



INFORMACIJSKI POOBLAŠČENEC
INFORMATION COMMISSIONER

'06

Letno poročilo Informacijskega pooblaščenca
za leto 2006



INFORMACIJSKI POOBLAŠČENEC
INFORMATION COMMISSIONER

'06

Letno poročilo Informacijskega pooblaščenca
za leto 2006



WATCH YOUR

0

POROČILO INFORMACIJSKEGA POOBLAŠČENCA

UVOD



Pravica do svobode izražanja in pravica do varstva zasebnosti - to sta gotovo temeljni načeli demokracije, ki ju v prakso prenašata in uveljavljata Zakon o dostopu do informacij javnega značaja in Zakon o varstvu osebnih podatkov. Informacijski pooblaščenec skrbi za izvajanje obeh kot neodvisni državni organ.

S sprejetjem Zakona o informacijskem pooblaščenču in razširitvijo pristojnosti nekdanjega Pooblaščenca za dostop do informacij javnega značaja na varstvo osebnih podatkov je z zagotavljanjem uresničevanja pravice vedeti in pravice do informacijske zasebnosti postalo delovanje Informacijskega pooblaščenca večplastno in raznoliko.

V poročilu za leto 2006 Informacijski pooblaščenec prvič predstavlja svoje delo na področju dostopa do informacij javnega značaja in varstva osebnih podatkov kot dolžnost do Državnega zbora Republike Slovenije, ki mu jo nalaga Zakon o Informacijskem pooblaščenču. Seveda je letno poročilo namenjeno tudi vsem, ki jih zanima področje našega dela.

Informacijski pooblaščenec ugotavlja, da je kljub temu da se zavezanci (javni sektor) vse bolj zavedajo pomena dostopa do informacij javnega značaja, v letu 2006 skokovito naraslo število pritožb prosilcev zoper molk oz. nedejavnost organov. Ob ustreznem ukrepanju Informacijskega pooblaščenca je bil molk organov odpravljen, pogosto tudi brez izdaje odločbe kot zavezujočega akta, torej s pogovori, z neformalnimi opozorili, kar vendarle kaže na to, da molk organov ni posledica hude brezbriznosti državnih uslužbencev do prava dostopa do javnih informacij, temveč le posledica nepoznavanja prava. Nekajkrat pa smo opazili, da je molk nastal tudi zaradi zavlačevanja pri dostopu do informacij, kar pa za uresničevanje te temeljne človekove pravice vsekakor ni spodbudno in je gotovo etično nedopustno. Hitrost postopka ima namreč pri dostopu do informacij javnega značaja izrazito poudarjen pomen, zato je spoštovanje z zakonom določenega razmeroma dolgega roka 20 delovnih dni nujno, če želimo, da ta temeljna človekova pravica v vsej svoji veljavi zaživi in živi v praksi.

V tretjem letu izvajanja Zakona o dostopu do informacij javnega značaja je zaznati boljše poznavanje dolžnosti zavezancev, predvsem pa večjo sposobnost komuniciranja uradnih oseb za dostop do informacij javnega značaja s prosilci. Poleg že omenjenega povečanja števila pritožb zaradi molka organov je naraslo tudi število vlog prosilcev, ki so prosili za pomoč pri razlagi Zakona o dostopu do informacij javnega značaja (tako glede oblikovanja zahteve kot tudi glede postopka). Informacijski pooblaščenec je dosledno opravljal svojo izobraževalno vlogo; upoštevajoč svoje pristojnosti in načelo nepristranskosti je svetoval tako organom kot prosilcem in s tem preprečeval nepotrebnih pritožbenih postopke, ki bi izvirali iz nezadostne komunikacije med prosilcem in organom zavezancem ali iz zavezančevega nezadostnega poznavanja posebnosti prava dostopa do informacij javnega značaja. Ker je zakonodajalec leta 2005 z novelo Zakona o dostopu do informacij javnega značaja uvedel pomembno novost - test interesa javnosti in tako zožil možnost neupravičenega zapiranja dostopa do informacij, je postala izobraževalna vloga Informacijskega pooblaščenca še izrazitejša. Napredek se je pokazal tudi pri obravnavi zahtev po ponovni uporabi informacij javnega značaja, pri čemer imajo organi zavezanci možnost, da ponovno uporabo za pridobitne namene zaračunajo.

V letu 2006 je bilo zoper odločbe Informacijskega pooblaščenca sproženih razmeroma malo upravnih sporov na Upravnem sodišču, kar kaže na večjo transparentnost in odprtost javnega sektorja glede njegovega delovanja in brez dvoma tudi na sprejemanje odločb Informacijskega pooblaščenca s strani organov zavezancev in prosilcev kot neke vrste precedenčnega prava. Nekatere odločitve Informacijskega pooblaščenca kot pritožbenega organa so že postale ustaljena praksa preglednega delovanja javnega sektorja: javnost plač javnih uslužbencev, javnost meril in pogojev pri izbiri ponudnika v postopku oddaje javnega naročila, javnost subvencij in drugih oblik državnih pomoči ...

Na področju varstva osebnih podatkov pa se je leta 2006 zagotovo zgodila »majhna revolucija«. To pravo je postalo prepoznavno pri zavezancih (v zasebnem in javnem sektorju) in posameznikih, ki so središčna točka izvajanja te temeljne človekove pravice. Informacijski pooblaščenec je v letu 2006 vodil številne postopke o prekrških na področju varstva osebnih podatkov, odločal o ugovorih posameznikov glede obdelave osebnih podatkov, dajal mnenja, pojasnila in stališča do vprašanj s področja varstva osebnih podatkov ter dajal navodila in priporočila glede varstva osebnih podatkov po posameznih področjih. Številne dejavnosti so bile povezane z vodenjem registra osebnih podatkov, saj je bilo do konca leta 2006 v register vpisanih manj kot 5 % upravljavcev osebnih podatkov (a kljub temu 6000 več kot leta 2005, ko je bilo do decembra vpisanih zgolj 973 upravljavcev zbirk osebnih podatkov). Vsi upravljavci zbirk osebnih podatkov so namreč o zbirkah osebnih podatkov dolžni voditi katalog zbirk ter o tem obvestiti Informacijskega pooblaščenca, ki podatke vpiše v register zbirk.

Med pomembnejše naloge Informacijskega pooblaščenca je sodilo tudi zagotavljanje uresničevanja določb Zakona o varstvu osebnih podatkov, ki so ga na terenu preverjali državni nadzorniki za varstvo osebnih podatkov, in sodelovanje z ministrstvi pri pripravi predpisov s področja osebnih podatkov.

Zaradi boljšega razumevanja zakona in vseh novosti je Informacijski pooblaščenec v letu 2006 izdal nekaj publikacij in vse leto skrbel za javnost svojega dela in ozaveščanje pravnih in fizičnih oseb prek rednih stikov z mediji in prek svoje spletne strani ter seveda z neposredno komunikacijo z zavezanci. Strokovnjaki Informacijskega pooblaščenca so sodelovali na številnih izobraževalnih konferencah, kongresih in okroglih mizah. V letu 2006 je Informacijski pooblaščenec s svojimi dejavnostmi zaznamoval 4. svetovni dan pravice vedeti. Za boljše obveščanje tako strokovne kot laične javnosti smo popolnoma prenovili in preoblikovali svojo spletno stran ter jo dopolnili tudi z vsebinami s področja varstva osebnih podatkov, tako so na spletu za ozaveščanje javnosti objavljena prav vsa pravna mnenja, ki jih je v letu 2006 nastalo kar 616.

Zaradi povečanega obsega dela in številnih novih pristojnosti ter mednarodnih obveznosti se je v letu 2006 povečalo število zaposlenih; zlasti število državnih nadzornikov za varstvo osebnih podatkov. 1. 1. 2006 je bilo pri Pooblaščencu zaposlenih 15 oseb, 31. 12. 2006 pa že 25 oseb. Vsi zaposleni na uradniških delovnih mestih imajo najmanj univerzitetno izobrazbo. Večina zaposlenih je univerzitetnih diplomiranih pravnikov.

Zaradi sprejetja Zakona o informacijskem pooblaščencu je Informacijski pooblaščenec v letu 2006 izvedel organizacijsko, poslovno, informacijsko in fizično združitev (selitev) dveh organov – Pooblaščenca za dostop do informacij javnega značaja in nekdanjega Inšpektorata za varstvo osebnih podatkov.

V skladu s 14. členom Zakona o informacijskem pooblaščencu je Informacijski pooblaščenec pripravil poročilo o svojem delu v letu 2006 in ga maja 2007 posredoval Državnemu zboru Republike Slovenije. Ta dokument vsebuje celovit pregled našega dela, na katerega sem s svojimi sodelavci osebno zelo ponosna.

Tudi v tem letu se bom trudila, da bo naše delo v ponos in pomoč državljanom in državi.

informacijska pooblaščenka

Nataša Pirc Musar

Informacijski pooblaščenec posebej opozarja na strogo načelo določenosti obdelave osebnih podatkov v zakonu. V ta namen je izdelal študijo in pregled celotne slovenske zakonodaje, ki zadeva varstvo osebnih podatkov. Določba drugega odstavka 38. člena Ustave Republike Slovenije določa, da zbiranje, obdelovanje, **namen uporabe**, nadzor in varstvo tajnosti osebnih podatkov določa zakon. Konkretizacijo te ustavne določbe pa predstavlja Zakon o varstvu osebnih podatkov, ki v 8. členu določa, da se osebni podatki načeloma lahko obdelujejo le, če obdelavo osebnih podatkov in osebne podatke, ki se obdelujejo, določa zakon. Obenem pa mora biti namen obdelave osebnih podatkov določen v zakonu, ob obdelavi na podlagi osebne privolitve posameznika pa mora biti posameznik predhodno pisno ali drugače ustrezno seznanjen z namenom obdelave osebnih podatkov.

Pregled slovenske zakonodaje, ki ureja obdelavo osebnih podatkov, je pokazal, da je tovrstnih trenutno veljavnih zakonov v Republiki Sloveniji (brez dopolnitev in uradno prečiščenih besedil) 1684. Med njimi jih kar 213 določa zbirke osebnih podatkov, kar predstavlja 13 % vseh zakonov.

Teh 213 zakonov določa skupno 857 zbirk osebnih podatkov, vendar jih 373, torej 44 %, ne določa namena obdelave osebnih podatkov. To pomeni, da so v tem delu zakoni v nasprotju z 38. členom Ustave Republike Slovenije. Prav tako je v nasprotju s to ustavno določbo zakonska dikcija, ki ureditev osebnih podatkov prepušča podzakonskemu predpisu. Tako določbo vsebuje kar 127 zakonov, torej 15 % vseh zakonskih določb, ki urejajo zbirke osebnih podatkov.

Ustavno sodišče je že v odločbi U-I-229/03 in tudi v odločbi št. U-I-298/04, ki je začela veljati 27. oktobra 2005 (Uradni list RS, št. 100/2005), zavzelo stališče, da to, da namen uporabe zbranih osebnih podatkov v zakonu ni določen, pomeni, da zakon z javno objavo teh podatkov celo omogoča, da se zbrani podatki uporabljajo za kakršen koli namen, kar je v neskladju z drugim odstavkom 38. člena Ustave. Podobna nevarnost se lahko pojavi tudi, če namen obdelave osebnih podatkov ni jasno določen, saj se lahko takrat osebni podatki uporabljajo v nasprotju s tem, za kar so bili zbrani. Da mora biti namen obdelave osebnih podatkov v zakonu določen eksplicitno, je presodilo tudi Ustavno sodišče, in sicer (opomba št. 3 k odločbi št. U-I-298/04, z dne 27. oktobra 2005, Uradni list RS, št. 100/2005), da zgolj načela v zakonu (v konkretnem primeru je bil to Zakon o plačilnem prometu) po oceni Ustavnega sodišča še ne opredeljujejo namena uporabe, kot to zahteva 38. člen Ustave Republike Slovenije za osebne podatke.

Na podlagi navedenega Informacijski pooblaščenec poziva predlagatelje zakonov, naj pri urejanju zbirk osebnih podatkov že v predlogu zakona določijo ne le vrste osebnih podatkov, ampak tudi namen njihovega zbiranja in nadaljnje obdelave. Pri tem je vsem zainteresiranim pripravljen svetovati in pomagati pri oblikovanju določb v zvezi z varstvom osebnih podatkov.

V zvezi z dostopom do informacij javnega značaja pa predlagatelje zakonov pozivamo, naj ne širijo izjem med prosto dostopnimi informacijami javnega značaja, predvsem pa naj jih ne določajo v drugih zakonih, ker s tem posegajo v vzpostavljen sistem transparentnosti in predvsem preglednosti nad izjemami po Zakonu o dostopu do informacij javnega značaja. Naj kot primer omenim Dansko, kjer se je zgodilo prav to. Zakonodajalec je namreč po letu 1984, ko so sprejeli zakon o dostopu do javnih informacij, sprejel okrog 400 različnih izjem in drugih ureditev dostopa do podatkov, zato danes o sistemu transparentnosti v tej državi ne morejo več govoriti, niti nihče več nima pregleda nad celoto. Pravica do svobode informacij tako umre po obrokih, zakon pa postane mrtva črka na papirju.

WATCH YOU

1.	INFORMACIJSKI POOBLAŠČENEC	
1.1.	Nastanek Informacijskega pooblaščenca	1
1.2.	Pristojnosti Informacijskega pooblaščenca	1
1.3.	Organiziranost Informacijskega pooblaščenca	4
1.4.	Finančna sredstva Informacijskega pooblaščenca	7
2.	DELO NA PODROČJU DOSTOPA DO INFORMACIJ JAVNEGA ZNAČAJA	
2.1.	Pravna ureditev na področju dostopa do informacij javnega značaja v Republiki Sloveniji	11
2.2.	Število vloženih pritožb in število rešenih zadev	12
2.3.	Število vloženih tožb na Upravnem sodišču, število sodb Upravnega sodišča	14
2.4.	Statistika po posameznih področjih ZDIJZ	14
2.5.	Storjeni prekrški na podlagi ZDIJZ in ZInfP	16
2.6.	Splošna ocena in priporočila na področju dostopa do informacij javnega značaja	16
2.7.	Predstavitev najodmevnejših in precedenčnih primerov po področjih	20
2.7.1.	Ponovna uporaba informacij javnega značaja	20
2.7.2.	Pravdni postopek	21
2.7.3.	Poslovna skrivnost	22
2.7.4.	Tajni podatki	23
2.7.5.	Kazenski postopek	24
2.7.6.	Dokument v izdelavi	24
2.7.7.	Notranje delovanje organa	25
2.7.8.	Ali je organ zavezanec	26
3.	DELO NA PODROČJU VARSTVA OSEBNIH PODATKOV	
3.1.	Koncept varstva osebnih podatkov v Republiki Sloveniji	29
3.2.	Dejavnost državnih nadzornikov za varstvo osebnih podatkov	30
3.2.1.	Pravice in dolžnosti državnega nadzornika	30
3.2.2.	Inšpekcijski nadzor v letu 2006	32

3.2.3.	Storjeni prekrški	35
3.2.4.	Najpogostejše ugotovljene nepravilnosti pri izvajanju inšpekcijskega nadzora	35
3.2.4.1.	Register zbirk osebnih podatkov	36
3.2.4.2.	Izvajanje videonadzora	36
3.2.4.3.	Neposredno trženje	38
3.2.4.4.	Zavarovanje osebnih podatkov	38
3.2.4.5.	Prekomerno zbiranje osebnih podatkov	39
3.2.4.6.	Zasebnost na delovnem mestu	40
3.2.4.7.	Objavljanje seznamov lastnikov stanovanj v večstanovanjskih stavbah	41
3.2.4.8.	Nezakonito posredovanje osebnih podatkov	42
3.2.4.9.	Zdravstveni osebni podatki	43
3.3.	Dajanje pisnih mnenj in pojasnil	45
3.4.	Dopustnost izvajanja biometrijskih ukrepov	47
3.5.	Ugotavljanje ustrezne ravni varstva osebnih podatkov v tretjih državah	50
3.6.	Izdajanje dovoljenj za povezovanje javnih evidenc	53
3.7.	Seznamitev z lastnimi osebnimi podatki	54
3.8.	Najodmevnejši primeri kršitev varstva osebnih podatkov	55
3.9.	Zahteve po presoji ustavnosti zakonov	57
3.10.	Splošna ocena varstva osebnih podatkov in priporočila	58
4.	DRUGE DEJAVNOSTI INFORMACIJSKEGA POOBLAŠČENCA	
4.1.	Sodelovanje pri pripravi zakonov in drugih predpisov	65
4.2.	Sodelovanje z javnostmi	66
4.3.	Mednarodno sodelovanje	67
4.3.1.	Sodelovanje na mednarodnih srečanjih	67
4.3.2.	Sodelovanje v delovnih skupinah Evropske unije	69

A black and white photograph of a weathered metal sign. The sign is rectangular with a thick border and is mounted on a dark, textured surface. The text "WATCH YOUR" is printed in large, bold, sans-serif capital letters. The sign shows signs of age and wear, with some discoloration and a rough texture. The background is dark and out of focus, suggesting an industrial or outdoor setting.

WATCH YOUR

1

INFORMACIJSKI POOBLAŠČENEC

1.1. Nastanek Informacijskega pooblaščenca

Državni zbor Republike Slovenije je 30. novembra 2005 sprejel Zakon o Informacijskem pooblaščenju¹, po katerem je bil 31. decembra. 2005 ustanovljen nov samostojen in neodvisen državni organ. Omenjeni zakon je združil dva organa, in sicer Pooblaščenca za dostop do informacij javnega značaja, ki je imel že prej status neodvisnega organa, in Inšpektorat za varstvo osebnih podatkov, ki je deloval kot organ v sestavi Ministrstva za pravosodje. Ob uveljavitvi Zakona o informacijskem pooblaščenju je Informacijski pooblaščenec za dostop do informacij javnega značaja nadaljeval delo kot Informacijski pooblaščenec, ki je prevzel inšpektorje in druge uslužbenke Inšpektorata za varstvo osebnih podatkov, pripadajočo opremo in sredstva. Hkrati je prevzel tudi vse nedokončane zadeve, arhive in evidence, ki jih je vodil Inšpektorat za varstvo osebnih podatkov. S tem so se pristojnosti organa, ki je skrbel za nemoteno izvajanje dostopa do informacij javnega značaja, močno spremenile in se razširile še na varstvo osebnih podatkov. Informacijski pooblaščenec je tako postal tudi državni nadzorni organ za varstvo osebnih podatkov in delo začel 1. januarja 2006.

S takšno ureditvijo, ki je primerljiva z ureditvijo v razvitih evropskih državah, se je pometila praksa dveh organov, povečuje pa se zavedanje pravice do zasebnosti in pravice vedeti – ti sta po novem še v večjem sožitju.

Predstojnika Informacijskega pooblaščenca, ki je funkcionar, imenuje Državni zbor Republike Slovenije na predlog predsednika Republike Slovenije. Informacijskega pooblaščenca vodi pooblaščenka Nataša Pirc Musar.

1.2. Pristojnosti Informacijskega pooblaščenca

Pristojnosti Informacijskega pooblaščenca ureja vrsta zakonov.

Informacijski pooblaščenec je po 2. členu ZInfP pristojen za:

- odločanje o pritožbi zoper odločbo, s katero je organ zavrgel ali zavrnil zahtevo ali drugače krtil pravico do dostopa ali ponovne uporabe informacije javnega značaja ter v okviru postopka na drugi stopnji tudi za nadzor nad izvajanjem zakona, ki ureja dostop do informacij javnega značaja, in za nadzor na njegovi podlagi izdanih predpisov;
- inšpekcijski nadzor nad izvajanjem zakona in drugih predpisov, ki urejajo varstvo ali obdelavo osebnih podatkov oziroma iznos osebnih podatkov iz Republike Slovenije, ter opravljanje drugih nalog, ki jih določajo ti predpisi;
- odločanje o pritožbi posameznika, kadar upravljavec osebnih podatkov ne ugotovi zahtevi posameznika glede njegove pravice do seznanitve z zahtevanimi podatki, do izpisov, seznamov, vpogledov, potrdil, informacij, pojasnil, prepisovanja ali kopiranja po določbah zakona, ki ureja varstvo osebnih podatkov;
- Informacijski pooblaščenec lahko na Ustavnem sodišču Republike Slovenije vložijo zahtevo po presoji ustavnosti zakonov, drugih predpisov ter splošnih aktov, izdanih

¹ Uradni list RS, št. 113/2005, v nadaljevanju ZInfP.

za izvrševanje javnih pooblastil, če se pojavi vprašanje ustavnosti in zakonitosti v zvezi s postopkom, ki ga vodi - tako na področju dostopa do javnih informacij kot varstva osebnih podatkov.

Informacijski pooblaščenec ima pristojnost pritožbenega organa tudi po Zakonu o medijih². Po ZMed se zavrnilni odgovor organov zavezancev na vprašanje, ki ga zastavi predstavnik medija, šteje kot zavrnilna odločba. Molk organa zavezanca ob takem vprašanju pa je prekršek in obenem tudi razlog za pritožbo. Pritožba zoper zavrnilno odločbo je dovoljena, če zavrnilni odgovor na vprašanje izhaja iz dokumenta, zadeve, dosjeja, registra, evidence ali drugega dokumentarnega gradiva. O pritožbi zoper zavrnilno odločbo odloča Informacijski pooblaščenec po določbah Zakona o dostopu informacij javnega značaja³.

Informacijski pooblaščenec je tudi prekrškovni organ, pristojen za nadzor nad izvajanjem ZInFP, ZDIJZ v okviru pritožbenega postopka, določbe 45. člena ZMed in Zakona o varstvu osebnih podatkov⁴.

ZDIJZ poleg zgoraj zapisanih določa še pristojnost za vodenje evidence vseh podeljenih izključnih pravic na področju ponovne uporabe informacij (5. odstavek 36.a člena). Ta pristojnost bo prav zaživela šele po 31. decembru 2008 (skrajni rok za prenehanje veljavnosti ekskluz. pogodb), zato se mi je zdaj ne zdi smiselno omenjati.

Natančnejše pristojnosti Informacijskega pooblaščenca na podlagi ZVOP-1:

- izvaja inšpekcijski nadzor nad izvajanjem določb ZVOP-1 (obravnavo prijave, pritožbe, sporočila in druge vloge, v katerih je izražen sum kršitve zakona);
- odreja inšpekcijske ukrepe iz 54. člena ZVOP-1 (prepoved obdelave osebnih podatkov, anonimiziranje, blokiranje, brisanje ali uničenje osebnih podatkov, kadar ugotovi, da se ti obdelujejo v nasprotju z zakonom);
- odreja druge ukrepe inšpekcijskega nadzora v skladu z zakonom o inšpekcijskem nadzoru in zakonom o splošnem upravnem postopku (5. točka prvega odstavka 54. člena ZVOP-1);
- opravlja preventivni inšpekcijski nadzor pri upravljalcih osebnih podatkov v javnem in zasebnem sektorju;
- vodi in vzdržuje register zbirk osebnih podatkov in skrbi, da je register ažuren in javno dostopen prek svetovnega spleta (28. člen ZVOP-1);
- omogoča vpogled in prepis podatkov iz registra zbirk osebnih podatkov (praviloma isti dan, najpozneje pa v osmih dneh (29. člen ZVOP-1);
- vodi postopke o prekrških na področju varstva osebnih podatkov (hitri postopek);
- vloži lahko kazensko ovadbo oziroma izvaja postopke v skladu z zakonom, ki ureja prekrške, če pri inšpekcijskem nadzoru ugotovi, da obstaja sum storitve kaznivega dejanja ali prekrška;
- odloča o ugovoru posameznika zoper obdelavo osebnih podatkov na podlagi četrtega odstavka 9. člena in tretjega odstavka 10. člena ZVOP-1;

2 Uradni list RS, št. 110/2006, uradno prečiščeno besedilo, v nadaljevanju ZMed.

3 Uradni list RS, št. 51/2006, uradno prečiščeno besedilo in 117/2006-ZDavP2, v nadaljevanju ZDIJZ.

4 Uradni list RS, št. 86/2004 in 113/2005-ZInFP, v nadaljevanju ZVOP-1.

- izdaja odločbe o zagotavljanju ustrezne ravni varstva osebnih podatkov v tretjih državah (63. člen ZVOP-1);
- vodi postopke ugotavljanja ustrezne ravni varstva osebnih podatkov v tretjih državah na podlagi ugotovitev inšpekcijskega nadzora in drugih informacij (64. člen ZVOP-1);
- vodi seznam tretjih držav o tem, ali imajo v celoti ali delno zagotovljeno ustrezno raven varstva osebnih podatkov ali te nimajo zagotovljene; če je ugotovljeno, da tretja država le delno zagotavlja ustrezno raven varstva osebnih podatkov, je v seznamu navedeno tudi, v katerem delu je ustrezna raven zagotovljena (66. člen ZVOP-1).
- vodi upravne postopke za izdajo dovoljenj o iznosu osebnih podatkov v tretjo državo (70. člen ZVOP-1);
- vodi upravne postopke za izdajo dovoljenj za povezovanje javnih evidenc in javnih knjig, kadar katera od zbirk osebnih podatkov, ki naj bi jih povezali, vsebuje občutljive osebne podatke ali pa je za povezavo potrebna uporaba istega povezovalnega znaka (na primer EMŠO ali davčna številka);
- vodi upravne postopke za izdajo ugotovitvenih odločb o tem, ali je nameravana uvedba biometrijskih ukrepov v zasebnem sektorju v skladu z določbami ZVOP-1;
- sodeluje z državnimi organi, pristojnimi organi Evropske unije za varstvo posameznikov pri obdelavi osebnih podatkov, mednarodnimi organizacijami, tujimi nadzornimi organi za varstvo osebnih podatkov, zavodi, združenji ter drugimi organi in organizacijami pri vseh vprašanjih, ki so pomembna za varstvo osebnih podatkov;
- daje in objavlja predhodna mnenja državnim organom ter nosilcem javnih pooblastil o usklajenosti določb predlogov predpisov z zakoni in drugimi predpisi, ki urejajo osebne podatke;
- daje in objavlja neobvezna mnenja o skladnosti kodeksov poklicne etike, splošnih pogojih poslovanja oziroma skladnosti predlogov s predpisi s področja varstva osebnih podatkov;
- pripravlja, daje in objavlja neobvezna navodila in priporočila glede varstva osebnih podatkov na posameznem področju;
- na spletni strani in na drug ustrezen način objavlja predhodna mnenja o usklajenosti predlogov zakonov in drugih predpisov z zakonom in drugimi predpisi s področja varstva osebnih podatkov ter zahtev po presoji ustavnosti predpisov (48. člen ZVOP-1), izdaja notranje glasilo ter strokovno literaturo, objavlja odločbe in sklepe sodišč, ki zadevajo varstvo osebnih podatkov, ter neobvezna mnenja, pojasnila, stališča in priporočila glede varstva osebnih podatkov na posameznem področju (49. člen ZVOP-1);
- daje izjave za javnost o opravljenih nadzorih in pripravlja letna poročila o svojem delu;
- sodeluje v delovni skupini za varstvo osebnih podatkov, oblikovani znotraj EU, ki povezuje neodvisne institucije za varstvo osebnih podatkov držav članic, deluje pa na podlagi 29. člena Direktive 95/46/EC (Working Party 29); v skupnih nadzornih organih za varstvo podatkov, ustanovljenih s Konvencijo o ustanovitvi Evropskega policijskega urada (Europol), Konvencijo o uporabi informacijske tehnologije za carinske namene in Konvencijo o izvajanju Schengenskega sporazuma o postopni odpravi mejnih kontrol na skupnih mejah, in z Evropskim nadzornikom za varstvo

podatkov, ustanovljenim z Uredbo (ES) št. 45/2001 Evropskega parlamenta in Sveta o varstvu posameznikov pri obdelavi osebnih podatkov v institucijah in organih Skupnosti in o prostem pretoku takih podatkov.

Informacijski pooblaščenec pa dobiva tudi nove pristojnosti. Tako bo:

- nadzoroval izvajanje Schengenskega sporazuma, ki v 128. členu določa nadzor s strani neodvisne institucije za nadzor pretoka osebnih podatkov pri izvajanju te konvencije;
- skrbel za preprečevanje zlorab ter za pravilno izvajanje evropske Direktive o zasebnosti in elektronskih komunikacijah 2002/58/EC in Direktive o hrambi telekomunikacijskih prometnih podatkov 2006/24/ES, ki je bila 15. decembra 2005 sprejeta v Bruslju na predlog ministrov držav članic.

1.3. Organiziranost Informacijskega pooblaščenca

Notranjo organiziranost in sistematizacijo delovnih mest, ki so potrebna za izvajanje nalog pri Informacijskem pooblaščenju, določa Pravilnik o delovnih mestih, nazivih in sistematizaciji delovnih mest pri Informacijskem pooblaščenju. Sistematizacija delovnih mest je prilagojena nalogam in delovnim procesom, ki potekajo pri Informacijskem pooblaščenju, in je oblikovana tako, da zagotavlja čim učinkovitejšo izrabo človeških virov.

Informacijski pooblaščenec opravlja svoje naloge v treh organizacijskih enotah:

- sektorju za informacije javnega značaja,
- sektorju za varstvo osebnih podatkov,
- administrativno-tehnični službi.

Naloge sektorja za informacije javnega značaja so:

- opravljanje strokovnih nalog s področja dostopa in ponovne uporabe informacij javnega značaja za Informacijskega pooblaščenca,
- izvajanje učinkovitega pravnega varstva v postopkih dostopa in ponovne uporabe informacij javnega značaja. V okviru tega se izvajajo te naloge:
 1. pripravljanje osnutkov sklepov v pritožbenem postopku;
 2. pripravljanje predlogov za izvajanje postopka;
 3. pripravljanje strokovnih podlag za odločanje in gradiva, ki so potrebna za delo Informacijskega pooblaščenca;
 4. pripravljanje osnutkov sprememb področnih zakonov kot tudi tolmačenje posameznih členov;
 5. sodelovanje pri razvojnih projektih;
 6. pripravljanje osnutkov odločb v pritožbenem postopku;
 7. strokovna podpora Informacijskemu pooblaščenju.

Naloge sektorja za varstvo osebnih podatkov:

- opravljanje strokovnih nalog s področja nadzora nad varstvom osebnih podatkov po zakonu, ki ureja varstvo podatkov, za Informacijskega pooblaščenca;
- izvajanje učinkovitega varstva osebnih podatkov pri obdelavi osebnih podatkov in inšpekcijskega nadzora, pri katerem se opravljajo te naloge:
 1. vodenje postopkov o prekrških (hitri postopek) s področja varstva osebnih podatkov;
 2. pripravljane osnutkov odločitev oziroma odločanje o pritožbi posameznikov glede seznanitve z lastnimi osebnimi podatki;
 3. vodenje oziroma pripravljane predlogov za vodenje upravnih postopkov za izdajo ugotovitvenih odločb;
 4. izvajanje inšpekcijskega nadzora;
 5. sodelovanje z različnimi organi in institucijami v Sloveniji in Evropski uniji na področju varstva osebnih podatkov;
 6. pripravljane strokovnih podlag za odločanje in gradiva, ki so potrebna za delo Informacijskega pooblaščenca;
 7. pripravljane predhodnih mnenj vladi, državnem zboru in drugim organom Republike Slovenije o skladnosti predlogov predpisov z akti, ki urejajo varstvo osebnih podatkov;
 8. pripravljane osnutkov sprememb področnih zakonov kot tudi tolmačenje posameznih členov;
 9. sodelovanje pri razvojnih projektih;
 10. strokovna podpora Informacijskemu pooblaščenču.

