INFORMACIJSKI POOBLAŠČENEC
REPUBLIKE SLOVENIJE

11

Letno poročilo Informacijskega pooblaščenca

za leto 2011

'11 Letno poročilo

Informacijskega pooblaščenca za leto 2011

0 UVOD

Leto 2011 je ponovno zaznamovala opazno višja raven zavedanja posameznikov o pomenu pravice do dostopa do informacij javnega značaja in do varstva osebnih podatkov, žal pa tudi nekaj zaskrbljujočih trendov.

Sodeč po obsegu zadev, ki jih je v tem letu obravnaval Informacijski pooblaščenec, smo ponovno priča tako rekoč rekordnemu številu zadev, ki jih prejmemo v obravnavo na obeh področjih delovanja Informacijskega pooblaščenca, pa naj gre za zaprosila za mnenja, prijave ali pritožbe. Takšne razmere so nedvomno posledica vse večje obveščenosti in osveščenosti posameznikov, ki vse bolj razumejo namen in pomen obeh človekovih pravic, katerih uveljavljanje in varstvo je v pristojnosti Informacijskega pooblaščenca. Hkrati pa moramo vsaj deloma tolikšno povečanje števila pritožbenih in inšpekcijskih zadev pripisati tudi nekaterim zaskrbljujočim ravnanjem, na eni strani organov zavezancev na področju dostopa do informacij javnega značaja kot tudi (pre)velikim apetitom po obdelavi osebnih podatkov najrazličnejših upravljavcev zbirk osebnih podatkov, tako v zasebnem kot tudi v javnem sektorju.

Informacijski pooblaščenec si pri svojem delu še naprej prizadeva za čim večjo odzivnost in strokovnost, ki pa ob tolikšnem povečevanju obsega zadev v reševanju postajata komajda še dosegljiv cilj. Kljub temu sem vesela, da nam je to tudi v letu 2011 uspelo in da javnost ta naša prizadevanja za učinkovito zaščito obeh temeljnih pravic: pravice do dostopa do informacij javnega značaja in varstva osebnih podatkov prepoznava, zato je Informacijskemu pooblaščencu tudi v preteklem letu izrazila visoko stopnjo zaupanja.

Po raziskavi Centra za raziskovanje javnega mnenja je bila januarja 2012 stopnja zaupanja Informacijskemu pooblaščencu ponovno značilno visoka (52 %), celo najvišja med izbranimi institucijami, stopnja nezaupanja pa med najnižjimi med opazovanimi institucijami (14 %). Ker tudi predhodne meritve kažejo visoko raven zaupanja in so deleži vselej v zgornji polovici ranga, lahko govorimo o konstantno izraženem zaupanju, kar me izjemno veseli ter hkrati zavezuje k nadaljevanju dela in iskanju možnosti za izboljšave.

Na področju dostopa do informacij javnega značaja ugotavljamo, da so prosilci bolje seznanjeni z institutom dostopa do informacij javnega značaja in se ga tudi pogosteje poslužujejo v praksi. Po drugi strani pa je Informacijski pooblaščenec pri organih zavezancih v preteklem letu žal opazil zaskrbljujoč upad pripravljenosti na sodelovanje s prosilci, kar se kaže tudi v povečanju števila pritožb na Informacijskega pooblaščenca in povečanju števila vloženih tožb s strani zavezancev zoper odločitve Informacijskega pooblaščenca. Navedeno je verjetno tudi posledica dejstva, da Vlada Republike Slovenije na tem področju (še) ni sprejela skupne strategije, iz katere bi sledilo, kakšni naj bodo cilji delovanja organov javnega sektorja na tem področju oziroma strategije, ki bi zavezance spodbujala k bolj transparentnemu delovanju. Informacijski pooblaščenec je tako v praksi opazil, da so določene kategorije zavezancev (predvsem manjše občine, javni zavodi na področju šolstva, zasebni izvajalci javnih služb in koncesionarji) slabo seznanjene z obveznostmi, ki jih zanje prinaša Zakon o dostopu do informacij javnega značaja, ne glede na to, da je bil zakon sprejet že leta 2003 in da je začetno

obdobje implementacije že zdavnaj mimo. Na to kažejo tudi nekatere ugotovitve in ocene nacionalnega sistema integritete v državi, ki jo je opravilo Društvo Integriteta - Transparency International Slovenija.

Na področju varstva osebnih podatkov v letu 2011 želim opozoriti predvsem na področje elektronskih komunikacij, saj zaznavamo povečane težnje po nadzorovanju uporabe elektronskih komunikacij, pri čemer prihaja do trenj med različnimi interesi in pravicami. Izpostaviti želim predvsem neprimerno ureditev omejevanja dostopnosti spletnih vsebin v določbah Zakona o igrah na srečo, ki ponudnikom dostopa do interneta nalaga blokiranje dostopa do spletnih iger na srečo ter zaskrbljujoč poskus širjenja pooblastil organov pregona v zvezi z uporabo podatkov, ki so jih dolžni hraniti operaterji elektronskih komunikacij. Vlada je namreč predlagala spremembe 149.b člena Zakona o kazenskem postopku, ki bi omogočile ne le pridobivanje podatkov za določeno telefonsko številko, temveč za celotno bazno postajo mobilne telefonije. Informacijski pooblaščenec je takšen predlog ocenil kot izrazito nesorazmeren in neučinkovit glede na težo tega posega v zasebnost. Predlog vlade so poslanci na obravnavi na ustreznem odboru zavrnili, do česar pa ne bi prišlo, če Informacijski pooblaščenec s trdnimi argumenti ne bi vztrajno opozarjal na nesorazmernost takšnih predlogov.

Omenjena izkušnja je ponovno pokazala na pomen dveh bistvenih opozoril, ki jih Informacijski pooblaščenec vztrajno izpostavlja. Prvič, da vzpostavitev velikih zbirk osebnih podatkov neizogibno vodi v povečanje apetitov po podatkih (gre za t.i. pojav function creep ali širitev prvotnega namena obdelave). In drugič, takšne težnje je zelo težko – včasih pa tudi nemogoče – zaustaviti. To pa kaže na potrebnost pravočasno izvedenih presoj pred vzpostavitvijo takšnih zbirk, ki morajo prestati test nujnosti, sorazmernosti in učinkovitosti, saj predstavljajo izrazita tveganja za raven varstva osebnih podatkov. Informacijski pooblaščenec v zvezi s tem opozarja, da bi veljalo vzpostaviti mehanizem pravočasnih presoj vplivov na zasebnost pri pripravi zakonodajnih predlogov, ki predvidevajo spremembe, ki bistveno povečujejo tveganja za zlorabe osebnih podatkov. Žal takšnih presoj nismo videli ne pri uvedbi obvezne hrambe podatkov v prometu elektronskih komunikacij (t.i. data retention), ne pri predlaganem širjenju namenov uporabe teh zbirk, pogrešamo pa tudi post festum analize, ki bi opravičevale nujnost, sorazmernost in učinkovitost takšnih projektov.

Informacijski pooblaščenec je leta 2011 precej pozornosti namenil preventivnemu delovanju. Zaradi velikega zanimanja in sprememb na tem področju smo v letu 2011 pripravili dopolnjen ponatis zloženke »Kako uporabljati Facebook …in preživeti« ter priročnika za upravljavce osebnih podatkov »Zavarujmo osebne podatke«. Poleg tega je Informacijski pooblaščenec pripravil še nekaj novih smernic, ki bodo v pomoč uporabnikom (smernice o orodjih za zaščito zasebnosti na internetu in smernice o računalništvu v oblaku). V letu 2011 je Informacijski pooblaščenec začel tudi s pripravo posebnih tematskih poročil, v katerih se osredotočamo na posamezne pomembnejše tematske sklope, kjer izvajamo nadzor. Kot prvo takšno poročilo smo pripravili poročilo »Klubi zvestobe – povečajmo drobni tisk«, v katerem smo opravili primerjavo med nekaterimi največjimi ponudniki klubov zvestobe z vidika spoštovanja načel varstva osebnih podatkov. Tudi lani je Informacijski pooblaščenec z različnimi dejavnostmi zaznamoval dan varstva osebnih podatkov in svetovni dan pravice vedeti. Poleg tega zaposleni strokovnjaki pri Informacijskem pooblaščencu svoje znanje in izkušnje delijo tudi s kolegi iz držav, ki so šele v fazi vzpostavljanja učinkovitega sistema dostopa do informacij javnega značaja in varstva osebnih podatkov, med drugim je Informacijski pooblaščenec partner v twinning projektu na področju varstva osebnih podatkov v Črni gori.

Na obeh področjih delovanja Informacijskega pooblaščenca me skrbi, da je zaznaven določen upad občutljivosti zavezanih organov oziroma upravljavcev osebnih podatkov za obe temeljni pravici, tako za dostop do informacij javnega značaja kot tudi za varstvo osebnih podatkov. Zato bi si s strani vlade na področju dostopa do informacij javnega značaja v bodoče želela aktivnejša prizadevanja za spodbujanje zavezancev k bolj transparentnemu delovanju, s čimer bomo skupaj prispevali tudi k večji integriteti javnega sektorja in zaupanju posameznikov v institucije. Na tem mestu ne morem mimo predloga, ki smo ga lanskega avgusta posredovali ministrstvu, pristojnemu za javno upravo, in v katerem utemeljujemo potrebnost širitve kroga zavezancev za dostop do informacij javnega značaja na družbe, v katerih ima država ali lokalna skupnost prevladujoč vpliv. Ob dejstvu ustanavljanja gospodarskih družb s strani subjektov javnega prava, torej z javnim denarjem in njihovimi dokapitalizacijami je zatrjevanje, da gre za sfero zasebnega prava in posledično zasebnih sredstev, sprenevedanje. Gospodarske družbe, v katerih ima prevladujoč vpliv država ali lokalna skupnost, poslujejo z javnim denarjem in/ali pod vplivom javne oblasti, kar posledično prinaša oziroma bi moralo prinašati tudi povečano

odgovornost za poslovanje do javnosti. Upam, da bomo v tem letu razumljeni, in se bo za predlagano spremembo našla tudi politična volja. Na področju varstva osebnih podatkov pa bi si želela, da bi vsi pokazali več skrbi in zavedanja o posledicah na videz nepomembnih ukrepov množičnega in nesorazmernega zbiranja osebnih podatkov, ki vodijo v družbo nadzora.

Družba, v kateri posameznik nima zaupanja v integriteto javnega sektorja in ima občutek, da nima več zasebnosti, ker se njegovi osebni podatki obdelujejo brez njegove vednosti in v nesorazmernem obsegu, ga video in avdio snemajo, je družba, v kateri ni prostora za kreativnost, ki je gonilo napredka … Glede na čase, ki jih živimo, pa oboje, tako integriteto kot življenjsko kreativnost, potrebujemo. Želim si, da bi o tem razmišljali tudi bralci tega poročila.

S spoštovanjem,

Nataša Pirc Musar,
informacijska pooblaščenka

KAZALO

1. INFORMACIJSKI POOBLAŠČENEC

1.1. Nastanek Informacijskega pooblaščenca 1
1.2. Pristojnosti Informacijskega pooblaščenca 1
1.3. Organiziranost Informacijskega pooblaščenca 3
1.4. Finančna sredstva Informacijskega pooblaščenca 5

2. DELO NA PODROČJU DOSTOPA DO INFORMACIJ JAVNEGA ZNAČAJA

2.1. Pravna ureditev na področju dostopa do informacij javnega značaja v Republiki Sloveniji 9
2.2. Število vloženih pritožb in število rešenih zadev 9
2.3. Število vloženih tožb na Upravnem sodišču Republike Slovenije, število sodb Upravnega in Vrhovnega sodišča Republike Slovenije 11
2.4. Statistika po posameznih področjih ZDIJZ 11
2.5. Storjeni prekrški po ZDIJZ, ZInfP in ZMed 15
2.6. Predstavitev najodmevnejših in precedenčnih primerov po področjih 15
2.6.1. Osebni podatek, notranje delovanje organa, avtorsko delo 15
2.6.2. Tajni podatki, zahteva za umik stopnje tajnosti 16
2.6.3. Ali je organ zavezanec, ali gre za informacijo javnega značaja 17
2.6.4. Avtorsko delo, osebni podatek 18
2.6.5. Dokument v izdelavi, poslovna skrivnost, avtorsko delo, okoljski podatki 19
2.6.6. Osebni podatki 20
2.6.7. Mediji, poslovna skrivnost 22
2.6.8. Poslovna skrivnost 23
2.6.9. Arhivsko gradivo 24
2.6.10. Notranje delovanje organa, osebni podatki, poslovna skrivnost 25
2.6.11. Ali gre za delovno področje organa? 26
2.7. Splošna ocena in priporočila na področju dostopa do informacij javnega značaja 27

3. DELO NA PODROČJU VARSTVA OSEBNIH PODATKOV

3.1. Koncept varstva osebnih podatkov v Repubiliki Sloveniji 31
3.2. Dejavnost državnih nadzornikov za varstvo osebnih podatkov 32
3.2.1. Pravice in dolžnosti državnega nadzornika 32
3.2.2. Inšpekcijski nadzor 32
3.2.3. Storjeni prekrški 35

3.3.	Dajanje pisnih mnenj in pojasnil	37
3.4.	Dopustnost izvajanja biometrijskih ukrepov	38
3.5.	Ugotavljanje ustrezne ravni varstva osebnih podatkov v tretjih državah	42
3.6.	Izdajanje dovoljenj za povezovanje javnih evidenc	44
3.7.	Seznanitev z lastnimi osebnimi podatki	46
3.8.	Zahteve po presoji ustavnosti zakonov	48
3.9.	Izbrani primeri kršitev varstva osebnih podatkov	49
3.9.1.	Neustrezno zavarovanje osebnih podatkov na spletnem forumu	49
3.9.2.	Nezakonito snemanje telefonskih pogovorov	50
3.9.3.	Nezakonit vpogled v Evidenco registriranih motornih in priklopnih vozil	50
3.9.4.	Izvajanje neposrednega trženja na podlagi podatkov iz Centralnega registra psov	51
3.9.5.	Izvajanje neposrednega trženja na podlagi podatkov iz javno dostopnih evidenc o lastništvu nepremičnin	51
3.9.6.	Zbiranje osebnih podatkov delavcev in kandidatov za zaposlitev	52
3.9.7.	Objava osebnih podatkov novorojenih otrok v občinskem glasilu in pošiljanje rojstnodnevnih čestitk občanom	53
3.9.8.	Obdelava osebnih podatkov kandidatov na volitvah	53
3.9.9.	Razkrivanje osebnih podatkov pri pošiljanju elektronske pošte	54
3.9.10.	Prekomerno razkrivanje osebnih podatkov prosilcem za dostop do informacij javnega značaja	55
3.9.11.	Objava fotografij, na katerih so določljivi posamezniki	55
3.9.12.	Oddaljen nadzor zaposlenih	56
3.9.13.	Objava osebnih podatkov upnikov podjetja v stečaju	57
3.10.	Splošna ocena stanja varstva osebnih podatkov in priporočila	58

4. DRUGE DEJAVNOSTI INFORMACIJSKEGA POOBLAŠČENCA

4.1.	Sodelovanje pri pripravi zakonov in drugih predpisov	63
4.2.	Sodelovanje z javnostmi	64
4.3.	Mednarodno sodelovanje	67
4.3.1.	Sodelovanje na mednarodnih srečanjih	67
4.3.2.	Sodelovanje v mednarodnih delovnih telesih	68
4.3.3.	Ostale mednarodne dejavnosti	70

1 INFORMACIJSKI POOBLAŠČENEC

1.1. Nastanek Informacijskega pooblaščenca

Državni zbor Republike Slovenije je 30. 11. 2005 sprejel Zakon o Informacijskem pooblaščencu[1], s katerim je bil 31. 12. 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 ZInfP je Pooblaščenec za dostop do informacij javnega značaja nadaljeval delo kot Informacijski pooblaščenec, ki je prevzel inšpektorje in druge uslužbence 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 pravno področje varstva osebnih podatkov. Informacijski pooblaščenec je tako postal tudi državni nadzorni organ za varstvo osebnih podatkov. Delo je začel 1. 1. 2006.

S takšno ureditvijo, ki je primerljiva z ureditvijo v razvitih evropskih državah, se je poenotila praksa dveh organov, še danes pa se povečuje zavedanje pravice do zasebnosti in pravice vedeti – ti sta zaradi te ureditve v še večjem sožitju.

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

1.2. Pristojnosti Informacijskega pooblaščenca

Informacijski pooblaščenec je po 2. členu ZInfP pristojen za:

- odločanje o pritožbi zoper odločbo, s katero je organ zavrgel ali zavrnil zahtevo ali drugače kratil 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 podlagi le-tega izdanih predpisov (pritožbeni organ na področju dostopa do informacij javnega značaja);
- 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 ugodi 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 vloži zahtevo 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, tako na področju dostopa do informacij javnega značaja kot na področju varstva osebnih podatkov.

Na področju dostopa do informacij javnega značaja ima Informacijski pooblaščenec tudi pristojnosti, ki mu jih podeljuje Zakon o medijih[2] (45. člen). Po ZMed se zavrnilni odgovor organov zavezancev na vprašanje, ki ga zastavi predstavnik medija, šteje kot zavrnilna odločba. Molk organa zavezanca ob takem vprašanju je prekršek in hkrati tudi razlog za pritožbo. O pritožbi zoper zavrnilno odločbo odloča Informacijski pooblaščenec po določbah Zakona o dostopu do informacij javnega značaja[3].

[1] Uradni list RS, št. 113/2005, 51/2007 – ZUstS-A; v nadaljevanju ZInfP.
[2] Uradni list RS, št. 110/2006 – uradno prečiščeno besedilo 1, s spremembami; v nadaljevanju ZMed.
[3] Uradni list RS, št. 51/2006 – uradno prečiščeno besedilo 2, s spremembami; v nadaljevanju ZDIJZ.

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 podatkov[4].

Informacijski pooblaščenec ima pristojnosti tudi na podlagi Zakona o elektronskih komunikacijah[5], in sicer:

- izvajanje inšpekcijskega nadzora nad hrambo prometnih in lokacijskih podatkov, pridobljenih ali obdelanih v zvezi z zagotavljanjem javnih komunikacijskih omrežij ali storitev v skladu s 107.a do 107.e členom ZEKom (drugi odstavek 112. člena ZEKom);
- na področju, ki ga nadzoruje, odločanje o prekrških za kršitve ZEKom in na podlagi le-tega izdanih predpisov kot prekrškovni organ v skladu z zakonom, ki ureja prekrške (147. člen ZEKom);
- skrb za preprečevanje zlorab ter za pravilno izvajanje evropske Direktive o zasebnosti in elektronskih komunikacijah 2002/58/EC oziroma novega predloga direktive o hrambi telekomunikacijskih prometnih podatkov, ki je bila 15. 12. 2005 sprejeta v Bruslju na predlog ministrov držav članic.

Z vstopom Republike Slovenije v schengensko območje je Informacijski pooblaščenec prevzel tudi nadzor nad izvajanjem 128. člena Konvencije o izvajanju Schengenskega sporazuma[6] in je neodvisen nadzorni organ za nadzor prenosa osebnih podatkov za namene te konvencije. Na podlagi 114. člena Schengenske konvencije namreč vsaka pogodbenica imenuje nadzorni organ, ki je po nacionalni zakonodaji pristojen za izvajanje neodvisnega nadzora podatkovnih zbirk nacionalnega dela schengenskega informacijskega sistema (SIS) in za preverjanje, da obdelava in uporaba podatkov, vnesenih v SIS, ne pomenita kršenja pravic oseb, na katere se podatki nanašajo. Za nadzor nad izvajanjem tehničnega podpornega dela SIS je glede varstva osebnih podatkov pristojen skupni nadzorni organ, za nadzor nacionalne podatkovne zbirke pa nacionalni nadzorni organ vsake pogodbenice – v Sloveniji je to Informacijski pooblaščenec.

Od leta 2008 ima Informacijski pooblaščenec pristojnosti po Zakonu o pacientovih pravicah[7], Zakonu o potnih listinah[8] in Zakonu o osebni izkaznici[9].

Pristojnosti Informacijskega pooblaščenca na podlagi ZPacP so:

- odločanje o pritožbi pacientov in drugih upravičenih oseb ob kršitvi določbe, ki ureja način seznanitve z zdravstveno dokumentacijo; izvajalec zdravstvenih storitev se v tem postopku šteje za prvostopenjski organ (deseti odstavek 41. člena ZPacP);
- odločanje o pritožbi v zakonu opredeljenih oseb zoper delno ali v celoti zavrnjeno zahtevo za seznanitev z zdravstveno dokumentacijo po pacientovi smrti (peti odstavek 42. člena ZPacP);
- odločanje o pritožbi upravičenih oseb zoper delno ali v celoti zavrnjeno zahtevo za seznanitev, ki se nanaša na dolžnost varovanja informacij o zdravstvenem stanju pacienta, vendar le, če gre za informacije, ki izvirajo iz zdravstvene dokumentacije (sedmi odstavek 45. člena ZPacP).

Pristojnosti Informacijskega pooblaščenca na podlagi ZOIzk:

- izvajanje nadzora nad 3.a členom ZOIzk, ki ureja, v kakšnih primerih in na kakšen način lahko upravljavci osebnih podatkov kopirajo osebne izkaznice, ter določa način hrambe kopij;
- v primeru kršitve navedene določbe 3.a člena ZOIzk kot prekrškovni organ odloča o prekršku v skladu z 19.a členom ZOIzk.

Pristojnosti Informacijskega pooblaščenca na podlagi ZPLD:

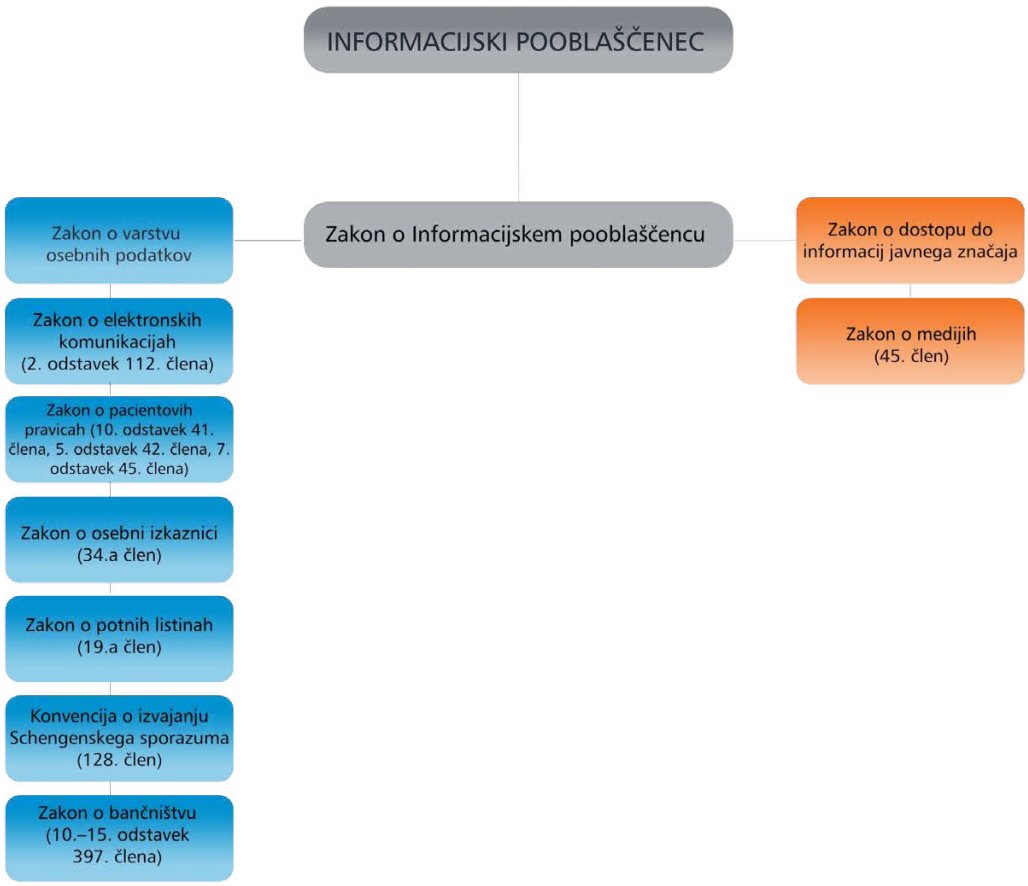
- izvajanje nadzora nad 4.a členom ZPLD, ki ureja, v kakšnih primerih in na kakšen način lahko upravljavci osebnih podatkov kopirajo potne listine, ter določa način hrambe kopij;
- v primeru kršitve navedene določbe 4.a člena ZPLD kot prekrškovni organ odloča o prekršku v skladu s 34.a členom ZPLD.

4 Uradni list RS, št. 94/2007 – uradno prečiščeno besedilo 1; v nadaljevanju ZVOP-1.
5 Uradni list RS, št. 13/2007 – uradno prečiščeno besedilo 1, s spremembami; v nadaljevanju ZEKom.
6 Uradni list Evropske unije, št. L239/2000.
7 Uradni list RS, št. 15/2008; v nadaljevanju ZPacP.
8 Uradni list RS, št. 29/2011 – uradno prečiščeno besedilo 4; v nadaljevanju ZPLD.
9 Uradni list RS, št. 35/2011; v nadaljevanju ZOIzk.

Leta 2009 je Informacijski pooblaščenec pridobil pristojnosti po Zakonu o bančništvu[10]:

- podaja soglasja upravljavcem sistema SISBON pred začetkom uporabe pravil sistema iz 1. točke trinajstega odstavka 309.a člena ZBan, ki določa, da mora upravljavec sprejeti pravila sistema, v katerih določi tehnične pogoje za dostop članov do sistema in druge ukrepe za zavarovanje osebnih podatkov (štirinajsti odstavek 390.a člena ZBan);
- izvajanje nadzora nad 309.a členom ZBan, ki ureja zbiranje in obdelovanje ter sistem izmenjave informacij o boniteti strank (sistem SISBON) in skladno s 397. členom ZBan vodi postopke o prekršku zaradi kršitve določb 309.a člena ZBan (deseti – petnajsti odstavek 397. člena ZBan).

Slika 1: Pristojnosti Informacijskega pooblaščenca.



1.3. Organiziranost Informacijskega pooblaščenca

Notranjo organizacijo in sistemizacijo delovnih mest, ki so potrebna za izvajanje nalog pri Informacijskem pooblaščencu, določata Akt o notranji organizaciji in sistematizaciji delovnih mest pri Informacijskem pooblaščencu in priloga le-tega, Sistemizacija delovnih mest pri Informacijskem pooblaščencu. Sistemizacija delovnih mest je prilagojena nalogam Informacijskega pooblaščenca in delovnim procesom, ki potekajo pri njem, ter je oblikovana tako, da zagotavlja čim učinkovitejšo izrabo človeških virov.

[10] Uradni list RS, št. 131/2006, s spremembami; v nadaljevanju ZBan.

Informacijski pooblaščenec opravlja svoje naloge v naslednjih notranjih organizacijskih enotah:

- v Kabinetu pooblaščenca;
- v Sektorju za informacije javnega značaja;
- v Sektorju za varstvo osebnih podatkov;
- v Administrativno-tehnični službi.

Slika 2: Organigram Informacijskega pooblaščenca.

Konec leta 2011 je imel Informacijski pooblaščenec 33 zaposlenih, od tega tri osebe za določen čas, ki so nadomeščale odsotne delavce. Zaposleni so bili:

- informacijska pooblaščenka,
- namestnica za področje varstva osebnih podatkov,
- namestnica za področje dostopa do informacij javnega značaja,
- namestnik za področje informacijskih tehnologij,
- generalna sekretarka,
- vodja državnih nadzornikov za varstvo osebnih podatkov,
- svetovalec (8),
- asistent svetovalca (2),
- državni nadzornik za varstvo osebnih podatkov (9),
- raziskovalec (4),
- informatik (1),
- administrativno-tehnični sodelavec (3).

Preglednica 1: Izobrazbena struktura zaposlenih pri Informacijskem pooblaščencu 31. 12. 2011.

	Srednja izobrazba	Višja strokovna šola	Univerzitetna izobrazba	Magisterij	Doktorat	*Skupaj*
Pooblaščenka			1			*1*
Namestniki			1	2		*3*
Generalna sekretarka			1			*1*
Svetovalec			7	1		*8*
Asistent svetovalca			2			*2*
Raziskovalec			4			*4*
Vodja državnih nadzornikov			1			*1*
Državni nadzornik			5	3	1	*9*
Informatik				1		*1*
Administrativno-tehnični sodelavec	2	1				*3*
Skupaj	*2*	*1*	*22*	*7*	*1*	*33*

Konec leta 2010 je imel Informacijski pooblaščenec enega zaposlenega več kot konec leta 2011. Vsi zaposleni na uradniških delovnih mestih imajo najmanj univerzitetno izobrazbo.

1.4. Finančna sredstva Informacijskega pooblaščenca

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 proračunskem letu 2011 je veljavni proračun pri Informacijskem pooblaščencu na začetku leta znašal 1.549.511,46 EUR. Od tega je bilo iz preteklega leta prenesenih 4.771,66 EUR evropskih sredstev za sodelovanje v projektu Legal Aspects of Public Sector Information (v nadaljevanju LAPSI), postavka 9586, ter 64.882,80 EUR evropskih sredstev za sodelovanje v twinning projektu, postavka 9596. Med letom je Informacijski pooblaščenec prejel 2.700,00 EUR sredstev iz prodaje dotrajanega službenega vozila, postavka 7459. V letu 2011 je bilo od evropskih sredstev za sodelovanje v LAPSI projektu, postavka 9586, porabljenih 4.329,78 EUR, ostala sredstva so se prenesla v leto 2012. V letu 2011 je bilo od evropskih sredstev za sodelovanje v twinning projektu, postavka 9596, porabljenih 47.618,59 EUR, ostala sredstva so se prenesla v leto 2012.

Za namene varčevanja v državnem proračunu je Informacijski pooblaščenec v proračun vrnil 10.000,00 EUR iz postavke 1267- plače. Informacijski pooblaščenec je iz postavke 1271– materialni stroški prerazporedil 6.464,37 EUR na postavko 1273– investicije za namen nakupa novega službenega vozila, s katerim je zamenjal staro in dotrajano vozilo, ki ga je prodal.

Veljavni proračun ob koncu leta je znašal 1.542.214,87 EUR. V ta znesek so vključena evropska sredstva za izvedbo projektov (LAPSI in twinning) ter prejeta kupnina za prodano službeno vozilo.

Proračun je bil realiziran 99,87 % - brez upoštevanja evropskih in namenskih sredstev.

Preglednici 2 in 3: Poraba proračunskih sredstev leta 2011.

PU 1215	Veljavni proračun na dan 31.12.2011	Prevzete obveznosti v letu 2011
PP 1267 Plače	1.139.957,00	1.139.495,82
PP 1271 Materialni stroški	303.534,63	302.103,22
PP 1273 Investicije in inv. vzdrževanje	26.365,37	26.365,37
Skupaj	**1.469.857,00**	**1.467.964,41**
PP 7460 Stvarno premoženje – sredstva kupnine od prodaje državnega premoženja	2.700,00	0,00
PP 7459 Stvarno premoženje – sredstva kupnine od prodaje državnega premoženja	0,00	0,00
PP 9378 Evropska sredstva za sodelovanje v projektu European Privacy	3,41	0,00
PP 9586 Pravni vidiki dostopa do IJZ	4.771,66	4.329,78
PP 9596 Twinning	64.882,80	47.618,59
Skupaj	**72.357,87**	**51.948,37**

	V EUR
Plače in drugi izdatki zaposlenim	**1.139.495,82**
Materialni stroški	**302.103,22**
Pisarniški in splošni material in storitve	38.279,92
Posebni material in storitve	998,70
Energija, voda in komunalne storitve	40.924,54
Prevozni stroški in storitve	31.630,37
Izdatki za službena potovanja	38.206,42
Tekoče vzdrževanje	5.775,76
Poslovne najemnine in zakupnine	121.301,34
Drugi operativni odhodki	24.986,17
Investicije in investicijsko vzdrževanje	**26.365,37**
Nakup prevoznih sredstev	13.902,00
Nakup opreme	12.078,89
Nakup nematerialnega premoženja	384,48
SKUPAJ	**1.467.964,41**

Leta 2011 je bilo za plače porabljenih več sredstev (in sicer 1.139.495,82 EUR) kot leta 2010 (takrat je ta znesek znašal 1.038.430,43 EUR). Za materialne stroške je bilo porabljenih manj sredstev (302.103,22 EUR) kot leta 2010 (325.614,69 EUR). Materialni stroški so bili potrebni za redno delovanje Informacijskega pooblaščenca (pisarniški material, potni stroški, čiščenje, obratovalni stroški, študentsko delo, poštne storitve, izobraževanje zaposlenih, izdelava brošur ipd.). Velik del stroškov je predstavljala najemnina za poslovne prostore.

2 DELO NA PODROČJU DOSTOPA DO INFORMACIJ JAVNEGA ZNAČAJA

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

Pravico dostopa do informacij javnega značaja je zakonodajalec zagotovil že z Ustavo Republike Slovenije[11]. Ta v drugem 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 zaščitena na ustavni ravni, se je začela uveljavljati šele 11 let po sprejetju Ustave, in sicer s sprejetjem Zakona o dostopu do informacij javnega značaja[12]. Dotlej so se posamezne določbe o javnosti informacij pojavljale le v nekaterih zakonih, celostno pa jih je uredil šele ZDIJZ. Tega je Državni zbor sprejel konec februarja 2003, veljati pa je začel 22. 3. 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 direktive Evropske skupnosti: Direktiva 2003/4/ES Evropskega parlamenta in Sveta o javnem dostopu do okoljskih informacij in razveljavitvi Direktive 90/313/EGS, ki je začela veljati 28. 1. 2003, in Direktive 2003/98/ES Evropskega parlamenta in Sveta o ponovni uporabi informacij javnega sektorja, ki je začela veljati 17. 11. 2003.

Leta 2005 je bil z novelo ZDIJZ 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 zagotovo test javnega interesa. Z novelo je bila tudi 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.

