiadások, üzemeltetési költségek és áfa nélkül. A közölt összegek ezer forintban értendők.

Adatvédelmi Biztos Irodájának 2006. évi közvetlen működési kiadásai

Személyi kiadások:	
Illetmények	195.731
Jutalom	19.050
Jubileumi jutalom	3.131
Napidíj	1.630
Megbízási díj	2.920
Egyéb juttatások	13.015
Személyi kiadások összesen:	**235.477**
Munkáltatót terhelő járulékok	**74.656**
Dologi kiadások:	
Adatvédelmi biztosok áprilisi konferenciája	15.542
Külföldi kiküldetés	7.021
Reprezentáció	720
Készletbeszerzés, telefon, gk. üzemeltetés	3.801
Nyomda	2.821
Fordítás, lektorálás, megbízás	1.992
Áfa és egyéb kiadások	6.467
Dologi kiadások összesen:	**38.364**
Összes kiadás*:	**348.497**

*Az összes kiadás nem tartalmazza az Adatvédelmi Iroda rezsi-, üzemeltetési és beruházási kiadásait, azok az országgyűlési biztosok közös hivatalának kiadásaiban jelennek meg.

A beszámolóban előforduló törvények jegyzéke

- a személyes adatok védelméről és a közérdekű adatok nyilvánosságáról szóló 1992. évi LXIII. törvény: *Avtv., adatvédelmi törvény*
- a bűnügyi nyilvántartásról és a hatósági erkölcsi bizonyítványról szóló 1999. évi LXXXV. törvény: *Bnyt.*
- a büntetőeljárásról szóló 1998. évi XIX. törvény: *Be.*
- a szabálysértésekről szóló 1999. évi LXIX. törvény: *Szabstv.*
- a polgári perrendtartásról szóló 1952. évi III. törvény: *Pp.*
- az adózás rendjéről szóló 2003. évi XII. törvény: *Art.*
- 1959. évi IV. törvény, a Polgári Törvénykönyv: *Ptk.*
- a helyi önkormányzatokról szóló 1990. évi LXV. törvény: *Ötv.*
- a sztrájkról szóló 1989. évi VII. törvény: *Sztv.*
- a személyi jövedelemadóról szóló 1995. évi CXVII. törvény: *Szja tv.*
- a hitelintézetekről és a pénzügyi vállalkozásokról szóló 1996. évi CXII. törvény: *Hpt.*
- a biztosítókról és a biztosítási tevékenységről szóló 2003. évi LX. törvény: *Bit.*
- a sajtóról szóló 1986. évi II. törvény: *Stv.*
- a köziratokról, a közlevéltárakról és a magánlevéltári anyag védelméről szóló 1995. évi LXVI. törvény: *Ltv.*
- a társasházakról szóló 2003. évi CXXXIII. törvény: *Tht.*
- a lakásszövetkezetekről szóló 2004. évi CXV. törvény: Lszt.
- az elmúlt rendszer titkosszolgálati tevékenységének feltárásáról és az Állambiztonsági Szolgálatok Történeti Levéltára létrehozásáról szóló 2003. évi III. törvény: *Ásztltv.*
- az elektronikus információszabadságról szóló 2005. évi XC. törvény: *Eitv.*
- a közigazgatási hatósági eljárás és szolgáltatás általános szabályairól szóló 2004. évi CXL. törvény: *Ket.*
- a rádiózásról és televíziózásról szóló 1996. évi I. törvény: *Rttv.*

Munkatársaink

Baka Péter
Balogh Gyöngyi dr.
Baracsi Nándor
Bártfai Zsolt dr.
Bíró János dr.
Bretz Gyuláné
Csajági István
Dudás Gábor dr.
Egerszegi Béla
Egri Katalin dr.
Érczy Dániel dr.
Fazekas Béla
Filipovits Viktória dr.
Forgács Nóra dr.
Freidler Gábor dr.
Gulyás Csaba
Halmos György dr.
Hegedűs Bulcsú dr.
Horváth Nóra dr.
Horváth Zoltánné
Jutasiné Diós Berta
Kartaly Béla
Kerekes Zsuzsanna dr.
Keszey Gábor dr.
Kiss Kornél
Kolozsváry Sándor
Kowács Györgyi dr.
Kőhalmy Lászlóné
Lakatos Lászlóné
Montvai Máté
Móricz György dr.
Németh Gábor Sándor dr.
Németh Gáborné
Pajó Ágnes dr.
Pető Szabolcs
Poltz Klaudia dr.
Révész Balázs dr.
Somogyvári Katalin dr.
Szabó Endre Győző dr.
Szabó Szilvia dr.
Széplaki Andrea
Sziklay Júlia dr.
Szöllősi Erzsébet dr.
Tóth Beáta dr.
Trócsányi Sára Ph.D.
Varga Ilona dr.
Weiser Gabriella
Zombor Ferenc dr.
Zs.-Szőke Andrea dr.