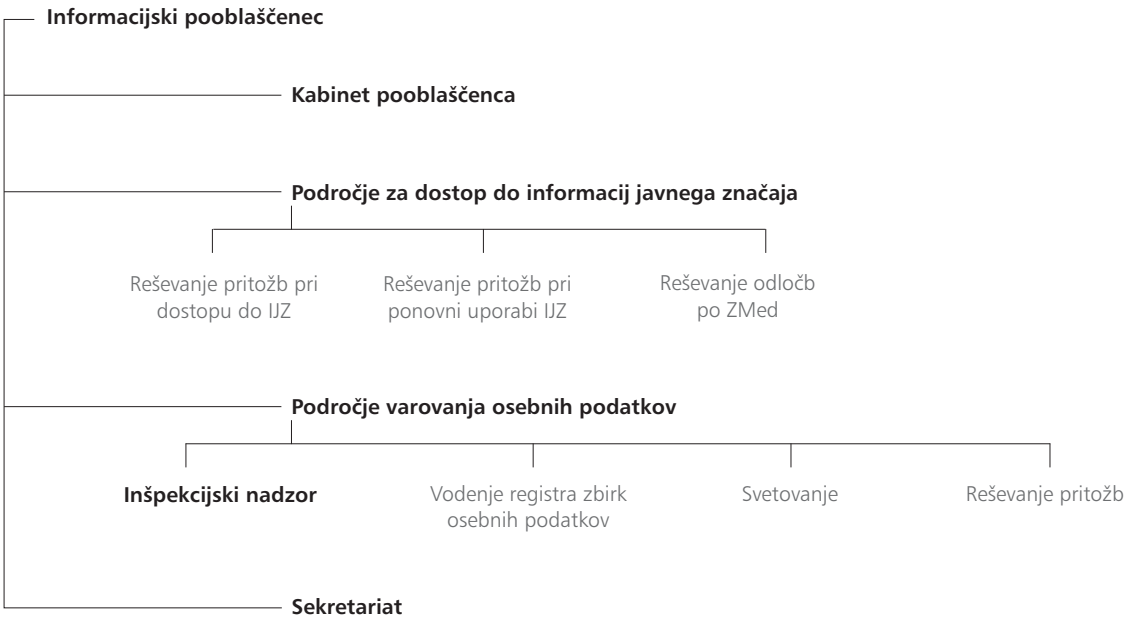
Naloge administrativno-tehnične službe:

- opravljanje zahtevnejših spremljajočih del, ki zahtevajo poznavanje javnih nalog Pooblaščenca, ter drugih strokovno-tehničnih nalog, in sicer:
 1. naloge s področja urejanja kadrovske zadeve;
 2. naloge s finančno-računovodskega področja;
 3. naloge s področja komuniciranja;
 4. naloge s področja varstva pri delu;
 5. pripravljane osnutkov aktov;
 6. vodenje, urejanje in hranjenje dokumentacije ter arhiva Informacijskega pooblaščenca;
 7. skrb za vzdrževanje informacijske opreme in storitev;
 8. zagotavljanje dostopa do zunanjih podatkovnih zbirk;
 9. izdelovanje raznih analiz;
 10. sodelovanje pri projektnih nalogah.

Konec leta 2006 je imel Informacijski pooblaščenec 25 zaposlenih:

- informacijska pooblaščenka,
- namestnica za področje varstva osebnih podatkov,
- namestnica za področje dostopa do informacij javnega značaja,
- generalna sekretarka,

- svetovalci (4),
- državni nadzorniki za varstvo osebnih podatkov (8),
- raziskovalci (4),
- drugi zaposleni (4),
- pripravnik.



Slika 1: Organigram Informacijskega pooblaščenca.

Preglednica 1:
Izobrazbena struktura zaposlenih pri Informacijskem pooblaščenču 31. 12. 2006.

Stopnja izobrazbe	Srednja izobrazba	Univerzitetna izobrazba	Magisterij	Doktorat	Skupaj
Delovno mesto					
Pooblaščenka		1			1
Namestnici		2			2
Generalna sekretarka			1		1
Svetovalci		4			4
Raziskovalci		3		1	4
Državni nadzorniki		6	2		8
Informatik			1		1
Pripravnik		1			1
Administrativno tehnični sodelavci	3				3
Skupaj	3	17	4	1	25

Zaradi povečanega obsega dela in številnih novih pristojnosti ter mednarodnih obveznosti se je v letu 2006 povečalo število zaposlenih, zlasti število državnih nadzornikov za varstvo osebnih podatkov. 1. januarja 2006 je bilo pri Informacijskem pooblaščenju zaposlenih 15 oseb, 31. decembra 2006 pa že 25 oseb. Vsi zaposleni na uradniških delovnih mestih imajo najmanj univerzitetno izobrazbo. Večina zaposlenih je univerzitetnih diplomiranih pravnikov. Med zaposlenimi na uradniških delovnih mestih imajo 4 opravljen magisterij, 1 pa doktorat.

1.4. Finančna sredstva Informacijskega pooblaščenca v letu 2006

Sredstva za delo Informacijskega pooblaščenca se zagotavljajo iz državnega proračuna in jih določi Državni zbor Republike Slovenije na predlog Informacijskega pooblaščenca (5. člen ZInfP). V letu 2006 je Informacijski pooblaščenec porabil skupaj 241.612.170,88 SIT proračunskega denarja. Od navedenega zneska se je porabilo:

- 152.674.816,56 SIT za plače, druge izdatke zaposlenih in prispevke za socialno varnost;
- 64.485.416,04 SIT za materialne stroške;
- 24.451.938,28 SIT za investicije in investicijsko vzdrževanje.

Preglednica 2: Poraba proračunskih sredstev leta 2006.

	v 000 SIT	v EUR
Plače	152.626	636.897
Materialni stroški		
Pisarniški in splošni material in storitve	21.577	90.039
Posebni material in storitve	550	2295
Energija, voda in komunalne storitve	5.718	23.860
Prevozni stroški in storitve	3.448	14.388
Izdatki za službena potovanja	5.986	24.979
Tekoče vzdrževanje	2.062	8604
Poslovne najemnine in zakupnine	19.462	81.213
Drugi operativni odhodki	5.668	23.652
Osnovna sredstva		
Nakup prevoznih sredstev	8.802	36.730
Nakup opreme	17.650	73.652
SKUPAJ	241.549	1.007.966

Zaradi povečanega obsega dela se je v letu 2006 povečalo število zaposlenih, zlasti število državnih nadzornikov za varstvo osebnih podatkov. Porabljena sredstva za plače so znašala 152.626.000 SIT.

Sredstva za materialne stroške, 65.491.000 SIT, so bila porabljena za redno delovanje Informacijskega pooblaščenca (pisarniški material, potni stroški, čiščenje, obratovalni stroški, študentsko delo, poštna storitve, izobraževanje zaposlenih, izdelava brošur ipd.) Večji del stroškov je predstavljala najemnina za poslovne prostore.

Zaradi uveljavitve ZInfP in povečanega števila zaposlenih se je Informacijski pooblaščenec preselil na novo lokacijo in za nemoteno delovanje kupil računalniško in pohištveno opremo ter novo službeno vozilo.





WATCH YOUR

2

**DELO NA PODROČJU DOSTOPA DO
INFORMACIJ JAVNEGA ZNAČAJA**

2.1. Pravna ureditev na področju dostopa do informacij javnega značaja v Republiki Sloveniji

Priporočila Sveta Evrope⁵ narekujejo, da države članice, torej tudi Slovenija, v svoji zakonodaji in praksi uredijo uresničevanje pravice dostopa do informacij javnega značaja tako, da bo lahko od organa javne oblasti vsakdo dobil želeno informacijo.

Pravico dostopa do informacij javnega značaja je zakonodajalec zagotovil že z Ustavo Republike Slovenije⁶. Ta v 2. odstavku 39. člena določa, da ima vsakdo pravico dobiti informacijo javnega značaja, za katero ima v zakonu utemeljen pravni interes, razen v primerih, ki jih določa zakon. Čeprav je pravica dostopa do informacij javnega značaja ena od temeljnih človekovih pravic in kot taka tudi povzdignjena na ustavno raven, se je začela uveljavljati šele 12 let po sprejetju ustave, in sicer s sprejetjem **Zakona o dostopu do informacij javnega značaja**⁷. Dotlej so se posamezne določbe o javnosti informacij pojavljale le v nekaterih zakonih (npr. Zakonu o varstvu okolja, Zakonu o naravnih in drugih nesrečah), celostno pa jih je uredil šele ZDIJZ. Tega je Državni zbor sprejel konec februarja 2003, veljati pa je začel 22. marca 2003.

ZDIJZ sledi usmeritvam mednarodnih aktov in Evropske unije. Njegov namen je zagotoviti javnost in odprtost delovanja javne uprave ter vsakomur omogočiti dostop do javnih informacij, torej tistih, ki so povezane z delovnimi področji organov javne uprave. Zakon ureja postopek, ki vsakomur omogoča prost dostop in ponovno uporabo informacij javnega značaja, s katerimi razpolagajo državni organi, organi lokalnih skupnosti, javne agencije, javni skladi in druge osebe javnega prava, nosilci javnih pooblastil in izvajalci javnih služb. S tem zakonom se v pravni red Republike Slovenije prenašajo te direktive Evropske skupnosti: Direktiva 2003/4/ES Evropskega parlamenta in Sveta, ki je začela veljati 28. januarja 2003, o javnem dostopu do okoljskih informacij in razveljavitvi Direktive 90/313/EGS in direktiva 2003/98/ES Evropskega parlamenta in Sveta, ki je začela veljati 17. novembra 2003, o ponovni uporabi informacij javnega sektorja.

Leta 2005 je bil z novelo ZDIJZ⁸ narejen še korak naprej. Novela je namreč zožila možnost neupravičenega zapiranja dostopa do informacij in uvedla številne novosti, kot so ponovna uporaba informacij javnega značaja in pristojnosti upravne inšpekcije na področju izvajanja tega zakona. Najpomembnejša novost je bil nedvomno test javnega interesa. Prav tako je bila z novelo poudarjena odprtost pri podatkih o porabi javnih sredstev in podatkih, povezanih z delovnim razmerjem ali opravljanjem javne funkcije. S tem se je Slovenija pridružila tistim demokratičnim državam, ki, kadar gre za javni interes, tudi izjeme obravnavajo s pridržkom.

Omejitev pravice do dostopa tajnih podatkov s področja javne varnosti, obrambe, zunanjih zadev ter obveščevalne in varnostne dejavnosti je sistematično urejena v Zakonu o tajnih podatkih⁹. Osební podatki so varovani z ZVOP-1, zaupnost nekaterih podatkov terjajo tudi Zakon o državni statistiki¹⁰, Zakon o davčni službi¹¹ in Zakon o davčnem postopku¹², Zakon o ohranjanju narave¹³ ter Zakon o gospodarskih družbah¹⁴.

5 Recommendation (1981) 19 in Recommendation (2002) 2.

6 Uradni list RS, št. 33/1991, 42/1997, 66/2000, 24/2003, 69/2004, 68/2006, v nadaljevanju Ustava RS.

7 Uradni list RS, št. 24/2003.

8 Uradni list RS, št. 61/2005.

9 Uradni list RS, št. 135/2003, uradno prečiščeno besedilo.

10 Uradni list RS, št. 45/1995, spremenjen 9/2001.

11 Uradni list RS, št. 1/2007, uradno prečiščeno besedilo.

12 Uradni list RS, št. 117/2006.

13 Uradni list RS, št. 22/2003, uradno prečiščeno besedilo.

14 Uradni list RS, št. 42/2006, spremenjen 60/2006.

2.2. Število vloženih pritožb in število rešenih zadev

ZDIJZ zagotavlja dostop do informacij, ki so že ustvarjene, in sicer v kakršni koli obliki. S tem zakon zagotavlja preglednost porabe javnega denarja in odločitev javne uprave, saj ta dela v imenu ljudi in za ljudi. Informacija javnega značaja je informacija, ki izvira z delovnega področja organa, obstaja pa v obliki dokumenta, zadeve, dosjeja, registra, evidence ali drugega dokumentarnega gradiva, ki ga je organ izdelal sam, v sodelovanju z drugim organom ali ga je pridobil od drugih oseb. Informacije javnega značaja so prosto dostopne vsem, pravni interes torej ni potreben, dovolj sta radovednost in želja po znanju ter obveščenosti. Vsakdo lahko te informacije pod določenimi pogoji uporabi tudi za pridobitne ali nepridobitne namene (ponovna uporaba informacij). Vsak prosilec ima na svojo zahtevo pravico pridobiti od organa informacijo javnega značaja, tako da jo dobi na vpogled ali dobi njen prepis, fotokopijo ali elektronski zapis. Vpogled v zahtevano informacijo je brezplačen. Za posredovanje prepisa, fotokopije ali elektronskega zapisa zahtevane informacije lahko organ prosilcu zaračuna materialne stroške. Ponovno uporabo informacij za pridobitne namene, razen za uporabo z namenom informiranja, zagotavljanja svobode izražanja, kulture in umetnosti in za uporabo informacij s strani medijev lahko organ zaračuna.

Vsak prosilec se mora najprej zavedati, da lahko pridobi katero koli informacijo javnega značaja, ki jo kot tako **opredeljuje zakon**. Pri tem prosilec ni treba izkazati pravne koristi (pravnega interesa) in tega organ od njih tudi ne sme zahtevati. Organ prav tako ne sme vprašati, za kateri namen prosilec potrebuje zahtevano informacijo, razen v primeru presoje pridobitnosti namena pri ponovni uporabi informacij. Organ mora o zahtevi odločiti v 20 delovnih dneh. V izjemnih okoliščinah lahko rok podaljša za največ 30 delovnih dni. O podaljšanju roka mora sprejeti sklep, in sicer najpozneje v 15 delovnih dneh po prejetju zahteve. Če organ v zakonitem roku ne odgovori, se šteje, da je zahtevo zavrnil.

Organ lahko prosilcu zavrne dostop do zahtevane informacije, če se zahteva nanaša na (prvi odstavek 6. člena ZDIJZ):

1. podatek, ki je na podlagi zakona, ki ureja tajne podatke, opredeljen kot tajen;
2. podatek, ki je opredeljen kot poslovna skrivnost v skladu z zakonom, ki ureja gospodarske družbe;
3. osebni podatek, katerega razkritje bi pomenilo kršitev varstva osebnih podatkov v skladu z zakonom, ki ureja varstvo osebnih podatkov;
4. podatek, katerega razkritje bi pomenilo kršitev zaupnosti individualnih podatkov o poročevalskih enotah, skladno z zakonom, ki ureja dejavnost državne statistike;
5. podatek, katerega razkritje bi pomenilo kršitev zaupnosti davčnega postopka ali davčne tajnosti, skladno z zakonom, ki ureja davčni postopek;
6. podatek, ki je bil pridobljen ali sestavljen zaradi kazenskega pregona ali v zvezi z njim ali zaradi postopka s prekrški, in bi njegovo razkritje škodovalo njegovi izvedbi;
7. podatek, ki je bil pridobljen ali sestavljen zaradi upravnega postopka, in bi njegovo razkritje škodovalo njegovi izvedbi;

8. podatek, ki je bil pridobljen ali sestavljen zaradi pravnega, nepravnega ali drugega sodnega postopka, in bi njegovo razkritje škodovalo njegovi izvedbi;
9. podatek iz dokumenta, ki je v postopku izdelave in je še predmet posvetovanja v organu, njegovo razkritje pa bi povzročilo napačno razumevanje njegove vsebine;
10. podatek o naravni oziroma kulturni vrednoti, ki v skladu z zakonom, ki ureja ohranjanje narave ali kulturne dediščine, ni dostopen javnosti zaradi varovanja naravne oziroma kulturne vrednote;
11. podatek iz dokumenta, ki je bil sestavljen v zvezi z notranjim delovanjem oziroma dejavnostjo organov, in bi njegovo razkritje povzročilo motnje pri delovanju oziroma dejavnosti organa.

Kljub navedenim izjemam se dostop do zahtevane informacije dovoli, če je javni interes za razkritje močnejši od javnega interesa ali interesa drugih oseb za omejitev dostopa do zahtevane informacije. To ne velja za podatke, ki so v skladu z zakonom, ki ureja tajne podatke, označeni z najvišjima stopnjama tajnosti, za podatke, ki vsebujejo ali so pripravljeni na podlagi tajnih podatkov tuje države ali mednarodne organizacije, s katero ima Republika Slovenija sklenjeno mednarodno pogodbo o izmenjavi ali posredovanju tajnih podatkov, za podatke, ki vsebujejo ali so pripravljeni na podlagi davčnih podatkov, ki jih organom v Republiki Sloveniji posreduje organ tuje države, ter za podatke iz 4. točke in 5. točke 6. člena, razen če je davčni postopek že pravnomočno končan oziroma je zavezanec za davek obveznost ugotovil v obračunu davka in ga ni plačal v predpisanem roku.

Kljub navedenim izjemam iz prvega odstavka se dostop do zahtevane informacije dovoli tudi, če gre za podatke o porabi javnih sredstev ali podatke, povezane z opravljanjem javne funkcije ali z delovnim razmerjem javnega uslužbenca. To ne velja za primere iz 1. in 5. do 8. točke prvega odstavka ter primere, ko zakon, ki ureja javne finance, ali zakon, ki ureja javna naročila, določata drugače in če gre za podatke o okoljskih emisijah, odpadkih, nevarnih snoveh v obratu ali podatke iz varnostnega poročila in druge podatke, za katere tako določa zakon, ki ureja varstvo okolja.

Če organ zahtevi po dostopu ugodí, ne izda posebne odločbe, ampak o tem naredi uradni zaznamek. Organ prosilcu nemudoma omogoči seznanitev z vsebino zahtevane informacije, tako da mu jo da na vpogled ali mu zagotovi njen prepis, fotokopijo ali elektronski zapis. Če organ zahtevo po dostopu delno ali v celoti zavrne, o tem izda pisno odločbo. Če organ prosilcu ne omogoči dostopa do informacije v roku in če ne izda in prosilcu ne vroči odločbe o zavrnitvi, se šteje, da je zahtevo zavrnil. Če uradna oseba organa ugotovi, da zahtevana informacija sploh ne obstaja, mora zahtevo prosilca zavrniti z odločbo. Če pa ugotovi, da informacija obstaja, vendar je sam nima v posesti, mora najpozneje v treh delovnih dneh od prejetja zahteve zadevo odstopiti organu, ki je glede na vsebino zahteve pristojen za njeno reševanje, in o tem obvestiti prosilca. Če organu ne uspe ugotoviti, kateri drugi organ je pristojen za reševanje zahteve, izda sklep o zavrnjenju zahteve. Prosilec ima pravico do pritožbe zoper odločbo, s katero je organ zahtevo zavrnil, ter zoper sklep, s katerim je organ zahtevo zavrgel. O pritožbi odloča Informacijski pooblaščenec. Prav tako ima prosilec pravico do pritožbe, če organ vztraja pri molku, če mu organ tudi po ponovljeni zahtevi ne omogoči seznanitve z informacijo, ki jo je navedel v zahtevi, in tudi, če ne dobi informacije v obliki, ki jo je zahteval.

Odgovorna oseba organa mora, če je to potrebno za obravnavo pritožbe, Informacijskemu pooblaščenцу na njegovo zahtevo nemudoma poslati dokumente, zadeve, dosjeje, registre, evidence ali dokumentarno gradivo, ki jih je zahteval prosilec. Informacijski pooblaščenec ima v okviru svojih pristojnosti tudi pravico do vpogleda v davčno tajnost. Če Informacijski pooblaščenec ob reševanju pritožbe v zadevah dostopa do informacij javnega značaja sumi, da organ prve stopnje z zahtevanimi informacijami razpolaga, vendar jih Informacijskemu pooblaščenцу ne posreduje v celoti ali delno, ima Informacijski pooblaščenec pooblastila po zakonu, ki ureja inšpekcijski nadzor. Če organ zoper odločbo Informacijskega pooblaščenca ni sprožil upravnega spora, je dolžan prosilcu skladno z odločbo Informacijskega pooblaščenca poslati zahtevane informacije.

V letu 2006 sta bili vloženi **102 pritožbi zoper odločbe, s katerimi so organi zavrnili zahteve po dostopu ali ponovni uporabi informacij javnega značaja**. Rešena je bila 101 pritožba. Iz leta 2005 je bilo prenesenih 9 zadev. Zaradi molka organa je Informacijski pooblaščenec prejel 402 pritožbi. Ob tem je Informacijski pooblaščenec pozval organ, naj čim prej odloči. V 389 primerih so zavezanci po pozivu odobrili dostop do želenih informacij javnega značaja, le 13 zadev glede molka organa je ostalo nerešenih.

2.3. Število vloženih tožb na Upravnem sodišču, število sodb Upravnega sodišča

Pritožba zoper odločbo Informacijskega pooblaščenca ni možna, mogoče pa je sprožiti upravni spor. Na Upravnem sodišču je bilo leta 2006 vloženih 15 tožb. Sodišče do konca leta 2006 ni odločilo še o nobeni izmed teh tožb, je pa izdalo dve sodbi o odločbah iz prejšnjih let:

- sodba U 614/2006-16, z dne 29. 11. 2006, izdana na podlagi tožbe, ki jo je sprožil notar Vojko Pintar proti odločbi Informacijskega pooblaščenca št. 021-53/2005/105
- sodba U 167/2006-16, z dne 11. 5. 2006, izdana na podlagi tožbe, ki jo je sprožila Slovenska odškodninska družba d. d. proti odločbi Informacijskega pooblaščenca št. 021-79/2005.

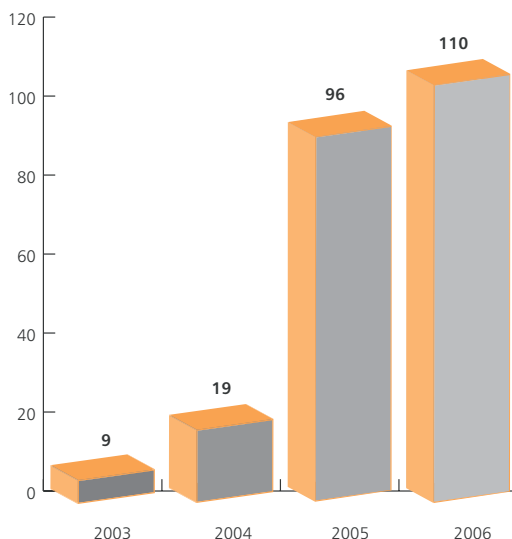
Sodišče je obe tožbi zavrnilo.

2.4. Statistika po posameznih področjih ZDIJZ

Število izdanih odločb na področju dostopa do informacij javnega značaja se iz leta v leto povečuje. V letu 2006 je bilo izdanih **110 odločb**.

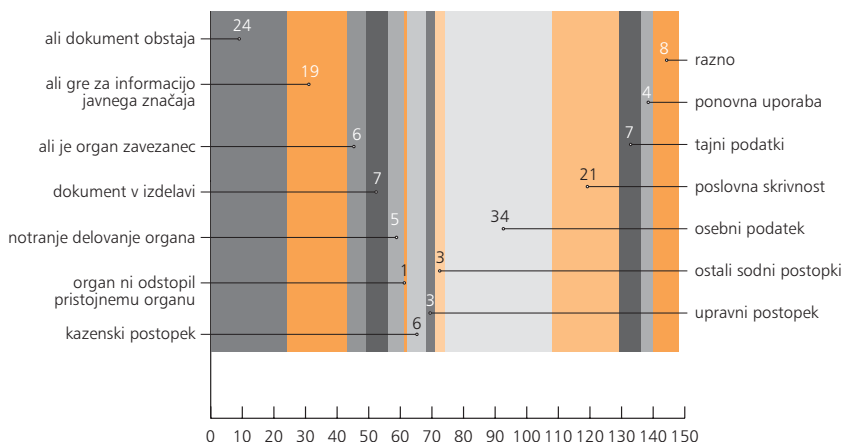
Slika 2:

Število izdanih odločb
na področju dostopa do
informacij javnega značaja v
obdobju 2003–2006.



Informacijski pooblaščenec je rešil zadevo v korist prosilcev v 51 primerih, v 43 primerih je pritožbo zavrnil, v 13 primerih delno odobril, po enkrat pa je zadevo vrnil v ponovno odločanje prvostopenjskemu organu, pritožbo zaradi nepopolnosti zavrnil ali odločbo prvostopenjskega organa opredelil za nično. V odločbah je največkrat presojal, ali zahtevani dokumenti vsebujejo osebne podatke, katerih razkritje bi pomenilo kršitev varstva osebnih podatkov v skladu z ZVOP-1. Sledile so odločbe, s katerimi je ugotavljal, ali zavezanec sploh ima dokument oz. informacijo javnega značaja, ki jo je prosilec zahteval. Razpolaganje z informacijo je namreč kakršno koli posedovanje, hranjenje, registriranje, evidentiranje, reproduciranje, izdelovanje, proizvajanje ali predelovanje informacije s strani organa, za njega ali pri njem. Organu ni treba ustvarjati ali pridobivati novih dokumentov, kakor mu tudi ni treba nadomeščati dokumenta, ki ga nima več v svoji posesti. Organu informacij za prosilca tudi ni treba zbirati, obdelovati ali analizirati. Seveda takšne ureditve ne moremo prenesti na sodobno tehnologijo, to je računalniške baze podatkov. Organi morajo v tem primeru podatke priklicati iz baz in tak priklic se ne šteje za izdelavo novega dokumenta. Če pa je zahtevani dokument že javno objavljen ali je dostopen v javni zbirki, organ izpolni zakonske zahteve že, če prosilca le napoti nanje. V precejšnjem deležu odločb je presojal, ali prosilci zahtevajo informacije oz. podatke, ki so v skladu z zakonom, ki ureja gospodarske družbe, opredeljeni kot poslovna skrivnost. V približno enakem številu pa so sledile odločbe, s katerimi je bilo odločeno:

- ali so zahtevane informacije podatki iz dokumentov, ki so v postopku izdelave, in so še predmet posvetovanja v organu, njihovo razkritje pa bi povzročilo napačno razumevanje njihove vsebine,
- ali so zahtevane informacije podatki, ki so na podlagi zakona, ki ureja tajne podatke, opredeljeni kot tajni,
- ali so zahtevane informacije podatki, ki so bili pridobljeni ali sestavljeni zaradi kazenskega pregona ali v zvezi z njim ali zaradi postopka s prekrški, in bi njihovo razkritje škodovalo izvedbi postopka,
- ali je organ, na katerega je bila zahteva po dostopu do informacije javnega značaja naslovljena, sploh zavezanec v skladu z ZDIJZ, ki v 1. členu določa, da so zavezanci za dostop do informacij javnega značaja vsi državni organi, organi lokalnih skupnosti, javne agencije, javni skladi in druge osebe javnega prava, nosilci javnih pooblastil in izvajalci javnih služb, torej ves javni sektor.



Slika 3:

Odločbe na področju ZDIJZ glede na različne izjeme. (Opomba: ena odločba se lahko nanaša na več izjem).

Pritožbe prosilcev zaradi zavrnitve dostopa do informacij javnega značaja so zadevale te skupine zavezancev:

- ministrstva, organe v njihovi sestavi in vladne službe (42),
- upravne enote in občine (18),
- sodišča in vrhovno državno tožilstvo (17),
- šolske ustanove (6),
- zdravstvene ustanove (6),
- javni skladi, zavode, agencije in druge osebe javnega prava (20),
- računsko sodišče (1).

V 61 primerih so bili prosilci fizične osebe, v enajstih primerih so se pritožili novinarji, v treh odvetniki in v dveh poslanca. Pravne osebe zasebnega sektorja oz. različni podjetniki so se zaradi neizročitve zahtevanih informacij Informacijskemu pooblaščenцу pritožili 12-krat, občine štirikrat, nevladne organizacije, različna združenja in društva pa 16-krat.

2.5. Storjeni prekrški na podlagi ZDIJZ in ZInfP

Informacijski pooblaščenec v letu 2006 ni izdal nobene odločbe o prekršku in nobenega plačilnega naloga.

2.6. Splošna ocena in priporočila na področju dostopa do informacij javnega značaja

Informacijski pooblaščenec opozarja, da je načelo odprtosti javnega sektorja njegova bistvena funkcija, saj javni sektor deluje javno in je javnosti tudi odgovoren. Javni sektor je zaradi porabe proračunskih oziroma javnih sredstev, predvsem pa zaradi izvajanja

javnih nalog, ves čas na očeh javnosti in s tem tudi pod drobnogledom medijev. Informacijski pooblaščenec kot del javnega sektorja deluje v duhu odprtosti in transparentnosti tudi pri izvajanju pristojnosti pritožbenega organa. Pritožbene postopke je namreč treba izpeljati tudi v skladu z interesi prosilca in s tem javnosti.

Zagotavljanje preglednega delovanja z izvajanjem ZDIJZ bi moralo javni sektor spodbuditi k spremembi miselnosti, da delo javnega sektorja poteka za zaprtimi vrati. Na podlagi splošnega vtisa o ravnanju organov zavezancev v pritožbenem postopku lahko sklenemo, da je bil začetni premik v miselnosti storjen. Javni sektor se zaveda, da izvaja naloge, ki so v javnem interesu. Zato je razumljivo, da mora ne le omogočati in dopuščati stalni nadzor javnosti, ampak da tak stalni nadzor javnosti tudi potrebuje. S tem namreč omogoča javnosti, da sodeluje pri izvajanju oblasti. Tako sodelovanje je za javni sektor dragoceno, saj je lahko le z dejavno obojestransko povezavo delo javnega sektorja kakovostno in koristno. Objektivne slabosti javnega sektorja so prevelika distanciranost od državljanov, vtis slabe organizacije dela in premajhna odzivnost na nove, pereče probleme oziroma izzive. Vse te slabosti je mogoče odpraviti tudi z doslednim spoštovanjem ZDIJZ in ZMed. Pri delu se pogosto opaža, da zavezanci ZDIJZ dojemajo kot zakon, ki jim nalaga zgolj delo s prosilci oziroma jih zagotavljanje dostopa do informacij javnega značaja odvrča od njihovih temeljnih nalog. Tako razmišljanje je v bistvu nepravilno, ker popolnoma zanemari smisel in cilj preglednega delovanja javnih oblasti. Prav tako je neutemeljen strah zavezancev, da bi lahko prosilci z nekaterimi informacijami javnega značaja manipulirali ali jih zlorabili. Informacije javnega značaja so prosto dostopne vsem in niso vezane na noben položaj, niti na državljanstvo. Zato se ni mogoče strinjati z argumentom, da prosilec s pridobitvijo informacij ugodi le svojemu interesu, na primer podjetniškemu interesu. Organ zavezanec pri posredovanju informacij javnega značaja interesa, zaradi katerega prosilec zahteva določene informacije, ne sme niti upoštevati niti presoja, saj velja načelo prostega dostopa do informacij javnega značaja. To pomeni, da prosilcu ni treba navesti, zakaj potrebuje dostop do informacij.