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. Zavezanci za dostop do informacij javnega značaja so vsi državni organi, organi lokalnih skupnosti, javne agencije, javni skladi in druge osebe javnega prava, nosilci javnih pooblastil in izvajalci javnih služb – zakon jih imenuje s skupno besedo organi. 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, zato pravnega interesa za pridobitev informacije ni treba izkazovati, dovolj sta radovednost ter želja po znanju in obveščenosti. Vsak prosilec ima na svojo zahtevo od organa pravico pridobiti informacijo javnega značaja, in sicer tako, da jo dobi na vpogled ali dobi njen prepis, fotokopijo ali elektronski zapis. Organ mora o zahtevi odločiti v 20 delovnih dneh, v izjemnih okoliščinah lahko rok podaljša za največ 30 delovnih dni. Če organ v zakonitem roku ne odgovori, se šteje, da je zahtevo zavrnil. Prosilec ima pravico do pritožbe zoper odločbo, s katero je

[11] Uradni list RS, št. 33/1991, 42/1997, 66/2000, 24/2003, 69/2004, 68/2006; v nadaljevanju Ustava.
[12] Uradni list RS, št. 24/2003, s spremembami; v nadaljevanju ZDIJZ.

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. Vpogled v zahtevano informacijo je brezplačen. Za posredovanje prepisa, fotokopije ali elektronskega zapisa zahtevane informacije lahko organ prosilcu zaračuna materialne stroške.

Organ lahko prosilcu dostop do zahtevane informacije zavrne, če se zahteva nanaša na eno izmed izjem, določenih v prvem odstavku 6. člena ZDIJZ (tajni podatek, poslovna skrivnost, osebni podatek, davčna tajnost, sodni postopek, upravni postopek, statistična zaupnost, dokument v izdelavi, notranje delovanje organa, varovanje naravne oziroma kulturne vrednote). Kljub navedenim izjemam iz prvega odstavka 6. člena ZDIJZ 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. Če so v dokumentu, ki ga zahteva prosilec, informacije, ki pomenijo eno od izjem iz 6. člena ZDIJZ, to ni razlog, da bi organ zavrnil dostop do celotnega dokumenta. Organ mora v skladu z 21. členom Uredbe o posredovanju in ponovni uporabi informacij javnega značaja[13] zavarovane informacije prekriti in prosilcu omogočiti vpogled v preostanek dokumenta (ali fotokopije ali elektronskega zapisa).

Če poda prosilec zahtevo za posredovanje informacij kot medij, velja, da informacije za medije po ZMed niso enake informacijam javnega značaja po določbah ZDIJZ. Po primerjavi obeh opredelitev so informacije za medije širši pojem kot informacije javnega značaja, saj med prve sodi tudi priprava odgovorov na vprašanja in informacije, ki jih organ na lastno pobudo, torej brez postavitve posebnega vprašanja, posreduje medijem. Organ mora po prejemu vprašanja medij o zavrnitvi ali delni zavrnitvi odgovora pisno obvestiti do konca naslednjega delovnega dne. V nasprotnem primeru mora organ odgovor poslati najpozneje v sedmih delovnih dneh od prejema vprašanja, pri čemer sme odgovor zavrniti le, če so zahtevane informacije izvzete iz prostega dostopa na podlagi ZDIJZ. Zavrnilni odgovor se po določbah ZMed šteje kot zavrnilna odločba. Informacijski pooblaščenec poudarja, da pritožba zoper zavrnilni odgovor ni dovoljena, kadar medij s prejetim odgovorom ni zadovoljen. Pritožba je dovoljena le, kadar iz odgovora izhaja, da so iz določenega materializiranega, že ustvarjenega dokumenta zahtevane informacije izvzete iz prostega dostopa po ZDIJZ. Mediji lahko zahtevajo posredovanje informacij za medije od vseh organov, ki jih kot zavezance določa ZDIJZ.

Leta 2011 je Informacijski pooblaščenec prejel 857 pritožb, od tega 308 zoper zavrnilne odločbe in 549 zoper molk prvostopenjskih organov.

V okviru pritožbenih postopkov zoper odločbe, s katerimi so organi zavrnili zahteve po dostopu ali ponovni uporabi informacij javnega značaja, je Informacijski pooblaščenec izdal 251 odločb (od tega 36 v zadevah, ki jih je prejel v reševanje pred letom 2011), deset prosilcev je pritožbo umaknilo, v petih primerih je Informacijski pooblaščenec pritožbo s sklepom zavrgel, v enakem številu primerov je združil zadeve, v treh primerih pa je pritožbo odstopil v odločanje pristojnemu organu.

Informacijski pooblaščenec je v pritožbenih postopkih zaradi molka organe najprej pozval, naj o zahtevi prosilca čim prej odločijo. V večini primerov so organi po pozivu Informacijskega pooblaščenca o zahtevi prosilca odločili in prosilcem zahtevane informacije javnega značaja posredovali. Z odgovorom organa je bil postopek zaradi molka zaključen, prosilci, ki so dobili zavrnilno odločbo, pa so imeli možnost pritožbe Informacijskemu pooblaščencu zaradi zavrnitve zahteve po dostopu do informacij javnega značaja. V 40 primerih je Informacijski pooblaščenec pritožbo zaradi preuranjenosti ali pomanjkljive vloge s sklepom zavrgel, v desetih primerih je prosilcem pojasnil, da za reševanje njihovih vlog ni pristojen in jih odstopil v reševanje pristojnim organom, devet posameznikov pa je pritožbe umaknilo.

[13] Uradni list RS, št. 76/2005 in 119/2007.

Pri reševanju pritožb posameznikov je včasih potreben tudi ogled brez prisotnosti stranke, ki zahteva dostop do informacije javnega značaja, t. i. ogled in camera, s pomočjo katerega Informacijski pooblaščenec ugotovi dejansko stanje dokumentov pri organu. Leta 2011 je bilo opravljenih 81 takšnih ogledov.

Leta 2011 je Informacijski pooblaščenec prejel 699 prošenj za pomoč in različnih vprašanj posameznikov glede dostopa do informacij javnega značaja, predvsem o tem, ali je določen dokument informacija javnega značaja. Informacijski pooblaščenec je vsem odgovoril v okviru svojih pristojnosti, največkrat jih je napotil na pristojno institucijo. Informacijski pooblaščenec je namreč drugostopenjski organ, ki odloča o pritožbi, in ni pristojen, da v fazi, ko mora odločati organ prve stopnje, odgovarja na konkretna vprašanja, ali je določen dokument informacija javnega značaja ali ne. V skladu z 32. členom ZDIJZ je za dajanje mnenj na področju dostopa do informacij javnega značaja pristojno Ministrstvo za javno upravo.

2.3. Število vloženih tožb na Upravnem sodišču Republike Slovenije, število sodb Upravnega in Vrhovnega sodišča Republike Slovenije

Pritožba zoper odločbo Informacijskega pooblaščenca ni dopustna, mogoče pa je sprožiti upravni spor. Leta 2011 je bilo zoper odločbe Informacijskega pooblaščenca na Upravnem sodišču vloženih 33 tožb (zoper 13,1 % izdanih odločb). Relativno majhen delež tožb, ki je že nekaj let skoraj na isti ravni, kaže na večjo uveljavitev transparentnosti in odprtosti javnega sektorja glede njegovega delovanja ter tudi na sprejemanje odločb Informacijskega pooblaščenca s strani organov in prosilcev.

Upravno sodišče je leta 2011 izdalo 23 sodb in dva sklepa v zvezi s tožbami, ki so bile vložene zoper odločbe Informacijskega pooblaščenca. V 12 primerih je tožbam ugodilo, izpodbijane odločbe odpravilo in zadeve vrnilo Informacijskemu pooblaščencu v ponovno odločanje, v devetih primerih je tožbe zavrnilo, v dveh primerih je sodišče tožilcu deloma ugodilo oziroma je izpodbijano odločbo odpravilo v delu in vrnilo Informacijskemu pooblaščencu v ponovno odločanje ter v preostalem delu zavrnilo, eno tožbo je sodišče s sklepom zavrglo, en postopek pa je s sklepom ustavilo.

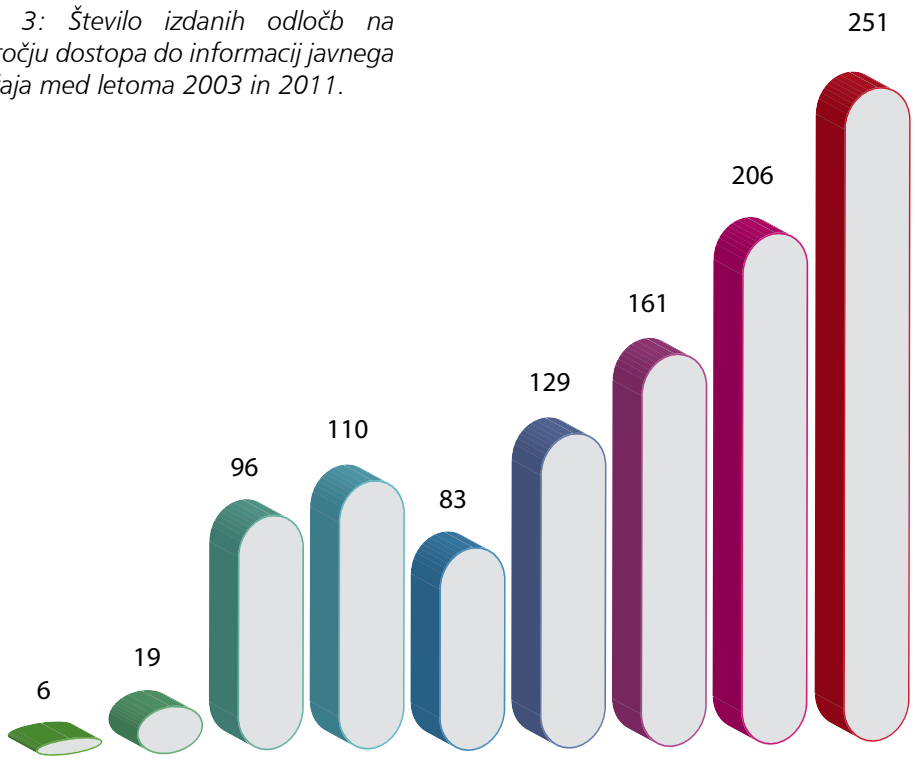
Leta 2011 ni bila zoper sodbe Upravnega sodišča na Vrhovno sodišče vložena nobena revizija.

Leta 2011 je Vrhovno sodišče odločilo v treh primerih, ko so bile zoper sodbe Upravnega sodišča vložene revizije. Sodišče je eno zahtevo za revizijo zavrglo, eno zavrnilo, v enem primeru pa je reviziji ugodilo, pri čemer je bil zavrnilni del sodbe razveljavljen in se je zadeva v tem obsegu vrnila sodišču prve stopnje v novo sojenje.

2.4. Statistika po posameznih področjih ZDIJZ

Število izdanih odločb na področju dostopa do informacij javnega značaja se je v primerjavi s preteklim letom močno povečalo. Leta 2009 je bilo izdanih 161 odločb, leta 2010 207, leta 2011 pa že 251.

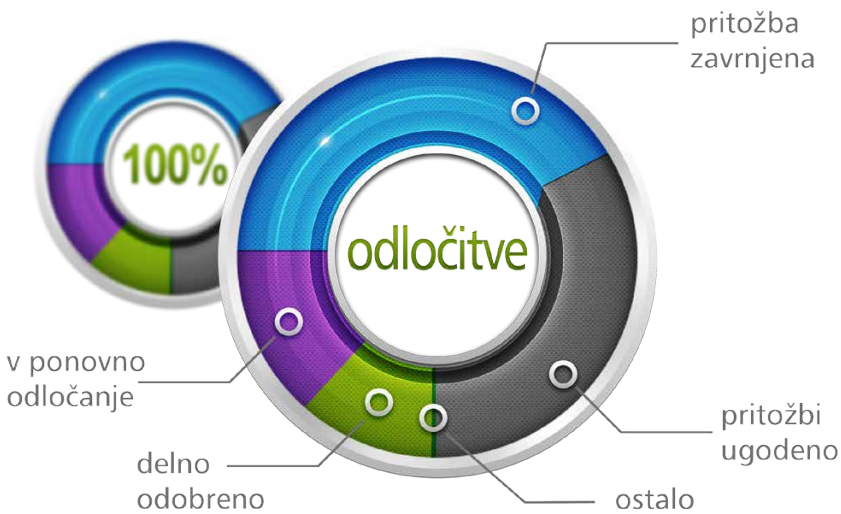
Slika 3: Število izdanih odločb na področju dostopa do informacij javnega značaja med letoma 2003 in 2011.



Informacijski pooblaščenec je v izdanih odločbah:

- v 94 primerih pritožbo zavrnil,
- v 83 primerih pritožbi ugodil in rešil zadevo v korist prosilca,
- v 42 primerih zadevo vrnil v ponovno odločanje prvostopenjskemu organu,
- v 28 primerih dostop do informacije delno odobril,
- v treh primerih pritožbo zavrgel,
- v enem primeru zaradi bistvenih kršil postopka odločil, da je odločba prvostopenjskega organa nična.

Slika 4: Odločitve Informacijskega pooblaščenca glede prejetih pritožb.

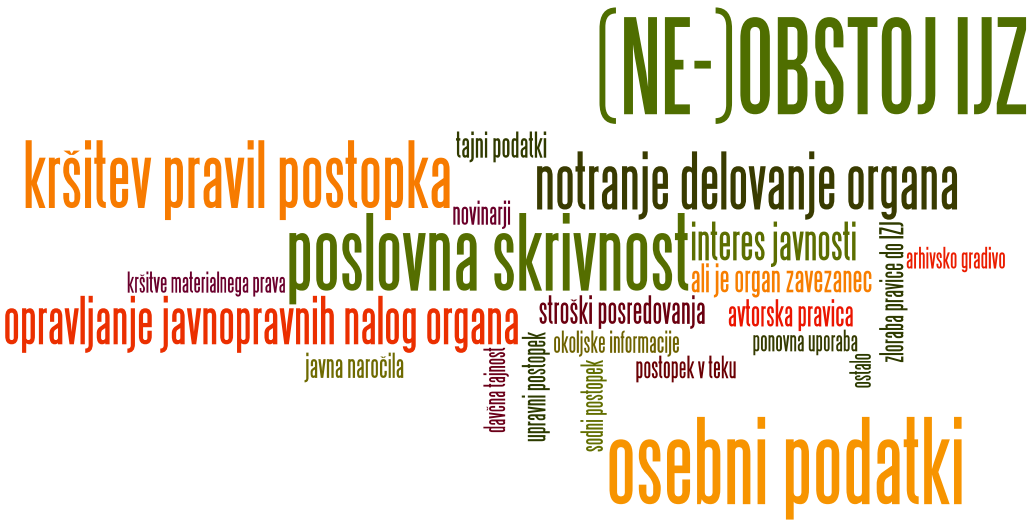


Informacijski pooblaščenec je v odločbah vsebinsko odločal oziroma presojal:

- ali zavezanec sploh ima dokument oziroma informacijo javnega značaja, ki jo je prosilec zahteval (79);
- ali zahtevani dokumenti vsebujejo osebne podatke, katerih razkritje bi pomenilo kršitev varstva osebnih podatkov v skladu z ZVOP-1 (72);
- ali prosilci zahtevajo informacije oziroma podatke, ki so v skladu z zakonom, ki ureja gospodarske družbe, opredeljeni kot poslovna skrivnost (48);
- ali gre za kršitev pravil postopka (41);
- ali so zahtevane informacije podatki iz dokumenta, ki je bil sestavljen v zvezi z notranjim delovanjem oziroma dejavnostjo organov, in bi njegovo razkritje povzročilo motnje v delovanju oziroma dejavnosti organa (14);
- ali gre za informacijo, ki je povezana z opravljanjem javnopravnih nalog organa (14);
- ali zahtevani dokument izpolnjuje pogoje za obstoj informacije javnega značaja v skladu s prvim odstavkom 4. člena ZDIJZ (12);
- ali je interes javnosti glede razkritja močnejši od javnega interesa ali interesa drugih oseb za omejitev dostopa do zahtevane informacije (11);
- ali je organ, na katerega je bila zahteva po dostopu do informacije javnega značaja naslovljena, sploh zavezanec v skladu s prvim odstavkom 1. člena ZDIJZ (11);
- ali je organ pravilno zaračunal stroške posredovanja informacij javnega značaja (10);
- ali je zahtevana informacija zavarovana skladno z zakonom, ki ureja avtorsko pravico – v takih primerih se prosilcu omogoči seznanitev z informacijo tako, da se mu jo da na vpogled (10);
- ali so zahtevane informacije podatki, ki so na podlagi zakona, ki ureja tajne podatke, opredeljeni kot tajni (9);
- izdaja odločbe v postopku, ko je prosilec zahteval dokument iz postopka javnega naročanja (7);
- izdaja odločbe v postopku, ko je bil prosilec novinar ali medij (6);
- ali gre za zlorabo pravice po ZDIJZ (5);
- ali so zahtevane informacije podatki, ki so bili pridobljeni ali sestavljeni zaradi upravnega postopka, in bi njihovo razkritje škodovalo izvedbi le-tega (4);
- 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 vsebine dokumentov (4);
- ali gre za okoljske podatke (4);
- ali so zahtevane informacije podatki, ki so bili pridobljeni ali sestavljeni zaradi pravdnega, nepravdnega ali drugega sodnega postopka, in bi njihovo razkritje škodovalo izvedbi le-tega (3);
- ali gre za ponovno uporabo informacije javnega značaja (3);
- ali gre za pravico po ZDIJZ (3);
- ali mora organ umakniti stopnjo tajnosti zahtevanega dokumenta (3);
- ali gre za arhivsko gradivo (2);
- ali je organ kršil materialno pravo (2);
- ali so zahtevane informacije podatki, katerih razkritje bi pomenilo kršitev zaupnosti davčnega postopka ali davčne tajnosti, skladno z zakonom, ki ureja davčni postopek (1);
- proaktivna objava informacij (1);
- ali gre za podatke, ki predstavljajo izjemo v skladu z zakonom, ki ureja državno statistiko (1);
- razno (3).

Informacijski pooblaščenec je leta 2011 izdal devet odločb v zadevah iz preteklih let, v katerih so bile vložene tožbe na Upravno sodišče, ki je odločilo, da mora Informacijski pooblaščenec o zadevah ponovno odločati.

Slika 5: 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, o katerih je Informacijski pooblaščenec odločil z odločbo, so zadevale naslednje skupine zavezancev:

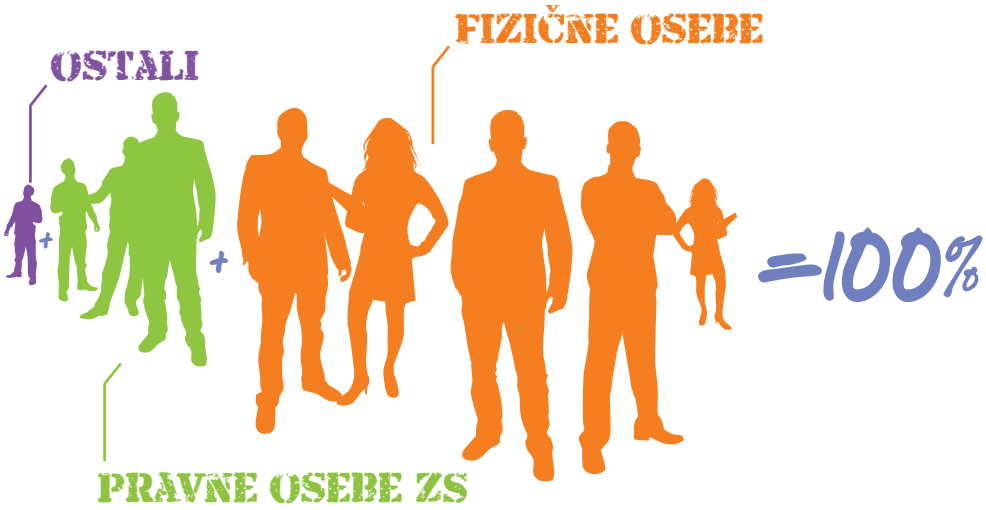
- ministrstva, organe v sestavi in druge državne organe (94),
- javne sklade, zavode, agencije, izvajalce javnih služb in nosilce javnih pooblastil (74),
- upravne enote, občine, krajevne skupnosti (48),
- sodišča, vrhovno državno tožilstvo, državno pravobranilstvo (29).

Šest pritožb se je nanašalo na pravne osebe zasebnega sektorja, za katere pa je bilo ugotovljeno, da niso zavezanci po ZDIJZ.

Slika 6: Pritožbe prosilcev glede na zavezanca.

V 173 primerih so bili prosilci fizične osebe, v 55 primerih so se pritožile pravne osebe zasebnega sektorja, od tega v 13 primerih nevladne organizacije, različna združenja in društva. Novinarji so se pritožili 16-krat, pravne osebe javnega sektorja pa sedemkrat.

Slika 7: Struktura prosilcev za dostop do informacij javnega značaja.



2.5. Storjeni prekrški po ZDIJZ, ZInfP in ZMed

Leta 2011 so bili uvedeni trije postopki o prekršku zaradi kršitve tretjega odstavka 10. člena ZInfP in storitve prekrška po drugem odstavku 15. člena ZInfP, ker organ, ki zoper odločbo Informacijskega pooblaščenca ni sprožil upravnega spora, prosilcu skladno z odločbo Informacijskega pooblaščenca ni poslal zahtevanih dokumentov. En postopek je bil zaključen z izrekom sankcije kršitelju. Informacijski pooblaščenec ni zaznal kršitev 23. člena ZDIJZ in 45. člena ZMed.

2.6. Predstavitev najodmevnejših in precedenčnih primerov po področjih

V nadaljevanju je predstavljenih 13 najzahtevnejših in najzanimivejših odločb iz leta 2011, ki so razvrščene po področjih.

2.6.1. Osebni podatek, notranje delovanje organa, avtorsko delo

Z odločbo št. 090-159/2010/15 z dne 24. 1. 2011 je Informacijski pooblaščenec odpravil odločbo Javne agencije za raziskovalno dejavnost Republike Slovenije (v nadaljevanju organ ali ARRS), ki je delno zavrnila zahtevo prosilca po vpogledu in fotokopiranju vlog in ocenjevalnih listov za projekte, ki so jih v letu 2009 podali našteti raziskovalci, doktorji znanosti, ter vpogled v vse zapisnike sej Znanstvenega sveta in Upravnega odbora ter vseh drugih stalnih in občasnih teles ARRS (zlasti panelnih razprav), ki zadevajo odločanje o vlogah za omenjene projekte.

Informacijski pooblaščenec je pri presoji dopustnosti razkritja imena in priimka recenzenta ugotovil, da ne gre za varovane osebne podatke, saj so recenzenti na zahtevanih dokumentih

navedeni v okviru svoje funkcije, ki jo opravljajo. Recenzent namreč na podlagi avtorske pogodbe opravlja neke vrste javno funkcijo, saj za organ pripravi strokovno oceno, ki je potrebna pri odločitvi o sofinanciranju projekta in je za svoje delo tudi plačan iz javnih sredstev.

Organ pa je izpostavil, da bi razkritje področja dela recenzenta vplivalo na samo delo in pristojnosti organa, kar bi posledično lahko tudi blokiralo delo organa. Informacijski pooblaščenec je zato opravil preizkus, ali je podana izjema iz 11. točke prvega odstavka 6. člena ZDIJZ, ki določa, da se prosilcu zavrne dostop do zahtevane informacije, če se zahteva nanaša na podatek iz dokumenta, ki je bil sestavljen v zvezi z notranjim delovanjem oziroma dejavnostjo organa in bi njegovo razkritje povzročilo motnje pri delovanju oziroma dejavnosti organa. Informacijski pooblaščenec je ugotovil, da podatek o področju delovanja recenzenta ne ustreza definiciji izjeme »notranjega delovanja organa«, ki je namenjena temu, da se varuje »notranje razmišljanje organa«, ne pa zunanjih subjektov, ki so vključeni v postopek javnega razpisa, zaradi svoje strokovnosti na določenem področju. Ta pristojnost (odločanje v postopkih javnega razpisa) predstavlja tipičen primer »zunanjega delovanja«, kot delovanja javnega sektorja nasproti zunanjim prijaviteljem projektov. Poleg tega je vsebina zahtevanih dokumentov vplivala (učinkovala) na dejanja in odločitve organa, ki spadajo v njegovo pristojnost. Takšna narava dokumenta zelo očitno nakazuje na prepričanje, da ne gre za dokument oziroma informacijo v zvezi z notranjim delovanjem. Dokument pa ne bi prestal niti t.i. škodnega testa, saj razkritje takšnega dokumenta oziroma informacije ne bi povzročilo motnje pri delovanju oziroma dejavnosti organa. Oseba, ki je imenovana za recenzenta, mora izpolnjevati določene pogoje, kriterije znanstvene in strokovne odličnosti, vendar če recenzent ob morebitnih zunanjih pritiskih ne zmore podati objektivnega, profesionalnega in nepristranskega mnenja oziroma ocene, potem je vprašljiva primernost takšne osebe. Zato Informacijski pooblaščenec ne more slediti navedbam organa, da bi z razkritjem imen in priimkov recenzentov organu nastala kakšna škoda. Navsezadnje so takšnim pritiskom izpostavljeni tudi mnogi drugi javni uslužbenci oziroma funkcionarji (npr. sodniki, državni tožilci, cariniki, policisti, ipd.), pa se, kljub njihovi javni izpostavljenosti, od njih (upravičeno) pričakuje strokovno, neodvisno in nepristransko opravljanje njihovih nalog.

Informacijski pooblaščenec je ugotovil tudi, da je organ neupravičeno izbrisal imena in priimke prisotnih in odsotnih članov Upravnega odbora. Vendar člani nedvomno opravljajo javno funkcijo (imenovani so s strani ustanovitelja, torej Republike Slovenije), zato njihova imena in priimki ne predstavljajo varovanih osebnih podatkov. Organ je nepravilno prekril tudi osebne podatke članov Upravnega odbora v sklepu o izboru prijav za (so)financiranje, in sicer je organ izločil informacijo, ki je v povezavi s konfliktom interesov in glasovanjem. V izvrševanje funkcije člana Upravnega odbora nedvomno sodi glasovanje ali izločitev od glasovanja, zato ta podatek po presoji Informacijskega pooblaščenca ne more predstavljati varovanega osebnega podatka.

Organ pa je pravilno izbrisal ime in priimek prijavitelja projekta, saj ime in priimek, skupaj z ostalimi podatki, predstavljata varovane osebne podatke, ker ni nobene pravne podlage, na podlagi katere bi bili lahko osebni podatki te osebe javno dostopni. Prav tako so varovani osebni podatki vodje raziskovalnega projekta, ki ni bil izbran v sofinanciranje, kontaktne osebe, skupaj z e-naslovom, imena in priimki recenzentov, za katera prijavitelj ne želi, da ocenjujeta njegovo prijavo, ipd., saj ne gre za podatek o porabi javnih sredstev ali o izvajanju javne funkcije.

Na koncu se je Informacijski pooblaščenec ukvarjal še z vprašanjem, ali vloge raziskovalnih projektov predstavljajo avtorsko delo. Po preučitvi vsebine posameznih vlog raziskovalnih projektov je Informacijski pooblaščenec ugotovil, da vloge nedvomno izpolnjujejo predpostavke za avtorsko delo (stvaritev, področje ustvarjalnosti, izraznost, individualnost, duhovnost). Neizbrane vloge raziskovalnih projektov torej predstavljajo avtorska dela, zaradi česar lahko organ prosilcu v tem delu omogoči seznanitev z informacijami le tako, da mu jih da na vpogled.

2.6.2. Tajni podatki, zahteva za umik stopnje tajnosti

Informacijski pooblaščenec je z odločbo št. 090-13/2011/2 z dne 10. 2. 2011 ugodil pritožbi prosilca in odpravil izpodbijano odločbo Ministrstva za obrambo Republike Slovenije (v nadaljevanju organ). Informacijski pooblaščenec je odredil, da mora organ zahtevo prosilca za umik stopnje tajnosti, skupaj s predlogom odločitve predstojnika organa, poslati v odločanje Vladi Republike Slovenije.

Prosilec je zahteval fotokopije ali digitalno preslikavo dokumentov v zvezi z nakupom oklepnikov Patria, ki so bili označeni s stopnjama INTERNO in ZAUPNO in zaradi česar je sodišče v sojenju nekdanjemu ministru za obrambo Karlu Erjavcu in nekdanjemu načelniku generalštaba Slovenske vojske generalpolkovniku Albinu Gutmanu izločilo javnost iz glavne obravnave. Prosilec je pozval organ, naj umakne oznako tajnosti z navedenih dokumentov in mu omogoči vpogled vanje, saj bo z umikom tajnosti z dokumentov javnosti omogočeno spremljanje sojenja v zadevi Patria. Prosilec se je skliceval tudi na to, da oznaka tajnosti zahtevanih dokumentov ni več smiselna, saj ima zaradi objave na spletni strani dostop do bistvenih delov celotna slovenska in tudi svetovna javnost. Po mnenju prosilca interes javnosti v tem primeru pretehta nad interesom varovanja tajnih podatkov, poleg tega pa gre za podatke o porabi javnih sredstev in za podatke, povezane z opravljanjem javne funkcije ali delovnega razmerja javnega uslužbenca.

Organ se je pri zavrnitvi zahteve skliceval na izjemo tajnih podatkov ter izjemo varstva izvedbe kazenskega pregona.

Informacijski pooblaščenec je ugotovil, da se organ do zahteve prosilca za umik stopnje tajnosti iz zahtevanih dokumentov sploh ni opredelil, prav tako pa njegove zahteve ni odstopil v obravnavo Vladi Republike Slovenije, kot to določa tretji odstavek 21. člena ZDIJZ. O zahtevi prosilca za umik stopnje tajnosti bi morala na predlog predstojnika organa namreč odločiti Vlada . Organ bi moral zato zahtevo prosilca odstopiti v odločanje Vladi, in sicer skupaj s predlogom predstojnika v roku 15 delovnih dni od prejema zahteve. Prav tako bi morala Vlada (in ne organ sam) odločiti o prevladujočem javnem interesu za razkritje zahtevanih dokumentov, na katerega se je skliceval prosilec, kot to določa drugi odstavek 21. člena ZDIJZ.

Odločbo je tako izdal stvarno nepristojen organ, saj zadeve ni odstopil Vladi, zato je Informacijski pooblaščenec zaradi bistvene kršitve pravil upravnega postopka po uradni dolžnosti odpravil odločbo in poslal zadevo v reševanje pristojnemu organu, Vladi Republike Slovenije.

2.6.3. Ali je organ zavezanec, ali gre za informacijo javnega značaja

Informacijski pooblaščenec je z odločbo št. 090-31/2011/2 z dne 25. 2. 2011 zavrnil pritožbo prosilke, ki je od družbe Pošta Slovenija, d.o.o. (v nadaljevanju organ) zahtevala fotokopijo zapisnika določene seje nadzornega sveta Pošte Slovenija, d.o.o. Fotokopija zapisnika se nanaša na poslovanje organa s podjetjem, ki je izdajalo brezplačni tednik Slovenski tednik, Pošta Slovenije, d.o.o., pa ga je distribuirala.

Glavno vprašanje v konkretnem primeru je bilo, ali zahtevane informacije (zapisniki sej nadzornega sveta organa) izvirajo iz opravljanja javnopravnih nalog organa. Informacijski pooblaščenec je zapisal, da je organ nedvomno zavezanec za posredovanje informacij javnega značaja na področju izvajanja javnega pooblastila. Vendar je za vse izvajalce javnih pooblastil značilno, da so lahko zavezani za dostop do informacij javnega značaja samo v tistem delu svoje dejavnosti, ki predstavlja izvajanje javnopravnih nalog, ne pa tudi z ostalimi dejavnostmi, ki nimajo povezave z izvajanjem teh nalog. V konkretnem primeru je bilo tako ugotovljeno, da prenos nenaslovljenih in delno naslovljenih pošiljk (torej tudi raznos nenaslovljenega brezplačnika) ni poštna storitev v smislu Zakona o poštnih

storitvah[14]. To pomeni, da lahko distribucijo nenaslovljene oziroma delno naslovljene pošte opravlja vsak subjekt, ki v skladu s splošnimi pogoji prosto nastopa na trgu. Pogodba, ki sta jo sklenila organ in podjetje, ki je izdajalo brezplačni tednik Slovenski tednik, tako ne spada v okvir nalog, ki jih organ opravlja v okviru podeljenega javnega pooblastila za izvajanje univerzalne poštne storitve, ampak v tržni del izvajanja dejavnosti organa.

Glede na navedeno je Informacijski pooblaščenec torej ugotovil, da navedena pogodba ne predstavlja informacije javnega značaja, posledično pa tudi ne tisti del zapisnika, ki se vsebinsko nanaša na to pogodbo. Vsebina zapisnika se namreč ne nanaša na vprašanje izvajanja javnopravnih nalog organa (to je izvajanje univerzalne poštne storitve), ampak gre za tržni del njegovega delovanja.

Informacijski pooblaščenec v obravnavanem primeru ni mogel slediti niti argumentu prosilke, da je zahtevano informacijo treba razkriti, ker je Pošta Slovenije, d.o.o., gospodarska družba v 100% državni lasti. Domet ZDIJZ se v skladu s 1. členom namreč nanaša samo na državne organe, organe lokalnih skupnosti, javne agencije, javne sklade in druge osebe javnega prava, nosilce javnih pooblastil in izvajalce javnih služb. Tudi če so družbe v 100% lasti države, niso zavezane za posredovanje informacij v skladu ZDIJZ, razen v kolikor so izvajalci javnih služb oziroma nosilci javnih pooblastil, pri čemer se v tem primeru njihova obveznost postopati po ZDIJZ razteza samo na ta del njihove dejavnosti (izvajanje javnopravnih nalog), ne pa na tržni del njihovega poslovanja.

2.6.4. Avtorsko delo, osebni podatek

Informacijski pooblaščenec je z odločbo št. 090-189/2010/6 z dne 2. 3. 2011 delno odpravil odločbo Ministrstva za promet, Direkcije za ceste (v nadaljevanju organ) in ji naložil, da prosilcu posreduje kopije soglasja, ki ga je investitor pridobil za rekonstrukcijo ceste ter kopije nekaterih vlog investitorja v zvezi z izdajo soglasja.

Prosilec je zahteval kopije dokumentacije, ki jo je določen posameznik vložil pri organu v zvezi s posegom v prostor, ki ga je nameraval opraviti, in pri katerem je bil zaustavljen s strani hrvaških policistov. Prav tako je prosilec zahteval dokumente, ki jih je ta posameznik "pokazal pred TV kamerami POP TV, 10. junija 2010" in s katerimi je ta utemeljeval nameravani poseg odstranjevanja robnikov in izvedbo priključka ceste, pri čemer je bil zaustavljen s strani hrvaških policistov.

Organ se je v izpodbijani odločbi med drugim skliceval na varstvo osebnih podatkov in navedel, da če razkrije zahtevano dokumentacijo, ki se nanaša na posameznika, ne more varovati osebnih podatkov svojih strank, saj že iz zahteve jasno izhaja, na katero osebo se dokumentacija nanaša. Organ je navedel, da uporaba instituta delnega dostopa ni možna, saj bi tudi s prikritjem osebnih podatkov posameznika, posameznika bilo možno prepoznati, saj je celotni slovenski javnost znano, na katero osebo se nanašajo dogodki na mejnem prehodu ob Dragonji in kdo večkrat pride v konflikt s hrvaškimi mejnimi policisti.

Informacijski pooblaščenec pa je ugotovil, da je iz odobrenih dokumentov mogoče izločiti identifikacijske osebne podatke tako, da preostali podatki nimajo več narave osebnih podatkov (t.j. podatkov, ki se nanašajo na točno določenega vložnika oziroma investitorja). Zato je mogoče in treba prosilcu zagotoviti delni dostop v skladu s 7. členom ZDIJZ in vseeno ohraniti »zaupnost« dokumentov. To zaupnost je treba razumeti v smislu, da se z delnim dostopom ohrani varstvo osebnih podatkov posameznika. Dejstvo, da prosilec to osebo pozna, ne vpliva na stališče o nedopustnosti razkritja, saj se razkritje presoja z vidika javnosti (kriterij univerzalnega prosilca) in ne zgolj z vidika konkretnega prosilca. Z delnim dostopom organ javnosti ne razkrije varovanih osebnih podatkov vložnika oziroma investitorja. Učinek odločitve o dostopnosti dokumentov, ki vsebuje osebne podatke, mora biti enak erga omnes, t.j. enak nasproti kateremu koli prosilcu. Tudi kateremu koli drugemu

[14] Uradni list RS, št. 51/2009.

prosilcu, ki vložnika oziroma investitorja ne pozna, bi bili dokumenti razkriti na enak način kot konkretnemu prosilcu.

Nazadnje je moral Informacijski pooblaščenec presoditi tudi obstoj varovanih avtorskih del, in sicer glede projektne dokumentacije, vodilnih map ipd. ter ugotovil, da so glede nekaterih dokumentov izpolnjeni vsi opredelilni elementi avtorskega dela. V podporo navedenemu je služil tudi prvi odstavek 5. člena Zakona o avtorski in sorodnih pravicah[15], ki med avtorska dela eksemplifikativno šteje tudi predstavitve znanstvene, izobraževalne ali tehnične narave (tehnične risbe, načrti, skice, tabele, izvedenska mnenja in druga dela enake narave). Zaradi navedenega je bilo mogoče prosilcu v skladu z drugim odstavkom 25. člena ZDIJZ odobriti le vpogled v določen del zahtevane dokumentacije.

2.6.5. Dokument v izdelavi, poslovna skrivnost, avtorsko delo, okoljski podatki

Informacijski pooblaščenec je v združenem pritožbenem postopku dveh prosilcev z odločbo št. 090-212/2010/18 z dne 11. 3. 2011 organu (Agencija za radioaktivne odpadke) naložil, da prosilcema posreduje fotokopijo zahtevanega dokumenta s prekritimi določenimi podatki, ki predstavljajo izjemo od prostega dostopa.

Prosilca sta zahtevala fotokopijo dokumenta Program razgradnje Nuklearne elektrarne Krško in ravnanja z nizko in srednje radioaktivnimi odpadki in izrabljenim jedrskim gorivom z letnico 2010, skupaj s prilogami, a je organ njuno zahtevo v celoti zavrnil.

Informacijski pooblaščenec je ugotovil, da sklep organa o določitvi zahtevanega dokumenta za poslovno skrivnost ni bil sprejet skladno z Zakonom o gospodarskih družbah[16], saj je bil sprejet za nazaj, torej po tem, ko sta prosilca zahtevala dokumente. Vendar pa so bili določeni deli zahtevanega dokumenta pravilno označeni kot poslovna skrivnost v pogodbi med NEK, d.o.o. in Siempelkamp NIS (stranskim udeležencem). Glede dostopa do tega dela dokumenta je Informacijski pooblaščenec odločil, da ga mora organ prekriti z uporabo instituta delnega dostopa. V preostalem, neoznačenem delu dokumenta je Informacijski pooblaščenec ugotovil, da ni podana izjema poslovne skrivnosti po objektivnem kriteriju, predvsem zato, ker je bil dokument posredovan izven kroga poslovanja organa brez omejitev oziroma sprejetih ukrepov za zavarovanje zaupnosti informacij v dokumentu. Informacijski pooblaščenec je ugotovil tudi, da so predmet poslovne skrivnosti lahko samo podatki, ki pomenijo konkurenčno prednost podjetja, organ pa pri izdelavi zahtevanega dokumenta sploh ne nastopa na trgu, ampak izvaja obvezno državnogospodarsko javno službo.

Informacijski pooblaščenec je v nasprotju s sklicevanjem organa ugotovil, da ni podana izjema dokumenta v postopku izdelave iz 9. točke prvega odstavka 6. člena ZDIJZ, saj ni izpolnjen noben od treh zahtevanih pogojev za obstoj omenjene izjeme. Skladno z Uredbo o posredovanju in ponovni uporabi informacij javnega značaja[17] je zahtevani dokument že zaključen in tako ne šteje za dokument v postopku izdelave. V konkretnem primeru gre za vsebinsko zaokroženo besedilo, ki ga je izdelala in s podpisi tudi formalno zaključila Projektna skupina, skupaj z direktorjema APO in organa. Tudi če bi šlo za dokument v izdelavi, organ ni izkazal nastanka škode v primeru razkritja dokumenta javnosti. Zgolj dejstvo, da bi razkritje in interpretacija variantnih podatkov dokumenta povzročilo napačno razumevanje in otežilo postopek usklajevanja in sprejemanja s strani obeh vlad, ne zadošča za obstoj elementa napačnega razumevanja vsebine dokumenta.

V konkretni zadevi pa je bilo pomembno tudi vprašanje, ali je podatke v zahtevanem dokumentu mogoče opredeliti kot podatke glede emisij v okolje, odpadkov, nevarnih snovi v obratu ali podatke iz varnostnega poročila in druge podatke, za katere tako določa zakon,

[15] Uradni list RS, št. 16/2007 – uradno prečiščeno besedilo 3, s spremembami.
[16] Uradni list RS, št. 65/2009 – uradno prečiščeno besedilo 3, s spremembami; v nadaljevanju ZGD-1.
[17] Uradni list RS, št. 76/2005, 119/2007; v nadaljevanju Uredba.

ki ureja varstvo okolja. Dostop do takšnih podatkov se namreč na podlagi 2. alineje tretjega odstavka 6. člena ZDIJZ dovoli ne glede na morebitne izjeme od prostega dostopa do informacij javnega značaja (v konkretnem primeru ne glede na izjemo poslovne skrivnosti, ki je podana glede določenega dela dokumenta). Informacijski pooblaščenec je ugotovil, da so podatki o nizko in srednje radioaktivnih odpadkih ter o izrabljenem jedrskem gorivu okoljski podatki; opredeljeni so celo kot radioaktivni odpadki. Določeni podatki iz zahtevanega dokumenta pa niso v neposredni zvezi s podatki glede emisij v okolje, odpadkov, nevarnih snovi v obratu v zvezi z razgradnjo NEK (npr. podroben tloris NEK, nekateri osebni podatki udeleženih v pripravi programa razgradnje NEK), zato se izjeme varstva poslovnih skrivnosti in osebnih podatkov lahko nanašajo na določen del dokumenta.

Informacijski pooblaščenec je na koncu ugotovil še, da zahtevani dokument ne predstavlja varovanega avtorskega dela, saj gre za uradno besedilo iz upravnega področja (izključitev iz avtorskopravnega varstva), zaradi česar mora organ prosilcu posredovati fotokopijo tega dokumenta.

Z obravnavano odločbo je Informacijski pooblaščenec torej organu naložil posredovanje zahtevanega dokumenta, vendar mora organ zaradi varstva poslovne skrivnosti določen del dokumenta prekriti. Izjema poslovne skrivnosti je podana le v delu dokumenta, ki je bil pravilno označen po subjektivnem kriteriju in ki ne predstavlja podatkov glede emisij v okolje, odpadkov, nevarnih snovi v obratu ali podatke iz varnostnega poročila in druge podatke, za katere tako določa zakon, ki ureja varstvo okolja.

2.6.6. Osebni podatek

Informacijski pooblaščenec je z odločbo št. 090-41/2011/5 z dne 15. 3. 2011 ugodil pritožbi prosilca in naložil organu (Zavod za pokojninsko in invalidsko zavarovanje), da prosilcu posreduje dokument o prejemnikih izjemnih pokojnin v letu 2009.

Prosilec je namreč od organa zahteval kateri koli dokument, ki vsebuje listo ali spisek vseh prejemnikov osebnih in družinskih pokojnin, ki so v letu 2009 prejemali izjemno pokojnino (pri tem pa je prosilec opozoril, da ne misli samo na kulturnike in športnike, temveč vse prejemnike).

Organ je zavrnil posredovanje liste ali spiska vseh prejemnikov osebnih in družinskih pokojnin, saj je podatek, ali določena oseba prejema pokojnino, varovan osebni podatek. Organ je presodil, da je kljub dejstvu, da se zahtevana informacija nanaša na podatke o porabi javnih sredstev, varstvo osebnih podatkov prejemnikov izjemnih pokojnin v tem primeru pomembnejša vrednota in bi se z razkritjem teh podatkov posameznikov povzročila resna škoda. Organ je menil, da ni izkazan javni interes za razkritje teh podatkov.

Informacijski pooblaščenec je ugotovil, da v konkretnem primeru ne gre za varovane osebne podatke posameznikov, saj podlago za njihovo razkritje predstavlja zakon, in sicer Zakon o izjemnem priznanju in odmeri starostne pokojnine osebam, ki imajo posebne zasluge[18]. Navedeni zakon v 3. členu določa, da se odločba o izjemnem priznanju in odmeri starostne pokojnine objavi v Uradnem listu. Informacijski pooblaščenec je z vpogledom na spletno stran: http://www.uradni-list.si/ ugotovil, da je dejansko objavljenih več sklepov Vlade Republike Slovenije o izjemnem priznanju in odmeri družinskih in starostnih pokojnin, ki vsebujejo tako podatke o prejemnikih izjemnih pokojnin, kot tudi podatke o višini tako odmerjenih pokojnin. Poleg navedene pravne podlage pa podlago za posredovanje o prejemnikih izjemnih pokojnin predstavlja tudi tretji odstavek 6. člena ZDIJZ, saj gre za podatke v zvezi s porabo javnih sredstev.

Sredstva za izplačevanje izjemnih pokojnin zagotavlja Republika Slovenija iz državnega proračuna. Zakon o pokojninskem in invalidskem zavarovanju[19] namreč določa, da se

[18] Uradni list RS, št. 14/1990.
[19] Uradni list RS, št. 109/2006 - uradno prečiščeno besedilo 4, s spremembami.

sredstva za pokrivanje obveznosti obveznega zavarovanja, ki nastanejo zaradi priznanja in odmere pravic iz pokojninskega in invalidskega zavarovanja pod posebnimi pogoji, med drugimi tudi za uživalce izjemnih pokojnin, zagotavlja iz državnega proračuna. Poračunavanje finančnih obveznosti med Republiko Slovenijo in Zavodom za pokojninsko in invalidsko zavarovanje ureja poseben zakon (Zakon o poračunavanju finančnih obveznosti Republike Slovenije iz pokojninskega in invalidskega zavarovanja[20]), ki določa, da je država dolžna v celoti ali delno povrniti izdatke tudi za uživalce izjemnih pokojnin. Iz navedenega jasno izhaja, da se sredstva za izjemne pokojnine, ki presegajo pokojnine, odmerjene po splošnih predpisih, zagotavljajo iz državnega proračuna, kar pomeni, da zahtevani podatki nedvomno predstavljajo podatke o porabi javnih sredstev.

V odločbi št. 090-91/2011/3 z dne 20. 5. 2011 je Informacijski pooblaščenec ugodil pritožbi prosilke, ki je od Občine Piran (v nadaljevanju organ) zahtevala fotokopijo zapisnika natečajne komisije za zasedbo prostega uradniškega delovnega mesta »direktor občinske uprave« na način, da bo varovana identiteta kandidatov.

Organ je zahtevo prosilke zavrnil z navedbo, da je bil natečaj neuspešen in ni bil izbran noben kandidat, zato zapisnik natečajne komisije vsebuje izključno podatke o neizbranih kandidatih, ki predstavljajo varovane osebne podatke. Ker kandidati niso bili izbrani, niso sklenili delovnega razmerja z organom in niso vstopili v nobeno drugo javnopravno razmerje v smislu izvajanja javne funkcije, tudi do porabe javnih sredstev ni prišlo, zato ne pride v poštev t.i. izjema od izjeme, ki dopušča razkritje osebnih podatkov, kadar gre za porabo javnih sredstev.

Informacijski pooblaščenec je po preučitvi zahtevanega dokumenta ugotovil, da bi moral organ uporabiti institut delnega dostopa. Prosilka namreč sploh ni zahtevala podatkov o neizbranih kandidatih, saj je v zahtevi izrecno zapisala, naj ji organ posreduje zahtevani dokument na način, da bo zadoščeno varovanju identitete kandidatov. Posredovanje osebnih podatkov neizbranih kandidatov torej sploh ni bil predmet zahteve in pritožbe prosilke. Informacijski pooblaščenec tako ni mogel slediti obrazložitvi organa, da je zahtevo prosilke treba zavrniti, ker zahtevani dokument vsebuje podatke o prijavljenih kandidatih.

V zvezi z osebnimi podatki članov natečajne komisije pa je Informacijski pooblaščenec ugotovil, da v tem delu ne gre za varovane osebne podatke, saj sta dve članici komisije zaposleni pri organu in sta javni uslužbenki, tretja članica pa je bila imenovana s sklepom župana in je tako v imenu in za račun organa opravljala javno funkcijo. Tretji odstavek 6. člena ZDIJZ namreč določa, da se ne glede na izjeme od prostega dostopa (npr. izjeme varstva osebnih podatkov) dovoli dostop do podatkov, povezanih z opravljanjem javne funkcije ali delovnega razmerja javnega uslužbenca.

Organ bi moral z uporabo instituta delnega dostopa prekriti imena in priimke, podatke o zaposlitvi in o delodajalcih neizbranih prijavljenih kandidatov, v preostalem delu pa prosilki posredovati fotokopijo zapisnika natečajne komisije.

Z odločbo št. 090-137/2011/5 z dne 26. 9. 2011 je Informacijski pooblaščenec zavrnil pritožbo prosilca zoper odločbo prvostopenjskega organa, Ministrstva za pravosodje. Prosilec je namreč zahteval informacije v zvezi z opravo strokovnega izpita (pravniškega državnega izpita, PDI) za navedene sodnike okrajnega in okrožnega sodišča v Kranju. Poleg tega je prosilec zahteval tudi izdajo overjenih (verodostojnih) kopij rokopisov pisnih izpitov za vsakega navedenega sodnika. V določenem delu pa je organ prosilcu ugodil in mu posredoval fotokopije potrdil o opravljenem PDI, prekril pa je podatke o datumu in kraju rojstva.

Prosilec se je pritožil tudi glede ugodilnega dela, saj je zahteval vpogled in ne posredovanja fotokopij, kar je storil organ. Vendar je Informacijski pooblaščenec ugotovil, da mu je organ s posredovanjem fotokopij omogočil širše izvrševanje njegove pravice, pri čemer prosilcu

[20] Uradni list RS, št. 81/2000, s spremembami.

ni zaračunal materialnih stroškov, kar pomeni, da prosilec iz tega razloga ni bil v slabšem pravnem položaju. Zato v tem delu pritožba ni bila utemeljena.

Nadalje je Informacijski pooblaščenec ugotovil, da ZDIJZ prosilcu ne daje pravice, da bi od organa zavezanca zahteval overjeno (verodostojno) kopijo rokopisa. Kot način seznanitve z zahtevano informacijo javnega značaja ZDIJZ določa le vpogled, prepis, fotokopijo ali elektronski zapis, zato je Informacijski pooblaščenec ugotovil, da je prosilec v tem delu zahteval nekaj, za kar v ZDIJZ ni pravne podlage.

Organ se je v izpodbijani odločbi skliceval na izjemo varstva osebnih podatkov po 3. točki prvega odstavka 6. člena ZDIJZ, zato je Informacijski pooblaščenec izvedel preizkus, ali zahtevani dokumenti vsebujejo osebne podatke, katerih razkritje bi pomenilo kršitev varstva osebnih podatkov. Informacijski pooblaščenec je ugotovil, da gre v zahtevanih dokumentih za osebne podatke, vendar ti osebni podatki niso v celoti varovani. Informacijski pooblaščenec je namreč ugotovil, da je potrdilo o opravljenem pravniškem državnem izpitu informacija v zvezi z opravljanjem javne funkcije sodnika, saj se opravljen pravniški državni izpit zahteva za imenovanje na funkcijo sodnika. Kadar gre za informacije v zvezi z opravljanjem javne funkcije ali delovnega razmerja javnega uslužbenca, je take informacije dopustno razkriti na podlagi tretjega odstavka 6. člena ZDIJZ, ki določa javnost takšnih podatkov ne glede na morebiten obstoj izjem od prostega dostopa do informacij javnega značaja. Po drugi strani pa pisni testi iz postopkov opravljanja pravniškega državnega izpita niso prosto dostopne informacije javnega značaja, ki bi bile v zvezi z opravljanjem javne funkcije, temveč so varovani osebni podatki. Pisnih nalog v okviru opravljanja PDI namreč ni mogoče šteti za izdelke posameznikov v funkcijah pravosodnih funkcionarjev, ampak izdelke kandidatov za opravljanje PDI. Posredovanje celotnega pisnega testa iz postopka opravljanja pravniškega državnega izpita za posameznega sodnika pa bi očitno preseglo tudi namen, ki ga zasleduje ZDIJZ, in bi nesorazmerno poseglo v sicer varovane osebne podatke.

Informacijski pooblaščenec je ugotovil, da je organ ravnal zakonito, zato je pritožbo prosilca kot neutemeljeno zavrnil.

2.6.7. Mediji, poslovna skrivnost

Z odločbo št. 090-103/2011/6 z dne 23. 6. 2011 je Informacijski pooblaščenec zavrnil zahtevo novinarke, ki je od Univerzitetnega kliničnega centra Ljubljana (v nadaljevanju organ) zahtevala podatek o višini donacije, ki jo je Helena Blagne Zaman nakazala Pediatrični kliniki ob organizaciji koncerta Helena Blagne in Dunajski dečki.

Prosilka je navedla, da je ob nakupu vstopnice za koncert Helene Blagne Zaman vsak obiskovalec prispeval 2 evra za opremo priročnega laboratorija Pediatrične klinike v Ljubljani. Prosilka je med drugim zahtevala odgovor na vprašanje v zvezi z višino sredstev, ki jo je organ prejel na podlagi dogovora.

Organ je prosilki pojasnil, da je bil dogovor usten in da je bil denar že nakazan na račun organa, vendar pa organ prosilki zaradi izjeme poslovne skrivnosti ni posredoval informacije o višini nakazanega zneska.

Informacijski pooblaščenec je ugotovil, da je organ pravilno ugotovil obstoj izjeme poslovne skrivnosti, in sicer zaradi sprejetega Sklepa o določitvi poslovne skrivnosti, izdanega s strani Helene Blagne Zaman, direktorice gospodarske družbe. Omenjeni sklep izpolnjuje tako pogoj seznanitve oseb kot tudi pogoj, da je bil izdan preden je bil organu posredovan podatek, ki se varuje s sklepom, zato so izpolnjeni vsi kriteriji za določitev poslovne skrivnosti po prvem odstavku 39. člena ZGD-1 (subjektivni kriterij).

Ne glede na obstoj izjeme poslovne skrivnosti pa je moral Informacijski pooblaščenec ugotoviti, ali je možna uporaba t.i. izjeme od izjeme in dovoliti dostop do zahtevanega podatka, ker bi se nanašal na porabo javnih sredstev. Tretji odstavek 6. člena ZDIJZ namreč

določa, da se kljub morebitnim izjemam (v konkretnem primeru izjeme poslovne skrivnosti) dovoli dostop do informacij javnega značaja, če gre za podatke o porabi javnih sredstev.

Informacijski pooblaščenec je ugotovil, da je organ javni zavod, ki glede na določbe Odloka o preoblikovanju javnega zdravstvenega zavoda Klinični center v javni zdravstveni zavod Univerzitetni klinični center[21] pridobiva sredstva za izvajanje dejavnosti med drugim z donacijami in s sponzorstvom. Iz določb Zakona o javnih financah[22] in na njegovi podlagi sprejetih predpisov izhaja, da donacije fizičnih in pravnih oseb z nakazilom na račun organa postanejo del sredstev organa in s tem nedvomno del javnih sredstev. Nadzorna funkcija pravice dostopa do informacij javnega značaja se odraža tudi v tem, da mora biti javnosti dana možnost preverjanja, koliko sredstev je organ skupno v določenem obdobju prejel iz naslova donacij (za katera se šteje, da so z nakazilom organu postala del javnih sredstev) ter kako so bila ta sredstva porabljena. Kljub temu pa je Informacijski pooblaščenec ocenil, da podatki o tem, kdo je donator in višina zneska konkretnega donatorja, nista podatka, ki bi bila neposredno povezana s porabo javnih sredstev.

Zaradi obstoja izjeme poslovne skrivnosti po 2. točki prvega odstavka 6. člena ZDIJZ in neobstoja izjeme porabe javnih sredstev, zaradi katerih bi moral organ dovoliti dostop do zahtevanih informacij ne glede na izjemo poslovne skrivnosti, je Informacijski pooblaščenec zavrnil pritožbo prosilca in tako potrdil zavrnilno odločbo organa.

2.6.8. Poslovna skrivnost

Informacijski pooblaščenec je z odločbo št. 090-88/2011/8 z dne 24. 6. 2011 ugodil pritožbi prosilca in organu Domu upokojencev Ptuj naložil, naj mu posreduje fotokopijo Pogodbe o opravljanju notranje revizije poslovanja za leto 2009 (s prekritjem določenih delov pogodbe, ki izpolnjujejo kriterij poslovne skrivnosti), saj je organ zahtevo prosilca napačno v celoti zavrnil.

Prosilec je dokumente zahteval od doma upokojencev, za katerega je Informacijski pooblaščenec ugotovil, da nedvomno sodi v krog organov zavezancev po ZDIJZ, saj kot javni zavod med drugim opravlja javno službo institucionalnega varstva starejših, ki je glede na določbe prvega odstavka 42. člena Zakona o socialnem varstvu[23] opredeljena kot javna služba na področju socialnega varstva.

Obveznost notranje revizije za organ izhaja iz javnopravnih norm (Zakon o računovodstvu[24] in podzakonskega predpisa), zato se organ ne more svobodno odločiti, ali bo notranjo revizijo izvedel ali ne, saj ga k temu zavezuje poseben pravni režim, ki velja za posredne proračunske uporabnike. Kljub temu, da samo opravljanje notranje revizije ne sodi neposredno v javno službo institucionalnega varstva, pa je Informacijski pooblaščenec ugotovil, da gre za informacije, ki sodijo v delovno področje organa, saj je organ notranjo revizijo zavezan opravljati zaradi svojega statusa posrednega proračunskega uporabnika.

Ob presoji obstoja izjem od prostega dostopa je Informacijski pooblaščenec ugotovil, da je gospodarska družba (stranski udeleženec), s katero je bila sklenjena pogodba o izvedbi notranje revizije poslovanja, sprejela sklep o določitvi poslovnih skrivnosti. Ta sklep po presoji Informacijskega pooblaščenca z vidika formalnega kriterija ustreza pojmu sklepa o poslovni skrivnosti iz prvega odstavka 39. člena ZGD-1, saj dovolj natančno identificira podatke oziroma dokumente, na katere se nanaša, poleg tega je bil izdan pravočasno. Dostop do zahtevanega dokumenta je torej omejen z izjemo poslovne skrivnosti.

21 Uradni list RS, št. 138/2006, s spremembami.
22 Uradni list RS, št. 11/2011 – uradno prečiščeno besedilo 4.
23 Uradni list RS, št. 3/2007 – uradno prečiščeno besedilo 2, s spremembami.
24 Uradni list RS, št. 23/1999, s spremembami.

Vendar je bilo ne glede na obstoj izjeme poslovne skrivnosti ugotovljeno, da zahtevan dokument v določenem delu vsebuje podatke, ki se nanašajo na porabo javnih sredstev. Organ je opravljanje notranje revizije plačal iz sredstev, ki jih je prejel za opravljanje javne službe, ti pa nedvomno predstavljajo podatke o porabi javnih sredstev. Organ je namreč v delu, ko izvaja institucionalno varstvo starejših kot javno službo, uporabnik javnih sredstev, iz določbe petega odstavka 20. člena Zakona o računskem sodišču[25] pa izhaja sklep, da pojem javnih sredstev ne zajema zgolj proračunskih sredstev, pač pa tudi sredstva, ki jih izvajalec javne službe za izvajanje javne službe pridobi iz drugih virov. Tretji odstavek 6. člena ZDIJZ določa, da se, ne glede na obstoj morebitnih izjem od prostega dostopa do informacij javnega značaja, dovoli dostop do podatkov, ki se nanašajo na porabo javnih sredstev.

Zaradi navedenega je Informacijski pooblaščenec odpravil odločbo organa in mu naložil posredovanje tistih delov pogodbe o opravljanju notranje revizije poslovanja, ki se nanaša na porabo javnih sredstev. Preostali del pogodbe pa je moral organ po odločbi Informacijskega pooblaščenca prekriti, saj je predstavljal izjemo poslovne skrivnosti.

2.6.9. Arhivsko gradivo

Z odločbo št. 090-121/2011/4 z dne 8. 8. 2011 je Informacijski pooblaščenec zavrnil pritožbo prosilca, novinarja, zoper odločbo Arhiva Republike Slovenije (v nadaljevanju organ), s katero je ta zavrnil prosilčevo zahtevo po vpogledu v določene dokumente, ki so nastali med delom Službe državne varnosti (v nadaljevanju SDV). Prosilec je namreč želel vpogled v določene dele (strani oziroma poglavja) nekaterih dokumentov, kot so Letno poročilo SDV za leto 1973, Poročilo SDV za leto 1976, 1981 in 1986, Informativni bilten SDV za leto 1968, 1969 in 1970 ter Posebna informacija SDV za leto 1971, 1983, 1984,1985 in 1986. Prosilec je tudi prosil organ, naj mu odgovori, kdaj bi bil ogled mogoč, in naj ga obvesti tudi o ceni za morebitno fotokopiranje posameznih dokumentov, če se bo prosilec za to odločil.

V zvezi z vztrajanjem prosilca, da bi moral organ o njegovi zahtevi odločiti po ZMed, po katerem je vložil svojo zahtevo, je Informacijski pooblaščenec pojasnil, da je organ ravnal pravilno, ko je njegovo zahtevo obravnaval po ZDIJZ, saj je prosilec v konkretnem primeru primarno zahteval vpogled v dokumente, kar pomeni, da je zahteval vpogled v informacije, ki naj bi izvirale iz delovnega področja organa ter se nahajale v obliki dokumenta, in ne odgovora na vprašanje.

Glede zahteve prosilca, da mu organ odgovori na vprašanji, kdaj bi mu organ lahko omogočil ogled dokumentov in koliko bi stalo kopiranje, je Informacijski pooblaščenec pojasnil, da je sicer res, da je prosilec oblikoval dve vprašalni povedi, vendar sta slednji eksistencialno vezani na začetno vsebino zahteve, ki se nanaša na dostop do dokumentov. Informacijski pooblaščenec je zato ugotovil, da tudi v tem delu ne gre za zahtevo, o kateri bi organ moral odločiti le na podlagi določb ZMed, saj sta navedeni vprašanji neločljiv del zahteve za dostop do dokumentov.

Informacijski pooblaščenec je v pritožbenem postopku ugotovil, da je organ zahtevo prosilca utemeljeno zavrnil, ker so zahtevani dokumenti arhivsko gradivo, ki je izločeno iz dometa informacij javnega značaja. Drugi odstavek 4. člena ZDIJZ namreč določa, da arhivsko gradivo, ki ga hrani v okviru javne arhivske službe pristojni arhiv v skladu z zakonom, ki ureja arhive, ni informacija javnega značaja po tem zakonu. Arhivsko gradivo pridobi svoj status z dnem, ko je odbrano iz dokumentarnega gradiva in izročeno organu, kar izhaja iz 34. člena (v povezavi s 40. členom) Zakona o varstvu dokumentarnega in arhivskega gradiva ter arhivih[26]. Glede zahtevanih dokumentov sta bila v konkretnem postopku že izvedena predpisana postopka odbiranja in izročitve, ki sta konstitutivna elementa arhivskega gradiva, torej je bilo nedvoumno ugotovljeno, da gre za arhivsko gradivo. V konkretnem

[25] Uradni list RS, št. 11/2001, 20/2006 – ZNOJF-1.
[26] Uradni list RS, št. 30/2006, v nadaljevanju ZVDAGA.

primeru izročitelj obravnavanih dokumentov sicer še ni fizično izročil organu, pravno pa že, saj sta bila glede teh dokumentov že izvedena postopek odbiranja in postopek izročitve, kot ga je določal Zakon o arhivskem gradivu in arhivih[27], v bistvenem pa je ta postopek enak tudi postopku po zdaj veljavnem ZVDAGA.

Za konec je Informacijski pooblaščenec še zapisal, da dejstvo, da na podlagi določb ZDIJZ prosilcu ni omogočen dostop do zahtevanih dokumentov, ki so arhivsko gradivo, ne pomeni, da ti dokumenti niso prosto dostopni na podlagi drugih zakonov, konkretno ZVDAGA.

2.6.10. Notranje delovanje organa, osebni podatek, poslovna skrivnost

Informacijski pooblaščenec je z delno odločbo št. 090-197/2011/37 z dne 14. 11. 2011 in končno odločbo št. 090-197/2011/47 z dne 9. 12. 2011 v določenem delu ugodil zahtevi prosilke, novinarke, ki je od Komisije za preprečevanje korupcije (v nadaljevanju organ) zahtevala kopije vseh poročil lobirancev, ki so organu poročali o stikih z lobisti in na podlagi katerih je organ na svoji spletni strani objavil podatke o lobističnih stikih. Delno odločbo je Informacijski pooblaščenec izdal, ker je bil del zahtevka že zrel za odločanje, glede preostalih dokumentov pa je bilo v postopek treba poklicati stranske udeležence, zato je o drugem delu zahtevka Informacijski pooblaščenec odločil, ko so bili izpolnjeni vsi procesni pogoji.

Lobiranec o vsakem stiku z lobistom, ki ima namen lobirati, sestavi zapis, v katerem navede podatke o lobistu: osebno ime in priimek, podatek, ali se je identificiral v skladu z določbami Zakona o integriteti in preprečevanju korupcije[28], področje lobiranja, ime interesne organizacije ali druge organizacije, za katero lobira lobist, navedba morebitnih prilog in datum, kraj obiska lobista ter podpis lobiranca. Lobiranec zapis posreduje v roku treh dni v vednost svojemu predstojniku in organu.

Informacijski pooblaščenec je ugotovil, da ni podana izjema notranjega delovanja organa, saj zahtevani dokumenti ne predstavljajo notranje korespondence med javnimi uslužbenci, zaposlenimi pri organu. Ne gre torej za mnenja, stališča, navodila, odredbe, opomnike, poročila ali podobne interne dokumente, ki bi si jih izmenjevali uslužbenci pri organu zaradi nekih notranjih potreb organa oziroma oblikovanja stališč organa. Ugotovljeno je bilo torej, da že prvi pogoj za obstoj izjeme notranjega delovanja organa (dokument, sestavljen v zvezi z notranjim delovanjem oziroma dejavnostjo organov) ni izpolnjen, zato se v ugotavljanje obstoja drugega kriterija (razkritje bi povzročilo motnje pri delovanju oziroma dejavnosti organa) oziroma v izvedbo škodnega testa Informacijski pooblaščenec ni spuščal.

V zvezi z izjemo varstva osebnih podatkov je Informacijski pooblaščenec ugotovil, da se v zahtevanih poročilih pojavljajo osebni podatki, ki so varovani in takšni, ki niso varovani. Nevarovani osebni podatki so osebni podatki javnih uslužbencev in funkcionarjev (ime, priimek, zaposlitev) na podlagi tretjega odstavka 6. člena ZDIJZ, osebni podatki registriranih lobistov, ki so objavljeni v registru lobistov in so javni na podlagi izrecne določbe šestega odstavka 58. člena ZIntPK (razen davčne številke). Javni so tudi podatki o zakonitih zastopnikih interesnih organizacij oziroma osebah, ki so pooblaščene za zastopanje, saj so tudi ti podatki javno objavljeni v javnih evidencah. Informacijski pooblaščenec je ugotovil, da so varovani osebni podatki o posameznikih, zaposlenih v zasebnih interesnih organizacijah, ki pa hkrati niso zakoniti zastopniki teh organizacij oziroma osebe, pooblaščene za zastopanje, vsi naslovi posameznikov (tudi registriranih lobistov), ki niso objavljeni v javnih evidencah, ter e-mail naslovi oziroma drugi kontaktni podatki javnih uslužbencev/funkcionarjev zaradi varstva komunikacijske zasebnosti.

Obstoj izjeme poslovne skrivnosti je Informacijski pooblaščenec zavrnil, saj bodisi ne gre za podatke, ki bi vplivali na tržni konkurenčni položaj subjekta, bodisi ne izpolnjujejo subjektivnega ali objektivnega kriterija za obstoj poslovne skrivnosti iz prvega odstavka 39. člena ZGD-1.

27 Uradni list RS, št. 20/1997, s spremembami.
28 Uradni list RS, št. 69/2011 - uradno prečiščeno besedilo 2; v nadaljevanju ZIntPK.

Informacijski pooblaščenec je skladno z navedenim ugodil pritožbi prosilke in organu naložil, da ji posreduje zahtevane kopije poročil lobirancev, pri čemer mora z uporabo instituta delnega dostopa prekriti varovane osebne podatke.

2.6.11. Ali gre za delovno področje organa?

Informacijski pooblaščenec je z odločbo št. 090-270/2011/2 z dne 9. 12. 2011 in več podobnimi odločbami ugodil zahtevi prosilca, ki je istovrstno zahtevo naslovil na več izobraževalnih institucij, ter odpravil odločbo prvostopenjskega organa in mu zadevo vrnil v ponovno odločanje.