Na podlagi pritožbenega postopka Informacijski pooblaščenec ocenjuje, da so tako organi zavezanci kot tudi prosilci premalo seznanjeni s temeljnim načinom dostopanja do informacij javnega značaja. Glavni način za dostop do informacij javnega značaja je namreč povezan z dejavno vlogo zavezancev. Dostop do informacij javnega značaja bi bil bistveno lažji, če bi zavezanci čim več informacij javnega značaja javnosti posredovali sami, vnaprej, brez posebne zahteve po dostopu v različnih oblikah, predvsem v elektronski obliki. Tako ravnanje nalaga tudi ZDIJZ. Tako so zavezanci dolžni čim več informacij objaviti na svetovnem spletu, in sicer:

1. prečiščena besedila predpisov, ki zadevajo delovno področje organa, povezana z državnim registrom predpisov na spletu;
2. programe, strategije, stališča, mnenja in navodila, ki so splošnega pomena ali so pomembna za poslovanje organa s fizičnimi in pravnimi osebami oziroma za odločanje o njihovih pravicah ali obveznostih, študije in druge podobne dokumente, ki zadevajo delovno področje organa;
3. predloge predpisov, programov, strategij in drugih podobnih dokumentov, ki zadevajo delovno področje organa;
4. vse objave in razpisno dokumentacijo v skladu s predpisi, ki urejajo javna naročila;
5. informacije o svoji dejavnosti ter upravnih, sodnih in drugih storitvah;
6. vse informacije javnega značaja, ki so jih prosilci zahtevali najmanj trikrat.

Obenem pa lahko zavezanci na svetovnem spletu objavljajo tudi druge informacije javnega značaja, za katere sami presodijo, da bi bile lahko predmet zanimanja in s tem predmet različnih zahtev po dostopu. Aktivno in sprotno objavljanje informacij na svetovnem spletu bi omogočilo najučinkovitejši in najhitrejši dostop do informacij javnega značaja. To bi obenem zmanjšalo število zahtev in pritožb po ZDIJZ in s tem razbremenilo zavezance. Podobno bi vzpostavitev čim več prosto dostopnih javnih evidenc in drugih preprosto javno dostopnih oblik informacij javnega značaja (objave v glasilih, publikacijah, medijih, strokovni literaturi in podobno) prosilcem prihranila vlaganje zahtev. V praksi se opaža, da številni zavezanci nimajo niti svoje spletne strani (med njimi je največ javnih zavodov in izvajalcev javnih služb), zato morajo prosilci za dostop do katere koli informacije javnega značaja vložiti posebno zahtevo.

Prav tako je mogoče opaziti, da zavezanci niso seznanjeni z izrecno zakonsko določbo, po kateri se prosilcu pri zahtevi po dostopu ni treba sklicevati na ZDIJZ oziroma da je zavezanec dolžan obravnavati zahtevo po ZDIJZ, če že iz narave zahteve izhaja, da gre za zahtevo po ZDIJZ. Zaradi tega zahteve po dostopu do informacij javnega značaja pogosto štejejo kot zahteve po pregledu in prepisu spisa po postopkovnem predpisu. Ti predpisi za pregled in prepis spisa zahtevajo pravni interes ali opravičeno korist, zato zavezanci prosilce za dostop do informacij javnega značaja napačno pozivajo k dopolnitvi zahteve ali pa zahtevo zavrnejo, ker pravni interes ni izkazan. V pritožbenem postopku se pri praksi zavezancev opaža tudi nezadovoljivo spoštovanje načela pomoči prava nevedni stranki pri sestavi in dopolnitvi zahteve po ZDIJZ. Pogosto je posledica takšnega pomanjkljivega sodelovanja tudi zahteva po večjem številu dokumentov. Obsežnost zahtevane dokumentacije je pri zavezanecih pogosto razlog za zavrnitev zahteve zaradi posplošenega sklicevanja na eno od izjem. Informacijski pooblaščenec opozarja, da bi lahko zavezanec z ustreznim, tudi neformalnim komuniciranjem, ki ga ZDIJZ omogoča, pogosto vzpostavil stik s prosilcem in mu tako omogočil pridobitev informacije, ki jo zahteva. Prosilci namreč pogosto zahtevajo obsežno dokumentacijo zgolj zaradi nepoznavanja informacij, s katerimi zavezanec resnično razpolaga in zato oblikujejo široko zahtevo po dostopu. Zavezanci bi zato v skladu z načelom pomoči prava nevedni stranki morali pomagati tudi tako, da bi skupaj s prosilcem poiskali tiste informacije javnega značaja, ki prosilca zanimajo. Tudi če bi se ugotovilo, da prosilec zahteva obsežno dokumentacijo, dostopa do nje ne bi smeli zavrniti zgolj zaradi morebitnega dela pri iskanju oziroma pripravi te dokumentacije. Celotna komunikacija med prosilcem in zavezancem bi zato morala potekati v duhu odprtosti, s tem pa prostega dostopa do informacij javnega značaja, ne pa s ciljem preprečiti prosilcu dostop do njih.

Informacijski pooblaščenec zavezancem priporoča tudi, da večjo pozornost posvetijo ponovni uporabi informacij javnega značaja. Ponovna uporaba informacij javnega značaja pomeni uporabo s strani fizičnih oseb ali pravnih oseb za pridobitne ali nepridobitne namene, razen za prvotni namen v okviru javne naloge, zaradi katerega so bili dokumenti izdelani. Uporaba informacij za izvajanje javnih nalog organa ali izmenjava informacij med organi za izvajanje javnih nalog se ne šteje za ponovno uporabo informacij. Institut ponovne uporabe informacij javnega značaja pomeni večjo preglednost in dorečenost uporabe informacij, ki jih komercialni ali nekomercialni uporabniki dobijo od javnega sektorja. Organi javnega sektorja zbirajo, proizvajajo, reproducirajo in razširjajo dokumente, da izpolnijo svoje javne naloge, določene z veljavnimi predpisi. Uporaba takih dokumentov za druge namene, kot so bili dokumenti izdelani, pa pome-

ni ponovno uporabo. Cilj ponovne uporabe je dodana vrednost informacije javnega značaja, zasebni sektor (prosiliec) pa naj bi ponudil več ali nekaj drugega, kot ponuja organ ob izvajanju svojih javnih nalog. Smisel nadaljnje uporabe ali izkoriščanja informacij javnega značaja je nadgradnja teh informacij s strani prosilca in s tem izpolnjevanje gospodarske funkcije pravice dostopa do informacij javnega značaja. Pri gospodarski funkciji se pokaže njen pomen za gospodarstvo, saj s ponovno uporabo informacij nastane trg z informacijami javnega sektorja, ki je eden izmed ključnih trgov pri širjenju komunikacijske tehnologije. Predvsem komercialni uporabniki tako pridobljene informacije obdelajo, naredijo oziroma izdelajo neko dodano vrednost in nato obogateno informacijo ponudijo nazaj na trg, pri čemer komercialne uporabnike k obogatitvi informacij zavezuje le trg, in nikakor ne sam zakon. Javni sektor, natančneje vsak posamezen organ, ima po določilu 1. odstavka 34. a člena ZDIJZ pravico, da ponovno uporabo za pridobitne namene zaračuna. To pa pomeni, da ponovno uporabo za pridobitne namene lahko zaračuna, ni pa tega dolžan storiti. Pomembna je tudi prepoved diskriminacije prosilcev, kar pomeni, da je ponovna uporaba informacij po enaki ceni in pod enakimi drugimi pogoji dovoljena in omogočena vsem prosilcem. Glede na pozitivne učinke ponovne uporabe bi bilo smiselno, da jo začnejo zavezanci promovirati. Poleg tega pa bi se v ta namen morala dosledno spoštovati določba, da mora zavezanec vse pogoje za ponovno uporabo informacij, običajno ceno in obračunske podlage pri posebnih zahtevah za ponovno uporabo informacij, vnaprej objaviti na svetovnem spletu.

Informacijski pooblaščenec priporoča, da ZDIJZ ostane tisti zakon, ki celovito in sistemsko ureja področje dostopa do informacij javnega značaja. Tako se spoštuje načelo javnosti dela za vse organe v javnem sektorju. Informacijski pooblaščenec opazuje, da želijo predlagatelji različnih predpisov posegati na področje dostopa do informacij javnega značaja in nekatere sklope informacij izvzeti iz načeloma prosto dostopnih informacij. Z različnimi predpisi želijo uvesti tudi nove vrste izjem med prosto dostopnimi informacijami, ki bi bile absolutne. Dodatne absolutne izjeme med prosto dostopnimi informacijami, ki so določene v ZDIJZ, niso niti potrebne niti smiselne, saj je zaradi pravne varnosti treba čim bolj težiti k enotni ureditvi dostopa do informacij javnega značaja. Pri dostopu do informacij javnega značaja razlikujemo med dvema kategorijama izjem. Za absolutne izjeme je značilno, da povzročijo zavrnitev dostopa takoj po ugotovitvi, da obstajajo. Za relativne izjeme pa je značilno, da mora organ pri presoji, ali neki podatek spada med take izjeme ali ne, opraviti test javne koristi ali škodni test, s katerim presodi, ali je javni interes za objavo dokumenta večji od interesa, da se dokument ne objavi. Če so izjeme izpeljane absolutno, je treba za vsak primer posebej ugotoviti le, ali obstaja katera od okoliščin, zaradi katerih je treba dostop do posamezne informacije omejiti. Če taka okoliščina (izjema) obstaja, se dostopa ne dovoli, v vseh drugih primerih pa je treba prosilcu informacijo posredovati. Pri absolutnih izjemah ni treba izvajati nobenega testa. Pri relativnih izjemah pa je treba za vsak primer ugotoviti, ali gre za eno od predpisanih izjem dostopa in za vsak dani primer pretehtati, ali gre res za upravičeno izjemo ali pa kljub vsemu prevlada pravica do dostopnosti informacij javnega značaja. Prav tako je pomembno, da je seznam izjem čim krajši in da so izjeme normativno oblikovane tako, da se lahko tudi v praksi interpretirajo čim bolj restriktivno. Tako kot vse izjeme se morajo tudi izjeme med prosto dostopnimi informacijami razlagati čim bolj ozko oziroma restriktivno. Izjeme med prosto dostopnimi informacijami so namreč kategorija, ki najbolj zaznamuje normativno ureditev in praktično uporabo ZDIJZ. Določno oblikovane izjeme, ki ne dopuščajo ekstenzivnih interpretacij, so bistvenega pomena za odprto delovanje družbe. Tolmačenje izjem sodi

med najzahtevnejše izzive zavezancev in pritožbenih organov na področju izvajanja normativnih ureditev. V luči teh smernic Informacijski pooblaščenec vedno odsvetuje sprejetje takšnih predpisov.

2.7. Predstavitev najodmevnejših in precedenčnih primerov po področjih

V nadaljevanju je po posameznih področjih predstavljenih nekaj najzahtevnejših odločb v letu 2006:

2.7.1. Ponovna uporaba informacij javnega značaja

V odločbi, izdani 12. decembra 2006, št. 021-69/2006/2, prosilca družbe Registri Noviforum d. o. o., zoper odločbo javnega zavoda ARNES, je Informacijski pooblaščenec odločil, da je pritožba neutemeljena. Prosilec je želel za ponovno uporabo pridobiti podatke iz registra domen pod vrhno domeno .SI, ki ga organ vodi na podlagi Sklepa o ustanovitvi javnega zavoda Akademska in raziskovalna mreža Slovenije¹⁵. Ponovna uporaba informacij javnega značaja v skladu s 3. odstavkom 4. člena ZDIJZ pomeni uporabo s strani fizičnih oseb ali pravnih oseb za pridobitne ali nepridobitne namene razen za prvotni namen v okviru javne naloge, zaradi katerega so bili dokumenti izdelani. V postopku odločanja se je Informacijski pooblaščenec najprej ukvarjal z vprašanjem, ali zahtevane informacije izvirajo z delovnega področja organa, oziroma, ali jih ta zbira v okviru svoje javne naloge. Ocenil je, da je bistvena 4. točka 2. odstavka 4. člena Sklepa o ustanovitvi ARNES, ki določa, da je ena od dejavnosti organa, da "upravlja slovenski internetni imenski prostor (domena .SI)". Iz navedene točke je jasno razvidno, da je Vlada Republike Slovenije organu s Sklepom o ustanovitvi ARNES kot eno izmed nalog naložila upravljanje internetnega imenskega prostora (domena .SI) in posledično tudi vzpostavitev vseh tehničnih in operativnih postopkov, ki jih ta naloga zahteva. Med njimi sta nujno tudi postopek registracije domen pod vrhno domeno .SI ter vodenje registra WHOIS vpisanih registrantov. Potem se je Informacijski pooblaščenec podrobno ukvarjal z vprašanjem obstoja poslovne skrivnosti po 2. odstavku 39. člena Zakona o gospodarskih družbah¹⁶ in s tem izjeme po 2. točki 1. odstavka 6. člena ZDIJZ. Pri tem se je oprl na pravnomočno odločbo, v kateri je podrobno argumentiral, da smejo tudi javnopravne osebe imeti in varovati svoje poslovne skrivnosti. Podrobna analiza prakse organizacije ICANN (Internet Corporation for Assigned Names and Numbers) in prakse registra EurID ter izvedba škodnega testa sta pripeljali do sklepa, da obstaja izjema poslovne skrivnosti kot izjema dostopa po 2. točki 1. odstavka 6. člena ZDIJZ.

V odločbi, izdani 25. septembra 2006, št. 021-6/2006/925.09.2006, prosilca Realis d. o. o., zoper odločbo Geodetske uprave Republike Slovenije, je Informacijski pooblaščenec ugodil pritožbi. Prosilec je od organa zahteval informacije za ponovno uporabo za pridobitne namene, in sicer digitalni ortofoto v merilu 1 : 5000, register prostorskih enot, hišne številke, register zemljepisnih imen (REZI 25), vse za celotno območje Republike Slovenije. Informacijski pooblaščenec je ugotovil, da je informacije, ki jih je zahteval prosilec, organ izdelal v okviru svoje javnopravne funkcije, saj gre za podatke, ki jih državni

15 Uradni list RS, št. 38/2002, 61/2005 (Sklep o ustanovitvi ARNES).

16 Uradni list RS, št. 42/2006, spremenjen 60/2006.

organi, organi lokalnih skupnosti in posamezniki potrebujejo za prostorsko načrtovanje, planiranje in evidentiranje v prostoru in se kot taki izdelujejo za javno korist. Organ, ki je ustanovljen za opravljanje nalog geodetske službe, mora voditi zbirke topografskih in kartografskih podatkov, katerih del so tudi informacije, ki jih je zahteval prosilec. Obveznost vodenja teh zbirk organu narekuje Zakon o geodetski dejavnosti¹⁷, konkretno pa tudi Uredba o tarifah za izdajanje geodetskih podatkov¹⁸, ki določa tarifo za dokumente, ki jih je zahteval prosilec. Ker organ med postopkom ni izračunal cene ponovne uporabe za zahtevane informacije, je Informacijski pooblaščenec izpodbijano odločbo odpravil ter vrnil organu prve stopnje v ponovno odločanje. Organu je naložil, da mora v skladu z določbami ZDIJZ in Uredbo o posredovanju in ponovni uporabi informacij javnega značaja¹⁹ izračunati ceno in navesti morebitne dodatne pogoje za ponovno uporabo ter obračunsko podlago, na kateri izračunana cena temelji.

V odločbi, izdani 4. avgusta 2006, št. 021-54/2006/3, prosilca Društvo za raziskovanje jam Ljubljana, zoper odločbo Geodetske uprave Republike Slovenije, je Informacijski pooblaščenec pritožbi ugodil in izpodbijano odločbo odpravil. Organu je naložil, naj prosilcu izroči zadnje razpoložljive različice topografskih slojev za območje celotne Slovenije, v elektronski obliki, v standardnih formatih na nosilcih DVD, in sicer:

- temeljne topografske načrte v merilu 1 : 5.000 in 1 : 10.000 – vsi sloji,
- državne topografske karte v merilu 1 : 25.000 – vsi sloji,
- digitalni modeli višin (25m metrska mreža),
- ortofoto v merilu 1 : 5000 – sivinski in vsi razpoložljivi barvni.

Prosilec je navedene dokumente zahteval za ponovno uporabo za nepridobitne namene. Organ je zahtevo na podlagi ZDIJZ zavrnil in navedel, da lahko prosilec zahtevane dokumente dobi na način in pod pogoji, kot jih določa Uredba o tarifah za izdajanje geodetskih podatkov. Informacijski pooblaščenec se s tem stališčem organa ni strinjal. Opozoril je, da je za ponovno uporabo informacij ključno, da organi javnega sektorja informacije prvenstveno zbirajo za izvrševanje svojih javnih nalog, že zbrane informacije pa lahko posredujejo prosilcem za nadaljnjo uporabo za pridobitne ali nepridobitne namene. Informacijski pooblaščenec je ugotovil, da informacije, ki jih je zahteval prosilec, spadajo med podatke, ki jih organ vodi v okviru geodetske službe, saj uredba zanje določa tarifo za uporabo. Informacijski pooblaščenec je pri tem tudi opozoril, da se mora država zavedati vseh posledic spoštovanja evropskih pravil in posledično tudi vseh posledic, ki so na področju ponovne uporabe v javnem sektorju nastale z ZDIJZ. Iz določb ZDIJZ je predvsem mogoče razbrati stališče zakonodajalca, da je treba vse informacije javnega značaja obravnavati enako. Upoštevajoč vse navedeno je Informacijski pooblaščenec sklenil, da je v tem primeru glede ponovne uporabe informacij javnega značaja treba uporabiti ZDIJZ in na njegovi podlagi izdano Uredbo o posredovanju in ponovni uporabi informacij javnega značaja.

2.7.2. Pravdni postopek

V odločbi, izdani 4. decembra 2006, št. 021-89/2006/7, prosilke Ive Ropac, novin- arke Dela, zoper odločbo Republike Slovenije, Okrožnega sodišča v Ljubljani, je In-

17 Uradni list RS, št. 8/2000, s spremembami in dopolnitvami

18 Uradni list RS, št. 60/2002, 116/2003, 45/2004, 66/2005 in 47/2006-ZEN.

19 Uradni list RS, št. 76/2005.

formacijski pooblaščenec pritožbi ugodil in izpodbijano odločbo odpravil. Organu je naložil, da mora prosilki v roku treh dni od pravnomočnosti odločbe posredovati sodbo Okrožnega sodišča v Ljubljani, opr. št. III P 1839/5, z dne 10. marec 2006, pri čemer je dolžan izbrisati podatke o tožniku (ime in priimek ter prebivališče). Organ se je skliceval na izjemo iz 8. točke 1. odstavka 6. člena ZDIJZ in je dostop do navedene sodbe zavrnil, ker sodni postopek še ni pravnomočno končan in bi posredovanje te sodbe lahko vplivalo na sodišče II. stopnje. Informacijski pooblaščenec se s to argumentacijo organa ni mogel strinjati. Če namreč sodišče ob raznih pritiskih, zlasti pa pri medijsko odmevnih primerih, ne bi bilo zmožno objektivnega, profesionalnega in nepristranskega sojenja, bi to lahko pomenilo kratenje pravice iz 23. člena Ustave RS, ki vsakomur zagotavlja, da o njegovih pravicah in dolžnostih ter o obtožbah proti njemu brez nepotrebnega odlašanja odloča neodvisno, nepristransko in z zakonom ustanovljeno sodišče. Takim pritiskom so izpostavljeni tudi mnogi drugi javni uslužbenci oziroma funkcionarji, pa se kljub temu od njih (upravičeno) pričakuje, da strokovno, neodvisno in nepristransko opravljajo svoje naloge. Zato je Informacijski pooblaščenec ocenil, da zavračanje dostopa do nepravnomočne sodbe zaradi morebitnega vplivanja na odločitve sodišča II. stopnje ne vzdrži resne pravne presoje. To pomeni, da izjema iz 8. točke 1. odstavka 6. člena ZDIJZ ni bila izkazana. Po uradni dolžnosti je Informacijski pooblaščenec ugotavljal, ali gre pri zahtevanem dokumentu še za kako drugo izjemo. Ugotovil je, da ta vsebuje številne varovane občutljive osebne podatke, ki so izjema po 3. točki 1. odstavka 6. člena ZDIJZ. Obenem je ocenil, da je mogoče uporabiti institut delnega dostopa in prosilki omogočiti delni dostop do zahtevanega dokumenta.

2.7.3. Poslovna skrivnost

V odločbi, izdani 4. decembra 2006, 021-62/2006/2, prosilke Jasne Tepina, novinarka RTV Slovenija, zoper odločbo Agencije Republike Slovenije za zdravila in medicinske pripomočke, je Informacijski pooblaščenec odločil, da pritožbi ugodil in se izpodbijana odločba odpravi. Organu je naložil, da prosilki v roku treh dni od pravnomočnosti odločbe omogoči vpogled v upravne odločbe, s katerimi je organ Kliničnemu centru in zdravnikom, zaposlenim v njem, odobril klinično preizkušanje zdravil v letih 2004 in 2005. Bistveno vprašanje, ki ga je Informacijski pooblaščenec presojal, je bilo, ali velja izjema po 7. točki 1. odstavka 6. člena ZDIJZ, po kateri lahko organ zahtevo po dostopu do informacije javnega značaja zavrne, če gre za podatek, ki je bil sestavljen zaradi upravnega postopka in bi njegovo razkritje lahko škodovalo njegovi izvedbi. Pri izvedbi škodnega testa, ki ga zahteva navedena izjema, je Informacijski pooblaščenec ugotovil, da gre pri zahtevanih dokumentih za upravne odločbe, ki so bile izdane v letih 2004 in 2005, in s katerimi je organ odobril klinično preizkušanje, kar pomeni, da so ti postopki že končani. Njihovo razkritje tako ne more škodovati izvedbi upravnih postopkov, zato ne gre za izjemo prostega dostopa po 7. točki 1. odstavka 6. člena ZDIJZ. Informacijski pooblaščenec tudi ni sprejel argumenta organa, da gre pri zahtevanih dokumentih za dokumentacijo iz vloge za pridobitev dovoljenja za promet z zdravilom, ki je last predlagatelja in je kot taka poslovna skrivnost po 51. členu Zakona o zdravilih²⁰. Predmet zahteve so bile namreč zgolj upravne odločbe, s katerimi je organ klinično preizkušanje dovolil, ne pa celotna dokumentacija v postopku. Po pregledu zahtevanih odločb je Informacijski pooblaščenec ugotovil, da zahtevane odločbe vsebujejo samo obvezne sestavine, ki jih določa Zakon o splošnem upravnem postopku²¹, in ne tudi drugih podatkov, ki bi lahko bili poslovna skrivnost v smislu 2. odstavka 39. člena Zakona o gospodarskih družbah.

20 Uradni list RS, št. 31/2006.

21 Uradni list RS, št. 24/2006, uradno prečiščeno besedilo.

V odločbi, izdani 29. novembra 2006, št. 021-33/2006/7, prosilke, zoper odločbo Fakultete za pomorstvo in promet, je Informacijski pooblaščenec odločil, da je pritožba delno utemeljena.

Organ je v obrazložitvi izpodbijanega dela odločbe kot glavni argument navedel, da pri izplačilih avtorskih honorarjev in izplačilih po podjemnih pogodbah za izredni in podiplomski študij ne gre za proračunska sredstva, zato v tem delu ni zavezanec po ZDIJZ. Informacijski pooblaščenec je zato najprej presojal, ali je organ tudi v tem delu dejavnosti zavezanec po ZDIJZ. Informacijski pooblaščenec je po pregledu področne zakonodaje ocenil, da tudi izredni študij spada v okvir javne službe, ki jo izvaja organ, zato je tudi v tistem delu dejavnosti, ki se nanaša na izredni študij, zavezanec po ZDIJZ. Tako redni kot izredni študij potekata v okviru nacionalnega programa visokega šolstva, ki določa javno službo v visokem šolstvu, zato je izredni študij zgolj ena izmed možnih oblik organiziranja študija v okviru nacionalnega programa visokega šolstva. Drugače pa je pri projektih, ki jih organ izvaja zunaj študijskih programov in nacionalnega programa visokega šolstva. Gre za projekte in opravila, ki jih pri organu naročijo drugi subjekti in so tudi financirani iz zasebnih sredstev. Pri tem pa gre po mnenju Informacijskega pooblaščenca nedvomno za zasebno dejavnost organa na trgu, kar seveda ne sodi v okvir javne službe, zato organ v tem delu ni zavezanec po ZDIJZ. Enako velja tudi za vsa izplačila, ki so jih zaposleni in zunanji sodelavci prejeli za dela, ki niso povezana s študijskimi programi (npr. izvedenska mnenja v imenu avtorja, prevodi, raziskovalna dela in založniška dejavnost zunaj študijskih programov). Tudi pri tem gre za zasebno dejavnost avtorjev na trgu, ki ne sodi v okvir javne službe, zato organ tovrstnih podatkov na podlagi ZDIJZ prosilcem ni dolžan posredovati. Informacijski pooblaščenec se je v nadaljevanju podrobno opredelil do izplačil po avtorskih in podjemnih pogodbah, izplačil za udeležbe na kongresih, konferencah, seminarjih, gostovanjih na tujih univerzah, izplačil potnih stroškov, dnevnic in drugih nadomestil za izredni študij, izplačil za prevoze na delo, za nadurno delo ter do soglasij za dopolnilno delo.

2.7.4. Tajni podatki

V odločbi, izdani 10. novembra 2006, št. 021-77/2006/6, prosilca Nenada Glucksa, novinarja Maga, zoper odločbo Sodnega sveta, je Informacijski pooblaščenec pritožbi ugodil. Prosilec je od organa zahteval sklep oziroma odločbo z obrazložitvijo, s katero je organ potrdil negativno oceno sodniške službe ene izmed sodnic. V izpodbijani odločbi se je organ skliceval na izjeme iz 1. in 3. točke 1. odstavka 6. člena ZDIJZ, ker naj bi šlo za tajne in osebne podatke. Informacijski pooblaščenec je ugotovil, da v tem primeru izjema iz 1. točke 1. odstavka 6. člena ZDIJZ ne velja. Že na prvi pogled je bilo namreč očitno, da se zahtevani podatki ne nanašajo na javno varnost, obrambo, zunanje zadeve, obveščevalno in varnostno dejavnost državnih organov RS oziroma na sisteme, naprave, projekte in načrte ali znanstvene, raziskovalne, tehnološke, gospodarske in finančne zadeve, ki so pomembni za omenjene naloge. Podatki v zahtevani odločbi pa tudi niso bili opredeljeni kot tajni na podlagi Zakona o tajnih podatkih²². Pri ugotavljanju obstoja izjeme iz 3. točke 1. odstavka 6. člena ZDIJZ je Informacijski pooblaščenec opozoril na 1. alinejo 3. odstavka 6. člena ZDIJZ, da se kljub določbi prvega odstavka dostop do zahtevane informacije dovoli, če gre za podatke o porabi javnih sredstev ali podatke, povezane z opravljanjem javne funkcije ali z delovnim razmerjem javnega uslužbenca, razen v primerih iz 1. in 5. do 8. točke 1. odstavka, ter takrat, ko zakon, ki ureja javne finance, ali zakon, ki ureja javna naročila, določa drugače. Poleg tega je Informacijski pooblaščenec tudi poudaril, da je za vsako državo izjemnega pomena zaupanje državljanov v sodstvo,

²² Uradni list RS, št. 50/2006.

ki mora biti že na podlagi ustave neodvisno, nepristransko in učinkovito, razkritje ocen sodniških služb sodečih sodnikov, ki predstavljajo sodni sistem, pa bi lahko privedlo do nezaupanja javnosti v sodstvo in s tem tudi do poslabšanja vtisa o sodstvu kot neodvisni in nepristranski veji oblasti, ki deluje strokovno in po najvišjih moralnih načelih. Obravnavani primer je bil netipičen, saj sodnica te funkcije ne opravlja več. K enakemu sklepu je Informacijskega pooblaščenca pripeljal tudi test interesa javnosti, zato je organu naložil, da mora prosilcu posredovati fotokopijo celotnega drugega in tretjega odstavka obrazložitve svoje odločbe št. 2/06-1187, z dne 10. julij 2006.

Odločba, izdana 15. maja 2006, št. 021-18/2006/8, je obravnavala pritožbo prosilca Pavla Gantarja, poslanca LDS, zoper odločbo Ministrstva za gospodarstvo. Informacijski pooblaščenec je pritožbi ugodil in organu naložil, da v roku treh dni od pravnomočnosti odločbe prosilcu posreduje dokument z naslovom "Republika Slovenija, Privatizacijska skupina za Telekom Slovenije, Predlog odprodaje dela državnega deleža v Telekomu Slovenije d. d., Ljubljana, december 2005". Pri temeljitem pregledu navedenega dokumenta je namreč Informacijski pooblaščenec ugotovil, da ne velja nobena izmed zahtevanih izjem iz 1. odstavka 6. člena ZDIJZ (tajni podatek, poslovna skrivnost, podatek iz dokumenta, ki je v postopku izdelave in je še predmet posvetovanja v organu), na katere se je v izpodbijani odločbi skliceval organ.

2.7.5. Kazenski postopek

Odločba, izdana 12. aprila 2006, št. 021-106/2005/5, je obravnavala pritožbo prosilke Majde Vukelič, novinarka časopisa Delo, zoper odločbo Vlade Republike Slovenije. Prosilka je od organa želela dobiti fotokopijo ovadbe, ki jo je policija vložila zoper predsednika uprave Vzajemne Marka Jakliča zaradi suma storitve kaznivega dejanja zlorabe položaja. Organ je zahtevo prosilke zavrnil, sklicujoč se predvsem na 6. točko 1. odstavka 6. člena ZDIJZ (podatek, pridobljen ali sestavljen zaradi kazenskega postopka ali v zvezi z njim) ter na 2. in 3. točko 1. odstavka 6. člena ZDIJZ (poslovna skrivnost in osebni podatek). Informacijski pooblaščenec je pritožbo prosilke zavrnil kot neutemeljeno, saj je ocenil, da v tem primeru velja izjema iz 6. točke 1. odstavka 6. člena ZDIJZ. Postopek kazenskega pregona je bil namreč še vedno v začetni fazi, to je v fazi t. i. "policijske preiskave", ki je za uspešno odkrivanje storilcev kaznivih dejanj ključnega pomena. Po mnenju Informacijskega pooblaščenca je šlo v obravnavanem dokumentu za tolikšno vsebnost in koncentracijo podatkov, ki so izjema po 6. točki 1. odstavka 6. člena ZDIJZ, da tudi instituta delnega dostopa ni bilo mogoče uporabiti, hkrati pa tudi interes javnosti za razkritje zahtevanih podatkov ni bil tolikšen, da bi prevladal nad interesom osumljenca ter javnim interesom za učinkovito izvedbo postopka kazenskega pregona. Ker je Informacijski pooblaščenec ugotovil, da je treba dostop do zahtevanega dokumenta v celoti zavrniti že na podlagi navedene izjeme ZDIJZ, pri čemer je opravil tudi test interesa javnosti, ni več presojal, ali sta veljali tudi izjemi iz 2. oziroma 3. točke 1. odstavka 6. člena ZDIJZ.

2.7.6. Dokument v izdelavi

Odločba, izdana 27. marca 2006, št. 021-10/2006/5, je obravnavala pritožbo prosilca Aleša Guliča, poslanca LDS, zoper odločbo Ministrstva za kulturo. Prosilec je od organa želel dobiti fotokopiji dokumenta z naslovom "Analiza vpliva potencialne uvedbe enotne davčne stopnje na kulturo v Sloveniji", ki ga je izdelal MFB Consulting d. o. o. oktobra 2005, in dokumenta z naslovom "Prednosti in pomanjkljivosti morebitne uvel-

javitve enotne davčne stopnje v Sloveniji za področje kulturnih dejavnosti na osnovi primerjalne analize s Slovaško ter njeno tovrstno izkušnjo", ki ga je izdelalo Društvo Apokalipsa, Stanislava Repar & kol.. Organ je zahtevo prosilca zavrnil, sklicujoč se na 9. točko 1. odstavka 6. člena ZDIJZ (dokument v postopku izdelave), ker raziskava ter primerjalna analiza posledic uvedbe enotne davčne stopnje še nista bili končani. Informacijski pooblaščenec je pritožbi ugodil in organu naložil, da prosilcu posreduje fotokopiji zahtevanih dokumentov, saj je ugotovil, da sta oba dokumenta že v celoti izdelana, in sicer s strani druge osebe, ki ju je poslala organu, tako da ta sploh ni sam vodil postopka izdelave dokumentov. Na to je kazalo tudi dejstvo, da je organ obema izvajalcema že plačal njuno storitev.

Odločba, izdana 23. marca 2006, št. 021-16/2006/4, je obravnavala pritožbo prosilca Amnesty International zoper odločbo Vlade RS. Prosilec je od organa želel dobiti elektronsko obliko ali fotokopijo predloga t. i. ustavnega zakona o izbrisanih z vsemi morebitnimi prilogami. Organ je zahtevo prosilca zavrnil, sklicujoč se na 1. točko 1. odstavka 6. člena ZDIJZ (tajni podatki) in 9. točko 1. odstavka 6. člena ZDIJZ (dokument v postopku izdelave). Informacijski pooblaščenec je pritožbi ugodil in organu naložil, da prosilcu posreduje dokument z naslovom »Predlog ustavnega zakona o dopolnitvi ustavnega zakona za izvedbo Temeljne ustavne listine o samostojnosti in neodvisnosti Republike Slovenije«, z dne 8. 12. 2005. Vsebina zahtevanega dokumenta se namreč ne nanaša na nobeno izmed v 5. členu Zakona o tajnih podatkih taksativno naštetih interesnih področij države, zato podatkov v zahtevanem dokumentu po omenjenem zakonu sploh ni dopustno določiti za tajne. Pri zahtevanem dokumentu tudi ni šlo za dokument v postopku izdelave v smislu 9. točke 1. odstavka 6. člena ZDIJZ. Dokument je Ministrstvo za notranje zadeve, ki je bilo pristojno za njegovo pripravo, poslalo v obravnavo organu, kar pomeni, da je pripravljavec dokumenta že končal v smislu 1. odstavka 7. člena Uredbe o posredovanju informacij javnega značaja in je ta predstavljal različico predloga ustavnega zakona.

2.7.7. Notranje delovanje organa

Odločba, izdana 28. februarja 2006, št. 021-61/2005/7, je obravnavala pritožbo prosilke Ranke Ivelja, novinarka Dnevnika, zoper odločbo Državnega izpitnega centra. V obrazložitvi so obširno pojasnjeni vsi argumenti, na podlagi katerih se je Informacijski pooblaščenec odločil, da so prosto dostopni podatki o:

- odstotku kandidatov, ki so na posamezni šoli maturo opravili v spomladanskem roku;
- številu dijakov, ki so na posamezni šoli v spomladanskem roku dosegli 30 točk in več;
- številu točk, ki jih je v povprečju dosegla posamezna šola v spomladanskem roku;
- številu točk, ki jih je v navedenih dveh šolskih letih v povprečju dosegla posamezna šola pri posameznem maturitetnem predmetu.

Informacijski pooblaščenec je ugotovil, da v tej zadevi ne gre niti za tajne podatke niti za dokumente v izdelavi oziroma za podatke v zvezi z notranjim delovanjem organa. Posebno pozornost je namenil argumentu organa, da gre za zavajajoče podatke, ki bi lahko povzročili napačno razumevanje. Informacijski pooblaščenec je opozoril, da nezanesljivost zahtevanih podatkov ni razlog za zavrnitev dostopa do teh informacij. Z vidika dostopa do informacij javnega značaja namreč informacij ni mogoče deliti na

pravilne in nepravilne, prave in neprave in javnosti seznanjati le s tistimi informacijami, za katere bi organi, zavezanci po ZDIJZ, sami ocenili, da so pravilne. To bi v skrajnem primeru lahko vodilo do prirejanja in manipuliranja z informacijami javnega značaja in pomenilo velik odmik od transparentnega in odprtega delovanja javnega sektorja, ki je temeljno načelo ZDIJZ.

2.7.8. Ali je organ zavezanec

V odločbi, izdani 28. junija 2006, št. 021-5/2006/15, prosilke Jasne Tepina, novinarka RTV Slovenija, zoper molk Univerzitetnega kliničnega centra Ljubljana (UKC), je Informacijski pooblaščenec pritožbo zaradi molka in zahtevo kot neutemeljeni zavrnil. Prosilka je zahtevala dostop do podatkov o vseh vrstah in oblikah izplačil (avtorske in podjetne pogodbe, stimulacije ...), ki jih nekateri zdravniki v UKC dobivajo za klinično preizkušanje zdravil. Prosilka je zahtevala podatke za leti 2004 in 2005. Organ je odgovoril, da gre za »lastne prihodke UKC-ja.« Informacijski pooblaščenec je v postopku odločanja ugotovil, da je organ javni zdravstveni zavod in da v teoriji ni sporno, da je javni zdravstveni zavod ena od oblik, s katero se zagotovi izvajanje javne službe. Za vse izvajalce javnih služb pa je značilno, da so lahko zavezani omogočanju dostopa do informacij javnega značaja samo v tistem delu svoje dejavnosti, ki predstavlja izvajanje javne službe, ne pa tudi pri drugih dejavnostih, ki niso povezane z izvajanjem javne službe. Za izvajalce javnih služb je namreč značilno, da opravljajo še zasebnopravne, tržne dejavnosti, v okviru katerih niso zavezani posredovati informacije javnega značaja zato, ker v delu dejavnosti, podvrženem tržnemu področju, informacije javnega značaja pojmovno ne morejo nastati. Zaradi navedenega je Informacijski pooblaščenec presojal, ali so zahtevani dokumenti prosto dostopne informacije javnega značaja ali izjeme prostega dostopa in ali gre za informacije, povezane z izvajanjem javne službe organa, ne pa z opravljanjem njegovih tržnih, zasebnopravnih dejavnosti. Po preučitvi področne zakonodaje je Informacijski pooblaščenec ugotovil, da klinično preizkušanje zdravil ne sodi v tisto vrsto zdravstvene dejavnosti, ki bi jo bil organ kot javni zdravstveni zavod dolžan izvajati kot javno službo. Informacijski pooblaščenec je kot glavno okoliščino, zaradi katere kliničnega preizkušanja ni mogoče uvrstiti med dejavnosti, ki se opravljajo kot javna služba, navedel, da tudi neenakomerna porazdelitev te storitve ne bi imela takih posledic, kot sta družbena neenakost in nepravičnost. Zato klinično preizkušanje zdravil ne predstavlja javne dobrine oziroma javne storitve. Prav tako kliničnega preizkušanja zdravil ne gre šteti med zdravstvene dejavnosti, ki se lahko v skladu z Zakonom o zdravstveni dejavnosti²³ opravljajo kot javna služba. Zaradi navedenega je Informacijski pooblaščenec pritožbo prosilke zavrnil, saj organ kot izvajalec javne službe v tem delu ni zavezanec za informacije javnega značaja. Informacijski pooblaščenec je v odločbi opozoril tudi na število pogodb o kliničnem preizkušanju zdravil, ki jih ima organ v svojih evidencah oziroma v posesti, v primerjavi s številom odločb, h katerim je Agencija organu dala soglasje za klinično preskušanje zdravil. Opozoril je tudi na avtorske pogodbe med zdravniki in organom o kliničnem preizkušanju zdravil in na to, da se dejavnost opravlja v prostorih in z opremo organa in na pacientih, ki so pri organu kot uporabniki javnih storitev. Vendar je za to področje pristojno predvsem Računsko sodišče Republike Slovenije kot najvišji revizijski organ za nadzor državnih računov, državnega proračuna in celotne javne porabe v Republiki Sloveniji v skladu s 1. členom Zakona o računskem sodišču²⁴. To je pozneje ugotovilo oškodovanje državnega premoženja tudi v tistem delu, na katerega je opozoril Informacijski pooblaščenec.

23 Uradni list RS, št. 23/2005.

24 Uradni list RS, št. 11/2001, 20/2006-ZNOJF.

WATCH YOU



WATCH YOUR

3

**DELO NA PODROČJU VARSTVA
OSEBNIH PODATKOV**

3.1. Koncept varstva osebnih podatkov v Republiki Sloveniji

Koncept varstva osebnih podatkov v Republiki Sloveniji temelji na določbi 38. člena Ustave RS, po kateri je varstvo osebnih podatkov v Republiki Sloveniji ena izmed ustavno zagotovljenih človekovih pravic in temeljnih svoboščin. Določba 38. člena Ustave RS zagotavlja varstvo osebnih podatkov, prepoveduje uporabo osebnih podatkov v nasprotju z namenom njihovega zbiranja ter vsakomur zagotavlja pravico do seznanitve z zbranimi osebnimi podatki, ki se nanašajo nanj, in pravico do sodnega varstva ob njihovi zlorabi. Za normativno urejanje varstva osebnih podatkov je zlasti pomemben drugi odstavek 38. člena Ustave RS, kjer je določeno, da zbiranje, obdelovanje, namen uporabe, nadzor in varstvo tajnosti osebnih podatkov določa zakon. Taka ustavna določba prepoveduje ureditev varstva osebnih podatkov v podzakonskih predpisih, obenem pa omogoča ureditev varstva osebnih podatkov v splošnem, sistemskem zakonu, poleg tega pa dopušča tudi možnost urejanja varstva osebnih podatkov v področnih zakonih, ki pa morajo prav tako spoštovati določbe 38. člena Ustave RS. Ustavodajalec se je torej odločil za t. i. »obdelovalni model«, in ne za t. i. »model zlorabe«, saj je določil predvsem pravila za urejanje dopustne obdelave osebnih podatkov na zakonski ravni in ne načelne svobode pri obdelavi osebnih podatkov, ki je lahko le izjemoma izrecno omejena z zakonom. Po tem modelu je na področju obdelave osebnih podatkov prepovedano vse, razen tistega, kar je z zakonom (na področju zasebnega sektorja tudi z osebno privolitvijo posameznika) izrecno dovoljeno. Vsaka obdelava osebnih podatkov namreč pomeni poseg v z ustavo varovano človekovo pravico do varstva osebnih podatkov. Zato je tak poseg dopusten, če je v zakonu določno opredeljeno, kateri osebni podatki se smejo obdelovati, jasno pa mora biti določen tudi namen obdelave osebnih podatkov, zagotovljeno mora biti ustrezno varstvo in zavarovanje osebnih podatkov. Namen obdelave osebnih podatkov mora biti ustavno dopusten, obdelovati pa se smejo le tiste vrste osebnih podatkov, ki so primerne in nujno potrebne za uresničitev zakonsko opredeljenega in ustavno dopustnega namena.

Ureditev varstva osebnih podatkov v sistemskem zakonu je potrebna zaradi enotne določitve načel, pravil in obveznosti kakor tudi zaradi zapolnitve pravnih praznin, ki bi lahko nastale v področnih zakonih. Poleg tega je tudi nepotrebno, da bi se definicije, obveznosti in ukrepi v zvezi z zavarovanjem osebnih podatkov, katalogi zbirk osebnih podatkov, registracija zbirk osebnih podatkov v zvezi s pravicami posameznika do seznanitve s podatki, ki se nanašajo nanj, ter vprašanja glede nadzora in pristojnosti nadzornega organa (ipd.) vedno predpisovali tudi v področnih zakonih. Namen sistema zakona torej ni v podrobnejšem predpisovanju načinov obdelave osebnih podatkov po posameznih področjih, ampak se kaže predvsem v tem, da se v njem določijo splošne pravice, obveznosti, načela in ukrepi, s katerimi se preprečujejo neustavni, nezakoniti in neupravičeni posegi v zasebnost in dostojanstvo posameznika pri obdelavi osebnih podatkov. Zato morajo področni zakoni jasno določati, katere zbirke osebnih podatkov se bodo vzpostavile in vodile na posameznem področju, vrste osebnih podatkov, ki jih bodo posamezne zbirke vsebovale, način zbiranja osebnih podatkov, morebitne omejitve pravic posameznika, zlasti pa namen obdelave zbranih osebnih podatkov. Z vidika varstva posameznika pa je zelo priporočljivo, da se v področnem zakonu določi tudi čas shranjevanja osebnih podatkov (rok hrambe osebnih podatkov).

Zakon o varstvu osebnih podatkov (v nadaljevanju ZVOP-1), ki ga je Državni zbor Republike Slovenije sprejel 15. julija 2004, velja od 1. januarja 2005. Sprejetje zakona je bilo potrebno predvsem zaradi vstopa Republike Slovenije v Evropsko unijo in s tem povezane dolžnosti uskladitve varstva osebnih podatkov z določbami Direktive 95/46/ES Evropskega parlamenta in Sveta o zaščiti posameznikov pri obdelavi osebnih podatkov in o prostem pretoku takih podatkov²⁵.

ZVOP-1 ni le sistemski zakon, ampak je v svojem VI. delu tudi t. i. »področni zakon«, ki s precej natančno določitvijo pravic, obveznosti, načel in ukrepov upravljavcem osebnih podatkov daje neposredno zakonsko podlago za obdelavo osebnih podatkov na področju neposrednega trženja, videonadzora, biometrije, evidentiranja vstopov v prostore in izstopov iz njih ter strokovnega nadzora.

Z uveljavitvijo Zakona o Informacijskem pooblaščenju se je v pravni red Republike Slovenije v celoti prenesla Direktiva 95/46/ES Evropskega parlamenta in Sveta o zaščiti posameznikov pri obdelavi osebnih podatkov in o prostem pretoku takih podatkov.

Poleg Ustave RS, ZVOP-1, ZInfP in zakonov, ki podrobneje predpisujejo obdelavo osebnih podatkov na posameznem področju, se v Republiki Sloveniji pri obdelavi neposredno uporabljajo tudi določbe Konvencije o varstvu posameznikov glede na avtomatsko obdelavo osebnih podatkov. Ta je bila ratificirana in objavljena leta 1994²⁶. Namen navedene konvencije Sveta Evrope je, na ozemlju vsake pogodbenice vsakemu posamezniku, ne glede na državljanstvo in prebivališče, zagotoviti spoštovanje njegovih pravic in temeljnih svoboščin in v tem okviru še posebej spoštovanje pravice do zasebnosti glede na avtomatsko obdelavo osebnih podatkov, ki se nanašajo nanj.

Zloraba osebnih podatkov je v 154. členu Kazenskega zakonika²⁷ opredeljena kot kaznivo dejanje, ki se preganja po uradni dolžnosti. Določeno je, da se z denarno kaznijo ali zaporom do enega leta kaznuje tistega, ki v nasprotju z zakonom uporabi osebne podatke, ki se smejo voditi samo na podlagi zakona ali na podlagi osebne privolitve posameznika, na katerega se podatki nanašajo, ali tistega, ki vdre v računalniško vodenno zbirko podatkov z namenom, da bi sebi ali komu drugemu pridobil kakšen osebni podatek. Če dejanje stori uradna oseba z zlorabo uradnega položaja ali uradnih pravic, se kaznuje z zaporom do dveh let.

3.2. Dejavnost državnih nadzornikov za varstvo osebnih podatkov

3.2.1. Pravice in dolžnosti državnega nadzornika

Državni nadzornik za varstvo osebnih podatkov opravlja inšpekcijski nadzor nad izvajanjem določb ZVOP-1 in je pri opravljanju nalog inšpekcijskega nadzora v skladu s svojimi pooblastili samostojen ter naloge opravlja v okviru in na podlagi ustave in zakonov.

25 Uradni list Evropskih skupnosti, št. L 281, 23. 11. 1995.

26 Uradni list RS, št. 11/1994 – Mednarodne pogodbe št. 3/1994.

27 Uradni list RS, št. 95/2004, uradno prečiščeno besedilo.

Splošna načela inšpekcijskega nadzora, splošne pravice, dolžnosti, pooblastila državnih nadzornikov, postopek inšpekcijskega nadzora, inšpekcijski ukrepi in druga vprašanja, povezana z inšpekcijskim nadzorom, so določeni v Zakonu o inšpekcijskem nadzoru²⁸, specifične pristojnosti državnega nadzornika pa so določene v 53. členu ZVOP-1. Ta določa, da je pri opravljanju inšpekcijskega nadzora nadzornik upravičen:

- pregledovati dokumentacijo, ki zadeva obdelavo osebnih podatkov, ne glede na njeno zaupnost ali tajnost, iznos osebnih podatkov v tretjo državo in posredovanje tujim uporabnikom osebnih podatkov;
- pregledovati vsebino zbirk osebnih podatkov, ne glede na njihovo zaupnost ali tajnost, in katalogov zbirk osebnih podatkov;
- pregledovati dokumentacijo in akte, ki urejajo zavarovanje osebnih podatkov;
- pregledovati prostore, v katerih se obdelujejo osebni podatki, računalniško in drugo opremo ter tehnično dokumentacijo;
- preverjati ukrepe in postopke za zavarovanje osebnih podatkov ter njihovo izvajanje;
- izvajati druge pristojnosti, določene z zakonom, ki ureja inšpekcijski nadzor, in z zakonom, ki ureja splošni upravni postopek;
- opravljati druge naloge, določene z zakonom.

Nadzornik, ki pri opravljanju inšpekcijskega nadzora ugotovi kršitev ZVOP-1 ali drugega zakona ali predpisa, ki ureja varstvo osebnih podatkov, ima glede na določbe 54. člena ZVOP-1 pravico takoj:

- odrediti, da se nepravilnosti ali pomanjkljivosti, ki jih ugotovi, odpravijo na način in v roku, ki ga sam določi;
- prepovedati obdelavo osebnih podatkov osebam javnega ali zasebnega sektorja, ki niso zagotovile ali ne izvajajo ukrepov in postopkov za zavarovanje osebnih podatkov;
- odrediti prepoved obdelave osebnih podatkov, anonimiziranje, blokiranje, brisanje ali uničenje osebnih podatkov, kadar ugotovi, da se osebni podatki obdelujejo v nasprotju z določbami zakona;
- prepovedati iznos osebnih podatkov v tretjo državo ali njihovo posredovanje tujim uporabnikom osebnih podatkov, če se iznašajo ali posredujejo v nasprotju z določbami zakona ali obvezujoče mednarodne pogodbe;
- odrediti druge ukrepe, določene z zakonom, ki ureja inšpekcijski nadzor, ter z zakonom, ki ureja splošni upravni postopek.

Zoper odločbo ali sklep nadzornika pritožba ni mogoča, dovoljen pa je upravni spor.

Če nadzornik pri inšpekcijskem nadzoru ugotovi, da obstaja sum storitve kaznivega dejanja ali prekrška, vložijo kazensko ovadbo oziroma izvede postopek v skladu z zakonom o prekrških.

Nadzornik je dolžan prijavitelja obvestiti o vseh pomembnejših ugotovitvah in dejanjih v postopku inšpekcijskega nadzora.

²⁸ Uradni list RS, št. 56/2002, 26/2007, v nadaljevanju ZIN.

Da pri opravljanju inšpekcijskega nadzorstva ne bi prišlo do kršitev informacijske zasebnosti posameznikov, je v 58. členu ZVOP-1 določeno, da je nadzornik dolžan varovati tajnost osebnih podatkov, s katerimi se seznani pri opravljanju inšpekcijskega nadzora, tudi po prenehanju opravljanja službe nadzornika. To dolžnost imajo vsi javni uslužbenci pri Informacijskem pooblaščenču.

3.2.2. Inšpekcijski nadzor v letu 2006

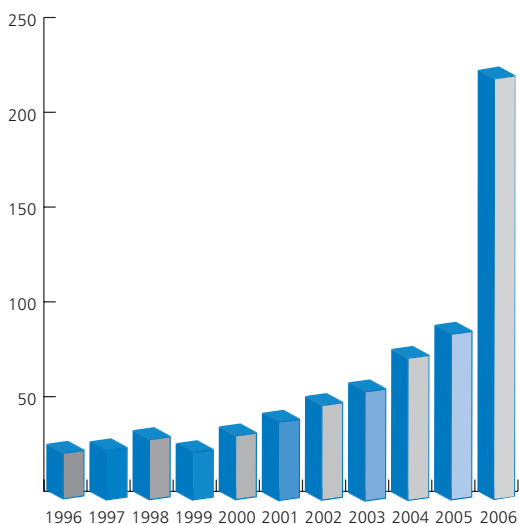
Neposredni inšpekcijski nadzor nad izvajanjem predpisov s področja varstva osebnih podatkov je zajemal:

- nadzor zakonitosti obdelave osebnih podatkov;
- nadzor ustreznosti ukrepov za zavarovanje osebnih podatkov ter izvajanja postopkov in ukrepov za zavarovanje osebnih podatkov po 24. in 25. členu ZVOP-1;
- nadzor izvajanja določb zakona, ki urejajo katalog zbirke osebnih podatkov, register zbirk osebnih podatkov in evidentiranje posredovanja osebnih podatkov posameznim uporabnikom osebnih podatkov;
- nadzor izvajanja določb zakona v zvezi z iznosom osebnih podatkov v tretjo državo in njihovim posredovanjem tujim uporabnikom osebnih podatkov.

Informacijski pooblaščenec je v letu 2006 prejel **231 prijav in pritožb zaradi suma kršitev določb ZVOP-1**, 88 v javnem in 143 v zasebnem sektorju. Število prijav in pritožb zaradi suma kršitev določb ZVOP-1 se v primerjavi s statističnimi podatki iz minulih let povečuje.

Slika 4:

Število vloženih prijav in pritožb zaradi suma kršitev določb ZVOP-1 v obdobju 1996–2006.



Inšpekcijske zadeve, ki so bile v letu 2006 uvedene v zvezi s **sumom zlorabe osebnih podatkov v javnem sektorju (88)**, so zadevale predvsem:

- posredovanje osebnih podatkov nepooblaščenim uporabnikom (35), npr. upravna enota je omogočila vpogled v centralni register prebivalstva; fakulteta je posredovala podatke o šolanju očetu, ki je izgubil roditeljsko pravico; zdravstveni delavci

so posredovali podatke pacientov kljub izrecni prepovedi; objava osebnih podatkov zaposlenega v zvezi z morebitnim disciplinskim postopkom na oglasni deski; objava osebnih podatkov v časopisu in na svetovnem spletu);

- zbiranje osebnih podatkov brez ustrezne zakonske podlage (17), npr. zbiranje podatkov o zdravstvenem stanju zaposlenih in študentov ob vpisu na fakulteto; pridobivanje podatkov o klicanih številkah s službenega mobilnega telefona; fotografiranje in snemanje učencev v šoli v naravi brez privolitve staršev;
- pomanjkljivo zavarovanje osebnih podatkov (16), npr. hramba zdravstvenih kartotek v nezaklenjenih omarah na hodnikih zdravstvenih ustanov; prost dostop do računalniških baz podatkov;
- pomanjkljive kataloge zbirk osebnih podatkov ter neposredovanje le-teh v register (9),
- prekomerno zbiranje osebnih podatkov (4), npr. na obrazcih za naročilo malice v šoli so zahtevali podatke o zaposlitvi in o številkah transakcijskih računov staršev;
- nezakonito izvajanje videonadzora (3), npr. v domu starejših občanov, na bazenu fakultete;
- izvajanje biometrije za evidentiranje prisotnosti na delu (2),
- pošiljanje reklamnega gradiva oz. neposredno trženje (2).

Največ sumov kršitev je bilo vloženih zoper zdravstvene ustanove (27), sledijo šole (13), upravne enote in občine (9), ministrstva (7), centri za socialno delo (6), sodišča (2), drugi državni organi (24).

Inšpekcijske zadeve, ki so bile v letu 2006 uvedene v zvezi s **sumom zlorabe osebnih podatkov v zasebnem sektorju (143)**, so zadevale predvsem:

- posredovanje osebnih podatkov nepooblaščenim uporabnikom (41), npr. zdravstveno osebje je razkrilo osebne podatke pacientov; objava osebnih podatkov na svetovnem spletu, televiziji in časopisih; študentski servisi so si delili baze podatkov; podjetje je posredovalo osebne podatke strank pogodbenim partnerjem za namene neposrednega trženja; posredovanje podatkov o lastnikih cepljenih psov vsem veterinarjem; zdravstvena ustanova je zasebni reševalni službi posredovala podatke o pacientih, ki bodo potrebovali prevoz; objava osebnih podatkov lastnikov stanovanj v večstanovanjskih stavbah na oglasnih deskah;
- nezakonito izvajanje videonadzora (28), npr. v garderobah trgovin, na otroških igriščih, na mestnem trgu, v kopališču, na mestnih avtobusih, v večstanovanjskih stavbah, v gostinskih lokalih;
- prekomerno zbiranje osebnih podatkov (24), npr. zahteva po pošiljanju davčne številke skupaj z rešitvijo križanke; zahteva trgovine po vpogledu v bančni izpisek pri sklepanju potrošniškega posojila; zbiranje EMŠO in davčne številke za sklenitev naročniškega razmerja; zbiranje podatkov kupcev ob reklamaciji; fotografiranje zaposlenih brez njihove privolitve;
- neposredno trženje (17), npr. pošiljanja reklamnega gradiva oz. neposredno trženje po navadni pošti ali elektronski pošti in telefonu;
- zbiranje osebnih podatkov brez ustrezne zakonske podlage (14), npr. pregledovanje službene elektronske pošte in obiska spletnih strani delavca s strani nadrejenega; pridobitev prometnih in lokacijskih podatkov o opravljenih pogovorih s službenim

mobilnim telefonom; snemanje telefonskega pogovora brez predhodnega obvestila; delodajalec je poizvedoval po zdravstvenem stanju zaposlenega pri njegovem osebnem zdravniku;

- pomanjkljive kataloge zbirk osebnih podatkov ter neposredovanja le-teh v register (10),
- pomanjkljivo zavarovane osebnih podatkov (9), npr. odklenjene pisarne s kadrovskimi evidencami; sledljivost vpogleda v zdravstvene osebne podatke ni bila zagotovljena.

Informacijski pooblaščenec je ob 231 prijavah uvedel 180 inšpekcijskih postopkov. Pri 27 prijavah je bilo že iz samih prijav razvidno, da opisano dejanje ne pomeni kršitve določb ZVOP-1. Državni nadzornik je prijaviteljem pisno pojasnil, zakaj opisano dejanje ne pomeni kršitve določb ZVOP-1 in zakaj uvedba postopka inšpekcijskega nadzora ne bi bila smiselna. V treh primerih inšpekcijski nadzor ni bil uveden zaradi nepopolne prijave, v osmih primerih pa so prijavitelji po pozivu, naj pošljejo več podatkov, svoje prijave umaknili. Štirje med njimi so potem želeli le mnenje o kršitvi osebnih podatkov, ki se jim je zgodila. V enem primeru je bila napaka odpravljena še pred uvedbo inšpekcijskega postopka, v enem primeru pa postopek ni bil uveden, ker je bil zaradi enakega prekrška že izpeljan inšpekcijski postopek in izdana odločba, zoper katero pa je bila vložena zahteva za sodno varstvo.

Informacijski pooblaščenec je odstopil v reševanje pristojnim institucijam 11 prejetih prijav. Kar pet prijav je zadevalo kršitev določb 109. člena Zakona o elektronskih komunikacijah²⁹, ki govori o neposrednem trženju po elektronski pošti.

Pri 41 prijavah se je po ogledu državnega nadzornika ali po pridobitvi pojasnila, ki so ga na poziv državnega nadzornika poslali domnevni kršilci, pokazalo, da do kršitev določb ZVOP-1 ni prišlo. V takih primerih je državni nadzornik na podlagi 28. člena ZIN izdal sklep o ustavitvi postopka.

Zaradi ugotovljenih manjših nepravilnosti je bilo v letu 2006 na podlagi 33. člena Zakona o inšpekcijskem nadzoru izrečenih 46 opozoril za odpravo nepravilnosti na zapisniku. Za manjše nepravilnosti, zaradi katerih je državni nadzornik za varstvo osebnih podatkov namesto izdaje upravne odločbe in uvedbe postopka o prekršku izrekel zgolj opozorilo na zapisniku, veljajo tiste nepravilnosti, pri katerih ni bilo neposrednega posega v pravice posameznikov oziroma posledica nepravilnosti ni bil poseg v informacijsko zasebnost posameznika. Takšne manjše nepravilnosti so predvsem pomanjkljivi katalogi zbirk podatkov, pomanjkljivi oziroma nedodelani notranji akti za zavarovanje osebnih podatkov, pomanjkljivo določeni pogoji in ukrepi za zagotovitev varstva in zavarovanja osebnih podatkov v pogodbah s pogodbenimi obdelovalci, manjše pomanjkljivosti v zvezi z izvajanjem postopkov in ukrepov za zavarovanje osebnih podatkov ter pomanjkljive nalepke o izvajanju videonadzora. V 7 primerih je državni nadzornik na podlagi razpoložljive dokumentacije kršitelje pozval, da odpravijo nepravilnosti. Ko so kršitelji po opozorilu na zapisniku ali po pozivu odpravili ugotovljene nepravilnosti, so bili izdani sklepi o ustavitvi postopka. 19 postopkov pa se je zaključilo z izdajo ureditvene odločbe, s katero je državni nadzornik kršiteljem naložil

29 Uradni list RS, št. 129/2006.

odpravo nepravilnosti. Zoper dve odločbi sta bili vloženi tožbi na Upravno sodišče.

V letu 2006 je Informacijski pooblaščenec odločil v 113 zadevah, druge pa so se kot nerešene prenesle v leto 2007.

3.2.3. Storjeni prekrški

Zaradi kršitev določb ZVOP-1 je bilo v letu 2006 uvedenih 41 postopkov o prekršku. Informacijski pooblaščenec je odločil v 26 postopkih, 15 pa se jih je preneslo v leto 2007. V 18 postopkih je odločil zoper pravne osebe zasebnega in v 8 postopkih zoper pravne osebe javnega sektorja.

Sankcije so bile izrečene zaradi:

- nezakonitega posredovanja osebnih podatkov (6) ,
- neposrednega trženja (2),
- kršitev določb o videonadzoru (6),
- pomanjkljivih katalogov zbirk osebnih podatkov in neposredovanja le-teh v register (5),
- pomanjkljivega zavarovanja osebnih podatkov (7).