Prosilec je zahteval več informacij v zvezi z varnostjo in zdravjem pri delu, med drugim izjavo o varnosti z oceno tveganja, vključno z ukrepi, potrebnimi za preprečevanje nevarnosti in zmanjšanje škodljivih posledic; načrt reševanja in umika oseb; načrt za dajanje prve pomoči; pogodbe in račune s priloženimi dokazili o opravljanju nalog organiziranja in zagotavljanja varnosti in zdravja pri delu ter nabavo sredstev itd.

Informacijski pooblaščenec je ugotovil, da je organ zahtevo prosilca zavrnil pavšalno in zelo skopo, skliceval pa se je na to, da pri zahtevanih dokumentih ni izpolnjen kriterij za obstoj informacije javnega značaja, saj ne gre za informacije z delovnega področja organa. Pri tem so se nekateri organi sklicevali na okrožnico Ministrstva za šolstvo in šport, ki je navedlo, da zahtevani dokumenti šol s področja varnosti in zdravja pri delu ne izvirajo iz delovnega področja šole, temveč so le nujno potreben pogoj za izvajanje dela oziroma zakonska obveznost šole kot delodajalca v razmerju do zaposlenih v zavodu. Delovno področje organa je vzgoja in izobraževanje in spada pod dejavnost, ki je v registru dejavnosti uvrščeno pod dejavnosti z oznako P in nekatere druge dejavnosti.

Tako teorija kot upravna in sodna praksa za informacije iz delovnega področja organa opredeljujejo vse dokumente, ki jih je organ pridobil oziroma ustvaril v zvezi s svojim delom in v postopkih, za katere je pristojen v skladu s splošnimi predpisi. Iz Komentarja ZDIJZ izhaja, da je informacija, ki izvira iz delovnega področja organa, tista informacija, ki je nastala v zvezi z izvajanjem javnopravnih nalog oziroma dejavnosti organa. Tudi mnogo mednarodnih dokumentov zaobjema široko opredelitev pojma delovnega področja organa oziroma same definicije informacije javnega značaja. Ministrstvo za javno upravo je tudi izdalo mnenje in v njem zapisalo, da so informacije javnega značaja vsi dokumenti, ki so kakorkoli povezani s programi delovanja, posameznimi postopki, ki jih vodi organ, notranjimi predpisi, katerim so podvrženi delavci organa in organ, dokumenti, ki izkazujejo finančno poslovanje itd. Tudi iz sodbe Vrhovnega sodišča Republike Slovenije (npr. sodba št. I Up 122/2006-3 z dne 25. 4. 2007) izhaja, da je mogoče govoriti o delovnem področju organov v smislu ZDIJZ tedaj, ko je izvajanje določenih nalog ali dejavnosti urejeno s predpisi javnega prava, ki določajo obveznost organov glede izvajanja teh nalog v okviru upravne ali druge javnopravne funkcije ter morebitne pravice, obveznosti ali pravne koristi posameznikov, ki iz tega posebnega javnopravnega režima izhajajo. Zahtevani dokumenti torej nedvomno sodijo v delovno področje organa.

Informacijski pooblaščenec je poleg napačne uporabe materialnega prava ugotovil tudi, da izpodbijane odločbe ni mogoče preizkusiti, ker iz izreka in obrazložitve odločbe ni razvidno, kateri konkretno opredeljeni dokumenti so bili predmet presoje organa, to pa izvira tudi iz nepopolno ugotovljenega dejanskega stanja. Zaradi navedenega je Informacijski pooblaščenec ugodil pritožbi prosilca in odpravil odločbo organa, načelo ekonomičnosti pa je narekovalo, da je zadevo vrnil organu v ponovno odločanje.

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

Informacijski pooblaščenec je v letu 2011 ponovno zaznal bistven porast zadev na področju dostopa do informacij javnega značaja. V letu 2011 je prejel 1556 zadev (leto prej 971 zadev). Kot že tri leta zapored, je tudi v zadnjem letu število pritožb na tem področju bistveno naraslo. V letu 2011 je Informacijski pooblaščenec prejel 857 pritožb, od tega 549 zoper molk prvostopenjskih organov in 308 zoper zavrnilne odločbe. Bistveno se je povečalo tudi število vprašanj, pobud in prošenj za pojasnila v zvezi z uporabo ZDIJZ v praksi (skupaj 699 zadev, v letu 2010 382 zadev). Ob tem Informacijski pooblaščenec opaža, da pritožbene zadeve postajajo vse zahtevnejše, tako po obsegu zahtevanih dokumentov kot po njihovi vsebini.

Na podlagi zgoraj navedenih podatkov in izvedenih postopkov v praksi Informacijski pooblaščenec ocenjuje, da so prosilci bolje seznanjeni z institutom dostopa do informacij javnega značaja in se ga tudi pogosteje poslužujejo v praksi. Po drugi strani pa je Informacijski pooblaščenec pri organih zavezancih v preteklem letu žal opazil upad pripravljenosti na sodelovanje s prosilci, kar se kaže tudi kot povečanje števila pritožb na Informacijskega pooblaščenca in povečanje števila vloženih tožb s strani zavezancev zoper odločitve Informacijskega pooblaščenca. Navedeno je verjetno tudi posledica dejstva, da Vlada Republike Slovenije na tem področju (še) ni sprejela skupne strategije, iz katere bi sledilo, kakšni naj bodo cilji delovanja organov javnega sektorja na tem področju oziroma strategije, ki bi zavezance spodbujala k bolj transparentnemu delovanju. Informacijski pooblaščenec je tako v praksi opazil, da so določene kategorije zavezancev (predvsem manjše občine, javni zavodi na področju šolstva, zasebniki izvajalci javnih služb in koncesionarji) slabo seznanjene z obveznostmi, ki jih zanje prinaša ZDIJZ, ne glede na to, da je bil zakon sprejet že leta 2003 in da je začetno obdobje implementacije že mimo. Posledično se na zahteve prosilcev zavezanci ne odzovejo ustrezno oziroma jih vsebinsko ne obravnavajo, večkrat zaračunajo prekomerne stroške in zahteve zavračajo iz razlogov, ki nimajo zakonske podlage. Glede na število prošenj za pojasnila in razlago tudi ugotavljamo, da so zavezanci pogosto v dvomu, kako izvajati zakon, določena vprašanja, ki so se pojavila v praksi, pa terjajo tudi spremembo zakonodaje (vprašanje (ne)varovanja avtorskih del zavezancev, stroški postopka, stranski udeleženci,..). V zvezi z navedenim Informacijski pooblaščenec poziva Ministrstvo za pravosodje in javno upravo, da čim prej pristopi k pripravi predloga potrebnih sprememb zakonodaje in k bolj aktivni vlogi na tem področju. Spodbujevalne in razvojne naloge ter svetovanje zavezancem v zvezi z uporabo ZDIJZ so namreč naloge resornega ministrstva. Informacijski pooblaščenec zavezancem lahko neformalno svetuje v zvezi z že obravnavanimi primeri v praksi, glede konkretnih primerov, ki jih še nima v postopku reševanja, pa se kot pritožbeni organ vnaprej ne sme izjasniti.

Informacijski pooblaščenec ponovno opozarja tudi na problem zaračunavanja stroškov dela javnih uslužbencev pri dostopu do informacij, na kar je opozoril tudi že v preteklih treh letnih poročilih. V zadnjem obdobju je Informacijski pooblaščenec na tem področju opazil izrazit porast pritožb, pri obravnavi konkretnih zadev pa je ugotovil, da so zavezanci za dostop do relativno majhnega števila dokumentov (50 ali manj strani) prosilcem zaračunavali tudi po več sto evrov stroškov dela javnih uslužbencev, pri čemer so želeli na prosilce prenesti tudi stroške (slabe) organizacije delovnega procesa in poslovanja z dokumentarnim gradivom. Informacijski pooblaščenec ob tem opozarja, da možnost zaračunavanja materialnih stroškov, ki jo daje zakonodaja, ne sme postati razlog, ki daje organom zavezancem moč, da prosilce odvrnejo od vlaganja zahtev za posredovanje informacij javnega značaja. Po naši oceni lahko namreč zaradi nerazumno visokih stroškov govorimo že o negaciji (izničenju) pravice do dostopa do informacij javnega značaja kot ustavne pravice. Pravica dostopa do informacij javnega značaja pa je temeljna človekova pravica, zagotovljena v drugem odstavku 39. člena Ustave. Višina stroškov posredovanja informacij javnega značaja mora tako ostati v najnižjem možnem obsegu oziroma ne sme nesorazmerno ovirati prosilčeve ustavne pravice dostopa do informacij javnega značaja. Razumni stroški dostopa do informacij javnega značaja so po oceni Informacijskega

pooblaščenca, ob obstoječih predpisih, dejansko nastali materialni stroški in v skladu z Uredbo o posredovanju in ponovni uporabi informacij javnega značaja, tudi razumni stroški dela javnih uslužbencev, vendar le v obsegu, ki ne pomeni prekomernega posega v ustavno zagotovljeno pravico dostopa do informacij. Prav tako zaračunavanje stroškov nikakor ne sme biti arbitrarno in v celoti odvisno od individualnih sposobnosti javnih uslužbencev, zaposlenih pri določenem zavezancu, oziroma od organizacije dela pri zavezancu. Ravno to pa je tisto, kar je Informacijski pooblaščenec opazil v več konkretnih pritožbenih postopkih in na kar izrecno opozarja kot na slabo prakso pri zavezancih.

Informacijski pooblaščenec se tudi sam trudi delovati v duhu odprtosti in transparentnosti, zato na svoji spletni strani redno, proaktivno objavlja odločbe iz pritožbenih postopkov po ZDIJZ, sodbe Upravnega sodišča Republike Slovenije, pripombe, ki jih podaja k predlogom različnih zakonov, pojasnila in druge novice s tega področja. Postopke, v katerih je sam zavezan organ za dostop do informacij, poskuša voditi hitro in učinkovito, brez nepotrebnega zavlačevanja (informacije oziroma zavrnilno odločbo posredujemo prosilcem navadno takoj oziroma najkasneje v roku enega delovnega tedna in ne čakamo na iztek zakonskega roka 20 delovnih dni). K takšni praksi pozivamo tudi organe zavezance.

V letu 2011 je Informacijski pooblaščenec prejel tri pritožbe s področja ponovne uporabe informacij javnega značaja. Iz navedenega izhaja, da so prosilci na tem področju slabo seznanjeni s pravnimi možnostmi, ki jih imajo v primeru, ko jim zavezanci vlogo za ponovno uporabo zavrnejo. Področje ponovne uporabe javnih informacij ima pomemben gospodarski potencial, ki pa v praksi ostaja premalo izkoriščen. Na to opozarja tudi Evropska komisija, ki je v letu 2011 s tem namenom pripravila predlog sprememb Direktive Evropskega parlamenta in Sveta z dne 17. februar 2003 o ponovni uporabi informacij javnega sektorja. Namen predloga sprememb navedene direktive (ki je v slovenski pravni red implementirana z ZDIJZ) je zagotoviti optimalen pravni okvir in spremembo kulture v javnem sektorju, da se spodbudi trg digitalnih vsebin za proizvode in storitve, ki temeljijo na podatkih javnega sektorja ter prepreči izkrivljanje konkurence na trgu. Predlagane spremembe naj bi tako pripomogle h gospodarski rasti in ustvarjanju novih delovnih mest.

Na področju ponovne uporabe je Informacijski pooblaščenec tudi v letu 2011 sodeloval v mednarodnem konzorciju pri projektu LAPSI, ki je namenjen izgradnji tematske mreže na področju ponovne uporabe informacij javnega značaja. Projekt se osredotoča na odkrivanje in odstranjevanje pravnih ovir pri dostopu in ponovni uporabi informacij javnega značaja, ki se postavljajo na področju prava, informatike, intelektualne lastnine, zasebnosti, konkurenčnega prava, upravnega in okoljskega prava ter oblikovanje strategij, kako te ovire preseči.

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, po kateri je varstvo osebnih podatkov v državi ena izmed z Ustavo zagotovljenih človekovih pravic in temeljnih svoboščin. Določba 38. člena Ustave zagotavlja varstvo osebnih podatkov, prepoveduje uporabo osebnih podatkov v nasprotju z namenom njihovega zbiranja, vsakomur zagotavlja pravico do seznanitve z zbranimi osebnimi podatki, ki se nanašajo nanj, ter pravico do sodnega varstva ob njihovi zlorabi.

Za normativno urejanje varstva osebnih podatkov je zlasti pomemben drugi odstavek 38. člena Ustave, v katerem je določeno, da zbiranje, obdelovanje, namen uporabe, nadzor in varstvo tajnosti osebnih podatkov določa zakon (splošen, sistemski zakon in področni zakoni). Gre za t. i. obdelovalni model z določenimi pravili za urejanje dopustne obdelave osebnih podatkov na zakonski ravni. 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. Tak poseg je zato 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 tisti osebni podatki, ki so primerni in nujno potrebni za uresničitev zakonsko opredeljenega in ustavno dopustnega namena.

Ureditev varstva osebnih podatkov v sistemskem zakonu je potrebna zaradi enotne določitve načel, pravil in obveznosti ter zaradi zapolnitve pravnih praznin, ki bi lahko nastale v področnih zakonih. Poleg tega ni treba, da bi se npr. definicije, obveznosti in ukrepi v zvezi z zavarovanjem osebnih podatkov, katalogi zbirk osebnih podatkov, registracije zbirk osebnih podatkov v zvezi s pravicami posameznika do seznanitve s podatki, ki se nanašajo nanj, ter vprašanja glede nadzora in pristojnosti nadzornega organa vedno predpisovali tudi v področnih zakonih. Namen sistemskega zakona torej ni podrobnejše predpisovanje načinov obdelave osebnih podatkov po posameznih področjih, temveč predvsem to, da se v njem enotno 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. Področni zakoni morajo zato 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 je zelo priporočljivo, da se v področnem zakonu določi tudi čas shranjevanja osebnih podatkov (rok hrambe osebnih podatkov).

Zakon o varstvu osebnih podatkov[29], ki ga je Državni zbor Republike Slovenije sprejel 15. 7. 2004, velja od 1. 1. 2005. Zakon je bilo treba sprejeti predvsem zaradi vstopa Republike Slovenije v Evropsko unijo in zaradi 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 podatkov[30].

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.

Poleg Ustave, 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 1994[31]. Namen omenjene konvencije Sveta Evrope je na ozemlju vsake pogodbenice vsakemu posamezniku, ne glede na njegovo državljanstvo in prebivališče, zagotoviti spoštovanje njegovih pravic in temeljnih svoboščin ter

[29] Uradni list RS, št. 86/2004; v nadaljevanju ZVOP-1.
[30] Uradni list Evropskih skupnosti, št. L 281, 23. 11. 1995.
[31] Uradni list RS, št. 11/1994 – Mednarodne pogodbe št. 3/1994.

v okviru tega še posebej spoštovanje pravice do zasebnosti v primeru avtomatske obdelave njegovih osebnih podatkov.

Julija 2007 je bila sprejeta novela ZVOP-1, to je Zakon o spremembah in dopolnitvah zakona o varstvu osebnih podatkov[32]. ZVOP-1A je uvedel dve pomembni novosti, in sicer z vidika administrativnih (in s tem posledično tudi finančnih) razbremenitev upravljavcev osebnih podatkov ter predpisovanja določenih olajšav z vidika oblik dostopa posameznikov do njihovih osebnih podatkov. Novela je bistveno zožila krog zavezancev za vpis zbirk osebnih podatkov v register in je prinesla določene pozitivne rešitve, predvsem olajšave za posameznike, na katere se osebni podatki nanašajo.

Določbe ZVOP-1A so bile usklajene s spremembami Zakona o prekrških[33] iz leta 2006 ter so upoštevale uvedbo evra kot plačilnega sredstva Republike Slovenije s 1. 1. 2007.

Uradno prečiščeno besedilo ZVOP-1 je bilo izdano septembra 2007.

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 svojih nalog v skladu s svojimi pooblastili samostojen. Naloge opravlja v okviru in na podlagi ustave in zakonov.

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 nadzoru[34], specifične pristojnosti državnega nadzornika pa so določene v 53. členu ZVOP-1.

3.2.2. Inšpekcijski nadzor

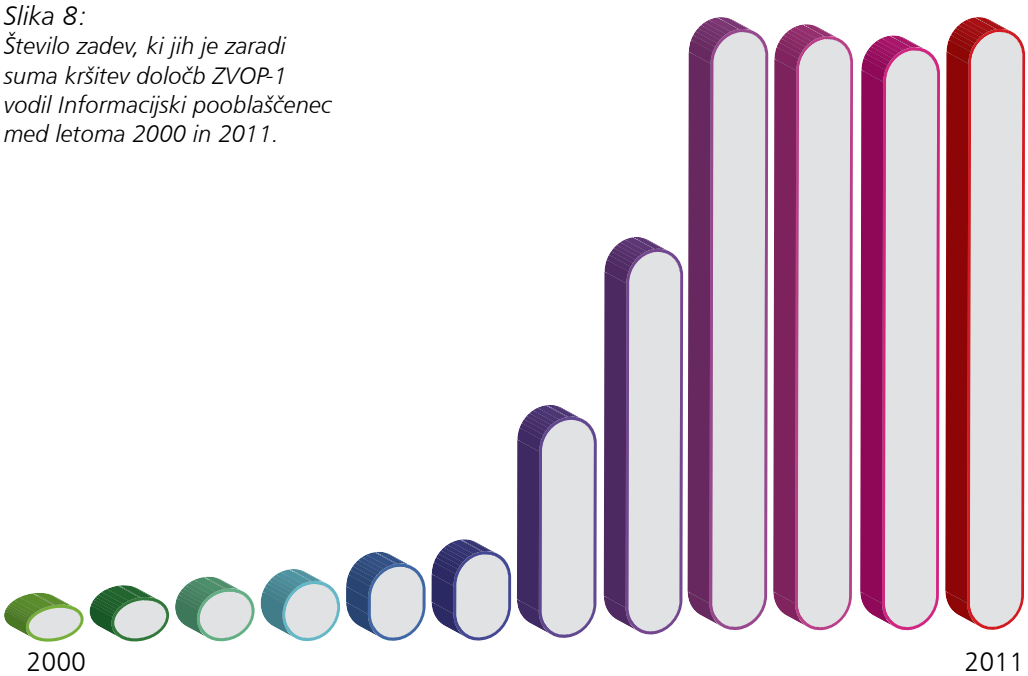
Neposredni inšpekcijski nadzor nad izvajanjem predpisov s področja varstva osebnih podatkov obsega:

- 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 nad izvajanjem določb zakona, ki urejajo katalog zbirke osebnih podatkov, register zbirk osebnih podatkov in evidentiranje posredovanja osebnih podatkov posameznim uporabnikom osebnih podatkov;
- nadzor nad izvajanjem določb zakona v zvezi z iznosom osebnih podatkov v tretjo državo in njihovim posredovanjem tujim uporabnikom osebnih podatkov.

Informacijski pooblaščenec je leta 2011 zaradi suma kršitev določb ZVOP-1 vodil 682 inšpekcijskih zadev, 246 v javnem in 436 v zasebnem sektorju. Zoper pravne osebe javnega sektorja je prejel 219 prijav, 27 postopkov je uvedel po uradni dolžnosti, medtem ko je zoper zasebni sektor prejel 398 prijav, 38 postopkov pa je uvedel po uradni dolžnosti. Število prijav in pritožb zaradi suma kršitev določb ZVOP-1 se je v primerjavi s statističnimi podatki za preteklo leto povečalo.

[32] Uradni list RS, št. 67/2007; v nadaljevanju ZVOP-1A.
[33] Uradni list RS, št. 3/2007 – uradno prečiščeno besedilo 4, s spremembami; v nadaljevanju ZP-1.
[34] Uradni list RS, št. 43/2007 – uradno prečiščeno besedilo 1; v nadaljevanju ZIN.

Slika 8:
Število zadev, ki jih je zaradi suma kršitev določb ZVOP-1 vodil Informacijski pooblaščenec med letoma 2000 in 2011.



Informacijski pooblaščenec je zaradi suma kršitev določb ZVOP-1 zoper pravne osebe javnega sektorja prejel 219 prijav. Pri 53 prijavah je bilo že iz samih prijav razvidno, da opisano dejanje ne pomeni kršitve določb ZVOP-1. Državni nadzornik je zato prijaviteljem pisno pojasnil, zakaj opisano dejanje ne pomeni kršitve teh določb in zakaj uvedba postopka inšpekcijskega nadzora ne bi bila smiselna. Leta 2011 je bilo izdanih tudi šest obvestil o neuvedbi inšpekcijskega postopka za prijave, prejete leta 2010. Sedem prijav je Informacijski pooblaščenec odstopil v reševanje pristojnim institucijam. Po preučitvi prijav je bilo uvedenih 159 inšpekcijskih postopkov, 27 pa jih je bilo uvedenih še po uradni dolžnosti. V okviru inšpekcijskih postopkov v javnem sektorju je bilo opravljenih 64 inšpekcijskih pregledov. Za odpravo ugotovljenih nepravilnosti je bilo izrečenih 11 opozoril na zapisnik in izdanih 23 ureditvenih oziroma upravnih odločb, od tega pet v zadevah iz preteklih let. V letu 2011 sta dva zavezanca na Upravno sodišče Republike Slovenija vložila tožbo zoper odločbo Informacijskega pooblaščenca, navedeno sodišče pa je odločilo v dveh upravnih sporih iz preteklih let. V obeh primerih je tožbo zavrnilo in potrdilo odločitev Informacijskega pooblaščenca. Leta 2011 je bilo zaključenih 134 zadev, od tega se jih je 38 nanašalo na pretekla leta.

V prijavah se je največ sumov kršitev določb ZVOP-1 nanašalo na:
- nezakonito razkrivanje osebnih podatkov: posredovanje osebnih podatkov nepooblaščenim uporabnikom s strani upravljavca zbirke osebnih podatkov in nezakonita objava osebnih podatkov, npr. na internetu ali v drugih medijih (98),
- nezakonito zbiranje oziroma zahtevanje osebnih podatkov (51),
- nezakonito izvajanje videonadzora (22),
- neustrezno zavarovanje osebnih podatkov (21),
- neposredno trženje (5),
- ostalo (22).

Prijave so bile vložene in postopki po uradni dolžnosti uvedeni zoper naslednje institucije v javnem sektorju:
- javne sklade, zavode, agencije in druge osebe javnega prava (106), od tega zoper vzgojno-izobraževalne ustanove 52 in 16 zoper zdravstvene ustanove,
- državne organe, ministrstva in organe v njihovi sestavi, upravne enote (88),
- sodišča in vrhovno državno tožilstvo, državno pravobranilstvo (27),
- občine (25).

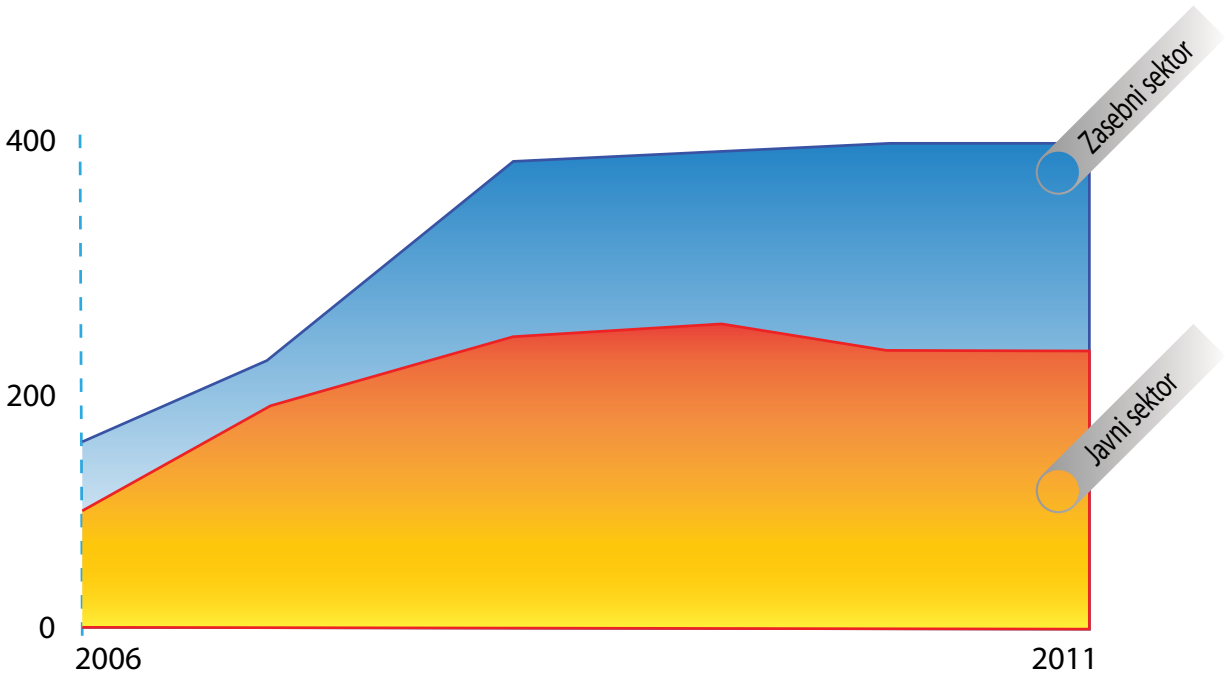
Informacijski pooblaščenec je zoper zasebni sektor prejel 398 prijav. V 98-ih primerih so bili prijavitelji obveščeni, da Informacijski pooblaščenec postopka inšpekcijskega nadzora ne bo uvedel, 15-krat pa je Informacijski pooblaščenec prijavo posredoval v reševanje pristojnim institucijam. Izdanih je bilo 11 obvestil o neuvedbi postopka za prijave, ki jih je Informacij-

ski pooblaščenec prejel leta 2010. Leta 2011 je bilo na podlagi prejetih prijav uvedenih 285 postopkov inšpekcijskega nadzora, 38 postopkov pa je bilo uvedenih še po uradni dolžnosti. Državni nadzorniki za varstvo osebnih podatkov so v zasebnem sektorju opravili 150 inšpekcijskih pregledov, od tega 40 v postopkih, uvedenih v preteklih letih. Zaradi ugotovljenih nepravilnosti je bilo izrečenih 27 opozoril na zapisniku o inšpekcijskem nadzoru in izdanih 56 ureditvenih odločb, od tega 20 v zadevah, uvedenih v prejšnjih letih. Leta 2011 so štirje zavezanci zoper prejeto odločbo sprožili upravni spor z vložitvijo tožbe na Upravno sodišče Republike Slovenije. V enem primeru je sodišče že odločilo, in sicer je tožbo zavrnilo, odločilo pa je tudi v dveh primerih iz leta 2010 – enkrat je tožbo zavezanca zavrnilo, enkrat pa je tožbi ugodilo, odpravilo izpodbijano odločbo Informacijskega pooblaščenca in mu zadevo vrnilo v ponoven postopek. Leta 2011 so bili ustavljeni 203 inšpekcijski postopki, od tega 69 postopkov, ki so bili začeti pred letom 2011.

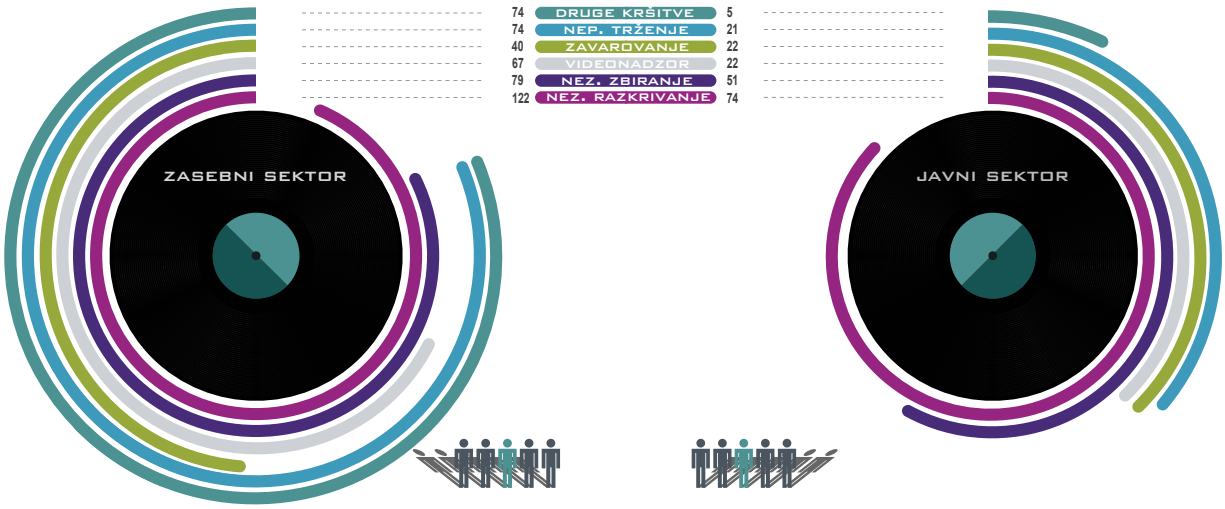
V okviru prejetih prijav je bilo največ sumov kršitev določb ZVOP-1 zaradi:

- nezakonitega razkrivanja osebnih podatkov: posredovanje osebnih podatkov nepooblaščenim uporabnikom s strani upravljavca zbirke osebnih podatkov in nezakonita objava osebnih podatkov, npr. na oglasnih deskah večstanovanjskih stavb, v medijih (120),
- nezakonitega zbiranja oziroma zahtevanja osebnih podatkov (77),
- zlorabe osebnih podatkov za namene neposrednega trženja (74),
- nezakonitega izvajanja videonadzora (67),
- neustreznega zavarovanja osebnih podatkov (22),
- ostalo (38).

Slika 9: Število zadev zaradi suma kršitev določb ZVOP-1 med letoma 2006 in 2011.



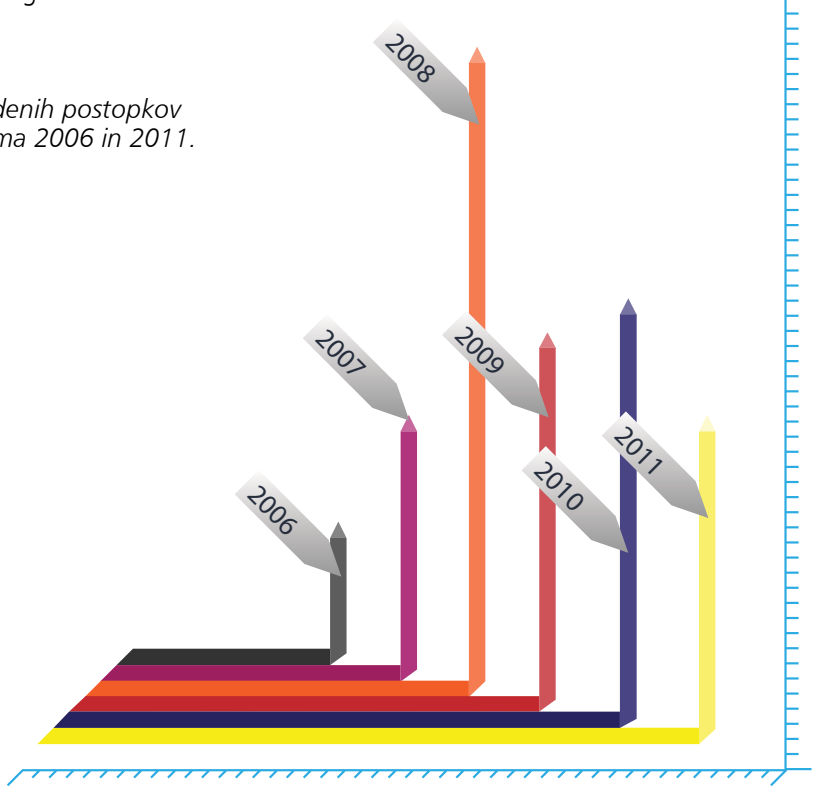
Slika 10: Prijave nezakonite obdelave osebnih podatkov leta 2011, primerjava med javnim in zasebnim sektorjem.



3.2.3. Storjeni prekrški

Zaradi kršitev določb ZVOP-1 je bilo leta 2011 uvedenih 136 postopkov o prekršku, 43 postopkov zoper pravne osebe javnega sektorja, 66 postopkov zoper pravne osebe zasebnega sektorja in 27 postopkov zoper posameznike. Postopek o prekršku se vodi v skladu z ZP-1. Za ugotovljeni prekršek lahko prekrškovni organ v skladu s 53. členom izreče opozorilo, če je storjeni prekršek neznaten in če pooblaščena uradna oseba oceni, da je glede na pomen dejanja opozorilo zadosten ukrep. Če je storjen hujši prekršek, prekrškovni organ izda odločbo o prekršku, s katero kršitelju izreče sankcijo. V skladu s 4. členom ZP-1 sta sankciji za prekršek globa in opomin, glede na 57. člen ZP-1 pa se lahko globa izreče tudi v obliki plačilnega naloga.

Slika 11: Število uvedenih postopkov o prekršku med letoma 2006 in 2011.



V postopkih o prekršku je Informacijski pooblaščenec leta 2011 izdal:
- 30 opozoril (7 v postopkih, uvedenih leta 2010),
- 64 odločb o prekršku (52 opominov, od tega 11 v postopkih, uvedenih leta 2010, in 12 glob, od tega pet v postopkih, uvedenih v preteklih letih),
- 7 plačilnih nalogov.