Zaradi ugotovljenih prekrškov je bilo izdanih:

- 13 odločb o prekrških, ki so kršiteljem naložile plačilo globe,
- 6 plačilnih nalogov,
- 7 opozoril.

Kršitelji so v 8 primerih globe plačali, v 11 primerih pa so vložili zahteve za sodno varstvo.

3.2.4. Najpogostejše ugotovljene nepravilnosti pri izvajanju inšpekcijskega nadzora

Ugotovljene kršitve in nepravilnosti na področju varstva osebnih podatkov večinoma niso bile posledica namernega kršenja določb ZVOP-1, ampak so predvsem posledica tega, da upravljavci osebnih podatkov slabo poznajo določbe ZVOP-1 ali pa varstvu osebnih podatkov posvečajo premalo pozornosti. V nekaterih primerih je bilo tudi ugotovljeno, da so bile kršitve določb ZVOP-1 posledica malomarnega nadzora nad obdelavo osebnih podatkov s strani odgovornih. Ugotovljeno je bilo tudi, da se tako upravljavci osebnih podatkov kot tudi posamezniki iz leta v leto bolj zavedajo pomena varstva osebnih podatkov, kar se kaže tudi v stalnem povečevanju števila prijav sumov zlorabe osebnih podatkov ter zaprosil za mnenja, pojasnila in priporočila, s katerimi se upravljavci osebnih podatkov in posamezniki dnevno obračajo na nadzorni organ.

3.2.4.1. Register zbirk osebnih podatkov

Veliko nepravilnosti je bilo ugotovljenih v zvezi z vodenjem katalogov zbirk osebnih podatkov (26. člen ZVOP-1) in pošiljanjem podatkov iz kataloga v register, ki ga vodi Informacijski pooblaščenec (27. člen ZVOP-1). Na začetku leta 2006 je samo 973 upravljavcev osebnih podatkov (v Sloveniji naj bi bilo okrog 140.000 upravljavcev osebnih podatkov) posredovalo podatke o zbirkah osebnih podatkov, ki jih vodijo. Po zakonu bi upravljavci morali posredovati podatke do 1. aprila 2006, a je Informacijski pooblaščenec »podaljšal« rok do 1. oktobra 2006 in zavezanca ponovno pozval, naj izpolnijo obveznost, do takrat pa jim ne bo izrekel globe. Do konca leta 2006 je podatke v register poslalo okrog 5876 upravljavcev osebnih podatkov. Register vključuje večji del upravljavcev v javnem sektorju, medtem ko upravljavci osebnih podatkov v zasebnem sektorju večinoma niti niso seznanjeni z dolžnostjo vpisa zbirk osebnih podatkov v register. Informacijski pooblaščenec je v letu 2006 poslal 36 pozivov k dopolnitvi prijave ali posredovanju podatkov v register zbirk osebnih podatkov, 6 opozoril kršilcem zaradi neupoštevanja poziva in en plačilni nalog. Med upravljavci osebnih podatkov, ki kršijo navedene določbe, je še vedno veliko državnih organov, organov lokalne samouprave ter zdravstvenih zavodov in izobraževalnih ustanov. Vodenje katalogov zbirk osebnih podatkov se je v obravnavanem obdobju sicer že izboljšalo, vendar velika večina upravljavcev osebnih podatkov še vedno nima izdelanih katalogov osebnih podatkov ali pa so ti neažurni in zastareli. Podobno velja tudi za pošiljanje podatkov iz katalogov v register pri Informacijskem pooblaščenca, saj veliko upravljavcev osebnih podatkov svojih podatkov iz katalogov v register še vedno ni poslalo, številni podatki v registru pa so netočni, saj upravljavci osebnih podatkov Informacijskega pooblaščenca ne obveščajo o spremembah podatkov v svojih zbirkah. Zaradi netočnih in neažurnih podatkov v registru je kratena pravica posameznika do seznanitve s podatki, saj posamezniki ob vpogledu v register, ki je objavljen na spletnih straneh Informacijskega pooblaščenca, ne morejo ugotoviti, katere zbirke osebnih podatkov resnično vodijo upravljavci osebnih podatkov.

3.2.4.2. Izvajanje videonadzora

V letu 2006 je 31 prijav in pritožb zadevalo izvajanje videonadzora delovnih prostorov, dostopov do službenih oziroma poslovnih prostorov ter videonadzora v večstanovanjskih stavbah. Videonadzor je urejen v 74. do 77. členu ZVOP-1. Oseba javnega ali zasebnega sektorja, ki izvaja videonadzor, mora o tem objaviti obvestilo. Obvestilo mora biti objavljeno vidno in razločno, tako da se posameznik lahko seznani z izvajanjem videonadzora najpozneje, ko se nad njim začne izvajati videonadzor. Tako obvestilo mora obvezno vsebovati informacijo, da se izvaja videonadzor, naslov osebe javnega ali zasebnega sektorja, ki ga izvaja, ter telefonsko številko za pridobitev informacije, kje in koliko časa se shranjujejo posnetki iz videonadzornega sistema. Videonadzor dostopa do uradnih službenih oziroma poslovnih prostorov se lahko izvaja, če je to potrebno za varnost ljudi ali premoženja, zaradi zagotavljanja nadzora vstopa v službene oziroma poslovne prostore in iz njih ali če zaradi narave dela obstaja možnost ogrožanja zaposlenih. Odločitev sprejme pristojni funkcionar, predstojnik, direktor ali drugi pristojni oziroma pooblaščen posameznik osebe javnega sektorja ali osebe zasebnega sektorja. V pisni odločitvi morajo biti pojasnjeni razlogi za uvedbo videonadzora. O izvajanju videonadzora je treba pisno obvestiti vse zaposlene pri osebi javnega ali zasebnega sektorja, ki opravljajo delo v nadzorovanem prostoru. Zbirka osebnih podatkov v zvezi z nadzorom dostopa do uradnih službenih oziroma poslovnih prostorov oziroma posnetki se lahko hranijo največ eno leto po nastanku,

nato se zbrišejo, razen če zakon določa drugače. Videonadzor v večstanovanjski stavbi se lahko uvede le, kadar je to potrebno za varnost ljudi in premoženja, pri čemer je za uvedbo videonadzora potrebna tudi pisna privolitev solastnikov, ki imajo v lasti več kot 70 odstotkov solastniških deležev. Z videonadzorom v večstanovanjski stavbi se lahko nadzoruje le dostop do vhodov in izhodov večstanovanjskih stavb ter skupni prostori. Omeniti je treba, da je prepovedano omogočiti ali izvajati sprotno ali poznejše pregledovanje posnetkov videonadzornega sistema prek interne kableske televizije, javne kableske televizije, interneta ali s pomočjo drugega telekomunikacijskega sredstva, ki lahko prenaša te posnetke. Izvajanje videonadzora znotraj delovnih prostorov se lahko izvaja le v izjemnih primerih, kadar je to nujno za varnost ljudi ali premoženja ali za varovanje tajnih podatkov ter poslovne skrivnosti in tega ni mogoče doseči z milejšimi sredstvi. Prepovedano je izvajati videonadzor v delovnih prostorih zunaj delovnega mesta, zlasti v garderobah, dvigalih in sanitarnih prostorih.

Pri opravljanju inšpekcijskega nadzora nad izvajanjem videonadzora so bile najpogostejše ugotovljene te nepravilnosti:

- Izvajalci videonadzora za evidenco posnetkov videonadzornega sistema, ki se po določbah 6. člena ZVOP-1, takrat, ko so posnete osebe prepoznavne, nedvomno šteje za zbirko osebnih podatkov, niso zagotovili kataloga zbirke osebnih podatkov in podatkov iz kataloga niso posredovali Informacijskemu pooblaščenču.
- Obvestila o tem, da se izvaja videonadzor, so bila večinoma pomanjkljiva, ker niso vsebovala naslova osebe, ki izvaja videonadzor, ter telefonske številke za pridobitev informacije o tem, kje in koliko časa se shranjujejo posnetki. Ta obvestila so bila v mnogih primerih tudi premajhna, bilo jih je premalo ali pa so bila postavljena na neprimernih krajih.
- Izvajanje videonadzora v slačilnicah oziroma garderobah trgovskih in športnih objektov.
- Predstojniki pred začetkom izvajanja videonadzora ali pozneje niso izdali pisne odločitve za izvajanje videonadzora oziroma v tej odločitvi niso pojasnili razlogov za njegovo uvedbo.
- Zaposleni pred začetkom izvajanja videonadzora o tem niso bili pisno obveščeni.
- Za izvajanje videonadzora v večstanovanjskih stavbah ni bila pridobljena pisna privolitev solastnikov, ki imajo v lasti več kot 70 odstotkov solastniških deležev.
- Videonadzor se je v večstanovanjskih hišah izvajal tako, da se je dogajanje, ki ga spremljajo kamere, sproti predvajalo na posebnem kanalu interne kableske televizije.

Če se videonadzor ne snema, ne nastane zbirka osebnih podatkov, zato ZVOP-1 takega videonadzora ne ureja. Je pa upravljavec, ki se odloči za tako obliko videonadzora, lahko podvržen odškodninski tožbi ali uvedbi kazenskega postopka. Zato Informacijski pooblaščenec priporoča, da upravljavci tudi v tem primeru obvestijo posameznike z obvestilom, ki vsebuje vse elemente iz 74. člena ZVOP-1. Informacijski pooblaščenec poudarja, da izvajanje videonadzora za izključno osebno uporabo, družinsko življenje ali druge domače potrebe ob upoštevanju 7. člena ZVOP-1 ni podvrženo določbam ZVOP-1 o videonadzoru. Kljub temu posameznik, ki bi snemal npr. sosedovo parcelo ali druge posameznike, tvega odškodninsko tožbo ali uvedbo kazenskega postopka.

3.2.4.3. Neposredno trženje

V obravnavanem obdobju je bilo precej nepravilnosti ugotovljenih tudi pri uporabi osebnih podatkov za neposredno trženje. Neposredno trženje je urejeno v 72. in 73. členu ZVOP-1. Člena določata, da lahko upravljavec osebnih podatkov uporablja osebne podatke posameznikov, ki jih je zbral iz javno dostopnih virov ali v okviru zakonitega opravljanja dejavnosti, tudi za namene ponujanja blaga, storitev, zaposlitev ali začasnega opravljanja del z uporabo poštnih storitev, telefonskih klicev, elektronske pošte ali drugih telekomunikacijskih sredstev oziroma za neposredno trženje. Za neposredno trženje se lahko uporablja le osebno ime, naslov stalnega ali začasnega prebivališča, telefonsko številko, naslov elektronske pošte ter številko telefaksa. Upravljavec osebnih podatkov je dolžan neposredno trženje izvajati tako, da posameznika ob tem obvesti o njegovih pravicah, to je, da lahko posameznik kadar koli pisno ali na drug dogovorjen način zahteva, da upravljavec osebnih podatkov trajno ali začasno preneha uporabljati njegove osebne podatke za neposredno trženje. Upravljavec osebnih podatkov je dolžan v 15 dneh ustrezno preprečiti uporabo osebnih podatkov za neposredno trženje ter o tem v nadaljnjih petih dneh pisno ali na drug dogovorjen način obvestiti posameznika, ki je to zahteval.

Večina prijav je zadevala pridobitev oziroma vir osebnih podatkov za neposredno trženje. Ugotovljeno je bilo, da so se za pošiljanje propagandnega gradiva oziroma ponudb najpogosteje uporabljali osebni podatki iz javno dostopnih zbirk. Najznačilnejše take zbirke so npr. telefonski imeniki, delniška knjiga, zemljiška knjiga, kataster stavb. S pridobivanjem podatkov iz teh evidenc določbe ZVOP-1 niso kršene. Izvajalci neposrednega trženja so določbe ZVOP-1 kršili predvsem, ko so uporabljali več osebnih podatkov, kot jih dopušča zakon, in ker posameznika ob izvajanju neposrednega trženja niso obvestili o njegovi pravici, da lahko kadar koli pisno ali na drug dogovorjen način od upravljavca osebnih podatkov zahteva prenehanje uporabe njegovih osebnih podatkov za neposredno trženje.

3.2.4.4. Zavarovanje osebnih podatkov

Nepravilnosti na področju varstva osebnih podatkov so se pogosto kazale tudi v pomankljivih notranjih aktih, v katerih morajo upravljavci osebnih podatkov skladno z določbami 24. in 25. člena ZVOP-1 predpisati organizacijske, tehnične in logično-tehnične postopke in ukrepe za zavarovanje osebnih podatkov. V 24. členu ZVOP-1 so določene zahteve, ki jih morajo postopki in ukrepi za zavarovanje osebnih podatkov izpolnjevati, v 25. členu pa je določeno, da morajo upravljavci osebnih podatkov postopke in ukrepe za zavarovanje osebnih podatkov predpisati v svojih aktih ter seveda zagotoviti njihovo izvajanje. V zvezi s tem je treba opozoriti, da ni dovolj, da se postopki in ukrepi za zavarovanje osebnih podatkov zgolj predpišejo v notranjih aktih upravljavcev osebnih podatkov, ampak je poleg tega treba zagotoviti, da se bodo predpisani postopki in ukrepi resnično izvajali. Zato je treba z akti, ki predpisujejo postopke in ukrepe za zavarovanje osebnih podatkov, seznaniti vse zaposlene, poleg tega pa morajo obdelovalci osebnih podatkov skladno z določbami 25. člena ZVOP-1 določiti tudi osebe, ki bodo odgovorne za zbirke osebnih podatkov, in osebe, ki zaradi narave dela lahko obdelujejo osebne podatke.

Nekateri upravljavci osebnih podatkov takih aktov sploh niso imeli, zgodilo pa se je tudi, da osebe, ki obdelujejo osebne podatke, s takimi akti niso bile seznanjene. Pogosti so bili primeri, ko upravljavci osebnih podatkov niso zagotovili ustreznega zavarovanja osebnih podatkov oziroma v svojih notranjih aktih niso izvajali predpisanih postopkov in ukrepov za zavarovanje osebnih podatkov. Najpogostejši primeri neustreznega zavarovanja osebnih podatkov so bili:

- neustrezno hranjenje dokumentacije, ki vsebuje osebne podatke, saj se je dokumentacija hranila v nezaklenjenih omarah in predalnikih, pogosto kar na hodnikih,
- neustrezno varovani oziroma nazaklenjeni prostori, v katerih so bili nosilci osebnih podatkov in računalniška oprema, s katero se obdelujejo osebni podatki,
- računalniško vodene zbirke osebnih podatkov niso bile zadostno varovane z gesli za identifikacijo in avtorizacijo oseb, ki obdelujejo osebne podatke,
- ni bila zagotovljena sledljivost obdelave osebnih podatkov oziroma sistem zavarovanja osebnih podatkov ni omogočal poznejšega ugotavljanja, kdaj so bili osebni podatki vneseni v zbirko osebnih podatkov, uporabljeni ali drugače obdelani, in kdo je to storil.

3.2.4.5. Prekomerno zbiranje osebnih podatkov

Upravljavci osebnih podatkov so pogosto prekomerno zbirali osebne podatke glede na namene, za katere so jih zbirali in nadalje obdelovali, s tem pa je bilo kršeno načelo sorazmernosti (3. člen ZVOP-1). Za prekomerno zbiranje osebnih podatkov je šlo v primerih, ko so organizatorji nagradnih iger zbirali davčne številke vseh udeležencev nagradne igre, čeprav jih v resnici potrebujejo le za tiste osebe, ki dobijo nagrado. Prekomerno zbiranje osebnih podatkov je bilo ugotovljeno tudi pri sklepanju pogodb. Tako so operaterji, ki opravljajo komunikacijske storitve, poleg davčne številke naročnikov zbirali tudi njihov EMŠO, torej dva tako imenovana ista povezovalna znaka oziroma dve osebni identifikacijski številki, čeprav za popolno identifikacijo posameznika zadošča že ena. To pomeni, da je zbiranje dveh osebnih številke, ki omogočata popolno identifikacijo posameznika, odveč in je to prekomeren poseg v zasebnost in dostojanstvo posameznika. Torej bi morali zbirati le tiste podatke, ki so res nujno potrebni in primerni za doseg cilja in ki ne izkazujejo drugih podatkov posameznika.

Ker popolno identifikacijo posameznika omogočata tako EMŠO kot tudi davčna številka, je z vidika natančne identifikacije posameznika davčna številka primernejša, saj EMŠO razkrije tudi datum rojstva, torej starost, in spol. Zato gre pri EMŠO v primerjavi z davčno številko za bistveno večji poseg v zasebnost. Informacijski pooblaščenec priporoča, da se EMŠO uporablja v izjemnih primerih, ko razkritje EMŠO res terja potreba po višji stopnji pravne varnosti. Predvsem pa je takrat, ko pravni posel terja višjo stopnjo zavarovanja, ob upoštevanju načela sorazmernosti iz 3. člena ZVOP-1, primerneje uporabiti davčno številko. V takih primerih navadno izvajalci nagradnih iger že vnaprej zahtevajo razkritje davčne številke, kar pa je v skladu z Zakonom o davčnem postopku³⁰ prepovedano, saj davčno razmerje do podelitve nagrade zmagovalcu nagradne igre ne nastane. Pravilno bi bilo, da izvajalci nagradne igre zahtevajo davčno številko šele potem, ko ugotovijo, kdo je nagrajenec, in zgolj od nagrajenca oziroma nagrajencev.

30 Uradni list RS, št. 117/2206.

V zvezi z neposrednim zbiranjem osebnih podatkov je treba opozoriti, da upravljavci osebnih podatkov ob njihovem zbiranju posamezniku pogosto ne posredujejo vseh informacij iz 19. člena ZVOP-1 ali pa so te informacije nepopolne (npr. podatki o upravljavcu osebnih podatkov in jasno opredeljen namen njihove obdelave, podatki o morebitnih uporabnikih osebnih podatkov in informacija o pravici do vpogleda, prepisa, kopiranja, dopolnitve, popravka, blokiranja ali izbrisa lastnih osebnih podatkov). Posredovanje informacij ob zbiranju osebnih podatkov je zlasti pomembno pri obdelavi osebnih podatkov na podlagi osebne privolitve posameznika, saj se lahko posameznik le na podlagi popolnih informacij odloči o tem, ali bo prostovoljno dovolil obdelavo svojih osebnih podatkov.

3.2.4.6. Zasebnost na delovnem mestu

V primerjavi s prejšnjimi leti so nove prijave oziroma pritožbe zoper delodajalce, ki pregledujejo oziroma nadzorujejo elektronsko pošto zaposlenih. Elektronski naslov je osebni podatek, ki nujno še ne določi posameznika. Vendar pa obstajajo elektronski naslovi, iz katerih so razvidni ime, priimek in zaposlitev posameznika, torej osebni podatki, ki (navadno) omogočijo razmeroma preprosto identifikacijo posameznika. Službeni elektronski naslovi so načeloma vedno osebni podatek. Nedvomno pa je tudi vsebina elektronskega sporočila del pravice do zasebnosti. Nerešeno vprašanje pa je, kakšno stopnjo zasebnosti lahko delojemalec na delovnem mestu upravičeno pričakuje in kdaj pomeni poseg v komuniciranje zaposlenega poseg v nedotakljivost njegove zasebnosti. Pri tem gre za navzkrižje interesa delodajalca, ki ima pravico do oblasti nad svojimi sredstvi in pravico, da nadzoruje, ali je oprema uporabljena skladno z namenom, za katerega je bila zaposlenemu dana v uporabo, in interesa posameznika (zaposlenega), ki utemeljeno pričakuje določeno stopnjo zasebnosti in zaupnosti tudi na delovnem mestu. Delodajalec načeloma nima pravne podlage za vpogled v t. i. prometne podatke o elektronski pošti zaposlenih (kdo je elektronsko pošto poslal oziroma komu je bila poslana). Z vpogledom v prometne podatke delodajalec načeloma krati pravico zaposlenega do varstva osebnih podatkov, z vpogledom v vsebino elektronske pošte pa krati (širšo) pravico do zasebnosti in pravico do tajnosti občil, ki sta varovani tudi z ustavo. To pa ne pomeni, da delodajalec ne more omejiti uporabe službenega elektronskega naslova, če bi se izkazalo, da delavec elektronskega naslova ne uporablja v skladu s politiko delodajalca o uporabi službenih sredstev (zaradi pošiljanja slikovnih ali zvočnih datotek se lahko upočasni delovanje omrežja, poveča se lahko število virusov ...). Oprema in službeni elektronski naslov sta namreč last delodajalca, zato lahko ta bedi nad svojimi sredstvi in tudi skrbi za pravilnost in zakonitost poslovanja, kot tudi za smotrnost porabe sredstev, delavec pa ima kot imetnik zgolj pravico do uporabe; zato lahko delodajalec prosto omejuje dostop do službenega elektronskega naslova. Priporočljivo je, da delodajalci vnaprej pisno obvestijo zaposlene, kako in v kakšnem obsegu lahko uporabljajo elektronsko pošto, Informacijski pooblaščenec pa priporoča tudi, da delodajalec v ta pravila zapiše, kdaj oz. ob katerih primerih bo vpogledal v prometne podatke o elektronski pošti in v vsebino. Namen tovrstne obdelave osebnih podatkov mora biti torej jasen in sorazmeren z dogodkom, ki bo povzročil vpogled v podatke (recimo daljša odsotnost delavca, ki veliko komunicira s strankami, odhod iz podjetja brez primopredaje poslov ...). Seveda morajo biti razlogi čim bolj jasno navedeni in izjemni, zato je treba vsak primer presoјati posebej.

Informacijski pooblaščenec je ugotavljal tudi, ali je osebni podatek tudi podatek o obisku spletnih strani na službenem računalniku na delovnem mestu. Prav gotovo gre za podatek, ki se nanaša na delavca kot posameznika, saj ob zasebni uporabi svetovnega spleta na službeni opremi (lahko) izkazuje svoje interese, počutje ali druga osebna stanja (denimo oddaja zahtevka za odobritev večjega posojila prek spletne strani banke nakazuje na premoženjsko stanje posameznika, nakup zdravila proti migreni na spletni strani proizvajalca zdravil nakazuje na zdravstveno stanje posameznika ipd.). Informacijski pooblaščenec meni, da je tudi podatek o obisku spletnih strani posameznika ali spremljanje njegovih dejavnosti na svetovnem spletu osebni podatek in kot tak varovan v skladu z ZVOP-1. Delodajalec v take podatke načeloma nima vpogleda, saj se pri takem podatku mešata t. i. prometni podatek in vsebina, s tem pa gre za poseg v dve ustavni pravici – pravico do varstva osebnih podatkov (38. člen Ustave RS) in širšo pravico do zasebnosti.

Informacijski pooblaščenec opozarja tudi na intranet oziroma intranetne portale, ki se v organizaciji uporabljajo predvsem za splošno interno komuniciranje, pregled dokumentacije in dostop do baz podatkov, dostop do elektronske pošte in interneta, uporabo drugih poslovnih aplikacij, objavo internih obvestil, okrožnic, pravilnikov in drugega gradiva. Organizacije želijo z uvedbo intranetnih portalov doseči cilje, kot so zmanjševanje dokumentacije, boljša obveščenost zaposlenih, lažji dostop do aplikacij z enega kraja, manjša obremenjenost pri komuniciranju prek elektronske pošte in podobno. Prek intraneta so pogosto dosegljivi tudi pomembni poslovni podatki, zato so intranetni portali praviloma implementirani na način, ki preprečuje dostop osebam, ki niso zaposlene v organizaciji ali niso pooblaščenec za dostop do podatkov na intranetu. Nekajkrat je bilo ugotovljeno, da so se na intranetu objavljali tudi osebni podatki zaposlenih (npr. čestitke ob rojstnem dnevu, podatki o bolniškem dopustu, dopustu ali plačah v zasebnem sektorju), kar pa je brez predhodne privolitve zaposlenih nedopustno in pomeni kršitev varstva osebnih podatkov.

3.2.4.7. Objavljanje seznamov lastnikov stanovanj v večstanovanjskih stavbah

V letu 2006 je Informacijski pooblaščenec reševal tudi prijave posameznikov, ki so zadevale nedovoljeno objavo neplačnikov na oglasni deski v večstanovanjskih stavbah. Storilci prekrška so bili običajno upravniki večstanovanjskih stavb. Lastniki stanovanj so pri skupnih stroških upravičeni izvedeti, kdo ne plačuje skupnih stroškov, saj le tako lahko izvejo, proti komu vložiti morebitni regresni zahtevki. Vendar pa je način, da se seznam plačnikov in neplačnikov obesi na oglasno desko bloka, nepravilen, saj se tako razkrijejo osebni podatki lastnikov stanovanj vsem, ki imajo dostop do oglasne deske, torej (pre)širokemu krogu ljudi. Takšna obdelava osebnih podatkov je tudi v nasprotju z načelom sorazmernosti iz 3. člena ZVOP-1. Pravilen način, kako obvestiti druge lastnike stanovanj o plačnikih oziroma neplačnikih, je, da upravnik večstanovanjske hiše obvesti vsakega lastnika posebej, na primer z obvestilom v zaprti ovojnici, ki jo vloži v poštni nabiralnik. Tako se osebni podatki lastnikov stanovanj po nepotrebnem ne razkrivajo drugim, sami lastniki pa so še vedno pravilno in zadostno obveščeni. Osebni podatki lastnikov stanovanj pa so popolnoma zavarovani, kadar gre za individualne stroške, torej stroške, ki niso skupni. V tem primeru upravniki večstanovanjskih hiš ne smejo objavljati osebnih podatkov plačnikov oziroma neplačnikov na oglasni deski, kakor tudi ne smejo o tem obveščati drugih lastnikov. Strošek, ki ni del skupnih stroškov, je namreč osebni podatek lastnika stanovanja.

3.2.4.8. Nezakonito posredovanje osebnih podatkov

V letu 2006 je bilo največ prijav posameznikov vloženih zaradi suma posredovanja osebnih podatkov nepooblaščenim uporabnikom. Veliko prijav se je izkazalo za ne-utemeljene. Kadar se osebni podatki posredujejo iz zbirk osebnih podatkov (razne evidence, registri, baze podatkov, kartoteke ipd.) je treba dosledno spoštovati 22. člen ZVOP-1, ki določa, da mora upravljavec zbirke osebnih podatkov ob plačilu stroškov posredovanja, če zakon ne določa drugače, posredovati osebne podatke uporabnikom osebnih podatkov. Uporabniki so fizične ali pravne osebe ali druge osebe javnega ali zasebnega sektorja, ki se ji posredujejo ali razkrijejo osebni podatki. Posredovanje osebnih podatkov je praviloma dopustno oziroma zakonito samo v primerih:

- da obstaja za posredovanje osebnih podatkov izrecna podlaga v zakonu,
- da je posameznik osebno privolil v posredovanje osebnih podatkov, pri čemer je treba upoštevati, da zakon za nekatere primere določa, da se osebni podatki lahko posredujejo samo na podlagi pisne privolitve posameznika,
- da je posredovanje osebnih podatkov potrebno zaradi izpolnjevanja pogodbenih obveznosti.

Informacijski pooblaščenec poudarja, da je pri posredovanju osebnih podatkov treba spoštovati 8., 9. in 10. člen ZVOP-1, ki določajo splošne pogoje obdelave osebnih podatkov ter pravne podlage za obdelavo osebnih podatkov v javnem in zasebnem sektorju. Posredovanje podatkov je namreč le eden izmed številnih načinov obdelave osebnih podatkov.

V zvezi s posredovanjem osebnih podatkov Informacijski pooblaščenec opozarja še na dve prijavi odvetnika, ki je pridobil podatke iz centralnega registra prebivalstva. To dejanje je zakonito in v skladu z določbami ZVOP-1 in 10. členom Zakona o odvetništvu³¹, po katerem je odvetnik upravičen od upravljavcev zbirk podatkov zahtevati posredovanje osebnih podatkov, vendar le takrat, kadar jih nujno potrebuje za opravljanje procesnih dejanj pri zastopanju stranke.

Pri posredovanju osebnih podatkov iz zbirk osebnih podatkov drugim uporabnikom se večkrat dogaja, da posredovanje osebnih podatkov sploh ni evidentirano ali pa je evidenca pomanjkljiva. Dolžnost evidentiranja posredovanja osebnih podatkov upravljavcem osebnih podatkov nalaga 22. člen ZVOP-1, ki določa, da mora upravljavec zbirke osebnih podatkov zagotoviti, da je za vsako posredovanje osebnih podatkov pozneje mogoče ugotoviti, kateri osebni podatki so bili posredovani, komu, kdaj in na kakšni podlagi, in sicer za obdobje, v katerem je mogoče zakonsko varstvo pravice posameznika zaradi nedopustnega posredovanja osebnih podatkov. Skrajni rok za hranjenje evidence posredovanih osebnih podatkov je praviloma pet let od nastanka škode, kar je splošni zastaralni rok, ki ga določa Obligacijski zakonik³². Ugotovljeno je bilo, da številni upravljavci osebnih podatkov nimajo urejene sledljivosti vpogledov v zbirke osebnih podatkov oziroma da posredovanja osebnih podatkov drugim osebam včasih sploh ne evidentirajo ali pa je tako evidentiranje pomanjkljivo.

31 Uradni list RS, št. 18/1993, s spremembami in dopolnitvami 24/2001.

32 Uradni list RS, št. 83/2001.

3.2.4.9. Zdravstveni osebni podatki

Ob delu Informacijskega pooblaščenca se je v letu 2006, podobno kot v minulih letih ob delu Inšpektorata za varstvo osebnih podatkov, pokazalo, da predvsem zdravstvene institucije, ki bi za zavarovanje zdravstvenih podatkov posameznikov morale najbolj skrbeti, tega ne počnejo. Državni nadzorniki so v nekaterih zdravstvenih domovih odkrili zdravstvene kartoteke v odklenjenih ali celo odprtih omarah na hodnikih, do katerih so imeli dostop vsi. To je seveda v nasprotju z določbami ZVOP-1 o zavarovanju osebnih podatkov, zlasti pa je nesprejemljivo in nedopustno, ker gre za občutljive zdravstvene podatke, ki se lahko obdelujejo le pod posebnimi pogoji, prav tako pa zanje velja strožji red zavarovanja. V zvezi z vprašanji o ustrezni hrambi in ukrepih za zavarovanje zdravstvene dokumentacije je Informacijski pooblaščenec že večkrat izrazil prepričanje, da morajo biti postopki in ukrepi za zavarovanje osebnih podatkov ustrezni glede na tveganje, ki ga predstavljata obdelava in narava zdravstvenih osebnih podatkov, ustrezni glede na konkretne okoliščine delovnega procesa pri posameznem izvajalcu zdravstvenih storitev in ustrezni glede na konkretne arhitekturno-tehnične rešitve ambulant in drugih prostorov ter stavbe, v kateri so.

Več prijav je bilo tudi zaradi zahteve delodajalcev po vpogledu v zdravstveno dokumentacijo zaposlenih. Informacijski pooblaščenec meni, da so delodajalci pri seznanjanju z občutljivimi zdravstvenimi podatki zelo omejeni, saj se lahko prek zdravniških potrdil seznanijo samo z nekaterimi podatki o zdravstvenem stanju zaposlenih, nikakor pa nimajo pravice do vpogleda v celotno zdravstveno dokumentacijo. V praksi je pogosto sporno tudi posredovanje zdravstvene dokumentacije, ki jo sicer vodi osebni zdravnik, zdravniku specialistu medicine dela za potrebe izvajanja preventivnih zdravstvenih pregledov. Čeprav je ta materija vsebinsko primerno urejena s podzakonskim aktom, ki za posredovanje zdravstvene dokumentacije zahteva soglasje zaposlenega, Informacijski pooblaščenec opozarja, da urejanje vprašanj na področju varstva osebnih podatkov s podzakonskim aktom ni v skladu z doktrino ustave in ZVOP-1 na področju varovanja zasebnosti in osebnih podatkov, saj področje varstva osebnih podatkov lahko določa zgolj zakon. Podobno velja za kartico zdravstvenega zavarovanja, ki ima za svoj obstoj in nabor osebnih podatkov sicer splošno podlago v zakonu, ki ureja zbirke podatkov na področju zdravstvenega varstva, vendar posamezna vprašanja obdelave osebnih podatkov ureja pravilnik. Res pa je, da je v praksi dostopanje do kartičnega zapisa ustrezno nivojsko omejeno.

Posebej je treba opozoriti na očitno sporno obdelavo zdravstvenih podatkov s strani zavarovalnic. Tako izvajalci zdravstvenih storitev kot tudi posamezniki, na katere se zdravstveni podatki nanašajo, namreč pogosto nasprotujejo sporočanju zdravstvenih podatkov zavarovalnicam. Najpomembnejši argument, ki upravičuje zavarovalnice, da lahko zahtevajo seznanitev z zdravstvenimi podatki, in izvajalce zdravstvenih storitev, da lahko te podatke posredujejo, je izrecna zakonska podlaga v 154. členu Zakona o zavarovalništvu³³ in 8. členu Zakona o obveznih zavarovanjih v prometu³⁴. Poleg tega zavarovalnice v praksi razpolagajo še z osebnimi privolitvami zavarovalcev, zavarovancev ali upravičencev iz zavarovanja, kar še dodatno utemeljuje dopustnost obdelave osebnih podatkov. Zakon o zavarovalništvu med drugim dopušča tudi vzpostavitev in vodenje zbirk podatkov za presojo zavarovalnega kritja in višine odškodnine, v

33 Uradni list RS, št. 79/2006, 9/2007.

34 Uradni list RS, št. 110/2006.

okviru katerih se lahko obdelujejo tudi podatki o predhodnih poškodbah in zdravstvenem stanju, vrsti telesnih poškodb, trajanju zdravljenja, posledicah zavarovanja in oškodovanca in podobno. Poleg tega isti zakon izrecno zavezuje upravljavce osebnih podatkov k posredovanju osebnih podatkov. Informacijski pooblaščenec meni, da določbe Zakona o zavarovalništvu in Zakona o zdravstveni dejavnosti³⁵ (v tistem delu, ki ureja poklicno skrivnost) niso v koliziji, ampak se dopolnjujejo. Predvsem zaradi presplošne opredelitve podatkov, do katerih naj bi bile zavarovalnice upravičene, Informacijski pooblaščenec poudarja, da sta tako zavarovalnica kot tudi izvajalec zdravstvenih storitev zavezana k spoštovanju načela sorazmernosti, saj zavarovalnice niso upravičene do tistih osebnih podatkov, ki presegajo potrebe sklepanja in izvrševanja zavarovalnih pogodb.

V praksi se je večkrat pokazalo, da je za zdravstveno stanje posameznika izvedelo več zdravstvenega osebja, kot bi smelo. Zdravstveno stanje posameznika se lahko razkrije samo tistim zdravstvenim delavcem, ki so v proces zdravljenja neposredno vključeni. Razkritje zdravstvenega stanja zdravstvenemu osebju, ki ni vključeno v proces zdravljenja, pomeni prekomerno obdelavo osebnih podatkov. Prav tako ni dovoljeno razkrivanje zdravstvenih podatkov polnoletnih pacientov drugim osebam (tudi sorodnikom), če pacienti v to niso izrecno privolili.

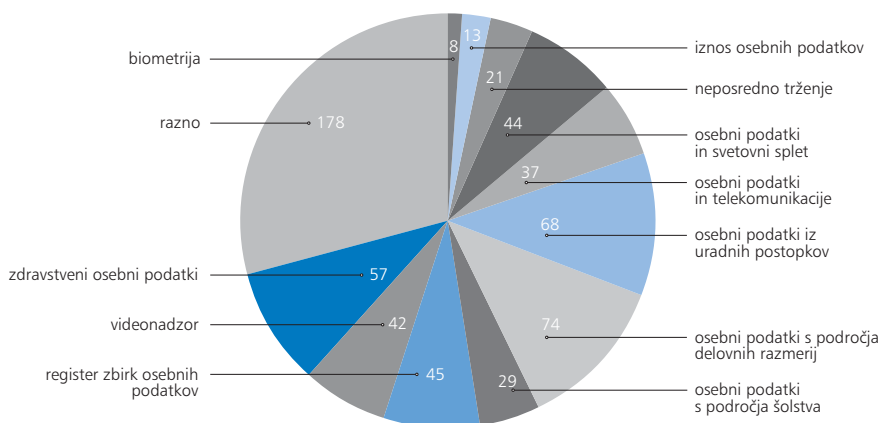
V zvezi z zdravstvenimi podatki Informacijski pooblaščenec poudarja še, da ima vsak posameznik načeloma pravico do vpogleda v svoj zdravstveni karton, saj gre pri tem za uresničevanje pravice posameznika do vpogleda v lastne osebne podatke. Zdravnik pa je dolžan posamezniku omogočiti vpogled v njegovo zdravstveno kartoteko. Čeprav je pozitivna zakonodaja na področju uresničevanja pravice do seznanitve z lastnimi osebnimi podatki s procesnoppravnega in materialnoppravnega vidika zadovoljivo določna in je že dlje časa nesporno, da se pravica do seznanitve z lastnimi osebnimi podatki nanaša tudi na osebne (torej tudi zdravstvene) podatke, ki jih vsebuje zdravstvena dokumentacija kot zbirka osebnih podatkov, je v praksi mogoče zaznati vrsto primerov nerazumevanja in posledično tudi nespoštovanja te že z ustavo zagotovljene pravice. Še pogostejše so sporni zgolj posamezni vidiki uresničevanja pravice do seznanitve, na primer vprašanje dopustnosti zaračunavanja fotokopij zdravstvene dokumentacije, dela ter dodatnih storitev, ki so s tem povezane. Glede teh vprašanj je Informacijski pooblaščenec zavzel stališče, da je ustrezno le zaračunavanje materialnih stroškov fotokopiranja, nedopustno pa je dodatno zaračunavanje dela, ki ga ima izvajalec zdravstvenih storitev npr. z odbiranjem gradiva. Za storitve, ki presegajo uresničevanje pravice do seznanitve (npr. potrjevanje avtentičnosti fotokopij), je zaračunavanje stroškov dopustno, če je pred tem posamezniku omogočeno, da na učinkovit način preveri, ali fotokopije resnično ustrezajo originalnim izvodom dokumentacije (s prostim vpogledom v originalno zdravstveno dokumentacijo ali z njenim prepisom). Poleg tega lahko izvajalec zdravstvenih storitev tovrstno storitev zaračunava samo, če pacient to storitev zahteva, saj bi v nasprotnem primeru »prisilna overitev« pomenila nedopustno omejitev pravice do seznanitve. Pravico do seznanitve lahko uresničuje posameznik, na katerega se osebni podatki nanašajo, sam ali pa njegov zakoniti zastopnik oziroma pooblaščenec.

35 Uradni list RS, št. 36/2004.

3.3. Dajanje pisnih mnenj in pojasnil

Neposredna pravna podlaga za dajanje neobveznih mnenj, pojasnil, stališč, navodil in priporočil s področja varstva osebnih podatkov so določbe 49. člena ZVOP-1. Informacijski pooblaščenec je v letu 2006 prejel 616 prošelj za pisna pojasnila ali mnenja v zvezi s konkretnimi vprašanji. Število zaprosil za mnenja in pojasnila se iz leta v leto povečuje (leta 2005 jih je bilo 34), kar lahko pripišemo temu, da je javnost vedno bolj seznanjena z Zakonom o varstvu osebnih podatkov in s pravicami posameznikov, ki iz njega izhajajo. Zaposila za mnenja in pojasnila so zadevala različna področja. Največ zaprosil je bilo na teh področjih:

- osebni podatki s področja delovnih razmerij (74),
- osebni podatki iz uradnih postopkov (68),
- zdravstveni osebni podatki (57),
- register zbirk osebnih podatkov (45),
- osebni podatki in svetovni splet (44),
- videonadzor (42),
- osebni podatki in telekomunikacije (37).



Slika 5: Zaposila za mnenja v letu 2006 po področjih.

Za mnenje in pojasnila so prosile tako fizične kot pravne osebe javnega in zasebnega sektorja. Fizične osebe so prosile za mnenje, ker pravne osebe javnega ali zasebnega sektorja pri obdelavi osebnih podatkov po njihovem mnenju niso ravnale v skladu z določbami ZVOP-1, pravne osebe javnega in zasebnega sektorja pa so največkrat želele nasvet, kako ravnati v konkretnih primerih, pa tudi tolmačenje oziroma razlago določb zakona. Informacijski pooblaščenec je v letu 2006 prejel 268 zaprosil fizičnih oseb, 184 od pravnih oseb javnega in 164 od pravnih oseb zasebnega sektorja. Največ fizičnih oseb je želelo mnenje in pojasnila glede osebnih podatkov iz uradnih postopkov in s področja delovnih razmerij (vsako področje 34), glede zdravstvenih osebnih podatkov in osebnih podatkov v povezavi s svetovnim spletom (vsako področje 27) ter videonadzora (24). Pravne osebe javnega sektorja so največkrat zaprosile za pojasnila glede

osebnih podatkov iz uradnih postopkov (27), zdravstvenih osebnih podatkov (21) in osebnih podatkov s področja delovnih razmerij (18). Med pravnimi osebami zasebnega sektorja pa je bilo največ vprašanj s področja registra zbirk osebnih podatkov (32), delovnih razmerij (22) in videonadzora (12).

Najpogostejša in najzanimivejša vprašanja, ki so bila v letu 2006 zastavljena Informacijskemu pooblaščenču, so zadevala:

- osebnne podatke, ki jih zahtevajo ponudniki interneta in telekomunikacijski operaterji ob sklenitvi naročniškega razmerja,
- objavo osebnih podatkov zaposlenih in razkrivanje osebnih podatkov znotraj delovnega kolektiva,
- pravico delodajalca do nadzora nad elektronsko pošto zaposlenih in nadzora nad dostopom do interneta,
- vrsto osebnih podatkov, ki se lahko objavijo na spletnih straneh brez osebne privolitve posameznikov (npr. člani društva ali družinska drevesa),
- vpogled delodajalca v izpisek klicev, opravljenih s službenim mobilnim telefonom,
- objavo poimenskega seznama zaposlenih s številom izostankov z dela zaradi bolezni za minulo leto,
- objavo plač zaposlenih na spletni strani delodajalca,
- dolžnosti podjetnikov glede vodenja katalogov zbirk osebnih podatkov in pošiljanje le-teh v register Informacijskega pooblaščenca,
- sprejemanje notranjih aktov o varstvu osebnih podatkov,
- obveznosti upravljavcev zbirk osebnih podatkov in postopek vpisa v register,
- zbirke osebnih podatkov, ki jih je treba prijaviti v register,
- pridobitev podatkov iz zdravstvenih kartotek umrlih svojcev,
- posredovanje zdravstvenih podatkov zavarovalnicam za razne postopke (npr. odškodnine, sklenitev življenjskih zavarovanj),
- pravice pacientov do vpogleda in pridobitve fotokopij svoje zdravstvene dokumentacije,
- pravico neizbranega kandidata na javnem natečaju za delovno mesto do vpogleda v podatke izbranega kandidata,
- snemanje zaposlenih pri delu brez njihove vednosti,
- videonadzor v gostinskih lokalih,
- videonadzor v garderobi javnega objekta,
- videonadzor večstanovanjskih stavb prek kabelske televizije,
- pogoje izvajanja videonadzora,
- namestitev kamer na stanovanjskih hišah za nadzor nad dostopom do hiš,
- prenašanje dogajanja v lokalu na internetu,
- možne ukrepe ob objavi neresničnih osebnih podatkov na spletni strani,
- fotografiranje in testiranje otrok v osnovnih šolah,
- objavo seznama staršev z navedbo plačilnega razreda na oglasni deski v vrtcu,
- objavo seznamov stanovalcev na oglasni deski,

- pošiljanje propagandnega gradiva na javno objavljene naslove,
- registriranje prihodov in odhodov zaposlenih s prstnim odtisom,
- uporabo osebnih podatkov občanov in občank za pošiljanje voščilnic,
- snemanje telefonskih pogovorov,
- izvajanje popisa nepremičnin in objavo podatkov o nepremičninah na internetu,
- nadzor zaposlenih prek GPS-naprave,
- zahteve po izpisku prometa na tekočem računu za podaljšanje socialne pomoči ali za pridobitev hitrega bančnega posojila,
- fotokopiranje osebnih dokumentov ob sklenitvi naročniškega razmerja,
- nadzor koriščenja bolniškega dopusta zaposlenega s pomočjo detektivske službe,
- zbiranje osebnih podatkov sodelujočih v nagradnih igrah.

Dajanje pisnih mnenj in pojasnil glede obdelave osebnih podatkov na posameznih področjih je pomemben del preventivnega delovanja Informacijskega pooblaščenca, ki je s tem veliko prispeval k izboljšanju stanja na področju varstva osebnih podatkov v Republiki Sloveniji. Poleg pisnih mnenj in pojasnil pa je Informacijski pooblaščenec dajal tudi ustna mnenja in pojasnila. V uradu je namreč vsem vsak dan od 8. do 16. ure na voljo en dežurni zaposleni, ki odgovarja na vprašanja po telefonu.

3.4. Dopustnost izvajanja biometrijskih ukrepov

Informacijski pooblaščenec je po določbi 80. člena ZVOP-1 pristojen za vodenje upravnih postopkov za izdajo odločb o tem, ali je nameravano izvajanje biometrijskih ukrepov v zasebnem sektorju v skladu z določbami ZVOP-1 ali ne.

Biometrija je veda o prepoznavi ljudi na podlagi njihovih telesnih, fizioloških ter vedenjskih značilnosti, ki jih imajo vsi posamezniki, ki so edinstvene in pri vsakem posamezniku stalne in je z njimi možno določiti posameznika, zlasti z uporabo prstnega odtisa, posnetka papilarnih črt s prsta, šarenice, očesne mrežnice, obraza, ušesa, DNK ter značilne drže.

Biometrijski ukrepi, kot posebna oblika obdelave osebnih podatkov, so urejeni v 3. poglavju VI. dela ZVOP-1, od 78. do 81. člena. Izvajanje biometrijskih ukrepov v javnem sektorju se lahko določi le z zakonom, če je to nujno za varnost ljudi ali premoženja ali za varovanje tajnih podatkov in poslovne skrivnosti in tega ni mogoče doseči z milejšimi sredstvi. Poleg tega se lahko biometrijske ukrepe določi z zakonom tudi, če gre za izpolnjevanje obveznosti iz obvezujoče mednarodne pogodbe ali za identifikacijo posameznikov pri prehajanju državne meje.

Zasebni sektor lahko izvaja biometrijske ukrepe le, če so nujno potrebni za opravljanje dejavnosti, za varnost ljudi ali premoženja ali za varovanje tajnih podatkov ali poslovne skrivnosti. Biometrijske ukrepe lahko izvaja le za svoje zaposlene, če so bili ti o tem predhodno pisno obveščeni.

Če izvajanje določenih biometrijskih ukrepov v zasebnem sektorju ni urejeno z zakonom, je upravljavec osebnih podatkov, ki namerava izvajati biometrijske ukrepe, dolžan pred uvedbo ukrepov posredovati Informacijskemu pooblaščenцу opis nameravanih ukrepov in razloge za njihovo uvedbo.

Informacijski pooblaščenec je po prejetju opisa nameravane uvedbe biometrijskih ukrepov dolžan v dveh mesecih odločiti, ali je nameravana uvedba biometrijskih ukrepov v skladu z določbami ZVOP-1 ali ne, pri čemer z vidika načela sorazmernosti preverja predvsem to, ali je nameravano izvajanje biometrijskih ukrepov res nujno za opravljanje dejavnosti vlagatelja, za varnost ljudi ali premoženja ali za varovanje tajnih podatkov ali poslovne skrivnosti. Zato mora vlagatelj v svoji vlogi navesti in utemeljiti razloge, zakaj je izvajanje biometrijskih ukrepov nujno za opravljanje njegove dejavnosti, za varnost ljudi ali premoženja ali za varovanje tajnih podatkov ali poslovne skrivnosti. Vlogo je treba kolkovati oziroma plačati upravno takso. Rok za izdajo odločbe se lahko podaljša za največ en mesec, če bi uvajanje biometrijskih ukrepov prizadelo več kot 20 zaposlenih pri osebi zasebnega sektorja ali če reprezentativni sindikat pri delodajalcu zahteva sodelovanje pri upravnem postopku. Upravljavec osebnih podatkov sme biometrijske ukrepe izvajati šele po prejetju odločbe, ki mu dovoli izvajanje biometrijskih ukrepov.

Zoper odločbo Informacijskega pooblaščenca pritožba ni mogoča, dovoljen pa je upravni spor.

Če izvajanje biometrijskih ukrepov v javnem sektorju ni določeno z zakonom, lahko javni sektor uvede biometrijske ukrepe v zvezi z vstopom v stavbo ali dele stavbe in evidentiranje prisotnosti zaposlenih na delu, pri čemer pa se smiselno uporabijo določbe drugega, tretjega in četrtega odstavka 80. člena ZVOP-1. To pomeni, da mora tudi oseba javnega sektorja, ki namerava za navedene namene izvajati biometrijske ukrepe, najprej pridobiti pozitivno odločbo Informacijskega pooblaščenca.

Informacijski pooblaščenec je v letu 2006 prejel 15 vlog za uvedbo biometrijskih ukrepov, 7 vlagateljev je bilo pravnih oseb zasebnega in 6 pravnih oseb javnega sektorja. Izdanih je bilo 12 odločb o dopustnosti izvajanja biometrijskih ukrepov, dve vlogi sta do konca leta ostali nerešeni, ena vloga pa je bila umaknjena. V šestih odločbah je bila uvedba biometrijskih ukrepov dovoljena, v treh odločbah je bilo dovoljeno omejeno izvajanje biometrijskih ukrepov, s štirimi odločbami pa je bilo izvajanje biometrijskih ukrepov zavrnjeno.

Pozitivne odločbe so bile izdane dvema telekomunikacijskima operaterjema, hotelu, zavodu za zaposlovanje, računalniškemu podjetju in podjetju, ki izdeluje bančne kartice, ker je bilo ugotovljeno, da je izvajanje biometrijskih ukrepov nujno za opravljanje dejavnosti, za varnost ljudi ali premoženja ali za varovanje tajnih podatkov ali poslovne skrivnosti. Informacijski pooblaščenec je tako dovolil izvajanje biometrične identifikacije z obdelavo prstnega odtisa zaposlenih, ki vstopajo v varovano območje proizvodnje, in personalizacije bančnih in drugih poslovnih kartic za vsesplošno uporabo in za preverjanje zaposlenih, ki vstopajo v systemske prostore, v katerih so shranjeni podatki, opredeljeni kot poslovna skrivnost podjetja (evidence imetnikov kartic, finančnih transakcij, kartičnih zlorab ipd.). Dovolil je tudi izvajanje biometrijskih ukrepov nad tistimi

zaposlenimi, ki so pooblaščenim vstopiti v prostor, kjer so strežniki in računalniška oprema, na katerih se hranijo in nadalje obdelujejo osebni podatki posameznikov, ki jih je upravljavec dolžan zbirati in nadalje obdelovati na podlagi zakonov s področja zaposlovanja in zavarovanja za primer brezposelnosti. Pozitivna odločba je bila izdana tudi za izvajanje biometrijskih ukrepov nad tistimi zaposlenimi, za katere je upravljavec dolžan evidentirati delovni čas, ki ga preživijo v jami, kjer so izpostavljeni ionizirajočemu sevanju, ter nad zaposlenimi, ki vstopajo v prostore, kjer je telekomunikacijska oprema, ki jo je operater dolžan varovati v skladu z zakonodajo s področja telekomunikacij.

Negativna odločba je bila izdana upravljavcu, ki je v vlogi navedel, da namerava uvesti biometrijske ukrepe le nad stanovalci študentskega doma, t. j. študenti, ne pa tudi nad svojimi zaposlenimi. Odločitev Informacijskega pooblaščenca izhaja iz dejstva, da stanovalci študentskega bloka niso v delovnem razmerju z upravljavcem, torej niso njegovi zaposleni. Navedena zahteva je bila tako v nasprotju z določbo ZVOP-1, ki določa, da lahko zasebni sektor izvaja biometrijske ukrepe le nad svojimi zaposlenimi, če so bili ti o tem prej pisno obveščeni. Iz enakega razloga je bila izdana negativna odločba upravljavcu, ki je želel uvesti biometrične ukrepe za evidentiranje članov plavalnega kluba ob vstopu v bazen. Dve negativni odločbi sta zadevali uvedbo biometrijskih ukrepov zaradi evidentiranja delovnega časa oziroma prisotnosti na delu pri upravljavcih iz zasebnega sektorja. Informacijski pooblaščenec je ugotovil, da evidentiranje prisotnosti na delu ni nujno za opravljanje dejavnosti družbe, zato bi bilo izvajanje biometrijskih ukrepov prekomeren in ne nujno potreben poseg v zasebnost zaposlenih, saj je evidentiranje prisotnosti mogoče izvesti na manj vsiljiv način.

Informacijski pooblaščenec predvsem presodi namen, ki ga zasleduje vložnik zahteve (upravljavec). Namen mora biti resen in utemeljen ter podprt z dovolj dokazi. Ne zadoštuje zgolj pavšalno navajanje, zakaj je uvedba biometrijskih ukrepov nujna. Ugotavlja se tudi, ali bi isti namen lahko zadovoljivo dosegli z načini preverjanja oz. ugotavljanja identitete, ki ne vključujejo biometrijskih ukrepov, ki torej manj posegajo v zasebnost in dostojanstvo zaposlenih. Informacijski pooblaščenec presoja tudi tehnični vidik biometrijskih ukrepov. Presoja, ali se postopek uporablja za preverjanje identitete (avtentikacija) ali za ugotavljanje identitete (identifikacija) in s tem povezano, ali se biometrični podatki shranjujejo na centralni lokaciji ali decentralizirano. Presoja tudi, kdo ima dostop do teh podatkov, ali so ti podatki ustrezno varovani, v kakšni obliki se shranjujejo itn.

Če torej upravljavec osebnih podatkov, ki želi uvesti biometrijske ukrepe tudi za evidenco delovnega časa, dokaže, da so nameni, ki jih zasleduje, takšni, da so biometrijski ukrepi ne samo potrebni, temveč da so nujno potrebni v skladu z enim od pogojev za uvedbo (varnost ljudi, varnost premoženja, opravljanje dejavnosti, varovanje tajnih podatkov, varovanje poslovnih skrivnosti) in da tega namena ni mogoče doseči na drug način, ki je s stališča zasebnosti in dostojanstva zaposlenih manj škodljiv oziroma vsiljiv, potem se tudi evidentiranje delovnega časa lahko izvede z biometrijskimi ukrepi. Praksa pa kaže, da upravljavci uvajajo biometrijske ukrepe za evidentiranje delovnega časa zgolj zato, ker je takšen način bolj praktičen od sistema z brezkontaktnimi karticami ali pa želijo preprečiti zlorabe s posojanjem kartic, pri čemer zadnji razlog zgolj pavšalno navedejo in ne ponudijo dovolj dokazov za svoje trditve.

V zvezi z izvajanjem biometrijskih ukrepov je treba omeniti, da nekaj upravljavcev osebnih podatkov, ki so izvajali biometrijske ukrepe že pred uveljavitvijo ZVOP-1, Informacijskemu pooblaščenču še vedno ni posredovalo vloge za dovolitev izvajanja biometrijskih ukrepov, s čimer tvegajo plačilo globe in prepoved nadaljnjega izvajanja biometrijskih ukrepov s strani državnega nadzornika za varstvo osebnih podatkov. Eden izmed zavezancev je moral zaradi ugotovljenih nepravilnosti prenehati uporabljati in odstraniti vse biometrične čitalce, s katerimi je vodil evidenco prisotnosti zaposlenih na delu.

3.5. Ugotavljanje ustrezne ravni varstva osebnih podatkov v tretjih državah

Skladno z določbami ZVOP-1 je Informacijski pooblaščenec na področju iznosa osebnih podatkov v tretje države pristojen za:

- izdajo odločb o zagotavljanju ustrezne ravni varstva osebnih podatkov v tretjih državah (63. člen);
- vodenje postopkov ugotavljanja ustrezne ravni varstva osebnih podatkov v tretjih državah na podlagi ugotovitev inšpekcijskega nadzora in drugih informacij (64. člen);
- vodenje seznama tretjih držav, za katere je ugotovil, da imajo v celoti ali delno zagotovljeno ustrezno raven varstva osebnih podatkov, ali da te nimajo zagotovljene; če je ugotovljeno, da tretja država le delno zagotavlja ustrezno raven varstva osebnih podatkov, je v seznamu navedeno tudi, v katerem delu je ustrezna raven zagotovljena (66. člen);
- vodenje upravnih postopkov za izdajo dovoljenj za iznos osebnih podatkov v tretjo državo (70. člen).

Po določbah ZVOP-1 morata biti za posredovanje osebnih podatkov uporabnikom v tretjih državah (države, ki niso članice Evropske unije ali Evropskega gospodarskega prostora) izpolnjena dva pogoja kumulativno, in sicer:

- za posredovanje oziroma sporočanje in dajanje osebnih podatkov na razpolago upravljavcu ali uporabniku osebnih podatkov v tretji državi mora obstajati katera izmed pravnih podlag, ki so za javni sektor določene v 9. členu ZVOP-1, za zasebni sektor pa v 10. členu ZVOP-1;
- ob izpolnjenem prvem pogoju je posredovanje osebnih podatkov upravljavcu osebnih podatkov v tretji državi (državi zunaj Evropske unije) dopustno, če Informacijski pooblaščenec izda odločbo, da država, v katero se podatki iznašajo, zagotavlja ustrezno raven varstva osebnih podatkov. Odločba ni potrebna, če je tretja država na seznamu držav iz 66. člena ZVOP-1, za katere je ugotovljeno, da v celoti zagotavljajo ustrezno raven varstva osebnih podatkov, če pa to zagotavljajo delno, se posredujejo tisti osebni podatki in za tiste namene, za katere je ugotovljena ustrezna raven varstva.

Kadar navedena pogoja nista izpolnjena, je posredovanje osebnih podatkov v tretjo državo dopustno le, če je izpolnjen kateri izmed pogojev, ki jih taksativno določa 70. člen

ZVOP-1. Po določbah tega člena se lahko osebni podatki iznesejo in posredujejo v tretjo državo, če:

- tako določa drugi zakon ali obvezujoča mednarodna pogodba;
- obstaja osebna privolitev posameznika, na katerega se nanašajo osebni podatki, in je ta seznanjen s posledicami takega posredovanja;
- je iznos potreben za izpolnitev pogodbe med posameznikom, na katerega se nanašajo osebni podatki, in upravljavcem osebnih podatkov ali za izvršitev predpogodbenih ukrepov, sprejetih kot odgovor na zahtevo posameznika, na katerega se nanašajo osebni podatki;
- je iznos potreben za sklenitev ali izvršitev pogodbe, ki je v korist posameznika, na katerega se nanašajo osebni podatki, sklenjene med upravljavcem osebnih podatkov in tretjo stranko;
- je iznos potreben zato, da se pred hujšim ogrožanjem zavaruje življenje ali telo posameznika, na katerega se nanašajo osebni podatki;
- se podatki iznesejo iz registrov, javnih knjig ali uradnih evidenc, ki so po zakonu namenjene zagotavljanju informacij javnosti in so na voljo za vpogled javnosti na splošno ali kateri koli osebi, ki lahko izkaže pravni interes, da so izpolnjeni pogoji, ki jih za vpogled določa zakon;
- upravljavec osebnih podatkov zagotovi ustrezne ukrepe zavarovanja osebnih podatkov ter temeljnih pravic in svoboščin posameznikov in navede možnosti njihovega uresničevanja ali varstva, predvsem v določbah pogodb ali v splošnih pogojih poslovanja.

Po določbah 63., 64., 68. in 70. člena ZVOP-1 vodi Informacijski pooblaščenec dve vrsti postopkov v zvezi z ugotavljanjem ustrezne ravni varstva osebnih podatkov v tretji državi, in sicer:

- na podlagi 63., 64. in 68. člena ZVOP-1 ugotavlja, ali tretja država zagotavlja ustrezno raven varstva osebnih podatkov;
- na podlagi drugega odstavka 70. člena ZVOP-1 ugotavlja, ali upravljavec osebnih podatkov pri posredovanju osebnih podatkov v tretjo državo, za katero še ni ugotovljeno, ali zagotavlja ustrezno raven varstva osebnih podatkov, v določbah pogodb ali v splošnih pogojih poslovanja zagotovi ustrezne ukrepe zavarovanja osebnih podatkov ter temeljnih pravic in svoboščin posameznikov ter navede možnosti njihovega uresničevanja. Informacijski pooblaščenec je pri odločanju v navedenih postopkih vezan na oceno pristojnega organa Evropske unije, ali tretje države zagotavljajo ustrezno raven varstva osebnih podatkov. Zoper njegovo odločitev pritožba ni mogoča, dovoljen pa je upravni spor.

V letu 2006 je bila izdana ena odločba o iznosu osebnih podatkov, ki je pravni osebi iz Ljubljane kot upravljavcu osebnih podatkov dovolila, da po prejetju odločbe za namen procesiranja kartic iznaša osebne podatke imetnikov plačilnih in kreditnih kartic v enotni procesni center v Združenih državah Amerike. Izneseni osebni podatki se bodo v ZDA hranili največ toliko časa, kolikor bo trajala pogodba, ob izteku pogodbe pa bodo vsi podatki takoj vrnjeni izvozniku ali izbrisani. Za namen procesiranja kartic lahko pravna oseba iznaša osebne podatke, ki so bili posebej določeni za fizične osebe, pravne osebe, imetnike poslovne kartice in za trgovce. Dovoljenje za iznašanje osebnih

podatkov velja za čas trajanja pogodbe med ameriško banko in slovenskim upravljavcem podatkov (5 let) oziroma do morebitne izdaje nove odločbe Informacijskega pooblaščenca o prepovedi nadaljnjega iznašanja osebnih podatkov.

Vse druge vloge za iznos osebnih podatkov so zadevale države, ki so nastale na ozemlju nekdanje Jugoslavije, večinoma za iznos na Hrvaško, v Bosno in Hercegovino ter v Srbijo in v Črno goro.