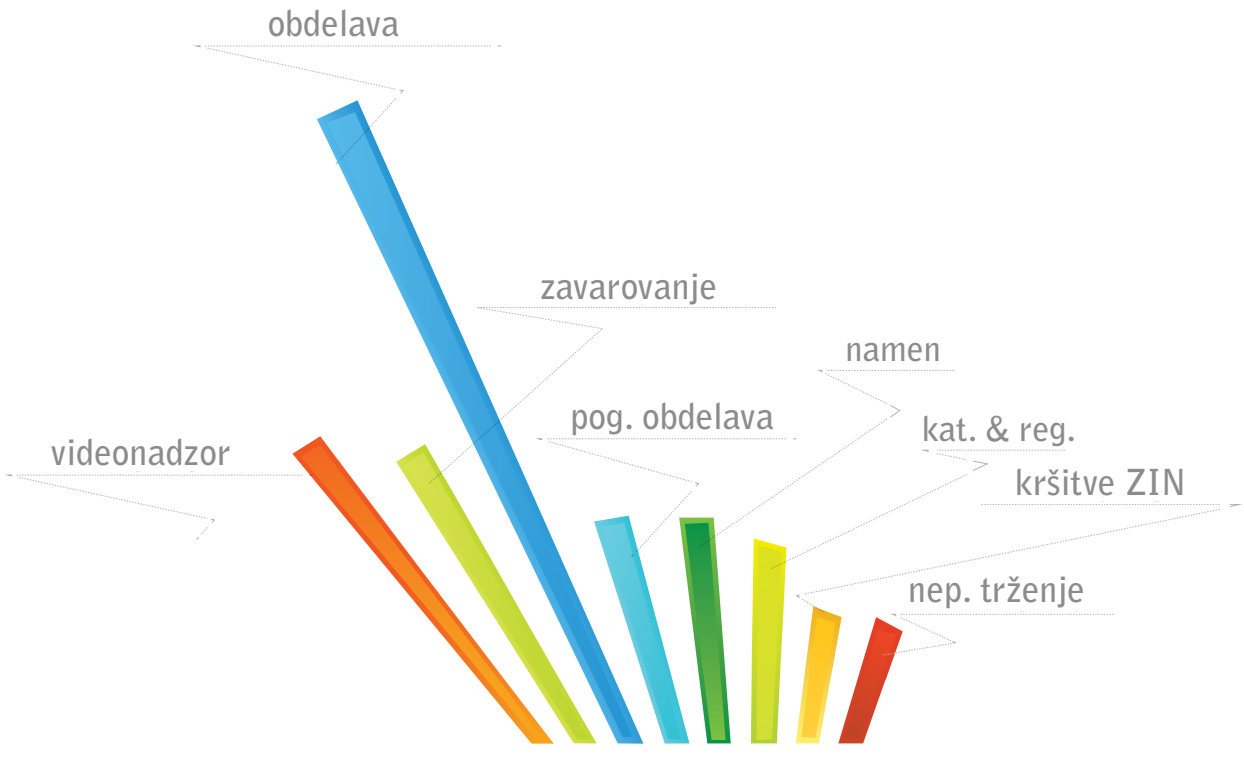
Informacijski pooblaščenec je zaradi ekonomičnosti v okviru postopkov inšpekcijskega nadzora izrekel tudi 75 opozoril po 53. členu ZP-1 za manjše kršitve (od tega 25 v inšpekcijskih postopkih, uvedenih pred letom 2011).

Kršitelji so zoper izdane odločbe vložili devet zahtev za sodno varstvo, od tega sedem zoper globe in dve zoper opomine.

Leta 2011 je Informacijski pooblaščenec ustavil 14 postopkov o prekršku (od teh je bilo šest uvedenih leta 2010), ker za izrek sankcije ni bilo dovolj dokazov ali ker je bilo ugotovljeno, da očitano dejanje ni prekršek.

Kršitve (v okviru enega postopka je lahko več kršitev) so zadevale:
- obdelavo osebnih podatkov: 8. člen ZVOP-1 (83),
- videonadzor: 74., 75., 76. in 77. člen ZVOP-1 (39),
- zavarovanje osebnih podatkov: 24. in 25. člen ZVOP-1 (37),
- pogodbeno obdelavo: 11. člen ZVOP-1 (21),
- namen zbiranja in nadaljnje obdelave osebnih podatkov: 16. člen ZVOP-1 (20),
- vzpostavitev katalogov zbirk osebnih podatkov in posredovanje podatkov v register zbirk osebnih podatkov: 26. in 27. člen ZVOP-1 (16),
- neizpolnjevanje ukrepov, izrečenih v postopkih inšpekcijskega nadzora, kršitve določb ZIN (11),
- neposredno trženje: 72. in 73. člen ZVOP-1 (10),
- evidenco posredovanja osebnih podatkov: tretji odstavek 22. člena ZVOP-1 (6),
- rok hrambe osebnih podatkov: 21. člen ZVOP-1 (4),
- izvajanje biometrijskih ukrepov: 78. – 81. člen ZVOP-1 (3),
- zavarovanje občutljivih osebnih podatkov: 14. člen ZVOP-1 (1),
- molk upravljavca v zvezi z zahtevo po izbrisu podatkov: 33. člen ZVOP-1 (1),
- fotokopiranje osebnih izkaznic in potnih listov: 3.a člen ZOIzk (1).

Slika 12: Najpogostejše kršitve določb ZVOP-1 leta 2011.



Leta 2011 je Informacijski pooblaščenec prejel 25 odločitev (sodba ali sklep), s katerimi so okrajna sodišča odločila o vloženih zahtevah za sodno varstvo zoper odločbe o prekrških, ki jih je izdal Informacijski pooblaščenec v preteklih letih:

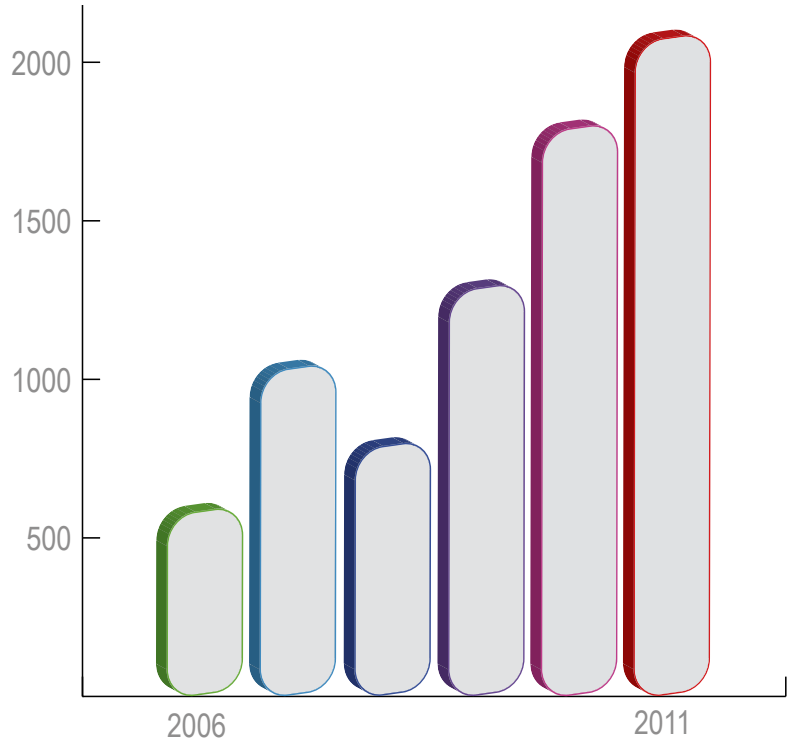
- zahteva za sodno varstvo je bila zavrnjena kot neutemeljena, odločba Informacijskega pooblaščenca pa potrjena (9),
- zahtevi za sodno varstvo je bilo ugodeno v delu, ki se nanaša na izrečeno sankcijo, tako da se je storilcem za prekršek spremenila sankcija, sicer je bila zahteva za sodno varstvo zavrnjena kot neutemeljena (8),
- zahtevi za sodno varstvo je bilo ugodeno, odločba Informacijskega pooblaščenca odpravljena, postopek o prekršku pa ustavljen (6),
- zahteva za sodno varstvo je bila zavržena (1),
- zahteva za sodno varstvo je bila vrnjena Informacijskemu pooblaščencu, ker je ni bilo mogoče preizkusiti (1).

V preteklem letu je Informacijski pooblaščenec zoper sodbo okrajnega sodišča Vrhovnemu državnemu tožilstvu predlagal vložitev zahteve za varstvo zakonitosti, tožilstvo pa je predlogu tudi sledilo. Vrhovno sodišče je primer vzelo v reševanje in odločilo, da je v primerih posega v osebne podatke posameznikov toliko prekrškov, kolikor je oškodovancev. S tem je sodišče tudi potrdilo stališče in prakso Informacijskega pooblaščenca.

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 leta 2011 prejel 2.143 prošenj za podajo pisnega pojasnila ali mnenja v zvezi s konkretnimi vprašanji, kar je več kot leta 2010, ko jih je prejel 1.859. Zaprosila za mnenja in pojasnila so vsebinsko zahtevnejša, kar lahko pripišemo temu, da je javnost vedno bolj seznanjena z ZVOP-1 in s pravicami posameznika, ki iz tega izhajajo. Za zahtevnejša vprašanja in vprašanja, na katera še ni odgovarjal, je Informacijski pooblaščenec izdelal obsežnejša pisna mnenja in pojasnila, medtem ko je posameznike, ki so zastavili vprašanja, na katera je Informacijski pooblaščenec v preteklosti že odgovarjal, le napotil na že izdelano mnenje. Poleg tega je Informacijski pooblaščenec izdal 14 mnenj prosilcem iz tujine. Informacijski pooblaščenec je dajal tudi ustna mnenja in pojasnila. V uradu je namreč vsak dan od 9. do 15.30 ure na voljo dežurni zaposleni, ki na vprašanja odgovarja po telefonu.

Slika 13: Število zaprosil za mnenja med letoma 2006 in 2011.



Zaprosila za mnenja in pojasnila so zadevala različna področja. Informacijski pooblaščenec izdana mnenja razvršča v 47 področij (npr. bančništvo, biometrija, davčni postopki, delovna razmerja, društva, elektronska pošta, enotna matična številka občana in davčna številka, iznos osebnih podatkov v tretje države, knjižničarstvo, mediji, neposredno trženje in nagradne igre, pogodbena obdelava, policijski postopki, postopki v centrih za socialno delo, register zbirk osebnih podatkov, sindikati, sodni postopki, stanovanjsko in nepremičninsko pravo, statistika in raziskovanje, svetovni splet, šolstvo, telekomunikacije in pošta, trgovinska dejavnost, upravljanje gospodarskih družb, uradni postopki, verske skupnosti, video- in avdionadzor, vpogled v lastne osebne podatke, vrtec, zavarovalništvo, zavarovanje osebnih podatkov, zdravstveni osebni podatki). Večina izdanih mnenj je objavljenih na spletni strani www.ip-rs.si.

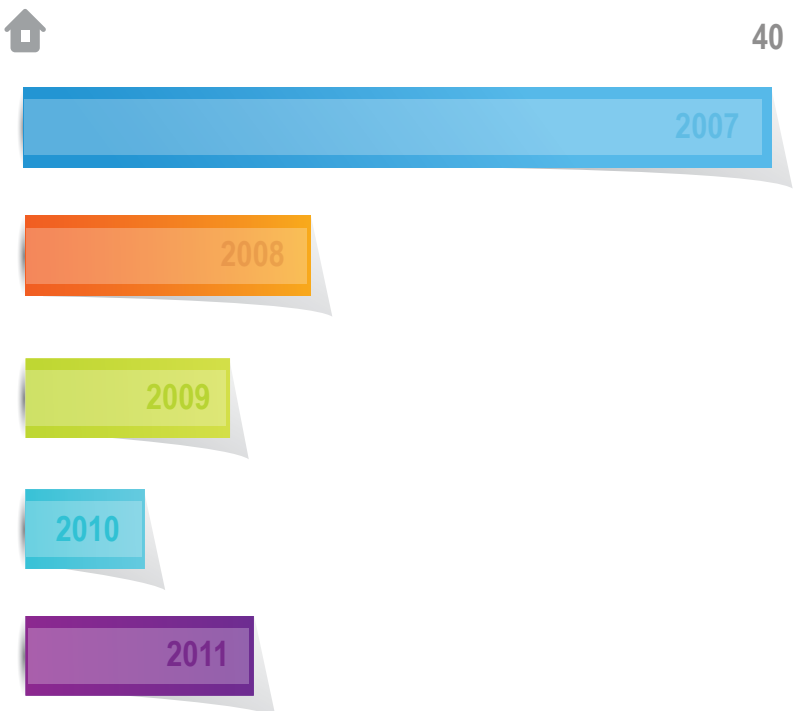
3.4. Dopustnost izvajanja biometrijskih ukrepov

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 skladu z določbami ZVOP-1 ali ne.

Biometrijski ukrepi so kot posebna oblika obdelave osebnih podatkov opredeljeni v tretjem poglavju VI. dela ZVOP-1, v 78.–81. členu.

Informacijski pooblaščenec presodi namen vlagatelja zahteve. Ta mora biti utemeljen in podprt z dovolj dokazi. Ugotavlja tudi, ali bi isti namen lahko zadovoljivo dosegel z načini preverjanja oziroma ugotavljanja identitete, ki ne vključujejo biometrijskih ukrepov in ki manj posegajo v zasebnost in dostojanstvo zaposlenih. Pri uvajanju teh ukrepov je namreč treba upoštevati, da njihovo izvajanje predstavlja neprimerno večji poseg v informacijsko zasebnost posameznika, saj gre za obdelavo tistih značilnosti posameznika, ki so za vsakogar edinstvene in stalne, in zloraba katerih bi imela za posameznika lahko hude, daljnosežne in nepopravljive posledice. Informacijski pooblaščenec presoja tudi tehnični vidik biometrijskih ukrepov (za preverjanje identitete – avtentikacija ali za ugotavljanje identitete – identifikacija).

Slika 15: Število vlog za izdajo odločbe o dopustnosti izvajanja biometrijskih ukrepov med letoma 2007 in 2011.



Število vlog za izdajo dovoljenja za uvedbo biometrijskih ukrepov, ki jih je prejel Informacijski pooblaščenec, se je od leta 2007 (40 vlog) do leta 2010 (6 vlog) zmanjševalo, v letu 2011 pa se je nekoliko povečalo (9 vlog). Leta 2011 je bilo izdanih osem odločb o dopustnosti izvajanja teh ukrepov, od tega dve za vlogi, prejeti leta 2010. V petih primerih je bila uvedba biometrijskih ukrepov dovoljena, v treh pa je bilo njihovo izvajanje zavrnjeno. En vlagatelj je svojo vlogo umaknil.

Informacijski pooblaščenec je zahtevi za izvajanje biometrijskih ukrepov ugodil v petih primerih:

· zahtevi vlagatelja za namen nadzora dostopa v telekomunikacijski prostor z uporabo čitalnika prstnih odtisov. Gre za zaprt del poslovnih prostorov, v katerem se nahaja premoženje velike vrednosti (strežnik s prometnimi in strežnik z retencijskimi podatki, telekomunikacijska centrala, računalniška oprema) in podatki, ki so razglašeni za poslovno skrivnost (podatki o naročnikih in uporabnikih, podatki o omrežju in tehnoloških značilnostih in investicijski načrti ter tehnološki elaborati). Informacijski pooblaščenec je zaključil, da navedena centrala in strežnika nedvomno predstavljajo premoženje, za varnost katerega je vlagatelj upravičen in dolžan sprejeti in izvajati ukrepe, s katerimi bo to premoženje kar najučinkoviteje zavaroval, prav tako je vlagatelj upravičen in dolžan izvajati take ukrepe tudi za zavarovanje poslovnih skrivnosti, ki se tudi hranijo v tem prostoru. Nepooblaščen vstop v ta prostor bi namreč lahko vlagatelju povzročil večjo premoženjsko škodo, ogrozil varnost pri njegovem poslovanju in povzročil zlorabo osebnih podatkov o naročnikih in uporabnikih storitev, za katere tudi ZEKom zahteva strožje varovanje in zloraba katerih bi pomenila grob poseg v komunikacijsko in informacijsko zasebnost njegovih naročnikov.

· zahtevi vlagatelja za namen nadzora dostopa v t. i. čiste prostore laboratorijev na sedežu vlagatelja. Biometrijski ukrepi temeljijo na prepoznavi obraza. V laboratorijih se odvija obdelava in shranjevanje popkovnične krvi in matičnih celic, ki predstavljajo unikatne vzorce, namenjene zdravljenju posameznika in morajo biti obdelane in shranjene v visoko tehnoloških laboratorijih, ki so izdelani po GMP standardih in zakonitostih farmacevtske industrije. Vlagatelj je v svoji vlogi izkazal, da je strogo nadzorovanje vstopa v t.i. čiste prostore laboratorija nujno potrebno za opravljanje njegove dejavnosti, strogo kontrolo dostopa in sledljivosti dostopa pa mu narekuje tudi Javna agencija za zdravila in medicinske pripomočke. Nepooblaščen dostop v čiste prostore, kjer je biološki material, ki ga za posameznike hrani in obdeluje vlagatelj, bi pomenil skrajno nevarnost za opravljanje dejavnosti vlagatelja, ki temelji na zaupanju posameznikov, katerih biološki material hrani. Informacijski pooblaščenec je zaključil, da je dejavnost vlagatelja taka, da zahteva najvišje standarde varovanja, hkrati pa gre tudi za varovanje premoženja (biološka tkiva so za posameznike neprecenljive vrednosti, prav tako je visoka vrednost infrastrukture in opreme laboratorijev) ter varovanje poslovnih skrivnosti.

· zahtevi vlagatelja za namen nadzora dostopa v prostor, v katerem je nameščen HVEE Tandentron ionski pospeševalnik oziroma tehnični del sistema HVEE Tandentron ionskega pospeševalnika z uporabo dveh čitalcev prstnih odtisov. Vlagatelj je navedel, da želi z izvajanjem biometrijskih ukrepov za vstopanje v ta prostor varovati svoje premoženje večje vrednosti (ionski pospeševalnik, raziskovalna oprema, arheološki in umetnostni objekti), poleg tega pa želi biometrijske ukrepe izvajati tudi zaradi varnosti ljudi, saj bi bili posamezniki ob nepooblaščenem vstopanju v ta prostor lahko izpostavljeni sevanju ionskega pospeševalnika. Poleg tega naj bi bila učinkovita omejitev dostopa do tega prostora zgolj na pooblaščene osebe potrebna za varnost ljudi tudi zato, ker so ionski izvori med obratovanjem priključeni na izvore visokih napetosti, kar ima ob neustreznem oziroma nestrokovnem ravnanju z opremo, ki se nahaja v tem prostoru, lahko za posledico tudi smrtno poškodbo posameznika. Informacijski pooblaščenec je zaključil, da je namen varstva ljudi in premoženja dovolj tehten, resen in utemeljen. Vlagatelj je namreč izkazal, da je premoženje, ki ga želi varovati z izvajanjem biometrijskih ukrepov tako pomembno, poleg tega je bilo v postopku ugotovljeno, da bi bila z nepooblaščenim vstopanjem v varovani prostor lahko resno ogrožena tudi varnost in zdravje posameznikov, zato je poseg v zasebnost, ki ga predstavlja izvajanje biometrijskih ukrepov v konkretnem primeru upravičen.

· zahtevi vlagatelja za namen nadzora dostopa v več laboratorijev, v katerih potekajo validacije zdravil in izvedba razvojno-raziskovalnih procesov za zunanje partnerje ter na glavnem vhodu v stavbo z uporabo čitalcev prstnih odtisov ali uporabo čitalcev, ki delujejo na podlagi prepoznave obraza. Po vpogledu v načrte stavbe je bilo ugotov-

ljeno, da namerava vlagatelj z biometrijskimi ukrepi zagotavljati dvostopenjsko varovanje ljudi, premoženja in poslovnih skrivnosti, in sicer vhode v stavbo, dodatno pa tudi vhode v tiste prostore znotraj stavbe, v katerih se neposredno bodisi izvajajo procesi ali nahajajo snovi, ki predstavljajo potencialno grožnjo ljudem in premoženju, bodisi nahajajo dokumenti, ki vsebujejo oziroma predstavljajo poslovno skrivnost. Za odločitev Informacijskega pooblaščenca je bila odločilna tudi narava oziroma vsebina dejavnosti vlagatelja. Ta na eni strani vključuje izvajanje procesov in rokovanje s snovmi (zdravila in druge substance), ki so toksične, eksplozivne ali drugače nevarne in katerih nepravilna uporaba ali zloraba bi lahko povzročila resne posledice za življenje in zdravje (lahko tudi večjega števila) ljudi in/ali povzročila veliko premoženjsko škodo. Na drugi strani pa gre za dejavnost vlagatelja, ki obsega tako delo s substancami, ki predstavljajo poslovne skrivnosti, kakor tudi raziskave, katerih namen je odkrivanje novih produktov, pri čemer tako procesi kot sami produkti praviloma predstavljajo poslovno skrivnost. Vzorci zdravil in substanc, ki se obdelujejo in hranijo v teh prostorih, in njihove recepture oziroma podatki o njihovi sestavi namreč predstavljajo poslovno skrivnost zunanjih partnerjev, za katere vlagatelj izvaja validacijo zdravil. Ob tem je Informacijski pooblaščenec upošteval tudi dejstvo, da gre pri vlagatelju za farmacevtsko dejavnost, ki na eni strani zahteva zelo visoke finančne vložke v raziskave in razvoj, na drugi strani pa imajo inovacije, ki so rezultat takih raziskav, tudi veliko premoženjsko vrednost, zato je povsem legitimen interes vlagatelja, da podatke, ki predstavljajo poslovne skrivnosti, kar najbolje zavaruje.

· zahtevi vlagatelja z namenom opravljanja dejavnosti, varovanja premoženja, varovanja poslovnih skrivnosti in tajnih podatkov s prepoznavo papilarnih linij nad tistimi zaposlenimi, ki bodo vstopali v določene prostore. Vlagatelj je v svoji vlogi izkazal, da je strogo nadzorovanje vstopa v te prostore nujno potrebno za opravljanje njegove dejavnosti uničevanja nosilcev podatkov, ki vsebujejo podatke, ki nosijo oznako tajnosti v skladu z ZTP, in podatkov z oznako zaupnosti v skladu z ZGD-1. Za samo opravljanje dejavnosti je nujno, da so nosilci podatkov strogo zavarovani. Subjekti, ki vlagatelju zaupajo nosilce s tajnimi podatki in poslovnimi skrivnostmi v uničenje, mu nalagajo dolžnost in odgovornost, da bo nosilce zaščitil pred nepooblaščenim dostopom v skladu z zakonom. V primeru, da vlagatelj te odgovornosti ne izpolni in ne poskrbi za varovanje na najstrožji ravni ter da se zgodi nepooblaščen dostop do varovanih podatkov, to lahko kritično vpliva na dejavnost vlagatelja oziroma mu povzroči nepopravljivo škodo, prav tako pa tudi subjektom, katerih podatki bi bili nepooblaščeno razkriti. Vlagatelj je po mnenju Informacijskega pooblaščenca izkazal tudi nujnost uvedbe biometrijskih ukrepov za namen varovanja premoženja. Podatki na nosilcih, ki jih vlagatelj hrani in uničuje, so za subjekte, ki so jih zaupali v uničenje, neprecenljive vrednosti, kar kaže tudi njihova oznaka tajnih podatkov oziroma poslovnih skrivnosti. Zaradi narave podatkov, ki so vlagatelju zaupani v uničenje, je upravičena njegova domneva, da bodo prostori, v katerih se nahajajo nosilci, podvrženi potencialnim poskusom nepooblaščenega dostopa.

Kot izhaja iz odločb, s katerimi je Informacijski pooblaščenec dovolil izvajanje biometrijskih ukrepov, se bodo biometrijski ukrepi izvajali le nad zaposlenimi pri vlagateljih za namen vstopa v posebne prostore, v katerih imajo vlagatelji premoženje večje vrednosti in podatke, ki so v skladu z zakonom opredeljeni kot tajni ali kot poslovna skrivnost. Informacijski pooblaščenec je ugotovil, da so nameni varovanja premoženja ali posebnih podatkov, ki jih zasledujejo vlagatelji, dovolj tehtni, resni in utemeljeni in da tehnične rešitve, ki jih načrtovani biometrijski ukrepi predvidevajo, s stališča načela sorazmernosti upravičujejo uvedbo biometrijskih ukrepov za vstop v posebne prostore in odtehtajo tudi poseg v informacijsko zasebnost zaposlenih, ki ga predstavlja izvajanje biometrijskih ukrepov.

Informacijski pooblaščenec je zavrnil tri vloge za izdajo dovoljenja za uvedbo biometrijskih ukrepov:

· vlogo vlagatelja za nadzor dostopa do pripravniške sobe, v kateri se nahajajo računalniki, s katerimi se dostopa do portala elektronske zemljiške knjige, ki dopušča vpogled v zaščitene izpise in računalniški strežnik, na katerem so shranjene notarske listine v elektronski obliki ter za nadzor dostopa do arhiva, v katerem se hranijo notarske listine v pisni obliki. Vlagatelj je navedel, da želi z izvajanjem biometrijskih ukrepov za vstopanje v ta dva prostora zagotavljati varnost premoženja, varovanje tajnih podatkov in poslovnih skrivnosti. Informacijski pooblaščenec je po preučitvi vseh pravno relevantnih dejstev ugotovil, da izvajanje biometrijskih ukrepov za vstopanje v pripravniško sobo in arhiv ni nujno potrebno za zavarovanje premoženja in poslovnih skrivnosti, saj lahko vlagatelj omenjene

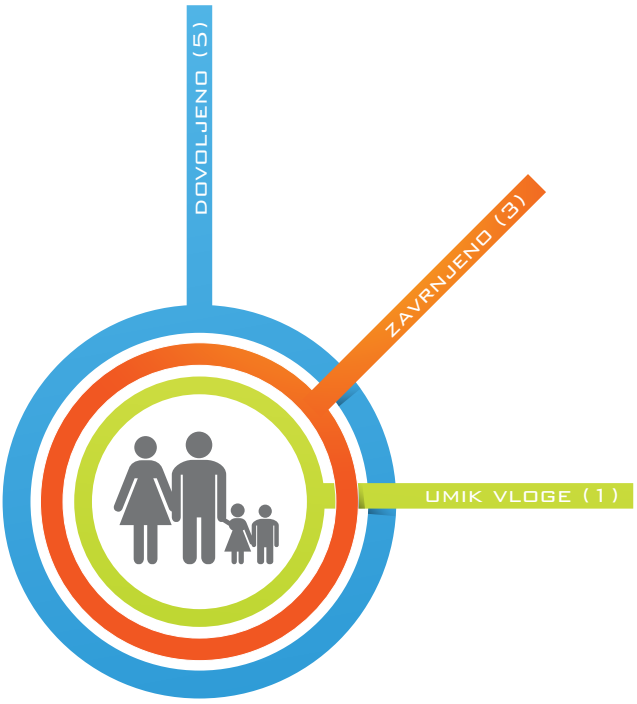
pravne dobrine v enaki meri zavaruje z drugimi ukrepi, ki v manjši meri ali pa sploh ne posegajo v informacijsko zasebnost zaposlenih, kot so zaklepanje varovanih prostorov s ključi ali različnimi karticami. Poleg tega vlagatelj lahko oziroma mora poskrbeti za dodatne ukrepe, s katerimi zagotavlja, da notarske listine, ki vsebujejo poslovne skrivnosti, niso dostopne vsakomur, ki vstopi v varovana prostora, to pa lahko stori tako, da notarske listine, ki se nahajajo v papirni obliki znotraj teh prostorov, hrani v zaklenjeni omari, sefu, itd., dostop do strežnika, na katerem se hranijo take listine v elektronski obliki, pa zavaruje z uporabniškimi imeni in gesli. S takim načinom zavarovanja varovanih dobrin je po prepričanju Informacijskega pooblaščenca mogoče zagotoviti enako stopnjo zavarovanja kot z izvajanjem biometrijskih ukrepov.

· vlogo vlagatelja, ki je med drugim navedel, da se je za uvedbo biometrijskih ukrepov odločil, ker je bilo treba zamenjati ključavnico in ker so sodobne biometrijske rešitve na voljo po dostopnih cenah. Vlagatelj je izpostavil pomanjkljivosti ključev, ki jih je mogoče odtujiti, izgubiti, posoditi ipd. Informacijski pooblaščenec je na podlagi vlagateljevih navedb zaključil, da je bilo njegovo glavno vodilo praktičnost in da uvedba biometrije na način, kot je predstavljen v zahtevi, ni nujno potrebna za kontrolo dostopa do prostorov vlagatelja, saj je ta namen možno doseči z milejšimi sredstvi, na primer z uporabo brezkontaktnih kartic ali s PIN kodami. Uporaba brezkontaktnih kartic (ali primerljivega načina za nadzor pristopa), ki bi jih imeli vsi zaposleni in ki delujejo kot aktivator ključavnice, bi omogočila nadzor nad tem, kdo od zaposlenih je vstopil ali izstopil v poslovne prostore podjetja. Uporabi brezkontaktnih kartic ali drugega sredstva za nadzor dostopa bi bilo z vidika možnih zlorab s posojanjem, izgubljanjem ipd. mogoče oporekati v primeru, ko bi vlagatelj uspel dokazati, da se zlorabe dogajajo v takšnem obsegu, da to predstavlja za organizacijo velik problem in da nadzora pristopa ne morejo rešiti na drug način, ki ne vključuje biometrijskih ukrepov. Biometrijskih ukrepov, ki se uvajajo le zato, ker so bolj priročni od ostalih sistemov varovanja, ni mogoče opredeliti kot nujno potrebnih za dosego namenov, opredeljenih v prvem odstavku 80. člena ZVOP-1 (varovanje premoženja, varovanje tajnih podatkov in poslovnih skrivnosti). Tudi evidentiranje prisotnosti na delovnem mestu s pomočjo biometrijskih ukrepov še ne pomeni, da je bil zaposleni na svojem delovnem mestu, in ne dokazuje, da je svoje delo opravljal skladno z zadolžitvami oziroma da ga je sploh opravljal. Dokazuje le, da je določeni posameznik ob določenem času prislonil svoj prst na napravo za biometrijsko prepoznavo prstnega odtisa, nikakor pa ne omogoča ugotavljanja, kaj je ta posameznik počel pred ali po tem. Biometrijsko evidentiranje delovnega časa tudi ne more zagotoviti dokaza, da je bil delavec v določenem času v določenem prostoru. Zaposleni se namreč lahko biometrijsko evidentira, a potem sploh ne vstopi v delovni prostor, zato bi se vlagatelj zahteve soočil z istimi težavami, kot če bi se za ta namen uporabljale magnetne kartice ali kak drug način.

· vlogo vlagatelja, ki je želel biometrijske ukrepe uvesti za dostop do posebnih blagajn in za registracijo delovnega časa zaposlenih in študentov, ker bi s tem varoval svoje premoženje oziroma preprečil izvajanje transakcij, kot so: vračilo gotovine, avtorizacija popusta za zaposlene, vračilo DDV s strani nepooblaščenih oseb. Čeprav pri transakcijah na teh blagajnah lahko pride do določenih zlorab in goljufij, je Informacijski pooblaščenec zaključil, da uvedba biometrijskih ukrepov za zavarovanje teh transakcij in s tem premoženja vlagatelja, ni nujno potrebna, ker lahko vlagatelj enako stopnjo zavarovanja svojega premoženja doseže z izvajanjem drugih ukrepov, ki v manjši meri ali pa sploh ne posegajo v informacijsko zasebnost zaposlenih. Primeri zlorab, ki jih je navedel vlagatelj, so posledica malomarnega ali celo naklepnega nepravilnega ravnanja odgovorne oziroma pooblaščene osebe. Informacijski pooblaščenec poudarja, da uvedba biometrijskih ukrepov ne onemogoča zlorabe sistema in da bi izvajanje teh ukrepov zagotovilo zgolj to, da bi zavarovano blagajno s pomočjo svojega prstnega odtisa lahko odklenile le tri pooblaščene osebe v posamezni poslovalnici. Izvajanje teh ukrepov pooblaščenim osebam ne more preprečiti, da ne bi potem dostop do blagajne omogočile drugim nepooblaščenim osebam ali da ne bi same zlorabile dostopa. Prav tako uvedba biometrijskih ukrepov ne bo preprečila izvajanja transakcij, ki jih navaja vlagatelj. Malomarno ravnanje z gesli in osebnimi številkami ne more biti razlog za uporabo biometrijskih ukrepov, saj ima vlagatelj na voljo tudi dosti drugih možnosti za nadgradnjo obstoječega sistema zavarovanja blagajn, ki ne vključujejo izvajanja biometrijskih ukrepov. V zvezi z izvajanjem biometrijskih ukrepov za registracijo delovnega časa nad vsemi zaposlenimi in študenti, je vlagatelj navedel, da v praksi občasno prihaja do nenatančnosti, popravljanja in ročnega spreminjanja podatkov o prihodih in odhodih ter prilagajanja urnikov s strani odgovornih oseb in da je namen uvedbe takih ukrepov opravljanje dejavnosti in varnost ljudi ter premoženja. Informacijski pooblaščenec je zaključil, da vlagatelj tudi za ta

namen ni izkazal nujnosti uvedbe biometrijskih ukrepov, poleg tega pa izvajanje biometrijskih ukrepov nad posamezniki, ki niso zaposleni pri vlagatelju (študenti), ni dovoljeno.

Slika 16: Izdane odločbe o dopustnosti izvajanja biometrijskih ukrepov leta 2011.



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 ustrezno raven varstva osebnih podatkov zagotavlja le delno, 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).

Informacijski pooblaščenec je leta 2011 prejel štiri vloge za iznos osebnih podatkov. Izdal je dve odločbi, obema vlagateljema je iznos osebnih podatkov dovolil.

· Telekomunikacijskemu operaterju (izvoznik podatkov) je Informacijski pooblaščenec dovolil, da po prejemu odločbe svojemu pogodbenemu obdelovalcu osebnih podatkov v tretji državi (uvozniku podatkov), to je družbi iz Srbije, iznaša in posreduje osebne podatke naročnikov in predplačnikov storitev za namen analiziranja prometnih tokov za ugotavljanje morebitnih pomanjkljivosti oziroma izgub podatkov v prihodkovnem toku. Uvoznik podatkov bo pridobil podatke s pomočjo oddaljenega dostopa do baze podatkov izvoznika podatkov. Kategorije podatkov, ki se bodo iznašali, vključujejo:

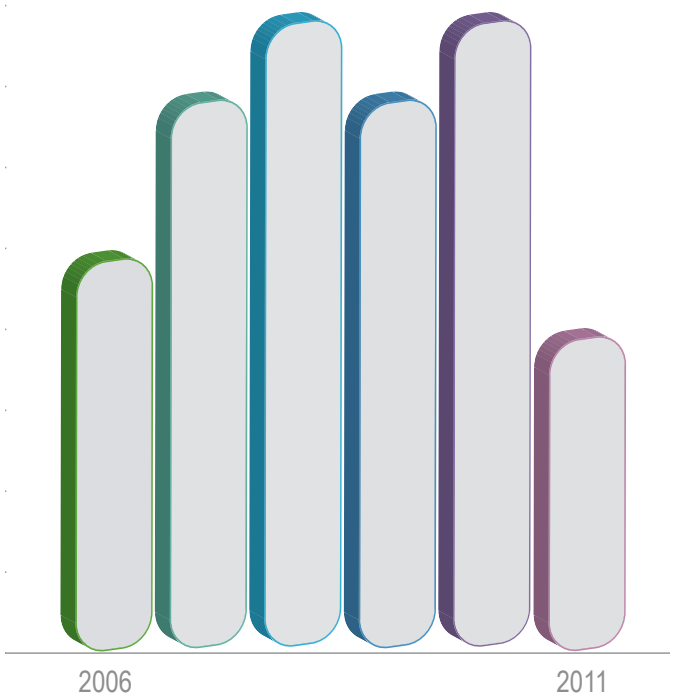
- podatke o naročnikih: splošni podatki (ime, priimek, naslov, davčna številka, EMŠO, številka potnega lista oziroma osebne izkaznice, številka bančne kartice, bančnega

računa, naziv banke, številka kreditne kartice, ime izdajatelja, datum veljavnosti), operativni podatki o naročniku (na kateri dan se mu izdaja račun, popusti, ki so bili aktivirani, ipd.), podatki o opremi (številka SIM kartice, telefonska številka, IMEI številka, profil stranke);
- podatke o prometu (podatki o nakupih, naročilih in kodah, število prenesenih bitov, podatki o polnitvi predplačniških računov, podatki o klicih v določeno omrežje, klicna številka, klicana številka, trajanje klica, podatki o prejetih klicih v tujini, ipd.);
- podatke o računih (znesek, datum zapadlosti).

Uvoznik podatkov bo izvozniku dostavljal rezultate analiz podatkov, potem pa jih bo uničil.

· Informacijski pooblaščenec je družbi, ki se ukvarja s prodajo računalniške opreme (izvoznik podatkov), dovolil, da po prejemu odločbe upravljavcem v sklopu krovne družbe v tretji državi (uvoznikom podatkov), to je 11 družbam s sedežem v Ljudski republiki Kitajski, iznaša in posreduje osebne podatke svojih zaposlenih ter podatke o poslovnih partnerjih. Podatki zaposlenih pri izvozniku podatkov, ki se bodo iznašali, so: ime, domač naslov, elektronski naslov, številka službenega telefona in faksa, mobilnega telefona, domačega telefona, datum rojstva in starost, serijska številka, ki jo določi izvoznik podatkov, EMŠO, številka potnega lista, naziv in obseg delovnega mesta, ime nadrejenega in struktura poročanja, pridobljena izobrazba in opravljena usposabljanja, delovne izkušnje, podatki o vzdrževanih osebah, kontakti v nujnih primerih, številke o kreditnih karticah, izdanih s strani izvoznika podatkov, podatki o bančnih računih za nakazilo plačila, davčna številka, ocene dela, višine plačil delavcu, pokojninski in drugi programi, prodajni načrt, stimulacije in provizije, podatki o odbitkih ali zadržanju plače, skupina delovnega mesta, podatki o službenem vozilu, datum začetka opravljanja dela, način zaposlitve, datum, trajanje zaposlitve, delovni čas, status zaposlitve, podatki o odsotnosti – porodniška, študijski dopust, dopust, šifra delovnega mesta, rang delovnega mesta, ali gre za vodstveni položaj, oddelek in lokacija delovnega mesta, plača, dopust, odsotnost – bolniški stalež, datum prenehanja delovnega razmerja in razlog prenehanja. Podatki poslovnih partnerjev izvoznika podatkov, ki bodo predmet iznosa, pa so: polno ime in naslov družbe, imena posameznih poslovnih kontaktov v družbi, naslovi, elektronski naslovi, telefonske številke in faksi posameznih kontaktov, naziv delovnega mesta, informacije o plačilu, pretekla komunikacija s strankami, podatki o poslovnih in pogodbenih razmerjih, podatki o preteklih provizijah, vodenju naročil in vračil, provizijah za storitve, izdanih računih in plačilih, pretekla komunikacija s strankami, tehnična pomoč in reševanje pritožb strank, poslovni dogovori z dobavitelji, prodajalci in ostalimi poslovnimi partnerji, država, kontaktno ime stranke, registrska številka države, podatki o pogodbah, zaželeni jezik, pozdrav. Podatki zaposlenih se bodo iznašali za namen izpolnjevanja pravic in obveznosti, ki izvirajo iz pogodbe o zaposlitvi in delovnega razmerja (npr. pridobivanje kadrov, upravljanje s plačami in stimulacijami, kadrovsko načrtovanje), v zvezi s podatki poslovnih partnerjev pa bodo uvozniki podatkov opravljali opravila, vezana na upravljanje z naročili, upravljanje prodaje, promocijo proizvodov, ipd.

Slika 17: Število vlog za izdajo odločbe glede iznosa osebnih podatkov med letoma 2006 in 2011.



3.6. Izdajanje dovoljenj za povezovanje javnih evidenc

Povezovanje zbirk osebnih podatkov je urejeno v 84., 85. in 86. členu ZVOP-1. 84. člen ZVOP-1 določa, da če najmanj ena izmed zbirk osebnih podatkov, ki naj bi se jih povezovalo, vsebuje občutljive osebne podatke ali če bi bila posledica povezovanja razkritje občutljivih podatkov ali je za povezovanje potrebna uporaba istega povezovalnega znaka, povezovanje brez predhodnega dovoljenja Informacijskega pooblaščenca ni dovoljeno. Ta povezavo dovoli na podlagi pisne vloge upravljavca osebnih podatkov, če ugotovi, da ta zagotavlja ustrezno zavarovanje osebnih podatkov. Postopki in ukrepi za njihovo zavarovanje morajo biti ustrezni glede na tveganje, ki ga predstavljata obdelava in narava nekaterih osebnih podatkov, ki se obdelujejo. Zoper odločbo Informacijskega pooblaščenca pritožba ni mogoča, dovoljen pa je upravni spor.

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.

Informacijski pooblaščenec je leta 2011 prejel 14 vlog za pridobitev dovoljenja za povezovanje zbirk osebnih podatkov. Izdanih je bilo osem odločb, od tega dve za vlogi, prejeti leta 2010. En vlagatelj je svoj zahtevek za izdajo odločbe o povezovanju zbirk osebnih podatkov umaknil. Informacijski pooblaščenec je šestim upravljavcem zbirk osebnih podatkov dovolil povezovanje z drugo ali drugimi zbirkami osebnih podatkov, enemu upravljavcu je delno ugodil, v enem primeru pa povezovanja zbirk ni dovolil. V okviru povezave zbirk osebnih podatkov se lahko posredujejo oziroma obdelujejo tiste vrste osebnih podatkov, ki jih določa veljavna zakonodaja oziroma je za pridobivanje in obdelavo osebnih podatkov podana pisna privolitev posameznikov, na katere se podatki nanašajo (slednje velja le pri Cetis, d.d.).

Vrhovnemu sodišču Republike Slovenije in Ministrstvu za notranje zadeve je Informacijski pooblaščenec dovolil vzpostavitev neposredne računalniške povezave med Informatizirano glavno knjigo zemljiške knjige (e-Zemljiška knjiga) ter Centralnim registrom prebivalstva. Kot povezovalni znak se uporabi EMŠO.

Nosilcu javnega pooblastila, družbi Cetis, d.d., in Ministrstvu za notranje zadeve je Informacijski pooblaščenec dovolil neposredno računalniško povezavo naslednjih zbirk osebnih podatkov:
- Evidenca izdanih kartic,
- Matični register,
- Register stalnega prebivalstva,
- Evidenca voznikov.

Povezava med zbirkami osebnih podatkov se lahko izvede na način, da se kot povezovalni znak uporabi EMŠO.

Splošni bolnišnici Izola in Ministrstvu za notranje zadeve je Informacijski pooblaščenec dovolil, da v okviru aplikacije e-Rojstva povežeta naslednje zbirke osebnih podatkov:
- Osnovno medicinsko dokumentacijo,
- Centralni register prebivalstva ter
- Matični register.

Kot povezovalni znak se uporabi EMŠO.

Ministrstvu za šolstvo in šport in Ministrstvu za notranje zadeve je Informacijski pooblaščenec dovolil vzpostavitev neposredne računalniške povezave med Centralno evidenco udeležencev vzgoje in izobraževanja ter Centralnim registrom prebivalstva. Povezava se lahko izvede z uporabo EMŠO.

Splošni bolnišnici Murska Sobota in Ministrstvu za notranje zadeve je Informacijski pooblaščenec dovolil, da v okviru aplikacije e-Rojstva povežeta naslednje zbirke osebnih podatkov:
- Osnovno medicinsko dokumentacijo,
- Centralni register prebivalstva ter
- Matični register.

Kot povezovalni znak se uporabi EMŠO.

Informacijski pooblaščenec je Ministrstvu za delo, družino in socialne zadeve dovolil, da Centralno zbirko podatkov o pravicah iz javnih sredstev poveže z:

- zbirkami osebnih podatkov, ki se vodijo v okviru Informacijskega sistema Centrov za socialno delo, katerih upravljavec je Ministrstvo za delo, družino in socialne zadeve,
- zbirkami osebnih podatkov, ki se vodijo v okviru Informacijskega sistema KURIR, katerih upravljavec je Ministrstvo za delo, družino in socialne zadeve,
- zbirkami osebnih podatkov Ministrstva za notranje zadeve, in sicer s Centralnim registrom prebivalstva, Evidenco gospodinjstev, Evidenco registriranih motornih in priklopnih vozil ter z Evidenco nadomestil in prejemkov na podlagi pogodbe o prostovoljni službi v pomožni policiji,
- zbirkama osebnih podatkov Ministrstva za finance, Davčne uprave Republike Slovenije, in sicer z Evidenco o davkih ter z Davčnim registrom,
- zbirkama osebnih podatkov Javnega jamstvenega in preživninskega sklada Republike Slovenije, in sicer z Evidenco o nadomestilih preživnine ter z Evidenco o pravicah iz naslova insolventnosti delodajalca,
- zbirkama osebnih podatkov Ministrstva za pravosodje, Uprave Republike Slovenije za izvrševanje kazenskih sankcij, in sicer s Centralno evidenco o osebah na prestajanju kazni zapora ter s Centralno evidenco o osebah, ki jim je izrečen vzgojni ukrep oddaje mladoletnika v prevzgojni dom,
- zbirko osebnih podatkov Centralno klirniško depotne družbe, d.d., in sicer s Centralnim registrom nematerializiranih vrednostnih papirjev,
- zbirkami osebnih podatkov Ministrstva za okolje in prostor, Geodetske uprave Republike Slovenije, in sicer z Zemljiškim katastrom, s Katastrom stavb ter z Registrom nepremičnin,
- zbirkama osebnih podatkov Zavoda za pokojninsko in invalidsko zavarovanje Slovenije, in sicer z Matično evidenco o zavarovancih ter z Matično evidenco zavarovancev in uživalcev pravic iz pokojninskega in invalidskega zavarovanja,
- zbirko osebnih podatkov Zavoda za zdravstveno zavarovanje Slovenije, in sicer z Evidenco o zavarovanih osebah obveznega zdravstvenega zavarovanja,
- zbirkami osebnih podatkov Agencije Republike Slovenije za javnopravne evidence in storitve, in sicer s Poslovnim registrom Slovenije, z Registrom transakcijskih računov ter z Zbirko letnih poročil,
- zbirko osebnih podatkov Ministrstva za promet, Uprave Republike Slovenije za pomorstvo, in sicer z Vpisnikom čolnov,
- zbirkami osebnih podatkov Zavoda Republike Slovenije za zaposlovanje, in sicer z Evidenco brezposelnih oseb, z Evidenco oseb, vključenih v programe aktivne politike zaposlovanja, z Evidenco iskalcev zaposlitve ter z Evidenco invalidov, ki jim je bila izdana odločba, da niso zaposljivi,
- zbirko osebnih podatkov Vrhovnega sodišča Republike Slovenije, in sicer z Informatizirano glavno knjigo zemljiške knjige,
- zbirko osebnih podatkov Ministrstva za obrambo, in sicer z Vojaško evidenco.

Povezava med zbirkami se lahko izvede tako, da se kot povezovalni znak uporabi EMŠO ali davčna številka. Pri pridobivanju podatkov iz zbirke osebnih podatkov Ministrstva za obrambo (Vojaška evidenca) je poleg uporabe istega povezovalnega znaka (EMŠO ali davčna številka) obvezna uporaba vsaj še enega podatka, npr. osebnega imena ali kraja bivališča posameznika. Odločba Informacijskega pooblaščenca še ni pravnomočna, saj je Vrhovno sodišče Republike Slovenije zoper odločbo vložilo tožbo na Upravno sodišče Republike Slovenije.

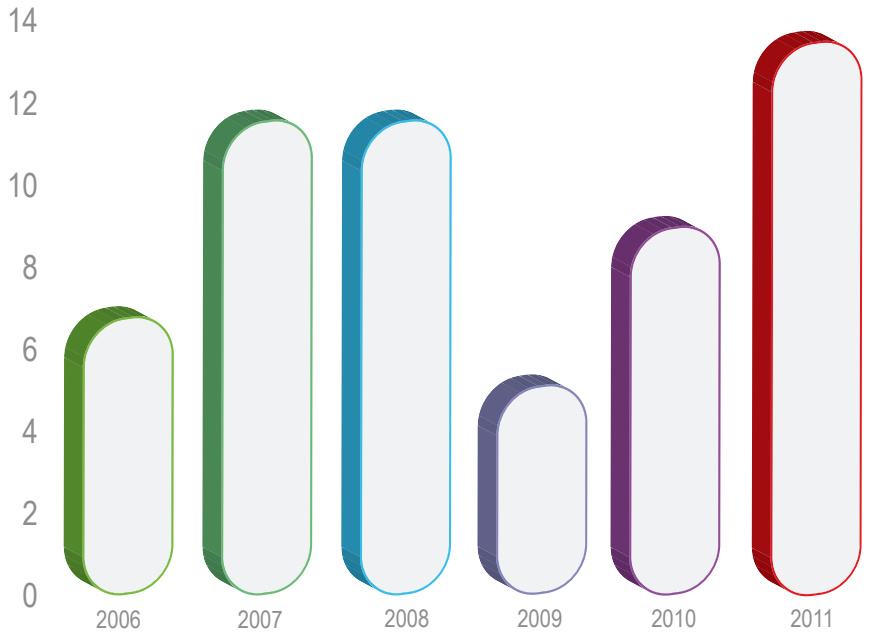
Inštitutu za varovanje zdravja Republike Slovenije in Ministrstvu za notranje zadeve je Informacijski pooblaščenec dovolil, da zbirko osebnih podatkov Zdravniško poročilo o umrli osebi (IVZ 46) ter zbirko osebnih podatkov Register obveznikov za cepljenje in izvajanje cepljenja (IVZ 49) vsako posebej povežeta s Centralnim registrom prebivalstva. Kot povezovalni znak se uporabi EMŠO.

Zahtevek Inštituta za varovanje zdravja za izdajo dovoljenja za povezavo Zbirke Programa SVIT (Državni program presejanja in zgodnjega odkrivanja predrakavih sprememb in raka na debelem črevesu in danki) s Centralnim registrom prebivalstva, katerega upravljavec je Ministrstvo za notranje zadeve, je Informacijski pooblaščenec zavrnil, ker Zbirko Programa SVIT ni mogoče šteti kot uradno evidenco, saj je področna zakonodaja ne določa. Za evidence, ki jih ne določa zakon, ni mogoče izdati dovoljenja za povezavo s Centralnim registrom prebivalstva.

Informacijski pooblaščenec je zavrnil zahtevek Ministrstva za finance, Davčne uprave Republike Slovenije, za izdajo dovoljenja za povezavo Evidence zaposlenih v Davčni upravi Republike Slovenije s Centralno kadrovsko evidenco, katere upravljavec je Ministrstvo za javno upravo. Zahtevek je bil zavrnjen, ker za nameravano povezovanje zbirk osebnih podatkov ni ustrezne zakonske podlage.

Ministrstvo za okolje in prostor je Informacijskemu pooblaščencu posredovalo obvestilo, da je povezalo zbirko osebnih podatkov Evidenca razgrajenih izrabljenih vozil z Evidenco registriranih vozil, katere upravljavec je Ministrstvo za notranje zadeve. Kot povezovalni znak se uporabi številka šasije vozila, zato odločba Informacijskega pooblaščenca, s katero bi izdal dovoljenje za povezovanje zbirk, v tem primeru ni potrebna, ampak v skladu z drugim odstavkom 84. člena ZVOP-1 zadošča obvestilo o nameravanem povezovanju zbirk osebnih podatkov.

Slika 18: Število vlog za izdajo odločbe glede povezljivosti zbirk osebnih podatkov med letoma 2006 in 2011.



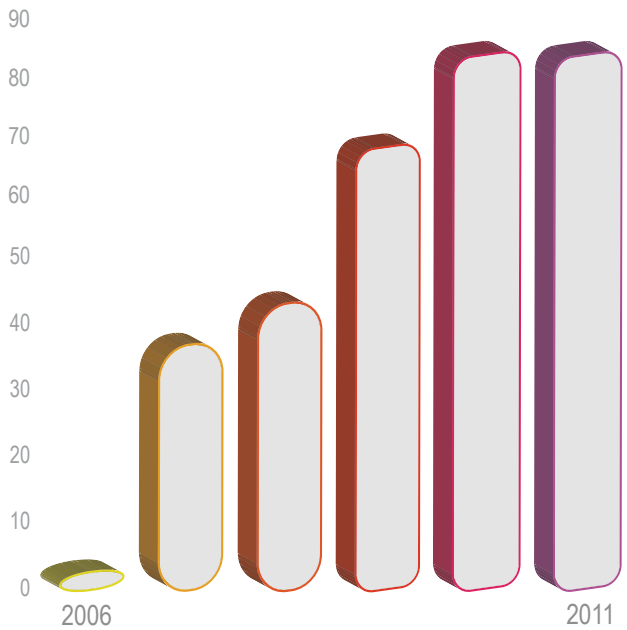
3.7. Seznanitev z lastnimi osebnimi podatki

Informacijski pooblaščenec je leta 2011 prejel 85 pritožb v zvezi s pravico do seznanitve z lastnimi osebnimi podatki, kar pomeni, da je število pritožb ostalo na isti ravni kot leta 2010. Leta 2008 je Informacijski pooblaščenec prejel 48 pritožb, leta 2009 pa 70. V skladu s tretjim odstavkom 38. člena Ustave je posamezniku zagotovljena pravica do seznanitve z zbranimi osebnimi podatki, ki se nanašajo nanj. Pravica posameznika do seznanitve z lastnimi osebnimi podatki je konkretizirana v ZVOP-1, v 30. in 31. členu.

V okviru pritožbenih postopkov v zvezi s seznanitvijo z lastnimi osebnimi podatki je Informacijski pooblaščenec reševal tudi pritožbe, ko posamezniki niso pridobili zdravstvene dokumentacije po ZPacP. Teh je bilo leta 2009 osem, leta 2010 štiri, leta 2011 pa 18 takih pritožb. Informacijski pooblaščenec je prejel dve pritožbi v zvezi z vpogledom v osebne podatke v Schengenskem informacijskem sistemu (SIS) in v zbirko osebnih podatkov Interpola.

Informacijski pooblaščenec opaža, da se je v primerjavi z letom 2010 povečalo število molkov upravljavcev osebnih podatkov, ko upravljavci na zahtevo posameznika v zvezi s seznanitvijo z lastnimi osebnimi podatki sploh ne odgovorijo. Leta 2010 je bilo pritožb zaradi molka 38 %, leta 2011 pa 52 %. Posameznik lahko v primeru molka upravljavca, pa tudi v primeru zavrnitve seznanitve vloži pritožbo Informacijskemu pooblaščencu.

Slika 19: Število pritožb v zvezi s pravico do seznanitve z lastnimi osebnimi podatki med letoma 2006 in 2011.

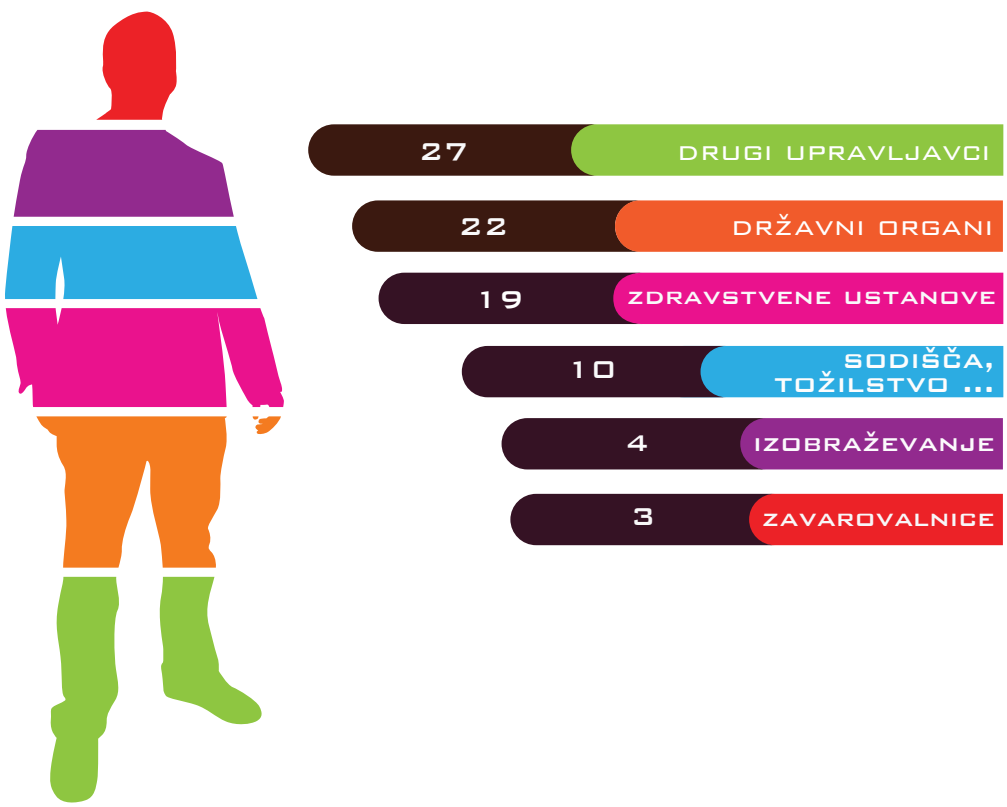


Vložene pritožbe zaradi zavrnitve seznanitve z lastnimi osebnimi podatki so zadevale naslednje skupine upravljavcev osebnih podatkov:

- državni organi, ministrstva in organi v njihovi sestavi (22),
- zdravstvene ustanove (19),
- sodišča, državno tožilstvo in državno pravobranilstvo (10),
- izobraževalne institucije (4),
- zavarovalnice (3),
- drugi upravljavci, npr. društva (27).

V šestih primerih so posamezniki vložili pritožbe, ker jim seznanitve z lastnimi osebnimi podatki niso omogočili njihovi delodajalci.

Slika 20: Pritožbe v zvezi s pravico do seznanitve z lastnimi osebnimi podatki glede na upravljavca osebnih podatkov leta 2011.



Informacijski pooblaščenec je po prejemu pritožbe najprej pozval upravljavca osebnih podatkov, da pojasni, zakaj posamezniku ni odgovoril ali zakaj mu ni omogočil seznanitve z osebnimi podatki. V 16 primerih so upravljavci posameznikom omogočili vpogled v zahtevane podatke ali pa so jim posredovali odgovor in zahtevane dokumente takoj po pozivu Informacijskega pooblaščenca, 13 upravljavcem je Informacijski pooblaščenec z odločbo naložil, da morajo prosilcu omogočiti seznanitev z lastnimi osebnimi podatki. Informacijski pooblaščenec je 15 pritožb posameznikov z odločbo zavrnil, ker njihove vloge niso predstavljale pritožbe zaradi zavrnitve seznanitve z lastnimi osebnimi podatki ali niso bile utemeljene, devet pritožb je s sklepom zavrgel, ker so bile nepopolne ali preuranjene, sedmim vlagateljem pa je svetoval, kako naj postopajo. Informacijski pooblaščenec je devet pritožb odstopil v reševanje pristojnim organom, štirje posamezniki pa so svoje pritožbe umaknili.

V enem primeru je Informacijski pooblaščenec reševal pritožbo zaradi previsokih stroškov, ki jih je upravljavec zaračunal posamezniku. Informacijski pooblaščenec je upravljavcu z odločbo naložil, da mora posamezniku vrniti previsoko zaračunani znesek, saj lahko upravljavci zaračunajo stroške le v skladu s Pravilnikom o zaračunavanju stroškov pri izvrševanju pravice posameznika do seznanitve z lastnimi osebnimi podatki[35].

V letu 2011 je pet upravljavcev zoper odločbo Informacijskega pooblaščenca vložilo tožbo na Upravno sodišče Republike Slovenije, v enem primeru pa je upravni spor sprožil prosilec zaradi sklepa o zavrženju pritožbe. V preteklem letu je Upravno sodišče Republike Slovenije odločilo v šestih zadevah, in sicer je v treh zadevah tožbo zoper odločbo Informacijskega pooblaščenca zavrnilo, v treh primerih pa je tožbi ugodilo, izpodbijano odločbo odpravilo in zadevo vrnilo Informacijskemu pooblaščencu v ponovno odločanje.

Zaradi potrebe po popolni ugotovitvi dejanskega stanja (ogled razpoložljivega dokumentarnega gradiva) je Informacijski pooblaščenec v prostorih upravljavcev osebnih podatkov opravil devet ogledov, na katere so bili vabljeni tudi prosilci.

3.8. Zahteve za presojo ustavnosti zakonov

Informacijski pooblaščenec lahko z zahtevo začne postopek za oceno ustavnosti oziroma zakonitosti predpisov na podlagi 23.a člena Zakona o Ustavnem sodišču[36], če se pojavi vprašanje ustavnosti ali 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 Ustavno sodišče, ampak se mora zahteva nanašati na konkreten postopek.

Leta 2011 je Informacijski pooblaščenec vložil zahtevo za oceno ustavnosti prvega in drugega odstavka 114. člena Zakona o evidentiranju nepremičnin[37], ki določata javnost imena, priimka, naslova stalnega prebivališča in letnice rojstva posameznikov, ki so kot lastniki nepremičnin vpisani v kataster stavb in zemljiški kataster, ter 117. člena ZEN, ki določa, da geodetska uprava v distribucijskem okolju zagotavlja podatke iz evidenc, ki jih vodi po tem zakonu, lahko pa tudi podatke, ki jih pridobi v skladu z zakonom iz drugih zbirk podatkov, in dodatno obdelane ali povezane podatke.

Informacijski pooblaščenec je Ustavnemu sodišču Republike Slovenije predlagal, da navedene določbe spozna za neskladne z Ustavo, saj zakon ne določa namena javnosti osebnih podatkov iz obeh katastrov, kar bi v skladu z določbo 38. člena Ustave moral. Poleg tega zakon ne opredeljuje pojma »distribucijsko okolje«, kar (javno) obdelavo osebnih podatkov posameznikov postavlja v še bolj negotov položaj. V zahtevi je Informacijski pooblaščenec želel Ustavnemu sodišču prikazati, da navedene zakonske določbe ne prestanejo ustavnega testa sorazmernosti, ki se zahteva za poseg v človekove pravice (v konkretnem primeru gre za poseg v pravico do varstva osebnih podatkov), in da bi le z odločitvijo o neskladnosti izpodbijanih določb z Ustavo sledilo svoji dosedanji praksi in praksi Sodišča Evropske unije.

Ustavno sodišče je namreč že ob odločanju o javnosti osebnih podatkov iz registra nepremičnin ugotovilo, da neskladnost z Ustavo pomeni že dejstvo, da zakon ne določa namena, saj če zakon ne določa namena javnosti osebnih podatkov, se ti podatki lahko

35 Uradni list RS, št. 85/2007 in 5/2012.
36 Uradni list RS, št. 64/2007 – uradno prečiščeno besedilo 1, s spremembami.
37 Uradni list RS, št. 47/2006, s spremembami, v nadaljevanju ZEN.

uporabljajo za kakršen koli namen, kar je samo po sebi v nasprotju z Ustavo. Informacijski pooblaščenec je izpostavil razlikovanje med ustreznostjo javnosti zemljiške knjige, ki ima namen v varnosti pravnega prometa z nepremičninami (kar opredeljuje že Zakon o zemljiški knjigi[38] , vsekakor pa to izhaja iz dejstva, da je zemljiška knjiga izvorna evidenca za podatke o pravicah na nepremičninah), in neustavnostjo javnosti obeh katastrov (ker namen javnosti v zakonu ni opredeljen in niti ne izhaja iz narave obeh katastrov, ki sta izvorni evidenci za podatke o nepremičnini kot predmetu pravic). Razlika je tudi v določnosti ZZK-1 in nedoločnosti ZEN glede načina dostopa do osebnih podatkov.

Nejasnost določbe 117. člena ZEN je v praksi pripeljala do tega, da si geodetska uprava kot »distribucijsko okolje« predstavlja spletni portal, preko katerega po lastni presoji združuje in na različne načine javno prikazuje osebne podatke, za katere zakon sploh ne določa namena javnosti. Informacijski pooblaščenec pa meni, da je nedopustno »distribucijsko okolje« razumeti kot svetovni splet, saj mora biti država pri posredovanju osebnih podatkov velikega števila posameznikov v svetovni splet izrazito previdna in restriktivna, najmanj pa mora spoštovati lastno ustavo in v zakonu določiti namen oziroma legitimen cilj, ki neizogibno terja javno objavo osebnih podatkov in ki ga drugače kot z javno objavo osebnih podatkov v svetovnem spletu ni mogoče doseči, koristi, ki jih prinaša doseganje legitimnega cilja, pa so večje od škode, ki posameznikom nastane s tem, ko da država njihove osebne podatke javnosti na voljo v svetovni splet. Tolikšna nejasnost zakonskih določb, kadar gre za obdelavo osebnih podatkov (še toliko bolj kadar gre za javno objavo osebnih podatkov v svetovnem spletu) pa je po mnenju Informacijskega pooblaščenca sama po sebi v neskladju z Ustavo.

Informacijski pooblaščenec je istočasno izpodbijal tudi Pravilnik o vrstah in vsebini potrdil iz zbirk geodetskih podatkov ter o načinu izkazovanja podatkov[39] v delih, kjer določa izdajanje t. i. lastninskega lista. Lastninski list je v skladu s Pravilnikom eden od potrdil iz zbirk geodetskih podatkov, ki vsebuje podatke o parcelah, stavbah in delih stavb, ki so v lasti ali v solastnini istega lastnika, ne glede na delež solastništva. Glede na to, da ima v skladu s 115. členom ZEN vsakdo pravico pridobiti potrdila, ki se izdajajo v skladu s Pravilnikom (ki je bil sprejet na podlagi 115. člena ZEN), torej Pravilnik določa obdelavo osebnih podatkov – posredovanje seznama vsega nepremičnega premoženja vsakomur – obdelavo osebnih podatkov pa sme v skladu z 38. členom Ustave določati le zakon in ne podzakonski akt.

Ustavno sodišče je zahtevo prevzelo v absolutno prednostno obravnavo, vendar do izdaje letnega poročila odločitve še ni sprejelo.

3.9. Izbrani primeri kršitev varstva osebnih podatkov

V nadaljevanju je predvsem s preventivnega vidika predstavljenih nekaj inšpekcijskih postopkov iz leta 2011 in pogosti primeri kršitev določb ZVOP-1.

3.9.1. Neustrezno zavarovanje osebnih podatkov na spletnem forumu

Informacijski pooblaščenec je prejel prijavo, iz katere je izhajalo, da so na določeni spletni strani objavljena uporabniška imena, naslovi elektronske pošte in gesla uporabnikov spletnega mesta za iskanje partnerjev. Informacijski pooblaščenec je uvedel inšpekcijski postopek, v katerem je uspešno identificiral storilca, ki je navedene podatke objavil na svoji spletni strani, prav tako pa je pri upravljavcu spletnega mesta opravil inšpekcijski ogled. Ugotovljeno je bilo, da je upravljavec izdelavo spletnega mesta zaupal določenemu indijskemu podjetju, ki pri tem ni upoštevalo zahtev slovenske zakonodaje, saj končni izdelek ni zagotavljal sledljivosti obdelave osebnih podatkov, prav tako pa je bilo pri programiranju storjenih kar nekaj napak, ki so storilcu omogočile, da je pridobil podatke o skoraj 7000 uporabnikih te strani, vključno z uporabniškimi imeni in gesli. Upravljavec spletnega mesta je prav tako zanemaril zakonske dolžnosti glede ureditve pogodbene obdelave osebnih podatkov z indijskim podjetjem, saj z njim ni sklenil ustrezne pisne pogodbe, prav tako pa je prišlo do iznosa osebnih podatkov v tretjo državo brez ustrezne zakonske podlage.

[38] Uradni list RS, št. 58/2003, s spremembami, v nadaljevanju ZZK-1.
[39] Uradni list RS, št. 22/2007 in 33/2009, v nadaljevanju Pravilnik.

Informacijski pooblaščenec je upravljavcu izdal ureditveno odločbo, s katero je začasno ustavil delovanje spletnega mesta in upravljavcu naložil, da o incidentu obvesti vse uporabnike spletnega mesta. Upravljavec spletnega mesta se je odločil, da zaradi tolikšnega števila napak spletnega mesta ne bo vzpostavil nazaj. Gre za očiten primer, kjer se lahko upravljavcem, ki se odločajo za cenene rešitve tujih ponudnikov, ki ne spoštujejo zahtev lokalne zakonodaje, na koncu izkaže, da so izbrali slabo in na koncu dražjo rešitev.

3.9.2. Nezakonito snemanje telefonskih pogovorov

Informacijski pooblaščenec je na podlagi prejete prijave zaradi suma nezakonite obdelave osebnih podatkov – nezakonitega snemanja telefonskih razgovorov pri zavezancu, ki se med drugim ukvarja s trženjem svojih storitev in produktov po telefonu, uvedel postopek inšpekcijskega nadzora. V okviru tega je bilo ugotovljeno, da je zavezanec izvajal snemanje telefonskih pogovorov v svojem klicnem studiu, in sicer tako dohodnih kot odhodnih klicev. Pri dohodnih klicih je bila stranka takoj, pred začetkom telefonskega pogovora, obveščena o tem, da se pogovor snema, medtem ko pri odhodnih klicih s snemanjem telefonskega pogovora ni bila seznanjena. Zavezanec je odhodne klice snemal z namenom internega spremljanja kakovosti storitve in lažjega reševanja reklamacij, ne pa tudi zaradi dokazovanja opravljene tržne transakcije oziroma opravljene poslovne komunikacije s stranko. Zavezanec je posnetke dohodnih klicev hranil eno leto, odhodnih pa tri mesece, dostop do posnetkov pa so imeli koordinatorji dela telefonskih svetovalcev zaradi opravljanja analiz in izobraževanja telefonskih svetovalcev ter vodja službe zaradi reševanja reklamacij.