Za mnenje o iznosu osebnih podatkov v omenjene države so prosili štirje upravljavci osebnih podatkov:

1. Upravna enota Gornja Radgona je spraševala, ali lahko hrvaškemu odvetniku posreduje podatek o stalnem prebivališču osebe, živeče v Sloveniji;
2. Upravna enota Celje je spraševala, ali lahko hrvaškemu Zavodu za pokojninsko zavarovanje posreduje podatek o datumu smrti osebe;
3. Upravna enota Maribor je želela mnenje, ali lahko Občinskemu sodišču iz Beograda izda podatke o stalnem prebivališču za slovenskega državljana, ki pred omenjenim sodiščem nastopa kot tožena stranka;
4. Ministrstvo za zunanje zadeve je spraševalo, ali lahko veleposlaništvo Republike Slovenije v Bosni in Hercegovini izda sodišču v Sarajevu podatke o izdaji vizuma bosenskememu državljanu za potovanje v Slovenijo.

Ob upoštevanju dejstva, da Informacijski pooblaščenec za Srbijo, Črno goro, Hrvaško in Bosno in Hercegovino še ni izdal odločbe, da zagotavljajo ustrezno raven varstva osebnih podatkov, oziroma navedenih držav ni na seznamu tretjih držav iz 66. člena ZVOP-1, je posredovanje osebnih podatkov v navedene države dopustno, če je izpolnjen kateri izmed pogojev, ki jih taksativno določa 70. člen ZVOP-1. Kadar kakšna država oz. njen državni organ podatke potrebuje za vodenje sodnega postopka, je posredovanje osebnih podatkov po določbi 1. točke prvega odstavka 70. člena ZVOP-1 možno na podlagi zakonske podlage, mednarodnih pogodb ali ratificiranih konvencij. Tako se lahko Hrvaški posredujejo podatki na podlagi in v skladu z Zakonom o ratifikaciji Pogodbe med Republiko Slovenijo in Republiko Hrvaško o pravni pomoči v civilnih in kazenskih zadevah³⁶, torej po diplomatski poti. Podatki se lahko npr. posredujejo tudi na podlagi Haaške konvencije o pridobivanju dokazov v civilnih ali gospodarskih zadevah v tujini, ki jo je Slovenija ratificirala³⁷, seveda, če je država prosilka podpisnica te konvencije. Upravljavec osebnih podatkov pa lahko posameznika seznani z zaprosilom za posredovanje njegovih osebnih podatkov, s posledicami posredovanja ter ga obenem zaprosi, da posreduje svojo pisno privolitev, če meni, da mu je posredovanje osebnih podatkov v korist.

Informacijski pooblaščenec je odgovoril tudi na vprašanje o iznosu osebnih podatkov v Romunijo in Bolgarijo po 1. januarju 2007. Informacijski pooblaščenec je pojasnil, da bosta obe državi v skladu s Pogodbo o pristopu, ki sta jo podpisali leta 2005, januarja 2007 sprejeti v Evropsko unijo kot državi članici. Zato se za iznos osebnih podatkov od dneva njunega pristopa uporablja 62. člen ZVOP-1. Velja namreč, da se določbe ZVOP-1 o iznosu podatkov v tretje države ne uporabljajo, kadar se posredujejo osebni podatki

36 Uradni list RS, št. 42/1994; Mednarodne pogodbe št. 10/2004.

37 Uradni list RS, št. 76/2000; Mednarodne pogodbe št. 19/2000.

upravljavcu osebnih podatkov, pogodbenemu obdelovalcu ali uporabniku osebnih podatkov, ki je bil ustanovljen, ima sedež ali je registriran v državi članici Evropske unije. Gre za implementacijo 1. člena Direktive 95/46/ES, ki določa, da države članice Evropske unije ne omejujejo in ne prepovedujejo prostega prenosa osebnih podatkov med državami članicami zaradi razlogov, povezanih z varstvom njihove zasebnosti pri obdelavi osebnih podatkov. Za upravljavce v Evropski uniji pri iznosu osebnih podatkov iz Republike Slovenije v države članice torej veljajo popolnoma enaka pravila kot za obdelavo osebnih podatkov v Republiki Sloveniji.

3.6. Izdajanje dovoljenj za povezovanje javnih evidenc

Po določbah 84. člena ZVOP-1 je zbirke osebnih podatkov iz uradnih evidenc in javnih knjig dovoljeno povezovati, če tako določa zakon. Upravljalci osebnih podatkov, ki povezujejo dve ali več zbirk osebnih podatkov, ki se vodijo za različne namene, so dolžni o tem predhodno pisno obvestiti Informacijskega pooblaščenca. Če najmanj ena zbirka osebnih podatkov, ki naj bi se jo povezovalo, vsebuje občutljive osebne podatke, ali če bi bila posledica povezovanja razkritje občutljivih podatkov ali je za izvedbo povezovanja potrebna uporaba istega povezovalnega znaka, povezovanje ni dovoljeno brez predhodnega dovoljenja Informacijskega pooblaščenca. Ta dovoli povezavo na podlagi pisne vloge upravljavca osebnih podatkov, če ugotovi, da upravljalci osebnih podatkov zagotavljajo ustrezno zavarovanje osebnih podatkov. Zoper odločbo Informacijskega pooblaščenca pritožba ni mogoča, dovoljen pa je upravni spor.

Iz navedenih določb 84. člena ZVOP-1 izhaja, da Informacijski pooblaščenec pri odločanju o izdaji dovoljenja za povezavo zbirk osebnih podatkov preverja predvsem to, ali upravljalci zbirk osebnih podatkov zagotavljajo ustrezno zavarovanje osebnih podatkov. Postopki in ukrepi za zavarovanje osebnih podatkov morajo biti ustrezni glede na tveganje, ki ga predstavlja obdelava in narava nekaterih osebnih podatkov, ki se obdelujejo. Zavarovanje osebnih podatkov po določbah 24. člena ZVOP-1 zajema organizacijske, tehnične in logično-tehnične postopke in ukrepe, s katerimi se varujejo osebni podatki, preprečuje naključno ali namerno nepooblaščenno uničevanje podatkov, njihova sprememba ali izguba ter nepooblaščen obdelava podatkov.

Poleg ugotavljanja ustreznosti zavarovanja osebnih podatkov mora Informacijski pooblaščenec pri odločanju o izdaji dovoljenja za povezovanje zbirk osebnih podatkov opraviti tudi vsebinski preizkus o tem, ali za povezovanje zbirk osebnih podatkov obstaja ustrezna zakonska podlaga. To namreč izhaja iz splošnega nadzora nad zakonitostjo in poštenostjo obdelave osebnih podatkov, ki jo pooblaščenca nalagata ZVOP-1 in ZInfP.

Informacijski pooblaščenec je v letu 2006 prejel 7 vlog za pridobitev dovoljenja za povezovanje zbirk osebnih podatkov. Tri vloge so bile odobrene, in sicer:

- Ministrstvu za javno upravo in Ministrstvu za notranje zadeve: povezava Centralne kadrovske evidence državne uprave in Centralnega registra prebivalstva;
- Zavodu Republike Slovenije za zaposlovanje in Ministrstvu za notranje zadeve: povezava Evidence brezposelnih oseb in Centralnega registra prebivalstva;

- Zavodu Republike Slovenije za zaposlovanje in Ministrstvu za delo, družino in socialne zadeve: povezava Informacijskega sistema centrov za socialno delo in Informacijskega sistema Zavoda Republike Slovenije za zaposlovanje.

Kot povezovalni znak se v vseh primerih uporabi enotna matična številka občana (EMŠO), povezujejo in izmenjujejo pa se lahko zgolj tiste vrste osebnih podatkov, ki jih določa zakon.

Ena vloga za izdajo dovoljenja za povezovanje zbirk osebnih podatkov je bila zaradi nepopolnosti zavržena.

3.7. Seznanitev z lastnimi osebnimi podatki

Informacijski pooblaščenec je prejel 3 pritožbe zaradi molka organa v zvezi s pravico do seznanitve z lastnimi osebnimi podatki. V skladu s 3. odstavkom 38. člena Ustave RS je posamezniku zagotovljena pravica do seznanitve z zbranimi osebnimi podatki, ki se nanašajo nanj (lastni osebni podatki), kot tudi pravica do sodnega varstva ob zlorabi lastnih osebnih podatkov. Pravica posameznika do seznanitve z lastnimi osebnimi podatki je nadalje konkretizirana v ZVOP-1. V okviru te pravice, ki je določena v 30. členu ZVOP-1, je upravljavec osebnih podatkov posamezniku predvsem dolžan omogočiti vpogled v katalog zbirke osebnih podatkov. Posameznik, na katerega se osebni podatki nanašajo, ima pravico te podatke pogledati, jih prepisati ali kopirati. Upravljavec osebnih podatkov je tudi dolžan potrditi, ali se podatki v zvezi s posameznikom obdelujejo ali ne. Gre za uresničevanje temeljnega načela Direktive 95/46/ES, ki poudarja, da mora posameznik prejeti tudi t. i. negativno informacijo oziroma informacijo, da se podatki v zvezi z njim ne obdelujejo. Obenem je upravljavec osebnih podatkov dolžan posamezniku posredovati tudi seznam uporabnikov, ki so jim bili posredovani osebni podatki, kdaj, na kateri podlagi in za kakšen namen. S tem se zagotavlja t. i. sledljivost osebnih podatkov, ki je podrobneje urejena v 22. členu ZVOP-1. Prav tako je upravljavec osebnih podatkov posamezniku dolžan dati informacije o namenu obdelave in vrsti osebnih podatkov, ki se obdelujejo, ter vsa potrebna pojasnila v zvezi s tem. Prav tako je upravljavec dolžan posamezniku na njegovo zahtevo dati informacijo o virih, na katerih temeljijo zapisi, ki jih o posamezniku vsebuje zbirka osebnih podatkov, in o načinu obdelave; informacije o namenu obdelave in vrsti osebnih podatkov, ki se obdelujejo, ter vsa potrebna pojasnila v zvezi s tem ter tudi pojasnilo glede tehničnih oziroma logično-tehničnih postopkov odločanja, če upravljavec izvaja avtomatizirano odločanje z obdelavo osebnih podatkov posameznika.

Postopek seznanitve posameznika z lastnimi osebnimi podatki ureja 31. člen ZVOP-1. Iz navedenega člena izhaja, da postopek temelji na zahtevi posameznika, pri čemer je upravljavec vezan na to zahtevo in mora posamezniku omogočiti takšno vrsto seznanitve z lastnimi osebnimi podatki, kot jo ta zahteva (vpogled, prepis, kopiranje, potrdilo). Roki, v katerih mora upravljavec ugoditi zahtevi posameznika za seznanitev z lastnimi osebnimi podatki, so odvisni od zahteve posameznika oziroma od pravice, ki jo ta uveljavlja. Upravljavec osebnih podatkov mora posamezniku omogočiti vpogled, prepis,

kopiranje in potrdilo najpozneje v 15 dneh, izpis, seznam, informacije ter pojasnilo pa dati v 30 dneh od dneva, ko je prejel zahtevo. Če upravljavec ne bo omogočil vpogleda, prepisa, kopiranja ali izdaje potrdila, izpisa, seznama, informacij ali pojasnila mora posameznika v istem roku pisno obvestiti o razlogih za svoje ravnanje. Če upravljavec v predpisanem roku ne ugotovi zahtevi prosilca, niti mu pisno ne pojasni, zakaj mu tega ne bo omogočil, ima prosilec na podlagi 2. člena ZInFP pravico do pritožbe pri Informacijskem pooblaščenču. Pritožba, določena v 2. čl. ZInFP, vsebuje dve vrsti pritožbe. Prva vrsta pritožbe je usmerjena zoper pisno obvestilo upravljavca osebnih podatkov o razlogih, zaradi katerih posamezniku ni omogočil vpogleda, prepisa, kopiranja, izdaje potrdila, izpisa, seznama, informacij in pojasnila iz 1. odstavka 30. člena ZVOP-1. Druga vrsta pritožbe pa je usmerjena zoper molk upravljavca osebnih podatkov.

Vložene pritožbe zaradi zavrnitve seznanitve z lastnimi osebnimi podatki so zadevale:

1. policijsko upravo, ki prosilcu ni posredovala podatkov, ali se obdelujejo osebni podatki v zvezi z njim, seznama uporabnikov, ki so jim bili posredovani njegovi osebni podatki, kdaj, na kateri podlagi in za kakšen namen, ter informacije o namenu obdelave in vrsti njegovih osebnih podatkov, ki se obdelujejo, ter vsa potrebna pojasnila v zvezi s tem;
2. zdravstveno ustanovo, ki prosilcu ni omogočila vpogleda v osebne podatke, ki so se nanašali na pokojnega očeta prosilca, čeprav je izkazal, da je zakoniti dedič prvega dednega reda po umrlem in da ima pravni interes za pridobitev zahtevanih osebnih podatkov;
3. državni izpitni center, ker prosilci ni dovolil vpogleda v izpitno dokumentacijo za maturo.

Po pozivu Informacijskega pooblaščenca zavezancem k pojasnitvi navedenih primerov sta policijska uprava in zdravstvena ustanova zahtevane podatke posredovali, medtem ko se je tretja pritožba izkazala za neupravičeno.

3.8. Najodmevnejši primeri kršitev varstva osebnih podatkov

V letu 2006 je Informacijski pooblaščenec izdal nekaj medijsko odmevnih odločb:

- odločbo o prekršku zunanjetrgovinskemu podjetju, ki je v specializirani blagovni hiši izvajalo videonadzor v delovnih prostorih zunaj delovnega mesta, in sicer v garderobah oziroma slačilnicah za pomerjanje oblačil, s čimer je kršilo določbo 77. člena ZVOP-1, ki prepoveduje izvajanje videonadzora v garderobah, dvigalih in sanitarnih prostorih. Ugotovljeno je bilo, da se posnetki dogajanja v trgovini hranijo, da dostop do videonadzornega sistema ni bil zaščiten, da ni bila zagotovljena sledljivost z vidika presnemavanja na prenosne medije in tudi ne vodena evidenca pregledovanja posnetkov. Informacijski pooblaščenec je kršilcu naložil takojšnje prenehanje izvajanja videonadzora v garderobah za pomerjanje oblačil, kar je kršilec storil. Informacijski pooblaščenec je zaradi kršitev določb ZVOP-1 izrekel globo, saj je kršilec z izvajanjem videonadzora v kabinah za preoblečenje grobo posegal v zasebnost in dostojanstvo oseb, ki so vstopile v kabino, s čimer je kršil tudi ustavne pravice do osebnega dostojanstva, varnosti in zasebnosti;

- odločbo o prekršku časopisni hiši, ki je v tedniku objavila imena in priimke prejemnikov najvišjih bruto in neto izplačanih plač zaposlenih v časopisni družbi, ter s tem osebne podatke 86 zaposlenih nezakonito uporabila in posredovala javnosti, čeprav za tako obdelavo osebnih podatkov ni imela podlage v zakonu ali v osebni privolitvi posameznika (marca 2007 je odločbo v postopku zahteve po sodnem varstvu potrdilo Okrajno sodišče v Ljubljani). Pri obdelavi osebnih podatkov zaposlenih v časopisni družbi je šlo za obdelavo osebnih podatkov na področju zasebnega sektorja, pri čemer sta obdelava ter varstvo njihovih osebnih podatkov podrobneje določena v Zakonu o delovnih razmerjih³⁸. Skladno z omenjenim zakonom in ob spoštovanju določb 10. člena ZVOP-1 bi lahko v časopisu podatke o plačah zaposlenih objavili le, če bi bilo to potrebno zaradi uresničevanja pravic in obveznosti iz delovnega razmerja ali v zvezi z delovnim razmerjem ali če bi imeli osebno privolitev posameznika, na katerega se podatki nanašajo. Javnost plač je določena³⁹ le za javni sektor, pri čemer je izrecno določeno, da javna podjetja in gospodarske družbe, v katerih ima večinski delež oziroma prevladujoč vpliv država (časopisna družba), niso del javnega sektorja. Tednik se je skliceval na pravico do svobode izražanja in javni interes, vendar pri tem ni upošteval 3. odstavka 15. člena Ustave RS in 10. člena Evropske konvencije o človekovih pravicah, po katerih so človekove pravice in temeljne svoboščine omejene s pravicami drugih. Poleg tega je pravico do svobode izražanja omejil tudi že Zakon o medijih⁴⁰, po katerem bi bil tednik upravičen pridobiti in objaviti sporne podatke le takrat, ko bi s tem preprečil hujše kaznivo dejanje ali neposredno nevarnost za življenje ljudi in njihovo premoženje, o čemer pa v obravnavanem primeru ni bilo mogoče govoriti. Objava podatkov je posegla v ustavne pravice do osebnega dostojanstva, varstva zasebnosti in osebnostnih pravic ter pravico do varstva osebnih podatkov, pravica do svobode izražanja pa v tem »trku« pravic ni prevladala;
- odločbo o prekršku časopisu, ki je objavil obdukcijske zapisnike treh žrtev, umrlih pred vhodom v diskoteko. Kršilec se je tudi v tem primeru skliceval na svobodo izražanja in javni interes, kar pa v tem primeru ni mogla biti pravna podlaga za obdelavo osebnih podatkov v zasebnem sektorju, zlasti pa za obdelavo občutljivih osebnih podatkov o zdravstvenem stanju oz. obdelavo osebnih podatkov umrlih, ki je posebej določena v 13. in 23. členu ZVOP-1. Poleg tega obdelava osebnih podatkov ni bila v skladu z namenom, za katerega so bili zbrani. Obdukcijski zapisniki so bili namenjeni za vodenje kazenskega postopka zoper lastnika diskoteke in nikakor ne za objavo v časopisu. Informacijski pooblaščenec je zaradi hude kršitve določb ZVOP-1 kršilcu izrekel globo.
- Informacijski pooblaščenec je preverjal tudi zakonitost obdelave osebnih podatkov v postopkih kliničnega preizkušanja zdravil, ugotavljal način zavarovanja osebnih podatkov pacientov ter možnosti dostopa do teh podatkov. Glede pridobivanja predhodnih pisnih soglasij pacientov za sodelovanje pri kliničnih raziskavah ni bilo ugotovljenih nepravilnosti, ugotovljeno pa je bilo, da zavezanci niso vzpostavili katalogov zbirk osebnih podatkov, ki nastajajo v zvezi s kliničnim preizkušanjem zdravil, da ni evidence vpogledov v arhivirane zdravstvene kartone ter da ni zagotovljena sledljivost.

38 Uradni list RS, št. 42/2002, 79/2006-ZZZPB-F.

39 Zakon o sistemu plač v javnem sektorju (Uradni list RS, št. 56/2002).

40 Uradni list RS, št. 110/2006, uradno prečiščeno besedilo.

- Informacijski pooblaščenec je obravnaval prijavo, v kateri je prijavitelj navedel, da je na spletni strani ene od zavarovalnic napačno vnesel številko zavarovalne police in s tem prišel do osebnih podatkov druge osebe. Pooblaščenec se je takoj odzval in ugotovil, da je bilo zaradi izjemno slabega zavarovanja možno priti do osebnih podatkov skoraj 24.000 otrok, dijakov in študentov zgolj z vnosom številke zavarovalne police. Ker so bile osebe v podatkovno bazo vnesene skoraj po abecednem vrstnem redu, je lahko nepooblaščenca oseba z ugibanjem v kratkem času prišla do osebnih podatkov zavarovancev, in sicer do imena in priimka, naselja, ulice in hišne številke, davčne številke, statusa zavarovanca in seveda številke zavarovalne police. Tako pridobljene osebne podatke je bilo mogoče tudi natisniti. Zavarovalnici je bila zaradi grobe kršitve dolžnosti zavarovanja osebnih podatkov izrečena globa.

3.9. Zahteve po presoji ustavnosti zakonov

Drugi odstavek 48. člena ZVOP-1 določa, da ima Informacijski pooblaščenec pravico na Ustavnem sodišču vlagati zahteve po presoji ustavnosti zakonov, drugih predpisov ter splošnih aktov, izdanih za izvrševanje javnih pooblastil, če se pojavi vprašanje ustavnosti in zakonitosti v zvezi s postopkom, ki ga vodi. Torej je pri vlaganju zahtev po presoji ustavnosti omejen, saj ne gre za splošno pooblastilo za vlaganje zahtev na Ustavnem sodišču, ampak se mora zahteva nanašati na konkretni postopek. Določba pomeni popravilo situacije, ko Informacijski pooblaščenec ni imel možnosti dati predhodnega mnenja o usklajenosti določb predlogov zakonov ter drugih predpisov z zakoni in drugimi predpisi, ki urejajo osebne podatke.

Informacijski pooblaščenec je v letu 2006 vložil dve zahtevi po presoji ustavnosti:

- **sedmega in osmega odstavka 128. člena Zakona o letalstvu**⁴¹, ki urejata gibanje in zadrževanje na javnem letališču ter v objektu navigacijskih služb zračnega prometa. Izpodbijana določba je po mnenju Informacijskega pooblaščenca v neskladju z 2., 15. in 38. členom Ustave RS ter 8. členom EKČP, zato je predlagal njeno razveljavitev in do dokončne odločitve sodišča zadržanje njenega izvajanja. Z izpodbijanim členom se namreč grobo posega v informacijsko zasebnost kot ustavno pravico posameznika, saj se predvideva prekomerno zbiranje osebnih podatkov, ki deloma ni niti razumno, v celoti pa ni sorazmerno s koristjo skupnosti in splošno varnostjo v državi, ki bi bila nujna v demokratični družbi. Zlet ne določa namena zbiranja oziroma obdelave osebnih podatkov s tako jasnostjo, da bi bila posamezniku zagotovljena potrebna pravna varnost. Poleg tega Zlet ne izpolnjuje zahteve, da morajo biti osebni podatki, ki naj bi se obdelovali, točno naštetih v samem zakonu, ampak osebne podatke našteva le eksemplifikativno. Čeprav zakon predvideva zbiranje osebnih podatkov neposredno od posameznika in na podlagi njegove dodatne osebne privolitve, mora biti tudi tovrstno vzpostavljano zbiranje osebnih podatkov podvrženo načelu sorazmernosti. V nasprotju z načelom sorazmernosti je zahteva po podatkih o bivanju v tujini, šolanju in obiskovanju seminarjev ali drugih vrst usposabljanja v tujini, podatki o prekrških, tekočih kazenskih postopkih, izrečenih disciplinskih ukrepih, vrsti in višini finančnih obveznosti.

41 Uradni list RS, št. 113/2006, uradno prečiščeno besedilo, v nadaljevanju Zlet.

Neustavna je tudi zakonska zahteva, da mora posameznik sporočati občutljive osebne podatke, ki presegajo namen, zaradi katerega naj bi bili zbrani (npr. uživanje alkohola, mamil, morebitne duševne težave oziroma bolezni).

prvega odstavka 96. člena, drugega odstavka 98. člena, 100. člena, petega in šestega odstavka 103. člena in prvega odstavka 114. člena Zakona o evidentiranju nepremičnin⁴², ki med drugim ureja evidentiranje nepremičnin, register nepremičnin, izdajanje podatkov in druga vprašanja, povezana z evidentiranjem nepremičnin. Zakon v izpodbijanih določbah našteva vrsto osebnih podatkov, ki naj bi se zbirali, namen njihove obdelave pa je nenatančen, presplošen oz. nedoločen. Brez zakonsko določenega namena obdelave se namreč ne morejo z gotovostjo določiti vrste in števila osebnih podatkov, ki se v skladu z zakonom lahko obdelujejo. Poleg tega bodo zbrani osebni podatki vključeni v register nepremičnin, ki je javna knjiga po določbi 114. člena ZEN. To, da namen uporabe zbranih osebnih podatkov v zakonu ni jasno določen, pomeni, da zakon z javno objavo teh podatkov celo omogoča, da se zbrani podatki uporabljajo za kakršen koli namen, kar je v neskladju z ustavo. Po določbi 100. člena se bodo v register nepremičnin, poleg s popisom zbranih podatkov, vključili tudi podatki iz več zbirk. Z vidika informacijske zasebnosti je združevanje podatkov v enotnem javnem registru nepremičnin nedopustno; v pravu varstva zasebnosti je treba zagovarjati načelo decentralizacije zbirk osebnih podatkov. Glede na število osebnih podatkov, prevzetih v register nepremičnin, ti pa so tudi javno dostopni, taka ureditev ne ustreza načelu sorazmernosti. Prekomerno je tako ne le zbiranje velikega števila osebnih podatkov, ampak tudi njihova javna objava, še zlasti pa združevanje v enem samem javno dostopnem registru. Z objavljanjem teh podatkov se posega tudi v nedotakljivost lastnine kot ustavne kategorije. Obstaja pa tudi utemeljena bojazen, da bodo uporabniki javno objavljene osebne podatke uporabili v številne, vnaprej neopredeljene namene, kar je nevzdržno z vidika pravne varnosti.

3.10. Splošna ocena stanja varstva osebnih podatkov in priporočila

Republika Slovenija je z uveljavitvijo ZVOP-1 ter ZInFP v svoj pravni red v celoti prenesla določbe Direktive 95/46/ES in s tem formalno v celoti izpolnila zahteve Evropske unije na tem področju. Z uveljavitvijo navedenih zakonov je slovenski nadzorni organ za varstvo osebnih podatkov – Informacijski pooblaščenec tudi formalno postal popolnoma samostojen in neodvisen.

ZVOP-1 načelno določa, da je varstvo osebnih podatkov namenjeno preprečevanju nezakonitih in neupravičenih posegov v informacijsko zasebnost posameznika na vseh bistvenih področjih. Določa tudi, da je na ozemlju Republike Slovenije vsakemu posamezniku, ne glede na državljanstvo in prebivališče, zagotovljeno varstvo osebnih podatkov. Smisel varstva osebnih podatkov torej ni varovanje osebnih podatkov kot takih, temveč varovanje pravic posameznika, na katerega se podatki nanašajo.

Ugotovitve pri opravljanju neposrednega inšpekcijskega nadzora na terenu, ki se opravlja že vse od leta 1995, kažejo, da Republika Slovenija na področju varstva osebnih po-

42 Uradni list RS, št. 47/2006, v nadaljevanju ZEN.

datkov v ničemer ne zaostaja za zahodno Evropo ter se srečuje s podobnimi oziroma zelo primerljivimi problemi. Ob tem ugotavljamo, da smo v ZVOP-1 nekatera področja varstva osebnih podatkov uredili celo natančneje in pregledneje, kot v večini drugih evropskih držav. To velja zlasti za področje neposrednega trženja, videonadzora, biometrije, evidentiranja vstopov v prostore in izstopov iz njih, povezovanja zbirk osebnih podatkov iz uradnih evidenc in javnih knjig ter strokovnega nadzora.

K izboljšanju stanja na področju varstva osebnih podatkov lahko največ pripomorejo upravljavci zbirk osebnih podatkov. Ti se vedno bolj zavedajo pomena varstva osebnih podatkov, kar dokazuje predvsem stalno povečevanje števila zaprosil za mnenja, pojasnila in stališča v zvezi s konkretnimi vprašanji, ki se upravljavcem osebnih podatkov zastavljajo pri delu. Vendar ugotovitve pri opravljanju inšpekcijskega nadzora kažejo, da stanje pri večini upravljavcev kljub vsemu ni tako, kot bi moralo biti, ter da se iz leta v leto odkrivajo tako rekoč enake nepravilnosti.

Glede na ugotovljeno stanje bodo morali upravljavci osebnih podatkov več pozornosti nameniti zlasti zagotavljanju ažurnih katalogov zbirk osebnih podatkov ter ažurnih podatkov v registru zbirk osebnih podatkov. Glede na to, da je register zbirk osebnih podatkov objavljen na spletni strani Informacijskega pooblaščenca, lahko upravljavci osebnih podatkov sami preverijo točnost in ažurnost podatkov, ki se nanašajo na njihove zbirke in Informacijskega pooblaščenca obvestijo o spremembah in dopolnitvah.

Upravljavci osebnih podatkov bodo morali v prihodnje več pozornosti nameniti tudi zavarovanju osebnih podatkov, kar pomeni, da bodo morali v notranjih aktih predpisati ustrezne postopke in ukrepe za zavarovanje osebnih podatkov, z akti seznaniti zaposlene in seveda zagotoviti izvajanje teh postopkov in ukrepov. Poleg tega bodo morali upravljavci več pozornosti nameniti določitvi oseb, ki so odgovorne za posamezne zbirke osebnih podatkov, ter določitvi oseb, ki lahko zaradi narave dela obdelujejo nekatere osebne podatke – zaradi omejevanja možnih zlorab mora biti ta krog ljudi čim ožji.

Veliko bodo morali upravljavci osebnih podatkov storiti tudi, da bodo izpolnili vse zakonske zahteve glede izvajanja videonadzora. V zvezi s tem bodo morali predvsem paziti, da bodo objavili ustrezna obvestila in da bodo pred začetkom izvajanja izdali pisno odločitev o uvedbi videonadzora, v kateri bodo pojasnjeni razlogi za to. Pred uvedbo videonadzora bodo morali izvajalci o tem pisno obvestiti zaposlene in se o morebitnem izvajanju videonadzora znotraj delovnih prostorov posvetovati z reprezentativnim sindikatom pri delodajalcu. Za evidenco videonadzora bodo morali izvajalci zagotoviti tudi katalog zbirke podatkov ter podatke iz kataloga posredovati Informacijskemu pooblaščenču, kar so do zdaj storili le redki.

Upravljavci osebnih podatkov bodo morali bistveno izboljšati tudi obveščanje posameznikov o zbiranju osebnih podatkov ter posameznikom ob tej priložnosti dati vse informacije, določene v 19. členu ZVOP-1. Pri tem bodo morali posameznika zlasti jasno oziroma nedvoumno seznaniti z namenom obdelave osebnih podatkov, saj se prepogosto dogaja, da je namen opredeljen preširoko oziroma sploh ni opredeljen. Upravljavci osebnih podatkov bodo morali ob zbiranju osebnih podatkov bolj paziti tudi na načelo sorazmernosti. Kot je bilo že navedeno, je v večini primerov nedopustno

zbirati dve osebni identifikacijski številki posameznika (npr. EMŠO in davčno številko), saj za nedvoumno identifikacijo posameznika zadostuje že ena od teh dveh števil. Poleg tega bodo morali organizatorji nagradnih iger, žrebanj in podobnega prenehati vnaprej zbirati davčno številko od vseh udeležencev, saj jo v resnici potrebujejo le od oseb, ki so dobile nagrado.

Normativni ureditvi varstva osebnih podatkov bodo morali večjo pozornost nameniti tudi predlagatelji zakonov ter zakonodajalec. Pri pripravi zakonskih določb, ki predpisujejo obdelavo osebnih podatkov na posameznem področju, bosta morala biti predlagatelj in zakonodajalec zlasti pozorna na načelo sorazmernosti, kar pomeni, da se bo v področnem zakonu določila le obdelava tistih podatkov, ki je ustrezna in po obsegu primerna glede na namene, za katere se osebni podatki zbirajo in nadalje obdelujejo. Poleg tega bo treba več pozornosti nameniti tudi načelu predhodne določitve namena obdelave osebnih podatkov, kar pomeni, da mora biti v zakonu jasno opredeljen namen obdelave osebnih podatkov, ki mora biti tudi ustavno dopusten. Priporoča pa se tudi, da se v zakonih čim natančneje določi rok (še) dopustne hrambe osebnih podatkov.