Ker ZVOP-1 v 8. členu določa, da se osebni podatki lahko obdelujejo le, če obdelavo osebnih podatkov in osebne podatke, ki se obdelujejo, določa zakon ali če je za obdelavo določenih osebnih podatkov podana osebna privolitev posameznika, ZEKom pa snemanje telefonskih pogovorov dopušča le v primerih, kadar gre za namen zagotavljanja dokazov o tržnih transakcijah ali drugih poslovnih komunikacijah oziroma ostalih komunikacij, ki so določene v petem in sedmem odstavku 103. člena ZEKom, medtem ko snemanje za druge namene, kljub predhodnemu obvestilu ni dovoljeno, je Informacijski pooblaščenec z odločbo zavezancu prepovedal snemanje odhodnih klicev, razen v primerih, ko klicani posameznik jasno izrazi, da želi postati naročnik neke storitve oziroma produkta in ob tem poda jasno in izrecno soglasje, da se s snemanjem strinja, pri čemer mora biti obveščen o namenu snemanja komunikacije ter o času hrambe posnetka. Zavezanec je v odrejenem roku za izvršitev ukrepa Informacijskega pooblaščenca obvestil, da je prenehal izvajati snemanje vseh odhodnih klicev. Zaradi nezakonite obdelave osebnih podatkov – nezakonitega snemanja telefonskih razgovorov je bil zavezancu izrečen ukrep po ZP-1.

3.9.3. Nezakonit vpogled v Evidenco registriranih motornih in priklopnih vozil

Informacijski pooblaščenec je prejel prijavo zaradi suma nezakonite obdelave osebnih podatkov – nezakonitega vpogleda v Evidenco registriranih motornih in priklopnih vozil. Prijavitelj je namreč na podlagi 30. člena ZVOP-1, ki določa pravico posameznika glede seznanitve z lastnimi osebnimi podatki, od Ministrstva za promet, ki upravlja in vodi Evidenco registriranih motornih in priklopnih vozil, pridobil seznam uporabnikov njegovih osebnih podatkov, povezanih z lastništvom vozila, in ugotovil, da so bili določeni vpogledi v podatke opravljeni na izpostavah, ki jih ni nikoli obiskal in ki niso imele potemtakem nobenega razloga za vpogled v navedene podatke.

Informacijski pooblaščenec je zoper uporabnike, ki so izvršili vpogled, uvedel postopek inšpekcijskega nadzora. Pri tem je bilo ugotovljeno, da je v enem primeru prišlo do nezakonitega vpogleda v podatke o lastniku motornega vozila, saj je uslužbenec, ki je imel dostop do Evidence registriranih motornih in priklopnih vozil, želel pridobiti podatke o stanju in lastništvu vozila potem, ko je vozilo opazil med prodajnimi oglasi za rabljena vozila. Uslužbenec je pri tem ravnal na »svojo roko« in v nasprotju s sprejetimi akti zavezanca, ki določajo dolžnost varovanja ter spoštovanja zaupnosti podatkov, ter seveda v nasprotju z določbami ZVOP-1, ki določa, da se osebni podatki lahko zbirajo le za določene in zakonite namene ter se ne smejo nadalje obdelovati tako, da bi bila njihova obdelava v neskladju s temi nameni, če zakon ne določa drugače. Zato je Informacijski pooblaščenec uslužbencu kot odgovorni osebi pravne osebe (zavezanca) izrekel globo.

3.9.4. *Izvajanje neposrednega trženja na podlagi podatkov iz Centralnega registra psov*

Informacijski pooblaščenec vsako pomlad že več let dobiva prijave zaradi suma nezakonitega pridobivanja osebnih podatkov lastnikov psov za namen neposrednega trženja. Ugotovljeno je bilo, da veterinarske ambulante lastnikom psov pošiljajo obvestila o cepljenju psov proti steklini, v katerih jih obveščajo, da razpisujejo splošno cepljenje psov proti steklini v določenem obdobju, večkrat pa lastnikom psov hkrati ponujajo tudi druge storitve (npr. cepljenje proti kužnim boleznim, sterilizacija, kastracija).

Ker so prijavitelji navedli, da niso stranke ambulant, od katerih so prejeli vabila, je Informacijski pooblaščenec v postopku inšpekcijskega nadzora ugotavljal vir pridobitve osebnih podatkov lastnikov psov. Ugotovljeno je bilo, da so veterinarske ambulante osebne podatke, ki so jih uporabile za namen neposrednega trženja, pridobile iz Centralnega registra psov (v nadaljevanju CRPsi), katerega upravljavec je Veterinarska uprava Republike Slovenije (v nadaljevanju VURS). Pri ugotavljanju nezakonitega dostopa do osebnih podatkov lastnikov psov v navedenem registru je bila VURS v veliko pomoč, saj je Informacijskemu pooblaščencu posredovala dnevnike sledljivosti obdelav osebnih podatkov lastnikov psov v navedenem registru s strani določene veterinarske ambulante za določeno obdobje. Iz teh dnevnikov je bilo razvidno, kdo in kdaj je dostopal do določenih osebnih podatkov v CRPsi. CRPsi nima statusa javnega registra, kar pomeni, da osebni podatki lastnikov psov niso prosto dostopni in se lahko uporabijo le v skladu z zakonsko določenimi nameni (vodenje evidenc psov in lastnikov psov, nadzor nad izvajanjem rednih cepljenj in kontrola ob ugrizih, statistični nameni). Izven opisanih namenov vpogled v podatke ali uporaba podatkov ni dopustna, kar pomeni, da veterinarske ambulante podatkov lastnikov psov in podatkov o cepljenjih ne smejo uporabljati za namene neposrednega trženja, čeprav imajo za namen opravljanja svoje dejavnosti do njih dostop. Veterinarske ambulante lahko za namen neposrednega trženja uporabljajo le osebne podatke tistih lastnikov psov, ki so njihove stranke oziroma ki jih pridobijo v okviru zakonitega opravljanja dejavnosti in podatke, ki jih dobijo iz javno dostopnih virov. Informacijski pooblaščenec za zlorabo osebnih podatkov iz CRPsi za namene neposrednega trženja veterinarski ambulanti in njeni odgovorni osebi izreče globo.

3.9.5. *Izvajanje neposrednega trženja na podlagi podatkov iz javno dostopnih evidenc o lastništvu nepremičnin*

Informacijski pooblaščenec je obravnaval primer, v katerem je ugotavljal zakonitost izvajanja neposrednega trženja geodetskih storitev, ko je podjetje svoje storitve ponujalo po navadni pošti posameznikom, za katere je pri pregledu evidenc na portalu prostor (http://e-prostor.si) ugotovilo, da njihova stavba nima evidentiranega zemljišča pod stavbo. 81. člen ZEN pa zahteva, da mora investitor v 30 dneh po izvedbi vseh zaključnih gradbenih del vložiti zahtevo za vpis stavbe v kataster stavb.

V skladu z določbami 72. člena ZVOP-1 lahko upravljavec osebnih podatkov (v konkretnem primeru geodetsko podjetje) za namene neposrednega trženja uporablja osebne podatke posameznikov, ki jih je zbral iz javno dostopnih virov ali v okviru zakonitega opravljanja dejavnosti. V konkretnem primeru je zavezanec, čeprav je podatke pridobil zakonito, tudi kršil določbe ZVOP-1, saj je za namen neposrednega trženja uporabil več podatkov, kot to dovoljuje drugi odstavek 72. člena, ki določa, da lahko upravljavec osebnih podatkov za namene neposrednega trženja uporablja le osebno ime, naslov stalnega ali začasnega prebivališča, telefonsko številko ter številko telefaksa, na podlagi osebne privolitve posameznika pa tudi druge osebne podatke. Zavezanec je za namen neposrednega trženja svojih storitev poleg imena, priimka in naslova posameznikov uporabil tudi podatek o tem, da kot lastniki nepremičnine svoje stavbe še niso vpisali v kataster stavb oziroma da njihova stavba nima evidentiranega zemljišča pod stavbo. V skladu z navedeno določbo bi za uporabo navedenega podatka moral imeti osebno privolitev posameznikov, na katere se nanaša osebni podatek. Geodetsko podjetje pri izvajanju neposrednega trženja ne sme razlikovati med posamezniki, katerih stavba ima evidentirano zemljišče pod stavbo, in med posamezniki, katerih stavba nima evidentiranega zemljišča pod stavbo, ampak lahko pošlje obvestilo o svojih storitvah vsem posameznikom v npr. nekem naselju. Informacijski pooblaščenec je kršitelju izrekel ukrep po ZP-1.

3.9.6. Zbiranje osebnih podatkov delavcev in kandidatov za zaposlitev

V inšpekcijskih postopkih, ki jih Informacijski pooblaščenec vodi zoper delodajalce, pregleda tudi personalne mape delavcev in preverja, katere osebne podatke delavcev delodajalec obdeluje. Informacijski pooblaščenec poudarja, da čeprav ZVOP-1 razlikuje med javnim in zasebnim sektorjem, veljajo na področju delovnega prava pri obdelavi osebnih podatkov delavcev enaka pravila za vse delodajalce. Osebni podatki delavcev se lahko obdelujejo le na podlagi zakona, to pa so Zakon o evidencah na področju dela in socialne varnosti[40] in Zakon o delovnih razmerjih[41], v javnem sektorju pa še Zakon o javnih uslužbencih[42]. Osebni podatki se lahko zbirajo, obdelujejo, uporabljajo in dostavljajo tretjim osebam samo, če je to določeno z zakonom ali če je to potrebno zaradi uresničevanja pravic in obveznosti iz delovnega razmerja ali v zvezi z delovnim razmerjem. To za vse delodajalce (tako v javnem kot tudi v zasebnem sektorju) pomeni, da ne morejo od delavca zahtevati katerihkoli osebnih podatkov, ampak morajo za vsak podatek izkazati, da ga zahteva ZEPDSV ali da je podatek nujno potreben zaradi uresničevanja pravic in obveznosti (delavca ali delodajalca) iz delovnega razmerja. Če delodajalec tega ne more izkazati, delavčevih osebnih podatkov ne sme obdelovati. Zbiranje osebnih podatkov tudi na podlagi osebne privolitve delavcev, na katero se sklicujejo številni delodajalci, ni dopustno. Delavec je namreč v položaju, ko je njegova avtonomija volje izrazito omejena in bo v strahu pred morebitnimi posledicami (izguba službe, mobing) posredoval zahtevane podatke, čeprav jih delodajalec ne potrebuje zaradi uresničevanja pravic in obveznosti iz delovnega razmerja. Zaradi tega položaja ni mogoče govoriti o pravi privolitvi (svobodna, prostovoljna), pač pa o prisili.

Če je Informacijski pooblaščenec ugotovil nezakonito obdelavo osebnih podatkov delavcev (največkrat so se takšni podatki nahajali na vprašalnikih, ki jih izpolnijo delavci ob sklenitvi pogodbe o zaposlitvi), je odredil njihov izbris. V skladu z ZDR se morajo osebni podatki delavcev, za zbiranje katerih ne obstaja več zakonska podlaga, takoj izbrisati in prenehati uporabljati.

Informacijski pooblaščenec opozarja še na pomembno razliko pri obdelavi osebnih podatkov med kandidati za zaposlitev in zaposlenimi delavci. Delodajalec lahko od kandidata za zaposlitev zbira le tiste osebne podatke, ki so potrebni za presojo o tem, ali ima kandidat ustrezna znanja in izkušnje za razpisano delovno mesto. Za ta namen delodajalec še ne potrebuje npr. EMŠO in davčne številke, številke transakcijskega računa, podatkov o otrocih. Ko delodajalec izbere kandidata in z njim sklene pogodbo o zaposlitvi, pa pridobi osebne podatke, ki jih mora obdelovati v evidencah v skladu z ZEPDSV, in vse ostale podatke, ki so potrebni za uresničevanje pravic in obveznosti iz delovnega razmerja (npr. podatke o otrocih za izračun letnega dopusta ali za ureditev zdravstvenega zavarovanja, konfekcijsko številko za delovno obleko). Delodajalec mora pri obdelavi osebnih podatkov kandidatov upoštevati načelo sorazmernosti, kar pomeni, da mora nabor podatkov prilagoditi delovnemu mestu.

Informacijski pooblaščenec je ugotovil tudi, da je veliko delodajalcev zahtevalo in hranilo kopije osebnih dokumentov delavcev za namen zagotavljanja točnosti in ažurnosti osebnih podatkov za pripravo pogodbe o zaposlitvi in vnos v kadrovske evidence, pri čemer pa kopije niso bile označene v skladu z ZOIzk ali ZPLD, poleg tega pa delodajalci niso razpolagali s pisnimi privolitvami delavcev, ki jih zahtevata navedena zakona. Informacijski pooblaščenec je v vseh primerih odredil uničenje kopij osebnih dokumentov. To pa ne pomeni, da delodajalec ob zbiranju osebnih podatkov nima pravice vpogledati v osebni dokument delavca in iz njega prepisati osebne podatke, za obdelavo katerih ima pravno podlago, saj mu to omogoča ZVOP-1 kot tudi ZOIzk in ZPLD.

3.9.7. Objava osebnih podatkov novorojenih otrok v občinskem glasilu in pošiljanje rojstnodnevnih čestitk občanom

Informacijski pooblaščenec je uvedel postopek inšpekcijskega nadzora zoper občino, ki je uredniškemu odboru za namen objave v občinskem glasilu posredovala osebne podatke otrok (ime in priimek, datum rojstva, naslov), rojenih v določenem letu. Občina se je med drugim sklicevala na to, da gre za osebne podatke otrok, katerih starši so vložili vlogo in

[40] Uradni list RS, št. 40/2006; v nadaljevanju ZEPDSV.
[41] Uradni list RS, št. 42/2002 s spremembami; v nadaljevanju ZDR.
[42] Uradni list RS, št. 63/2007 – uradno prečiščeno besedilo 3, s spremembami.

dobili enkratni denarni prispevek ob rojstvu otroka ter za osebne podatke otrok, za katere je občina plačevala otroško prehrano do 4. meseca starosti, torej gre le za otroke, katerim je iz občinskega proračuna namenila finančna sredstva.

Informacijski pooblaščenec je ugotovil, da občina za posredovanje podatkov otrok uredniškemu odboru občinskega glasila za namen objave ni imela pravne podlage. Dejstvo, da so starši iz občinskega proračuna prejeli enkratno denarno pomoč ob rojstvu otroka ali sredstva za prehrano otroka, ne pomeni, da so se s posredovanjem podatkov svojih otrok za namen objave v občinskem glasilu tudi strinjali. Ker starši ob podaji vloge za pridobitev občinskih sredstev niso bili izrecno seznanjeni z drugimi nameni obdelave osebnih podatkov, občina osebnih podatkov otrok brez privolitve staršev ne bi smela posredovati uredniškemu odboru za objavo v občinskem glasilu. Zato je občina tekom postopka dopolnila obrazec Vloga za enkratni prispevek ob rojstvu otroka s pisno izjavo starša, ali objavo podatkov novorojenčka v občinskem glasilu dovoli ali ne.

V zvezi z razkritjem podatkov o porabi občinskih proračunskih sredstev Informacijski pooblaščenec poudarja, da ZDIJZ v 6. členu določa, da se dostop do zahtevane informacije dovoli, če gre za podatke o porabi javnih sredstev. Podatki o višini izplačanih sredstev iz občinskega proračuna tako predstavljajo podatke o porabi javnih sredstev in so informacija javnega značaja, vendar pa osebni podatki otrok, ki so bili objavljeni v občinskem glasilu, ne predstavljajo informacij javnega značaja, ampak varovane osebne podatke po ZVOP-1. Informacije javnega značaja bi v konkretnem primeru predstavljala le osebna imena prejemnikov pomoči, torej staršev, in zneski, ki so jih od občine prejeli.

Informacijski pooblaščenec je izdal mnenje, v katerem je zaključil, da župani za obdelavo rojstnih podatkov svojih občanov za namen pošiljanja rojstnodnevnih čestitk nimajo zakonske podlage, čeprav je bil pred leti ravno s tem namenom spremenjen Zakon o lokalni samoupravi[43] - sprememba ZLS-O, ko je bila v 21. člen dodana nova, 18. točka. 21. člen ZLS namreč določa naloge, ki jih za zadovoljevanje potreb svojih prebivalcev opravlja občina, in za kar sme pridobivati in nadalje obdelovati osebne podatke občanov. Med naštetimi nalogami se nobena izrecno ne nanaša na pošiljanje rojstnodnevnih voščilnic in tudi sicer pošiljanja čestitk nikakor ne bi bilo moč razumeti kot nalogo, ki bi jo občina opravljala z namenom zadovoljevanja potreb svojih prebivalcev. V 18. točki drugega odstavka 21. člena ZLS je sicer določeno, da lahko občina podeljuje denarne pomoči in simbolične nagrade ob posebnih priložnostih ali obletnicah občanov, vendar pa po mnenju Informacijskega pooblaščenca s tem ni zajeto tudi pošiljanje rojstnodnevnih čestitk, saj pri tem ne gre za konkretno pomoč oziroma nagrado, ki jo občina podeljuje svojim občanom.

3.9.8. Obdelava osebnih podatkov kandidatov na volitvah

Informacijski pooblaščenec je ob pregledovanju spletnih strani Državne volilne komisije (v nadaljevanju zavezanec ali DVK) ugotovil, da so na njih objavljeni osebni podatki kandidatov na volitvah v Državni zbor leta 2008, 2004 in 2000 in lokalnih volitvah 2010, 2006 in 1998. Informacijski pooblaščenec je zato po uradni dolžnosti začel postopek inšpekcijskega nadzora nad izvajanjem določb ZVOP-1 in opravil inšpekcijski ogled spletne strani http://volitve.gov.si. Zavezanec je na navedeni spletni strani oziroma njenih podstraneh objavil naslednje osebne podatke kandidatov na državnozborskih volitvah: osebno ime, datum rojstva, kraj rojstva, naslov prebivališča, poklic in delo, ki ga opravlja.

Področni zakon, ki določa obdelavo osebnih podatkov kandidatov na volitvah, je Zakon o volitvah v državni zbor[44], ki določa nabor osebnih podatkov kandidatov, ki jih mora vsebovati predlog liste kandidatov (ime, priimek, rojstni podatki, poklic in delo, ki ga opravlja, in stalno prebivališče). Volilna komisija volilne enote nato sestavi sezname potrjenih list kandidatov v volilni enoti in sezname kandidatov, o katerih se glasuje v posameznih volilnih okrajih in jih najpozneje petnajst dni pred dnem glasovanja objavi v medijih ali na drug način, ki ga določi DVK, upoštevajoč načelo čim širše obveščenosti volivcev ter načelo gospodarnosti.

[43] Uradni list RS, št. 94/2007 – uradno prečiščeno besedilo 2, s spremembami – sprememba ZLS-O je v Uradnem listu RS, št. 76/2008, v nadaljevanju ZLS.

[44] Uradni list RS, št. 109/06 – uradno prečiščeno besedilo 1, s spremembami, v nadaljevanju ZVDZ.

ZVDZ ureja objavo osebnih podatkov kandidatov samo za čas pred volitvami, ne ureja pa objave osebnih podatkov tudi v času po volitvah, npr. koliko časa so ti podatki objavljeni. Zato je treba uporabiti ZVOP-1 kot sistemski predpis, ki na splošno ureja vsa vprašanja varstva osebnih podatkov, zlati 16. in 21. člen, ki opredeljujeta namen obdelave in rok hrambe osebnih podatkov. Osebni podatki kandidatov na preteklih državnozborskih volitvah so bili torej objavljeni za namen informirane oziroma svobodne odločitve volivcev, kateri listi oziroma kandidatu bodo namenili svoj glas. Iz določb ZVDZ ne izhaja kakšen drug namen objave obravnavanih osebnih podatkov kandidatov. Ker je namen obdelave osebnih podatkov – njihove objave na spletnih staneh - že bil dosežen, izida volitev pa ni mogoče izpodbijati z nobenim pravnim sredstvom več, mora zavezanec postopati po drugem odstavku 21. člena ZVOP-1 in osebne podatke kandidatov, ki so bili objavljeni na podlagi 61. člena ZVDZ, iz spletnih strani, ki jih upravlja oziroma nadzoruje njihovo vsebino, izbrisati. Zavezanec namreč nima več zakonske podlage za (nadaljnjo) obdelavo osebnih podatkov kandidatov na preteklih državnozborskih volitvah na način, da so ti še vedno, tudi po izpolnitvi namena, javno objavljeni na spletu. Zato je Informacijski pooblaščenec v delni odločbi odredil, da mora zavezanec iz spletnih strani izbrisati sezname potrjenih list kandidatov in sezname kandidatov, o katerih se je glasovalo v posameznih volilnih okrajih na državnozborskih volitvah v letih 2008, 2004 in 2000. O objavi osebnih podatkov kandidatov na preteklih lokalnih volitvah, na volitvah v Državni svet in volitvah Predsednika Republike Slovenije bo Informacijski pooblaščenec odločal posebej.

3.9.9. Razkrivanje osebnih podatkov pri pošiljanju elektronske pošte

Informacijski pooblaščenec je prejel več prijav zoper istega zavezanca, v katerih je bilo navedeno, da je zavezanec obvestila o neizbranosti kandidata za razpisano delovno mesto neizbranim kandidatom pošiljal po e-pošti tako, da so vsi neizbrani kandidati videli naslove elektronske pošte drugih neizbranih kandidatov – prejemnikov istega obvestila. Informacijski pooblaščenec je po pregledu elektronskega sporočila "Obvestilo o neizbiri" potrdil navedbe prijaviteljev.

Zavezanec je pojasnil, da so kandidati svoje vloge za razpisano prosto delovno mesto podali po elektronski pošti in po navadni pošti. Po zaključenem postopku izbire kandidata se je zavezanec zaradi racionalnega trošenja sredstev odločil, da pošlje obvestilo o neizbiri po elektronski pošti tistim kandidatom, ki so tudi svojo vlogo posredovali po elektronski pošti. Pojasnil je, da aplikacija, ki jo uporablja za evidentiranje dokumentarnega gradiva, predvideva tudi odpremo izhodne pošte preko elektronske pošte in da je bil prepričan, da posamezen prejemnik obvestila o neizbiri, ki je bil pri odpremi dokumenta uvrščen v polje »Obveščanje po pošti/Elektronska pošta«, ne bo videl preostalih naslovnikov (na enak način kot to omogoča skrita kopija v navadnem elektronskem sporočilu). Zavezanec je navedel, da do prve pritožbe neizbranega kandidata ni vedel, da je bilo elektronsko sporočilo poslano na takšen način. Noben uporabnik aplikacije ni vedel, da se v primeru pošiljanja več prejemnikom vidijo elektronski naslovi vseh prejemnikov. Zavezanec je takoj, ko je bil o dogodku obveščen (še pred uvedbo inšpekcijskega postopka), vsem prejemnikom obvestila o neizbiri poslal dopis, v katerem se je opravičil in pojasnil, kako je do dogodka prišlo. Tokrat je zavezanec dopis poslal preko druge aplikacije, ki omogoča pošiljanje preko skrite kopije. Poleg tega je zavezanec vsem svojim zaposlenim podal ustrezna navodila za pošiljanje elektronske pošte več prejemnikom. Informacijski pooblaščenec je zaradi neustreznega zavarovanja elektronskih naslovov pri pošiljanju zavezancu izrekel ukrep po ZP-1.

Informacijski pooblaščenec pripominja še, da je v preteklem letu vodil kar nekaj inšpekcijskih postopkov zaradi nezakonitega razkrivanja elektronskih naslovov. V vseh primerih je bilo ugotovljeno, da pošiljatelj elektronskega sporočila ni zagotovil zavarovanja uporabljenih elektronskih naslovov prejemnikov elektronskega sporočila, saj je elektronske naslove vpisal v rubriko »Za« (angleško »To«) ali pa v rubriko »Kp« (angleško »Cc«), s čimer je prejemnikom elektronskega sporočila razkril elektronske naslove vseh ostalih prejemnikov istega sporočila. Informacijski pooblaščenec zato opozarja, da je potrebno v takšnih primerih elektronske naslove prejemnikov navesti v rubriki »Skrito« (»Skp« oziroma »Bcc«), s čimer se zagotovi, da prejemniki ne vidijo elektronskih naslovov ostalih prejemnikov sporočila.

3.9.10. Prekomerno razkrivanje osebnih podatkov prosilcem za dostop do informacij javnega značaja

Informacijski pooblaščenec je v letu 2011 vodil tudi postopke inšpekcijskega nadzora zoper organe po ZDIJZ, ki so prosilcem posredovali informacije javnega značaja, pri čemer pa so razkrili tudi osebne podatke, ki ne predstavljajo informacij javnega značaja, ampak podatke, varovane po ZVOP-1.

V postopkih inšpekcijskega nadzora je bilo ugotovljeno, da so organi (zavezanci) pri anonimizaciji dokumentov, ki so bili predmet zahtev po ZDIJZ, pozabili izbrisati oziroma so spregledali določene osebne podatke (npr. pod rubriko vročiti niso izbrisali prejemnika dokumenta ali na kopiji dokumenta, ki dokazuje izobrazbo javnega uslužbenca, niso izbrisali dekliškega priimka javne uslužbenke). Tako so bili nepooblaščenim osebam – prosilcem po ZDIJZ razkriti osebni podatki (osebni podatki stranke v določenem postopku in osebni podatki javnega uslužbenca, ki niso povezani z delovnim razmerjem javnega uslužbenca), za razkritje katerih bi morala obstajati podlaga v zakonu. Položaj javnih uslužbencev, kot je bilo že večkrat navedeno, je specifičen, saj ima oseba, zaposlena v javnem sektorju, bistveno zmanjšano pričakovanje zasebnosti zaradi načela odprtosti delovanja javnih organov. Tako ime, naziv, položaj, plača, službeni naslov in tisti deli iz uspešne prijave na delovno mesto, ki izkazujejo kvalifikacije osebe, potrebne za določeno delovno mesto, niso varovani osebni podatki, ampak dostopni vsakomur.

Če zahtevani dokumenti vsebujejo informacije javnega značaja, ima do njih v skladu z določili ZDIJZ dostop vsakdo. Edini razlog za zavrnitev dostopa je v teh primerih morebitni obstoj kakšne izmed izjem, ki jih določa zakon, med njimi so tudi osebni podatki. Če dokumenti vsebujejo varovane osebne podatke, mora organ, če je to možno, izvesti delni dostop do zahtevane dokumentacije na način, da v dokumentu prekrije varovane osebne podatke, pri čemer mora paziti, da delno razkritje ne bi ogrozilo zaupnosti varovanih informacij oziroma da iz preostalih podatkov v dokumentih ne bo mogoče določiti posameznih oseb, na katere se dokumenti nanašajo, hkrati pa mora paziti, da prekritje oziroma izločitev podatkov ne bi ogrozila zaupnosti dokumenta.

3.9.11. Objava fotografij, na katerih so določljivi posamezniki

Informacijski pooblaščenec je v letu 2011 končal postopek, v katerem je z vidika ZVOP-1 presojal prostorske fotografije, ki jih je na splet objavil zavezanec. Predmet postopka so bile prostorske fotografije, na katerih so se nahajali tudi določljivi posamezniki. Inšpekcijski postopek je bil sicer ustavljen, ker je zavezanec brez zahteve Informacijskega pooblaščenca s spleta neselektivno umaknil vse prostorske fotografije, posnete v Sloveniji.

V postopku so bile obravnavane prostorske fotografije razdeljene v tri skupine, glede na namen njihove objave in glede na to, ali so na njih tudi določljivi posamezniki. V prvo skupino fotografij sodijo tiste, na katerih ni določljivih posameznikov. Informacijski pooblaščenec se s to skupino fotografij ni ukvarjal, saj so predmet varstva osebnih podatkov posamezniki in njihovi osebni podatki.

Drugo skupino predstavljajo fotografije, ki po svoji vsebini tvorijo slikovni prikaz poročanja o nekem dogodku (teki, festivali, javna družabna srečanja...), na njih pa so tudi določljivi posamezniki. Objava takšnih fotografij iz vidika varstva osebnih podatkov praviloma ni sporna. V tem primeru zakoniti interes fotografa za objavo fotografije, npr. njegovo umetniško ustvarjanje in publicistično udejstvovanje, prevlada nad interesom posameznika, ki se udeleži nekega dogodka, pri tem pa je tudi slikovno zabeležen.

Tretjo skupino pa sestavljajo fotografije, katerih namen je prikazati geografsko lokacijo, posamezne dele naselij oziroma arhitekturo, na njih pa se nahajajo tudi določljivi posamezniki, fotografija pa ne beleži nekega posebnega dogodka. V zvezi s to skupino fotografij Informacijski pooblaščenec meni, da se da zasledovani namen, torej na spletu objavljen prikaz posameznega dela naselja, arhitekturo, oziroma kot jih je opisal zavezanec, "prikaz naravne in kulturne dediščine našega planeta (s poudarkom na prikazu Slovenije)", z enako kvaliteto doseči tudi tako, da na fotografiji ni določljivih posameznikov. Interes fotografa po objavi fotografije v tem primeru ne prevlada nad interesom npr. mimoidočega, da se sam

odloči, ali želi biti na fotografiji določljiv. Fotografije iz te skupine se morajo pred objavo na spletu predrugačiti tako, da posameznik ne bo več niti določljiv. Zavezanec se je odločil, da namesto zamegljevanja obrazov določljivim posameznikom iz te skupine nadene maske.

Vprašanja razmejitve med posameznikovo pravico do varstva osebnih podatkov na eni strani in svobodo izražanja fotografov na drugi strani, so, kot se je izkazalo, zahtevna. Informacijski pooblaščenec meni, da ta razmejitev v konkretnem primeru poteka med drugo in tretjo skupino fotografij. Res pa je tudi, da je ta meja lahko zelo tanka, ni npr. iz vsake fotografije že enostavno razvidno, da gre npr. za fotografijo dogodka. Informacijski pooblaščenec je z obrazložitvijo sklepa o ustavitvi postopka skušal narediti test, s katerim naj bi se presojalo, ali je treba z vidika varstva osebnih podatkov, fotografije pred objavo na spletu predrugačiti tako, da posamezniki ne bodo niti določljivi. Ob tem ne gre spregledati, da je treba v zvezi z drugo in tretjo skupino fotografij upoštevati tudi splošno pravico posameznika do zasebnosti oziroma njegovo pravico na lastni podobi iz 35. člena Ustave. Varstvo teh pravic je praviloma prepuščeno posameznikom, pristojnost Informacijskega pooblaščenca pa ni podana. Navedeno pomeni, četudi je fotografija skladna z ZVOP-1, to še ne pomeni, da posameznik nima možnosti tožiti zaradi posega v osebnostne pravice, katerih del je tudi pravica na lastni podobi.

Predvsem splet je v zvezi z objavo fotografij in varstvom osebnih podatkov prinesel povsem novo dinamiko. Objavljene fotografije so preprosto dostopne vsakomur z dostopom do spleta. Čedalje več orodij na spletu pa omogoča tudi prepoznavo obrazov, ki se potem lahko združujejo v nove zbirke podatkov. Zato npr. na spletu objavljenih fotografij ni mogoče enostavno primerjati z npr. tiskano izdajo fotografij.

Informacijski pooblaščenec je izdal tudi mnenje glede t.i. ulične fotografije in varstva osebnih podatkov. V zvezi s tem je treba opozoriti na vsebinske razlike med ulično fotografijo, ki je obravnavana v tem mnenju, in med fotografijo, katere namen je predstaviti del naselja, arhitekturo oziroma fotografijo, ki je posneta na ulici. Dejstvo, da sta praviloma obe fotografiji posneti iz javne površine, npr. ulice, še ne pomeni, da sta obe fotografiji z vidika varstva osebnih podatkov enaki in da je treba uporabiti enaka pravila. Bistvo ulične fotografije, kot posebne zvrsti dokumentarne fotografije, je slikovno zabeležiti posameznike na javnih mestih v posebnih okoliščinah, situacijah, interakcijah z živo in neživo naravo oziroma z drugimi posamezniki. Namen ulične fotografije je pokazati nek utrip mesta, ulice, življenja v njih … Prostorska fotografija se tudi zaradi tega, ker prikaže vso okolico okrog fotografske opreme, težko uvrsti pod ulično fotografijo. Celotni vtis prostorske fotografije (ki ne beleži dogodka) je predvsem v doživetju dela naselja in arhitekture.

3.9.12. Oddaljen nadzor zaposlenih

Informacijski pooblaščenec je v letu 2011 vodil tudi inšpekcijski postopek, v katerem je obravnaval oddaljen dostop službe za informatiko zavezanca do računalnikov zaposlenih.

V postopku inšpekcijskega nadzora je bilo ugotovljeno, da zavezanec uporablja programsko orodje za nudenje pomoči uporabnikom na daljavo. Zavezanec uporablja orodja za oddaljen dostop, ker ima enote na več lokacijah. Če ima uporabnik težave z računalnikom, sporoči to informatiku, ki mu nudi pomoč na daljavo s svoje delovne postaje z uporabo programskega orodja, ki omogoča oddaljen vpogled v zaslonsko sliko uporabnika, oddaljen prevzem tipkovnice in miške, oddaljen zagon programov, prenos datotek med računalnikom in računalnikom informatika, oddaljeno diagnostiko trenutnega stanja zasedenosti spomina, delovanja servisov, dnevnika dogodkov, omrežnih povezav in zbujanje računalnikov na daljavo. Uporabniku ni potrebno predhodno dovoliti dostopa. Programska oprema uporabniku z dovolj pravicami omogoča spremljanje oziroma nadzor zaposlenega, s čimer se obdelujejo osebni podatki zaposlenega, za kar mora zavezanec imeti ustrezno pravno podlago. Delodajalec lahko obdeluje delavčeve osebne podatke le, če je to potrebno zaradi uresničevanja pravic in obveznosti iz delovnega razmerja ali v zvezi z delovnim razmerjem in ne kadarkoli. Z uporabo programske opreme za oddaljen dostop zavezanec odpravlja težave z računalniki, ki pri poslovanju zavezanca predstavljajo obvezen in osnovni delovni pripomoček, saj zaposleni brez njega ne morejo izpolnjevati svojih obveznosti iz delovnega razmerja. S tem skrajša odzivni čas in težave zaposlenih z računalnikom hitreje odpravi. Upoštevati pa je treba, da se lahko s temi orodji, ki primarno služijo odpravi napak oziroma diagnosticiranju na računalniku zaposlenega, poseže tudi v zasebnost zaposlenega, ki jo upravičeno pričakuje tudi na delovnem mestu oziroma v obdelavo njegovih

varovanih osebnih podatkov. Ob uporabi računalnika (izdelava dokumentov, komunikacija s sodelavci in z zunanjim svetom) nastajajo osebni podatki, saj se nanašajo na zaposlenega, ki uporablja računalnik. Poleg tega ima zaposleni lahko na službeni opremi tudi svoje zasebne dokumente oziroma zasebno korenspodenco, ki tudi predstavljajo osebne podatke.