V Republiki Sloveniji se je namreč že zgodilo, da je Ustavno sodišče razveljavilo določbe zakonov ravno zato, ker je zakon predpisoval zbiranje in prekomerno obdelavo osebnih podatkov, ker zakon ni opredelil namena obdelave osebnih podatkov ali pa v zakonu sploh ni bilo natančno opredeljeno, kateri osebni podatki se bodo obdelovali.

Zaradi ugotovitev pri opravljanju inšpekcijskega nadzora bo moral tudi Informacijski pooblaščenec v prihodnje še več pozornosti nameniti preventivnemu delovanju. V okviru preventivnega delovanja bo treba predvsem okrepiti dejavnosti izobraževanja in ozaveščanja oseb, ki so pri upravljavcih osebnih podatkov odgovorne za obdelavo osebnih podatkov. V okviru svojih pristojnosti bo Informacijski pooblaščenec lahko v sodelovanju s stroko na lastno pobudo pripravljaj, objavljaj in upravljavcem osebnih podatkov posredoval neobvezna pisna navodila in priporočila glede tistih vprašanj ali področij, na katerih bo odkril največ nepravilnosti. V okviru preventivnega delovanja bo moral okrepiti tudi preventivni inšpekcijski nadzor na tistih področjih oziroma pri tistih upravljavcih osebnih podatkov, ki obdelujejo več zbirk osebnih podatkov oziroma obdelujejo tudi občutljive osebne podatke. To so zlasti upravljavci osebnih podatkov s področja zdravstvene dejavnosti, socialne varnosti, zavarovalništva, poleg tega pa mednje štejemo tudi večje delodajalce, državne organe, organe lokalnih skupnosti, nosilce javnih pooblastil ter druge upravljavce osebnih podatkov v javnem sektorju.

Obdelava osebnih podatkov v sodobnem svetu je že nekaj časa neločljivo povezana z uporabo informacijsko-komunikacijskih tehnologij. Danes so na papirju kvečjemu le še manjše baze podatkov, obdelave večjih količin podatkov pa si brez uporabe informacijsko-komunikacijskih tehnologij ni več mogoče predstavljati. Ob upoštevanju vseh prednosti, ki jih prinašajo sodobne tehnologije, pa ni mogoče spregledati dejstva, da sodobne tehnologije povečujejo možnosti nadzora, količine, hitrosti in trajanja obdelave (osebnih) podatkov in posledično možnosti kršitve ustavne pravice do zasebnosti in kršitve zakonodaje s področja varstva osebnih podatkov. Obdelava osebnih podatkov, ki vključuje tako rekoč vsa dejanja v povezavi z osebnimi podatki, je danes eden izmed ključnih virov poslovanja za marsikatero sodobno podjetje, in podatki o tem, kako se

Ljudje vedo, katerim demografskim skupinam pripadajo, kakšne so njihove kupne navade, kje in kdaj se gibljejo in podobno, so za zasebni sektor izjemne vrednosti. Metaforično bi lahko rekli, da so v 21. stoletju »rudniki podatkov« več vredni kot rudniki zlata. Vrednosti osebnih podatkov se zaveda tudi javni sektor, zlasti v okrepljenem boju proti terorizmu, a osebne podatke žal prepogosto zbira in obdeluje brez izdelanih analiz, na zalogo, brez namena, zapisanega v zakonu, brez pretehtane sorazmernosti med varnostjo in posegom v zasebnost posameznikov.

Glede na hiter razvoj sodobnih informacijsko-komunikacijskih tehnologij nič ne kaže, da bi obstajale težnje po zmanjševanju možnosti vdora v zasebnost na splošno in zlorabe osebnih podatkov. Ravno obratno, nekatere nove tehnologije in storitve, kot so RFID (Radio Frequency Identification), RuBee, biometrija, tehnologije za nadzor nad lokacijo in gibanjem posameznika in podobno, predstavljajo nove grožnje za posameznikovo zasebnost. Možnosti, ki so se še pred kratkim zdele kot znanstvena fantastika, postajajo čedalje realnejše. Nanotehnologije, RFID in sorodne tehnologije, biometrija itd. kažejo težnje po premiku v t. i. internet objektov, kjer večino virov in ponorov podatkov ne ustvarjajo več ljudje, ampak objekti, toda objekti, ki pripadajo posamezniku, kot so njegov potni list, oblačila ali celo deli telesa. V okolju vsenavzočnih mrežno povezljivih tehnologij se posameznik čedalje manj zaveda kdo, kdaj, kje in na katere načine obdeluje njegove osebne podatke.

Informacijski pooblaščenec se pri odnosu do teh tehnologij pridružuje stališčem evropskih kolegov iz delovne skupine Article 29 in si nikakor ne želi omejevanja podjetniške pobude in oviranje razmaha novih tehnologij, zlasti tistih, ki bi koristile posamezniku in družbi, a si ob tem prizadeva, da se tehnologije, ki so same po sebi nevtralne, uporabljajo na način, ki je prijazen do zasebnosti posameznika, in ne obratno. S stališča varstva osebnih podatkov bodo tako vedno imeli prednost tisti načini obdelave osebnih podatkov, pri katerih je vdor v zasebnost manjši. Pri tem so temeljna izhodišča, da manjšo grožnjo predstavljajo decentralizirane zbirke osebnih podatkov, boljše možnosti nadzora posameznika nad svojimi osebnimi podatki, z nameni sorazmerna uporaba enoličnih identifikatorjev in podobno.

S hitro rastjo uporabe informacijsko-komunikacijskih tehnologij se torej povečujejo tudi možnosti zlorabe osebnih podatkov. Informacijski pooblaščenec zato posebno pozornost namenja nadzoru spoštovanja določb ZVOP-1, ki urejajo zavarovanje zbirk osebnih podatkov, obenem pa skuša seznanjati s koraki, ki jih za varstvo lastnih osebnih podatkov, zlasti v povezavi z uporabo interneta, lahko uporabi posameznik. Pri tem je ena izmed ključnih varovalk na strani uporabnika večja ozaveščenost posameznikov, zato je Informacijski pooblaščenec na svoji spletni strani opisal nekatere možnosti zlorabe osebnih podatkov na internetu in dal priporočila za varno uporabo interneta oziroma za obrambo pred nevarnostmi. Posebno pozornost je namenil t. i. ribarjenju podatkov (ang. phishing), »pharming« napadom in nezaželenim elektronskim sporočilom (ang. spam). Pri ribarjenju podatkov želijo spletni goljufi s pomočjo lažnih spletnih strani in elektronskih sporočil od ljudi tako ali drugače izvabiti osebne podatke, kot so številke kreditnih kartic, uporabniška imena in gesla, digitalna potrdila, in druge osebne podatke. Napadi »pharming« so bolj nevarni za uporabnika, saj jih je težje prepoznati. Uporabnik je prepričan, da je na pravi strani, saj je vtipkal pravi URL-naslov strani, v resnici pa ga je eden od omenjenih načinov napada preusmeril na lažno stran.

Informacijski pooblaščenec v luči prizadevanj za varstvo osebnih podatkov na internetu in varnejši internet sploh podpira tudi dejavnosti slovenske točke za ozaveščanje o varni rabi interneta SAFE-SI (<http://www.safe.si/>) in anonimne spletne prijavnice točke SPLET-NO-OKO.SI za prijavo primerov otroške pornografije in sovražnega govora na internetu (<https://www.spletno-oko.si/>).





WATCH YOUR

4

**DRUGE DEJAVNOSTI INFORMACIJSKEGA
POOBLAŠČENCA**

Poleg navedenih dejavnosti je Informacijski pooblaščenec opravljal še druge dejavnosti:

- sodeloval je z ministrstvi in drugimi organi ter organizacijami pri pripravi zakonov in drugih predpisov, ki po posameznih področjih predpisujejo obdelavo osebnih podatkov;
- obveščal javnost o svojem delu in jo izobraževal (izdajanje publikacij, seznani tev posameznikov z njihovimi pravicami prek svetovnega spleta, organizacija okroglih miz),
- izobraževal različne ciljne skupine, ki se pri svojem delu srečujejo z ZDIJZ in ZVOP-1;
- sodeloval na seminarjih, konferencah, posvetih in sestankih, tudi v tujini;
- opozarjal upravljavce osebnih podatkov in jim pomagal, zlasti pri določanju organizacijskih in ustreznih logično-tehničnih postopkov in ukrepov za zavarovanje osebnih podatkov ter pri pripravi ustreznih notranjih aktov.

4.1. Sodelovanje pri pripravi zakonov in drugih predpisov

V skladu z določbami 48. člena ZVOP-1 daje Informacijski pooblaščenec predhodna mnenja ministrstvom, državnemu zboru, organom samoupravnih lokalnih skupnosti, drugim državnim organom ter nosilcem javnih pooblastil o usklajenosti določb zakonov ter drugih predpisov z zakoni in drugimi predpisi, ki urejajo osebne podatke. Informacijski pooblaščenec je v letu 2006 sodeloval pri pripravi teh zakonov in drugih predpisov:

- Zakonu o javnih naročilih⁴³,
- Zakonu o javnih uslužbencih⁴⁴,
- Zakonu o agenciji za nepremičninske evidence (v pripravi),
- Zakonu o zdravstvenem varstvu in zdravstvenem zavarovanju⁴⁵,
- Zakonu o omejevalnih ukrepih, ki jih Republika Slovenija uvede ali izvaja skladno s pravnimi akti in odločitvami, sprejetih v okviru mednarodnih organizacij⁴⁶,
- Zakonu o preprečevanju omejevanja konkurence⁴⁷,
- Zakonu o detektivski dejavnosti⁴⁸ (v postopku spreminjanja),
- Zakonu o zdravniški službi⁴⁹,
- Zakonu o občinskem redarstvu⁵⁰,
- Zakonu o skupni promociji kmetijskih, ribiških in drugih proizvodov (v pripravi),
- Zakonu o soobstoju gensko spremenjenih rastlin z ostalimi kmetijskimi rastlinami (v pripravi),
- Zakonu o elektronskih komunikacijah⁵¹,

43 Uradni list RS, št. 128/2006.

44 Uradni list RS, št. 32/2006, uradno prečiščeno besedilo, sprememba 33/2007

45 Uradni list RS, št. 38/2006.

46 Uradni list RS, št. 127/2006.

47 Uradni list RS, št. 99/2004, uradno prečiščeno besedilo, sprememba 40/2007.

48 Uradni list RS, št. 113/2005, uradno prečiščeno besedilo.

49 Uradni list RS, št. 47/2006.

50 Uradni list RS, št. 139/2006.

51 Uradni list RS, št. 129/2006.

- Zakonu o inšpekcijskem nadzoru⁵²,
- Zakonu o notariatu⁵³,
- Zakonu o pacientovih pravicah (v pripravi),
- Zakonu o policiji⁵⁴,
- Zakonu o sodnem registru⁵⁵,
- Zakonu o Ustavnem sodišču⁵⁶ (v postopku spreminjanja),
- Zakonu o spremembah in dopolnitvah zakona o tujcih⁵⁷,
- Zakonu o zaposlovanju in delu tujcev⁵⁸.

4.2. Sodelovanje z javnostmi

Informacijski pooblaščenec veliko pozornosti posveča tudi medijem. Mediji lahko namreč veliko pripomorejo k seznanjanju širše javnosti s pravicami, ki jih imajo posamezniki in katere s svojim delom ščiti tudi Informacijski pooblaščenec. Gre za temeljni človekovi pravici, določeni tudi v 38. in 39. členu Ustave RS.

V letu 2006 je Informacijski pooblaščenec organiziral tri novinarske konference:

- 25. september 2006: Dan pravice vedeti.
- 10. julij 2006: (Ne)razmejitev med javnim in zasebnim delom službe zdravnikov Univerzitetnega kliničnega centra.
- 6. junij 2006: Obisk srbskega pooblaščenca za dostop do informacij javnega značaja.

S sporočili za javnost je Informacijski pooblaščenec obveščal javnost o svojem delu, predvsem o aktualnih primerih, s katerimi je želel ažurno opozoriti na kršitve, ki jih je zaznal pri svojem delu. Dal pa je tudi številne izjave za javnost.

Načelo preglednosti delovanja in ozaveščanja javnosti je Informacijski pooblaščenec upošteval tudi pri zasnovi svoje spletne strani (www.ip-rs.si). Ta stran vsebuje oziroma ponuja:

- predstavitev zgodovine Informacijskega pooblaščenca in predstavitev zaposlenih,
- predstavitev obeh področij delovanja, torej varstva osebnih podatkov in dostopa do informacij javnega značaja, in pristojnosti na obeh področjih,
- domačo in tujo zakonodajo,
- odgovore na najpogostejše zastavljena vprašanja,
- ažurno objavo vseh izdanih odločb in mnenj,

52 Uradni list RS, št. 56/2002, sprememba 26/2007.

53 Uradni list RS, št. 115/2006.

54 Uradni list RS, št. 78/2006.

55 Uradni list RS, št. 91/2005, sprememba 60/2006.

56 Uradni list RS, št. 15/1994.

57 Uradni list RS, št. 79/2006.

58 Uradni list RS, št. 4/2006.

- seznanitev z aktualnimi dogodki (sodbe in novice) na obeh področjih,
- možnost prijave na e-novice (prejemanje novih odločb Informacijskega pooblaščenca in sporočil za medije),
- vse publikacije, ki jih Informacijski pooblaščenec izdaja,
- različne obrazce, namenjene fizičnim osebam za uveljavljanje njihovih pravic (zahteva po dostopu in ponovni uporabi informacij javnega značaja, prijava kršitev določb ZDIJZ in ZVOP-1) in upravljavcem zbirk osebnih podatkov za lažje delo pri vlaganju različnih zahtev in zagotovitvi ustreznega varovanja osebnih podatkov (vloge za iznos osebnih podatkov, obrazec za prijavo biometrijskih ukrepov, zahteve po izdaji odločbe glede povezljivosti evidenc, vzorec katalogov zbirk osebnih podatkov in pravilnika o zavarovanju osebnih podatkov).

V letu 2006 je bilo izdanih osem publikacij:

- »Tudi danes imate pravico vedeti!«;
- »Vstop v zasebnost prepovedan!« (tudi v angleškem jeziku);
- »Poročilo Inšpektorata za varstvo osebnih podatkov za leto 2005«;
- »Vstopite, dostop je prost!«;
- »Access to my Privacy Denied!«;
- »Pristojnosti Informacijskega pooblaščenca« (tudi v angleškem jeziku);
- »Kako in kdaj uporabljati test javnega interesa« (izdano konec leta 2005 – skupaj z Ministrstvom za javno upravo);
- »Access to Public Information in Slovenia« (skupaj z Ministrstvom za javno upravo).

4.3. Mednarodno sodelovanje

4.3.1. Sodelovanje na mednarodnih srečanjih

V letu 2006 so se zaposleni pri Informacijskem pooblaščenca udeležili več mednarodnih seminarjev in konferenc, na nekaterih so sodelovali s svojimi prispevki.

- 28. november 2006, Luxembourg, Luksemburg: delovna skupina Evropske komisije za informacije javnega značaja, raziskovalec Informacijskega pooblaščenca je predstavil slovenske primere, ki zadevajo to področje.
- 20. do 22. november, Podgorica, Črna gora: okrogla miza o implementaciji Zakona o svobodnem dostopu do informacij.
- 20. november 2006, Budimpešta, Madžarska: 2. evropska konferenca o dostopu do informacij javnega značaja.
- 11. do 15. november 2006, Atene, Grčija: 14. delavnice za varstvo osebnih podatkov pod pokroviteljstvom grškega nadzornega organa za varstvo osebnih podatkov.
- 9. november 2006, Skopje, Makedonija: konferenca »Dostop do informacij javnega značaja – implementacija zakona in uporaba v praksi«, svetovalka Informacijskega pooblaščenca je predstavila slovensko ureditev in izkušnje na tem področju.

- 8. november 2006, Zagreb, Hrvaška: konferenca o varstvu osebnih podatkov »Privatnost 2006«, pooblaščenka je predavala o slovenskih izkušnjah na področjih dostopa do informacij javnega značaja in varstva osebnih podatkov.
- 2. in 3. november 2006, London, Velika Britanija: 28. mednarodna konferenca varstva osebnih podatkov in Pooblaščenec za varstvo osebnih podatkov.
- 28. oktober 2006, Novi Sad, Srbija: Strokovni seminar sodnikov in tožilcev, pooblaščenka in državni nadzornik sta predavala o slovenski ureditvi dostopa do informacij javnega značaja in varstvu osebnih podatkov.
- 6. oktober 2006, Gradec, Avstrija: delavnice »Varstvo osebnih podatkov in e-uprava in RFID tehnologija«.
- 4. in 5. september 2006, Monte Carlo, Monako: Srečanje neodvisnih frankofonskih avtoritet, pristojnih za varstvo osebnih podatkov.
- 28. do 30. avgust 2006, Ciudad de Mexico, Mehika: mednarodna konferenca »Transparentnost in dostop do informacij«, pooblaščenka je nastopila kot govornica na konferenci.
- 10. do 12. julij, Nikozija, Ciper: sestanek ekspertne skupine »za Schenegen«.
- 30. junij 2006, Beograd, Srbija: mednarodna konferenca »Implementacija prava dostopa do informacij javnega značaja v Srbiji, poldrugo leto kasneje«, pooblaščenka je nastopila kot eden izmed osrednjih govornikov in je predstavila slovensko ureditev.
- 7. do 10. junij, Bitola, Makedonija: regionalni seminar o varstvu osebnih podatkov v policijskih obveščevalnih metodah.
- 25. maj 2006, Kensington, London, Velika Britanija: mednarodna konferenca FOI Live 2006, pooblaščenka je nastopila kot eden izmed osrednjih govornikov konference, ki je v Veliki Britaniji najpomembnejši vsakoletni dogodek na področju informacij javnega značaja.
- 22. in 23. maj 2006, Manchester, Velika Britanija: četrta letna konferenca Informacijskih pooblaščenec, pooblaščenka je imela predavanje o pristojnosti pooblaščenec in varuhov človekovih pravic na področju dostopa do javnih informacij.
- 17. in 18. maj 2006, Bruselj, Belgija: Mednarodna delavnica o varstvu osebnih podatkov.
- 11. in 12. maj 2006, Varšava, Poljska: konferenca »Javna varnost in varstvo osebnih podatkov«.
- 24. in 25. april 2006, Budimpešta, Madžarska: konferenca evropskih nadzornikov za varstvo osebnih podatkov.
- 27. in 28. marec 2006, Madrid, Španija: 13. izvedba delavnic pod pokroviteljstvom Evropske konference nadzornih organov za varstvo osebnih podatkov.
- 17. februar 2006, Luxembourg, Luksemburg: konferenca Evropske komisije o informacijah javnega sektorja.

4.3.2. Sodelovanje v delovnih skupinah Evropske unije

Informacijski pooblaščenec kot državni nadzorni organ za varstvo osebnih podatkov pri svojem delu sodeluje tudi s pristojnimi organi Evropske unije za varstvo osebnih podatkov. Sodelovanje na mednarodni ravni in sodelovanje pri zakonodajnih postopkih Evropske unije mu zapoveduje tudi Direktiva 95/46/ES.

Najpomembnejši mednarodni organ, s katerim sodeluje Informacijski pooblaščenec, je Delovna skupina 29. To je skupina, ki Evropski komisiji daje strokovna mnenja s področja varstva osebnih podatkov, sestavljajo pa jo predstavniki neodvisnih nadzornih organov za varstvo osebnih podatkov vseh držav članic Evropske unije. Ustanovljena je bila na podlagi člena 29. Direktive 95/46/ES (od tod tudi njeno ime) z namenom varstva posameznikov pri obdelavi osebnih podatkov. Pristojnosti delovne skupine so:

- proučuje vprašanja, ki zajemajo uporabo nacionalnih predpisov, sprejetih na podlagi direktive, da bi prispevala k njihovi enotni uporabi,
- Komisiji daje mnenje o ravni varstva v Skupnosti in v tretjih državah,
- Komisiji svetuje o vseh predlaganih spremembah te direktive, o vseh dodatnih ali posebnih ukrepih za zaščito pravic in svoboščin fizičnih oseb pri obdelavi osebnih podatkov ter o vseh drugih predlaganih ukrepih Skupnosti, ki vplivajo na take pravice in svoboščine,
- dajanje mnenj o kodeksih ravnanja, ki se pripravijo na ravni Skupnosti.

Med najodmevnejšimi temami, ki so bile obravnavane v minulem letu, je treba izpostaviti vprašanje iznosa osebnih podatkov v Združene države Amerike. Skupina je pomembno prispevala k iskanju rešitev glede varstva osebnih podatkov državljanov Evropske unije, tako glede prenosa evidenc imen letalskih potnikov (PNR) kot tudi zbirk finančnih podatkov prek omrežja SWIFT. Vedno večjo zaskrbljenost pristojnih organov Evropske unije namreč vzbuja tako imenovana »ameriška protiteroristična zakonodaja«, ki ustvarja ozračje kratenja pravice do zasebnosti in varstva osebnih podatkov državljanov Evropske unije. Evropska komisija se je zato odločila, da omenjene prenose podatkov evropskih državljanov prouči v sodelovanju z evropskimi organi za zaščito osebnih podatkov in tako zagotovi spoštovanje vseh načel zaščite osebnih podatkov držav članic, opredeljenih v Direktivi 95/46/ES.

Informacijski pooblaščenec je na podlagi raziskav proučil prenos podatkov slovenskih državljanov v Združene države Amerike v obeh primerih. Sodeluje tudi pri dogovorih in iskanju rešitev za ustrezno zaščito varstva zasebnosti v okviru Delovne skupine 29.

V okviru pristojnosti delovne skupine, da Komisiji daje mnenja o ravni varstva osebnih podatkov v Skupnosti in v tretjih državah, so bila Komisiji v minulem letu dana naslednja mnenja in delovni dokumenti:

- mnenje o uporabi pravil Evropske unije o varstvu podatkov v notranjih shemah za prijavo nepravilnosti na področjih računovodstva, notranjih računovodskih kontrol, revizijskih zadev, boja proti podkupovanju, bančnemu in finančnemu kriminalu,

- mnenje o vprašanih zasebnosti pri zagotavljanju storitev pregledovanja elektronske pošte,
- mnenje o Direktivi 2006/24/ES Evropskega parlamenta in Sveta o hrambi podatkov, pridobljenih ali obdelanih v zvezi z zagotavljanjem javno dostopnih elektronskih komunikacijskih storitev ali javnih komunikacijskih omrežij in spremembi Direktive 2002/58/ES,
- mnenje o obvestilu o predlagani pripravi predpisa Ministrstva za zdravje in socialne zadeve Združenih držav Amerike o nadzoru nalezljivih bolezni in zbiranju podatkov o potnikih, z dne 20. november 2005 (Nadzor nalezljivih bolezni, predlog 42 CFR del 70 in del 71),
- mnenje o odločitvi Sodišča evropskih skupnosti, z dne 30. maj 2006, v združenih zadevah C-317/04 in C-318/04 o prenosu evidence imen letalskih potnikov Združenim državam Amerike,
- mnenje o predlogu Uredbe Sveta o pristojnosti, pravu, ki se uporablja, priznavanju in izvrševanju sodnih odločb ter sodelovanju v preživninskih zadevah,
- mnenje o odločitvi Sodišča evropskih skupnosti, z dne 30. maj 2006, v združenih zadevah C-317/04 in C-318/04 o prenosu evidence imen letalskih potnikov Združenim državam Amerike in o nujnosti novega sporazuma,
- delovni dokument o možnih posledicah sistema eCall za varstvo podatkov in zasebnost,
- mnenje o pregledu regulativnega okvira za elektronske komunikacije in storitve s poudarkom na Direktivi o zasebnosti in elektronskih komunikacijah,
- mnenje o izvajanju Direktive Sveta 2004/82/ES o dolžnostih prevoznikov, da posredujejo podatke o potnikih,
- mnenje o obdelavi osebnih podatkov Družbe za svetovne medbančne finančne telekomunikacije (SWIFT).

Z namenom vstopa Republike Slovenije v schengensko območje je Informacijski pooblaščenec z vidika implemetiranja ustreznih evropskih standardov varovanja osebnih podatkov v letu 2006 sodeloval pri izpolnjevanju priporočil Schengenske evalvacijske komisije (SCHEVAL). SCHEVAL je za področje varstva osebnih podatkov po evalvaciji, ki je bila v Sloveniji izvedena marca 2006, pozitivno ocenil delo in pristojnosti Informacijskega pooblaščenca in izrekel zgolj nekaj minimalnih pripomb k zakonodaji, ki jih bodo pristojna ministrstva odpravila do konca leta 2007.

Nadalje se je Informacijski pooblaščenec (za zdaj) le kot opazovalec udeležil tudi rednih sestankov Skupnega nadzornega organa, ustanovljenega na podlagi 115. člena Konvencije o izvajanju Schengenskega sporazuma, ki je odgovoren za nadzor varovanja osebnih podatkov v okviru Schengenskega informacijskega sistema. S tega vidika je Skupni nadzorni organ v letu 2006 tudi z dajanjem mnenj sodeloval pri razpravi o sprejemanju nove pravne podlage za Schengenski informacijski sistem II, predvsem o predlogu Sklepa Sveta o vzpostavitvi, delovanju in uporabi druge generacije Schengenskega informacijskega sistema (SIS II) (COM(2005)230 konč.), kot tudi pri Uredbi Evropskega parlamenta in Sveta o vzpostavitvi, delovanju in uporabi druge generacije Schengenskega informacijskega sistema (SIS II) (COM (2005)236 konč.). Mnenja o navedenih dokumentih so bila dana predvsem z vidika implementacije uveljavljenih standardov in pravil varovanja osebnih podatkov in z vidika širšega konteksta obdelovanja ter varo-

vanja osebnih podatkov v celotnem tretjem stebru. Prav tako je Skupni nadzorni organ obravnaval težave pri uveljavitvi in uporabi 96. in 99. člena (tudi v zvezi z 111. členom) Konvencije o izvajanju Schengenskega sporazuma.

Informacijski pooblaščenec se je na podlagi 1. odstavka 18. člena v zvezi s 1. odstavkom 17. člena Konvencije o uporabi informacijske tehnologije za carinske namene kot nacionalni nadzorni organ za varstvo osebnih podatkov, ki so vključeni v carinski informacijski sistem, udeležil tudi rednih sestankov Skupnega nadzornega organa, ki je pristojen za nadzor delovanja carinskega informacijskega sistema, za preučitev vseh morebitnih težav pri uporabi ali razlaganju, ki se lahko pojavijo med njegovim delovanjem, za preučitev težav, ki lahko nastanejo v zvezi z izvajanjem neodvisnega nadzora s strani nacionalnih nadzornih organov držav članic ali pri izvajanju pravice posameznikov do dostopa do sistema, ter za pripravo predlogov za skupno reševanje težav. V okviru nalog, določenih v 3. odstavku 18. člena Konvencije o uporabi informacijske tehnologije za carinske namene, je za leto 2006 treba izpostaviti predvsem koordinirane nacionalne inšpekcije oziroma poizvedbe v zvezi z implementacijo smernic informacijske varnosti, kot jih je predlagal OLAF (Evropski urad za boj proti goljufijam).

Prav tako je Informacijski pooblaščenec na podlagi 1. odstavka 19. člena v zvezi s 1. odstavkom 20. člena Uredbe Sveta (ES) 2725/2000 o vzpostavitvi sistema »Eurodac« za primerjavo prstnih odtisov zaradi učinkovite uporabe Dublinske konvencije sodeloval pri prvem koordiniranem pregledovanju Evropskega nadzornika za varstvo osebnih podatkov in nacionalnih nadzornih organov v zvezi s spremljanjem dejavnosti centralne enote in enot držav članic.

Predvsem pa je treba poudariti aktivno sodelovanje Informacijskega pooblaščenca v Skupnem nadzornem organu, ustanovljenem na podlagi 24. člena Konvencije na podlagi člena K.3 Pogodbe o Evropski uniji o ustanovitvi Evropskega policijskega urada. Skupni nadzorni organ za Europol je tako izvajal pristojnosti, določene v omenjenem členu, med katerimi je bil še poseben poudarek na:

- organizaciji konference z naslovom Varstvo osebnih podatkov v Europolu – stalen izziv;
- mnenjih o predlogu sklepa Sveta o ustanovitvi Evropskega policijskega urada (Europol) (SEC(2006) 1682) (SEC(2006) 1683) in drugih predlaganih aktih oziroma predlogih njihovih sprememb;
- mnenjih v okviru pristojnosti, določenih z Europolovo konvencijo, in pravilih, sprejetih na njeni podlagi, kot na primer izdajanje mnenj na podlagi pravil o prenosu osebnih podatkov tretjim državam in tretjim telesom, pravil o sprejetju podatkov od tretjih oseb pri Europolu in pravil, veljavnih za Europolove analitične delovne datoteke;
- opravi vsakoletno inšpekcijo v Europolu.

Prav tako se je v okviru Skupnega nadzornega organa za Europol zaradi izvrševanja svojih pristojnosti glede na določilo 24. čl. Konvencije na podlagi člena K.3 Pogodbe o Evropski uniji o ustanovitvi Evropskega policijskega urada sestal notranji odbor za obravnavanje pritožb, predvidenih v 7. odstavku 19. člena in 4. odstavku 20. člena konvencije. Tudi v tem odboru ima Informacijski pooblaščenec svojega predstavnika.

Vsemu opisanemu delu pa je dala širši kontekst tudi razprava o osnutku Okvirnega sklepa o varstvu osebnih podatkov v tretjem stebru v okviru delovne skupine Skupnega nadzornega organa, t. i. Police working party, na rednih sestankih, ki se jih je udeležil tudi Informacijski pooblaščenec. Osnutek Sklepa namreč predstavlja velike spremembe pri varovanju osebnih podatkov v tretjem stebru Evropske unije in s tem povezane načrte nadaljnjega, tudi vsebinskega delovanja Skupnega nadzornega organa za varstvo osebnih podatkov in vloge Informacijskega pooblaščenca v njem.





Poročilo pripravili:

Odgovorna urednica:

Nataša Pirc Musar

Izvršni urednici:

Sonja Bien Karlovšek,
Mojca Prelesnik

Glavna urednica in avtorica besedil:

dr. Monika Benkovič Krašovec,
državna nadzornica za varstvo osebnih podatkov

Avtorji besedil:

Sonja Bien Karlovšek, namestnica informacijske pooblaščenke

Jože Bogataj, državni nadzornik za varstvo osebnih podatkov

Urban Brulc, raziskovalec

Andreja Mrak, raziskovalka

mag. Tanja Slak, državna nadzornica za varstvo osebnih podatkov

mag. Andrej Tomšič, svetovalec

Alenka Žaucer, svetovalka

Lektorica:

Petra Kranjec

Oblikovanje

Bons, d.o.o.

Tisk

Tiskarna Premiere, d.o.o.

Ljubljana, maj 2007

ISSN 1854-9500