V postopku je bilo ugotovljeno, da zavezanec ne zagotavlja sledljivosti obdelave osebnih podatkov, tako kot to zahtevajo določbe ZVOP-1. Zato je Informacijski pooblaščenec zavezancu z odločbo naložil, da mora v vseh primerih, ko osebe, ki jih ima pod nadzorom (njegovi zaposleni, pogodbeni izvajalci…), z uporabo informacijsko-komunikacijske opreme izvajajo oddaljen dostop do računalnikov drugih zaposlenih, zagotoviti organizacijske, tehnične in logično-tehnične postopke in ukrepe, s katerimi bo mogoče poznejše ugotavljanje, kdaj (datum in ura, minuta) je bilo do računalnika zaposlenega oddaljeno dostopano, kdo je do računalnika zaposlenega oddaljeno dostopal in za kakšen namen. Le tako se lahko namreč ugotavlja zakonitost obdelave osebnih podatkov. Če zavezanec ne bo zagotovil opisane sledljivosti, oddaljenih dostopov do računalnikov zaposlenih ne sme izvajati. Zavezancu je bilo odrejeno tudi, da mora sprejeti interni akt, v katerem mora celovito opisati postopek uporabe oddaljenega dostopa do računalnikov zaposlenih in s tem aktom seznaniti vse pri njemu zaposlene osebe. Zavezanec je zoper odločbo sprožil upravni spor.

3.9.13. Objava osebnih podatkov upnikov podjetja v stečaju

Informacijski pooblaščenec je po uradni dolžnosti začel inšpekcijski postopek pri zavezancu. Po pregledu spletne strani zavezanca je ugotovil, da je na njih objavil več dokumentov, v katerih so se poleg imen in priimkov delavcev-upnikov nahajali tudi njihovi naslovi, davčne številke, zneski prijavljenih in priznanih terjatev po posameznem pravnem naslovu oziroma po posamezni podlagi nastanka obveznosti, in sicer znesek terjatve iz naslova stroškov (prehrana, prevoz…), znesek terjatve iz naslova regresa za letni dopust, znesek terjatve iz naslova neizkoriščenega dopusta tekočega leta, znesek terjatve iz naslova neplačane plače zadnjih treh mesecev, znesek terjatve iz naslova odpravnine in znesek terjatve iz naslova plače po zaključku stečaja, znesek bruto plače zadnjih treh mesecev, znesek odpravnine, znesek odškodnine za neizkoriščen dopust, znesek regresa, znesek drugih terjatev (neprednostnih). Informacijski pooblaščenec je takoj po pregledu spletnih strani izdal začasno odločbo, s katero je zavezancu odredil nepovraten umik dokumentov z navedenimi osebnimi podatki zaradi zavarovanja pravice posameznikov do varstva osebnih podatkov in preprečitve nadaljnje škode, ki bi lahko nastala zaradi nadaljnje objave osebnih podatkov. Informacijski pooblaščenec je do izdaje začasne odločbe ugotovil, da v veliki verjetnosti ne obstaja pravna podlaga za objavo navedenih osebnih podatkov upnikov. V odločbi so bila navedena dejstva ugotovljena z verjetnostjo, na podlagi gotovosti dejstev in okoliščin pa je Informacijski pooblaščenec po končanem postopku izdal odločbo, s katero je, tako kot to določa Zakon o splošnem upravnem postopku[45], razveljavil začasno odločbo in ustavil postopek, ker je zavezanec izvršil ukrepe iz začasne odločbe in tako odpravil ugotovljene nepravilnosti.

Zakon o finančnem poslovanju, postopkih zaradi insolventnosti in prisilnem prenehanju[46] natančno določa vsebino osnovnega seznama preizkušenih terjatev in s tem tudi nabor osebnih podatkov upnika, ki jih vsebuje tak seznam, kadar je upnik fizična oseba, ki je prijavila terjatev. Tak seznam ne sme vsebovati davčnih številk upnikov - fizičnih oseb, saj za obdelavo teh osebnih podatkov ne obstaja pravna podlaga. Seznam upravitelj predloži sodišču. Osnovni seznam preizkušenih terjatev mora sodišče objaviti v treh delovnih dneh po prejemu seznama. ZFPPIPP določa tudi, da je treba na spletnih straneh za objave v postopkih zaradi insolventnosti objaviti med drugim tudi sezname preizkušenih terjatev. Spletne strani za objave v postopkih zaradi insolventnosti upravlja AJPES. Zavezanec je pojasnil, da je na svojih spletnih straneh objavil enak seznam kot naj bi bil, skladno z zakonskimi določili, predložen sodišču in istega dne objavljen na javno dostopnih straneh AJPES-a. Glede na to, da so spletne strani AJPES-a javne in brezplačno dostopne vsakomur, je zavezanec podatke povzel in jih objavil tudi na svojih spletnih straneh, na katerih naj bi upnike obveščal tudi o drugih pomembnih sklepih sodišča v stečajnem postopku. Informacijski pooblaščenec je v zvezi s tem ugotovil še, da je bil tudi na spletnih straneh AJPES-a objavljen dokument zavezanca, ki je vseboval davčne številke fizičnih oseb, za objavo katerih ni obstajala pravna podlaga,

[45] Uradni list RS, št. 24/2006-UPB2, s spremembami.
[46] Uradni list. RS, št. 126/2007 s spremembami in dopolnitvami, v nadaljevanju ZFPPIPP

zato je tudi AJPES-u izdal začasno odločbo, s katero mu je naložil izbris vseh davčnih številk fizičnih oseb iz tega dokumenta. AJPES je začasno odločbo Informacijskega pooblaščenca ustrezno izvršil.

Informacijski pooblaščenec je ob zaključku postopka ugotovil, da bi smiselno enako odločitev, kot jo je sprejel v začasni odločbi, sprejel tudi v drugi odločbi, če zavezanec začasne odločbe ne bi izvršil, le da zavezancu ne bi naložil nepovratnega izbrisa zneskov terjatev iz naslova regresa za letni dopust, zneskov terjatev iz naslova neizkoriščenega dopusta tekočega leta, zneskov terjatev iz naslova neplačane plače zadnjih treh mesecev, zneskov terjatev iz naslova odpravnine in zneskov terjatev iz naslova plače po zaključku stečaja, ki se nanašajo delavce - upnike ter nepovratnega izbrisa zneskov bruto plač zadnjih treh mesecev, zneskov odpravnine, zneskov odškodnine za neizkoriščen dopust, zneskov regresa, zneskov drugih terjatev (neprednostnih). Informacijski pooblaščenec je v zvezi s tem ponovno proučil pravno podlago za obdelavo naštetih osebnih podatkov v seznamih preizkušenih terjatev, ki so bili objavljeni, in ugotovil, da ZFPPIPP zavezancu daje pravno podlago za obdelavo naštetih osebnih podatkov v navedenih dokumentih in za objavo teh zneskov na njegovi spletni strani.

3.10. Splošna ocena stanja varstva osebnih podatkov in priporočila

Informacijski pooblaščenec je na področju varstva osebnih podatkov v letu 2011 zaznal porast prijav in pritožb. Število zadev, v katerih je Informacijski pooblaščenec odločal, se je v primerjavi z letom 2010 na splošno povečalo. Tako se je povečalo število zaprosil za mnenja in različnih vprašanj s področja varstva osebnih podatkov (1.859 leta 2010 in 2.143 leta 2011) ter število inšpekcijskih zadev (599 leta 2010 in 682 leta 2011), prav tako se je povečalo število vlog za izdajo dovoljenja za povezovanje zbirk osebnih podatkov (9 leta 2010 in 14 leta 2011) in za izvajanje biometričnih ukrepov (6 leta 2010 in 9 leta 2011). Število postopkov za seznanitev z lastnimi podatki je ostalo na enaki ravni (85 leta 2010 in 2011), število vlog za iznos osebnih podatkov v tretje države se je prepolovilo (8 leta 2010 in 4 leta 2011), nekoliko se je zmanjšalo tudi število prekrškovnih zadev (179 leta 2010, 136 leta 2011).

Pri obravnavi pritožb zaradi zavrnitve seznanitve z lastnimi podatki ugotavljamo, da je precejšen delež teh pritožb vložen zaradi molka upravljavca osebnih podatkov. Upravljavec osebnih podatkov mora namreč po prejemu zahteve posameznika za seznanitev z lastnimi podatki posamezniku v določenem roku (najpozneje v 15 ali 30 dneh) bodisi omogočiti vpogled, prepis in kopiranje osebnih podatkov oziroma mu posredovati zahtevan izpis, seznam prejemnikov, potrdilo ter informacije in obvestila v zvezi z njegovimi osebnimi podatki, ali pa ga v istem roku obvestiti, zakaj tega ne bo storil. Če upravljavec tega ne stori, se šteje, da je zahtevo zavrnil in posameznik lahko zaradi molka upravljavca vloži pritožbo pri Informacijskem pooblaščencu. Pri tem je potrebno opozoriti, da molk upravljavca ne pomeni zgolj zavrnitev posameznikove zahteve, pač pa pomeni tudi storitev prekrška po 13. točki prvega odstavka 91. člena ZVOP-1, zaradi česar Informacijski pooblaščenec v takšnem primeru zoper upravljavca osebnih podatkov uvede postopek o prekršku.

Na področju neposrednega trženja ugotavljamo porast neposrednega trženja s pošiljanjem neželenih elektronskih sporočil. Pri izvajanju takšnega neposrednega trženja izvajalci neposrednega trženja posameznikov v mnogih primerih ne obveščajo o njihovi pravici, da lahko kadar koli pisno ali na drug dogovorjen način zahtevajo prenehanje uporabe svojih osebnih podatkov za namene neposrednega trženja, najdejo pa se tudi primeri, ko s pošiljanjem neželenih elektronskih sporočil ne prenehajo niti po tem, ko je posameznik že zahteval prenehanje uporabe svojih osebnih podatkov za te namene. V zvezi s tem je potrebno še opozoriti, da izvajalci neposrednega trženja pogosto ne znajo oziroma ne morejo izkazati, na kakšen način so prišli do naslovov elektronske pošte, iz česar je mogoče sklepati, da so do naslovov prišli na nezakonit način. V zvezi z izvajanjem neposrednega trženja po elektronski pošti je potrebno še opozoriti, da je Informacijski pooblaščenec v obravnavanem obdobju podobno kot lani obravnaval tudi več prijav zaradi nezakonitega razkritja elektronskih naslovov prejemnikov e-sporočila. Pri obravnavi teh prijav je bilo v več primerih ugotovljeno, da izvajalec neposrednega trženja ni zagotovil zavarovanja uporabljenih elektronskih naslovov prejemnikov elektronskega sporočila, saj elektronskih naslovov ni zapisal v rubriko »Skrito« (»Skp« oziroma angleško »Bcc«), pač pa jih je zapisal v rubriko »Za« (angleško »To«) ali pa v rubriko »Kp« (angleško »Cc«), s čimer je prejemnikom e-sporočila razkril elektronske naslove vseh ostalih prejemnikov istega sporočila. V nekaterih takšnih primerih je tako izvajalec neposrednega trženja vsem prejemnikom

elektronskega sporočila razkril elektronske naslove vseh svojih strank, torej podatke, ki za marsikatero podjetje predstavljajo celo poslovno skrivnost. Informacijski pooblaščenec zato ponovno opozarja, da je potrebno v takšnih primerih elektronske naslove prejemnikov navesti v rubriki »Skrito« (»Skp« oziroma »Bcc«), s čimer se zagotovi, da prejemniki ne vidijo elektronskih naslovov ostalih prejemnikov sporočila.

Informacijski pooblaščenec na področju izvajanja videonadzora ugotavlja, da se takšen nadzor še vedno nezadržno širi, in sicer tudi na območja, kjer takšen nadzor sploh ni dopusten. Takšni primeri so npr. savne, garderobe, dvigala ter nekatere javne površine (npr. sprehajalne poti). Kot najpogosteje ugotovljene nepravilnosti v zvezi z izvajanjem videonadzora se še vedno pojavlja neustrezno oziroma pomanjkljivo evidentiranje pregledovanja oziroma uporabe posnetkov, uporaba posnetkov za nezakonite namene (npr. kontrola zaposlenih), slabo vidna in nepopolna obvestila o izvajanju videonadzora, neobstoj pisne odločitve o uvedbi videonadzora, izvajanje videonadzora znotraj delovnih prostorov brez posvetovanja z reprezentativnim sindikatom ter neizdelani katalogi za zbirko posnetkov videonadzornega sistema.

Kar zadeva izvajanje postopkov in ukrepov za zavarovanje osebnih podatkov iz 24. in 25. člena ZVOP-1 je potrebno opozoriti na pogosto neustrezno zavarovanje osebnih podatkov, ki se zbirajo prek interneta. Ugotovljeni so bili primeri, ko upravljavec osebnih podatkov ni poskrbel niti za najosnovnejše ukrepe zavarovanja osebnih podatkov, saj je bilo v nekaterih primerih brez kakšnega posebnega računalniškega znanja, s pomočjo iskalnikov kot je Google, že zgolj z vnosom osebnega imena možno priti do podatkov o naslovih elektronske pošte, uporabniških imenih in geslih za dostop do uporabniških računov posameznikov, ki so se registrirali na določenem portalu ali pa do osebnih imen, e-naslovov ter telefonskih številk posameznikov, ki so prek spletne strani naročili določen izdelek. Upravljavci se namreč v zvezi z zavarovanjem osebnih podatkov pogosto ne zavedajo niti tega, da v današnjem času iskalniki Google predstavljajo dano dejstvo, zaradi česar se mora vsakdo, ki na spletu objavlja ali prek njega zbira osebne podatke, zavedati, da bodo zelo zmogljivi iskalniki lahko našli vse na spletu objavljene osebne podatke, če jih upravljavec ne bo predhodno ustrezno zavaroval.

Informacijski pooblaščenec ugotavlja, da se številni upravljavci zbirk osebnih podatkov soočajo z dilemo, ali se odločiti za uporabo storitev t.i. računalništvo v oblaku. Računalništvo v oblaku obljublja dostopnost do računalniških zmogljivosti iz katere koli lokacije na ekonomičen, prilagodljiv in nadgradljiv način, zato ne preseneča, da se za oblak zanima čedalje več organizacij, ki obdelujejo osebne podatke. To pa neizogibno poraja dvome glede skladnosti z zakonodajo na področju varstva osebnih podatkov in zasebnosti. Zlasti javne oblike računalništva v oblaku vzbujajo pomisleke glede varstva osebnih podatkov, ki izvirajo iz narave računalništva v oblaku, ki prinaša specifična tveganja, ta pa se kažejo predvsem na področju ureditve pogodbene obdelave oziroma zunanjega izvajanja storitev, informacijske varnosti oziroma zavarovanja osebnih podatkov ter izvoza podatkov v tretje države. Organizacije, ki se odločajo za uporabo oblaka, pogosto nimajo zadostnih informacij o tem, kje se bodo njihovi osebni podatki sploh nahajali in kako bodo dejansko varovani, brez tovrstnih podatkov pa je težko izvesti ustrezne analize tveganj pred odločitvijo za oblak. Dodatno težavo predstavlja dejstvo, da so ponudniki oblaka večinoma globalne korporacije, ki malim upravljavcem pogosto ne nudijo dosti možnosti prilagajanja pogojev uporabe, čeprav naj bi bili upravljavci osebnih podatkov tisti, ki naj bi določali pogoje obdelave osebnih podatkov – pri oblaku so pogosto soočeni le z izbiro vzemi ali pusti. Informacijski pooblaščenec je že izdal nekaj mnenj o računalništvu v oblaku, konec leta 2011 pa je pričel s pripravo smernic, ki naj bi upravljavcem pomagale pri odločitvah za uporabo računalništva v oblaku. Po oceni Informacijskega pooblaščenca smo trenutno v fazi, kjer zaupanje v oblak ni popolnoma vzpostavljeno, poteka pa veliko število standardizacijskih, certifikacijskih in drugih aktivnosti, katerih namen je vzpostaviti ravno to zaupanje, ki si ga želijo tako ponudniki, kot uporabniki in nadzorni organi.

Informacijski pooblaščenec v zvezi s stanjem na področju elektronskih komunikacij opozarja, da prihaja do povečanih teženj po nadzorovanju uporabe elektronskih komunikacij, pri čemer prihaja do trenj med različnimi interesi in pravicami. Izpostaviti želimo predvsem po mnenju Informacijskega pooblaščenca neprimerno ureditev omejevanja dostopnosti spletnih vsebin v določbah Zakona o igrah na srečo[47], ki ponudnikom dostopa do interneta nalaga blokiranje dostopa do spletnih iger na srečo ter primer širjenja pooblastil organov pregona v zvezi z uporabo podatkov, ki so jih dolžni hraniti operaterji elektronskih komunikacij (t.i. data retention). Vlada je namreč predlagala spremembe 149.b člena Zakona o

[47] Uradni list RS, št. 14/2011 – uradno prečiščeno besedilo 3.

kazenskem postopku[48], ki bi omogočile ne le pridobivanje podatkov za določeno telefonsko številko, temveč za celotno bazno postajo mobilne telefonije. Informacijski pooblaščenec je takšen predlog ocenil kot izrazito nesorazmeren in neučinkovit glede na poseg v zasebnost. Predlog Vlade so poslanci na obravnavi na ustreznem odboru zavrnili, do česar pa ne bi prišlo, če Informacijski pooblaščenec s trdnimi argumenti ne bi vztrajno opozarjal na nesorazmernost takšnih predlogov. Omenjena izkušnja je bila zelo dragocena, saj je opozorila na dve izkušnji, ki ju vztrajno poudarjamo. Prvič, da vzpostavitev velikih zbirk osebnih podatkov neizogibno vodi v povečanje apetitov po podatkih (gre za t.i. pojav function creep ali širitev prvotnega namen obdelave). In drugič, takšne težnje je zelo težko – včasih pa tudi nemogoče – zaustaviti. To pa opozarja na pomen pravočasno izvedenih presoj pred vzpostavitvijo takšnih zbirk, ki morajo prestati test nujnosti, sorazmernosti in učinkovitosti, saj predstavljajo izrazita tveganja za raven varstva osebnih podatkov. Informacijski pooblaščenec v zvezi s tem opozarja, da bi veljalo vzpostaviti mehanizem pravočasnih vplivov na zasebnost pri pripravi zakonodajnih predlogov, ki predvidevajo spremembe, ki bistveno povečujejo tveganja za zlorabe osebnih podatkov. Žal takšnih presoj nismo videli ne pri obvezni hrambi podatkov v prometu elektronskih komunikacij (data retention), ne pri širjenju namenov uporabe teh zbirk, pogrešamo pa tudi post festum analize, ki bi upravičevale nujnost, sorazmernost in učinkovitost takšnih projektov.

Informacijski pooblaščenec je v preteklem letu nadaljeval s preventivnim delom in je nadaljeval s presojami vplivov na zasebnost. Na Informacijskega pooblaščenca se je tako podobno kot v prejšnjih letih obrnilo večje število upravljavcev iz javnega in zasebnega sektorja s prošnjo za predhodno analizo projektov v smislu pravočasne identifikacije in odprave tveganj pri izvedbi projektov, ki so jih načrtovali. Informacijski pooblaščenec je tako v letu 2011 podajal svoje presoje glede zelo različnih projektov, kot so: eArhiviranje, uporaba pametnih (biometrijskih) pisal in biometrijskih podpisnih tablic, sistem obveščanja in spremljanja bolnikov, varnost osebnih podatkov v dokumentnih sistemih, programska oprema za analizo zlorab v zavarovalništvu, osebni podatki pri uporabi brezžičnih omrežij, javna naročila za izdelavo IT aplikacije, zbiranje geolokacijskih informacij in snemanje ulic, projekt izobraževanja starejših glede uporabe računalništva (projekt Simbioz@), uporaba biometrije na samopostrežnih aparatih ter več zahtev s področja računalništva v oblaku.

Informacijski pooblaščenec je v preteklem letu veliko svojih resursov namenil projektu priprave notranjih pravil za potrebe ustrezne elektronske hrambe dokumentacije skladno z ZVDAGA in je tako kot eden prvih državnih organov v maju 2011 na Arhiv Republike Slovenije oddal zahtevek za potrditve notranjih pravil (zahtevek je bil potrjen v letu 2012).

Informacijski pooblaščenec je v letu 2011 aktivno sodeloval v številnih skupinah, med katerimi velja izpostaviti medresorsko delovno skupino, ki se je ukvarjala z uvedbo varnejših in uporabniku prijaznejših e-identitet, pri katerih je bila v sodelovanju z Ministrstvom za javno upravo, Ministrstvom za notranje zadeve in Ministrstvom za visoko šolstvo, znanost in tehnologijo pripravljena celovita analiza stanja e-identitet v Sloveniji, analiza možnih pravnih ter izvedbenih možnosti in primerjalna analiza z drugimi državami. Izvedene so bile ankete in posveti z deležniki, kot so ponudniki storitev, overitelji, državljani ter zaposleni v javni upravi. Prenova sistema e-identitet omogoča boljše in učinkovitejše storitve e-uprave z večjo stopnjo uporabe pri ciljnih skupinah, obenem pa prenova ob ustreznih odločitvah omogoča tudi višjo raven varovanja osebnih podatkov, kot jo nudijo trenutna sredstva za identifikacijo in avtentikacijo posameznika v virtualnem svetu.

Informacijski pooblaščenec je prav tako aktivno sodeloval pri delu medresorske delovne podskupine za Pripravo dokumenta razvojnega načrtovanja na področju informacijske družbe za obdobje 2011-2015 pri prednostnem področju Varnost, zasebnost in zaupanje.

Informacijski pooblaščenec je v letu 2011 razširil svoj instrumentarij na področju ozaveščanja javnosti, ki skozi celotno njegovo delovanje predstavlja pomemben kontrapunkt inšpekcijskemu delovanju. Poleg velikega števila mnenj, smernic in brošur se je pooblaščenec odločil tudi za pripravo posebnih poročil. Namen poročil je osvetliti določena področja, na katerih prihaja do zbiranja in obdelav osebnih podatkov, ki si po oceni Informacijskega pooblaščenca zaslužijo posebno pozornost. Informacijska družba omogoča več načinov in nove načine zbiranja podatkov o nas, zato je pomembno, da tovrstne obdelave podatkov razumemo. Poročila Informacijskega pooblaščenca naj bi izpostavljala

[48] Uradni list RS, št. 32/2007 – uradno prečiščeno besedilo 4, s spremembami.

pomembne vidike takšnih obdelav osebnih podatkov v upanju, da bodo omogočila boljše razumevanje temeljnih načel varstva osebnih podatkov in zasebnosti ter sprožila ustrezen odziv tako v strokovni kot v splošni javnosti. Brez ustreznega zavedanja in razumevanja teh konceptov bo namreč v okolju novih tehnologij naše temeljne pravice čedalje težje obvarovati. V letu 2011 je bilo tako pripravljeno prvo poročilo na temo klubov zvestobe[49]. Klubi zvestobe namreč postajajo vedno pomembnejše orodje za zbiranje podatkov o potrošnikih, ti podatki pa se nato uporabljajo za segmentiranje uporabnikov in ciljno trženje. Preučili smo nekatere pomembne vidike delovanja klubov zvestobe - ali so splošni pogoji poslovanja dostopni ter jasni in enostavni, kakšni so pogoji za pridobitev kartice zvestobe, katere osebne podatke podjetje zahteva za pridobitev kartice zvestobe in za katere namene zbira osebne podatke, komu se zbrani osebni podatki posredujejo, koliko časa se hranijo in kakšni so pogoji izstopa iz kluba zvestobe. Namen poročila o klubih zvestobe je bil opraviti primerjavo med nekaterimi največjimi ponudniki klubov zvestobe z vidika spoštovanja načel varstva osebnih podatkov. Z drugimi besedami - naš cilj je večja transparentnost delovanja klubov zvestobe - povečati želimo drobni tekst, ki ga posamezniki pogosto ne preberemo. Odločitev o tem, ali dobimo dovolj v zameno za svoje osebne podatke, je na koncu še vedno odločitev vsakega posameznika, naša želja pa je, da je ta odločitev informirana in da obdelave tako zbranih podatkov potekajo skladno z zakonom.

Konec leta 2011 je Okrajno sodišče v Novem mestu potrdilo doslej najvišjo globo, ki jo je Informacijski pooblaščenec izrekel zavarovalnici zaradi nezakonite obdelave osebnih podatkov. V postopku o prekršku je namreč ugotovil, da so bili z ene zavarovalnice na drugo posredovani osebni podatki o 2382-ih nekdanjih zavarovancih prve brez podlage v zakonu ali v osebni privolitvi posameznika, na katere se osebni podatki nanašajo, ti podatki pa so bili nato uporabljeni za neposredno trženje s strani druge zavarovalnice. Sodišče je zahtevo za sodno varstvo, ki sta jo vložila kršitelja, zavrnilo in potrdilo odločbo z izrečeno globo pravni osebi v višini 112.590 evrov, odgovorni osebi pa v višini 20.000 evrov.

[49] https://www.ip-rs.si/fileadmin/user_upload/Pdf/Porocila_IP/Klubi_zvestobe.pdf

4 DRUGE DEJAVNOSTI INFORMACIJSKEGA POOBLAŠČENCA

4.1. Sodelovanje pri pripravi zakonov in drugih predpisov

Informacijski pooblaščenec skladno z določbo 48. člena ZVOP-1 daje predhodna mnenja ministrstvom, državnemu zboru, organom samoupravnih lokalnih skupnosti, drugim državnim organom ter nosilcem javnih pooblastil o usklajenosti določb predlogov zakonov ter ostalih predpisov z zakoni in drugimi predpisi, ki urejajo osebne podatke.

Leta 2011 je Informacijski pooblaščenec sodeloval pri pripravi naslednjih zakonov in drugih predpisov:

- Predlog državnotožilskega reda (mnenje z dne 19. 12. 2011),
- Predlog direktive o evropskem preiskovalnem nalogu (mnenje z dne 6. 12. 2011),
- Predlog Uredbe Evropskega parlamenta in Sveta o spremembi Uredbe Sveta (EGS) št. 3821/85 o tahografu v cestnem prometu (mnenje z dne 8. 11. 2011),
- Gradivo v okviru delovne skupine za spremembo ZDIJZ in uredbe – dodatni predlog (mnenje z dne 18. 8. 2011),
- Predlog spremembe 166. člena Zakona o davčnem postopku (mnenje z dne 12. 10. 2011),
- Osnutek Zakona o zbirkah podatkov v zdravstvu (mnenje z dne 22. 9. 2011),
- Zakon o spremembah in dopolnitvah Zakona o evidentiranju nepremičnin (mnenje z dne 24. 8. in pripomba z dne 22. 9. 2011),
- Osnutek Zakona o obravnavanju mladoletnih prestopnikov (mnenje z dne 11. 9. 2011),
- Predlog Zakona o funkcionarjih (mnenje z dne 12. 8. 2011),
- Predlog Zakona o cestninjenju (mnenje z dne 12. 8. 2011),
- Zakon o finančnem poslovanju, postopkih zaradi insolventnosti in prisilnem prenehanju (mnenje z dne 12. 8. 2011),
- Predlog Zakona o spremembah in dopolnitvah Zakona o evidentiranju nepremičnin (pripomba z dne 15. 7. 2011),
- Zakon o prijavi prebivališča (pripomba z dne 11. 7. 2011),
- Zakon o državnem geodetskem referenčnem sistemu (mnenje z dne 6. 7. 2011),
- Predlog Zakona o spremembah in dopolnitvah Zakona o elektronskem poslovanju in elektronskem podpisu (mnenje z dne 5. 7. 2011),
- Zakon o zagotavljanju prostega dostopa do dokumentov o trgovini z orožjem v letih 1990-1994 (pripomba z dne 27. 6. 2011),
- Delovno besedilo Sporazuma med Vlado Republike Slovenije in Vlado Združenih držav Amerike o krepitvi sodelovanja pri preprečevanju in boju proti težjim oblikam kriminala (mnenje z dne 22. 6. 2011),
- Zakon o množičnem vrednotenju nepremičnin (mnenje z dne 8. 6. 2011),
- Zakon o spremembah in dopolnitvah zakona o visokem šolstvu (mnenje z dne 6. 6. 2011),
- Predlog Zakona o spremembah in dopolnitvah Zakona o kazenskem postopku (EVA 2010-2011-0009)-ponovno medresorsko usklajevanje (mnenje z dne 26. 5. 2011),
- Predlog Zakona o spremembah in dopolnitvah Zakona o preprečevanju pranja denarja in financiranja terorizma (mnenje z dne 9. 5. 2011),
- Predlog Zakona o spremembah in dopolnitvah Kazenskega zakonika (mnenje z dne 4. 5. 2011),
- Predlog Zakona o spremembah in dopolnitvah Zakona o elektronskem poslovanju in elektronskem podpisu (mnenje z dne 4. 5. 2011),
- Predlog Zakona o spremembah in dopolnitvah Zakona o volitvah v državni zbor (mnenje z dne 4. 4. 2011),
- Osnutek predloga Zakona o priznavanju in vrednotenju izobraževanja (pripomba z dne 16. 3. 2011),
- Osnutek novega Zakona o usmerjanju otrok s posebnimi potrebami (pripomba z dne 9. 3. 2011),
- Predlog Zakona o štipendiranju (pripomba z dne 31. 1. 2011).

4.2. Sodelovanje z javnostmi

Informacijski pooblaščenec je leta 2011 vseskozi skrbel za javnost svojega dela prek svoje spletne strani ter ozaveščal pravne in fizične osebe z rednimi in doslednimi odnosi z mediji (sporočila za javnost, izjave, komentarji, intervjuji pooblaščenke, novinarske konference). Vse leto je skrbel za njeno ažurnost in pestrost.

Spletna stran Informacijskega pooblaščenca, www.ip-rs.si, vsebuje:

- predstavitev zgodovine Informacijskega pooblaščenca in predstavitev zaposlenih,
- predstavitev obeh področij delovanja, to je varstva osebnih podatkov (pravice posameznika, inšpekcijski nadzor, obveznosti upravljavcev, informacijske tehnologije in osebni podatki, iskalnik po odločbah in mnenjih, register zbirk) in dostopa do informacij javnega značaja (dostop do informacij, dostop do informacij za medije, ponovna uporaba, iskalnik po odločbah, katalog informacij javnega značaja, test interesa javnosti) ter pristojnosti na obeh področjih,
- predstavitev domače in tuje zakonodaje za obe področji,
- odgovore na najpogosteje zastavljena vprašanja z obeh področij,
- predstavitev mednarodnega delovanja Informacijskega pooblaščenca,
- uporabne povezave (npr. na spletne strani sorodnih organov v Evropski uniji in drugod po svetu),
- izdane publikacije (priročniki in smernice, poročila, e-novice, domači in tuji članki z obeh področij),
- vzorce oziroma obrazce, namenjene fizičnim osebam za uveljavljanje njihovih pravic (zahteva za dostop do informacij javnega značaja, pritožba zoper molk ali zavrnilno odločbo organa, zahteva za ponovno uporabo informacij javnega značaja, prijava zlorabe osebnih podatkov, pritožba zaradi kršitve pravice do seznanitve z lastnimi osebnimi podatki, zahteva za seznanitev s podatki v Nacionalnem schengenskem informacijskem sistemu v Sloveniji) in upravljavcem zbirk osebnih podatkov za lažje delo pri vlaganju različnih zahtev in zagotovitvi ustreznega varovanja osebnih podatkov (zahteva za izdajo odločbe glede povezljivosti evidenc, obvestilo o povezovanju evidenc, prijava biometrijskih ukrepov pred njihovo uvedbo, vloga za iznos osebnih podatkov v tretje države, katalogi zbirk osebnih podatkov, pravilnik o zavarovanju osebnih podatkov, pogodba za potrebe pogodbene obdelave osebnih podatkov po 11. členu ZVOP-1, opozorila in obvestila ob neposrednem trženju),
- ažurno objavo izdanih mnenj s področja varstva osebnih podatkov,
- ažurno objavo odločb, s katerimi odloča o izvajanju biometrijskih ukrepov,
- ažurno objavo vseh odločb, s katerimi odloča o pritožbah v zvezi z informacijami javnega značaja,
- predstavitev zahtev za oceno ustavnosti, ki jih je na Ustavno sodišče Republike Slovenije vložil Informacijski pooblaščenec,
- objavo sodb Upravnega sodišča Republike Slovenije in Vrhovnega sodišča Republike Slovenije v zadevah, ki jih je vodil Informacijski pooblaščenec in zoper katere so bile vložene tožbe,
- pripombe Informacijskega pooblaščenca na predloge predpisov,
- katalog Informacijskega pooblaščenca in Centralni katalog informacij javnega značaja in register zbirk osebnih podatkov,
- seznanitev z aktualnimi dogodki na obeh področjih (sodbe Evropskega sodišča za človekove pravice in novice),
- možnost prijave na e-novice (prejemanje novih odločb Informacijskega pooblaščenca in sporočil za medije).

Informacijski pooblaščenec je z izvajanjem različnih delavnic in seminarjev skrbel za stalno izobraževanje zavezancev, sodeloval pa je tudi na različnih konferencah, delavnicah in okroglih mizah.

Informacijski pooblaščenec je leta 2011 nadaljeval preventivno delo in je veliko pozornosti namenil nadaljnji širitvi orodij in pripomočkov za dvig ozaveščenosti. S pomočjo smernic naj bi upravljavci dobili priporočila, kako naj v praksi zadostijo zahtevam ZVOP-1. Namen smernic je namreč podati skupne praktične napotke za upravljavce zbirk osebnih podatkov na jasen, razumljiv in uporaben način in s tem odgovoriti na najpogosteje zastavljena vprašanja s področja varstva osebnih podatkov, s katerimi se srečujejo posamezni upravljavci. Pravno podlago za izdajo smernic Informacijskemu pooblaščencu daje 49. člen ZVOP-1, ki

med drugim določa, da Informacijski pooblaščenec daje neobvezna mnenja, pojasnila in stališča o vprašanjih s področja varstva osebnih podatkov in jih objavlja na spletni strani ali na drug primeren način ter pripravlja in daje neobvezna navodila in priporočila glede varstva osebnih podatkov na posameznem področju. Leta 2011 je izdal Smernice o orodjih za zaščito zasebnosti na internetu.

Informacijski pooblaščenec je tudi leta 2011 obeležil Evropski dan varstva osebnih podatkov, ki je 28. januarja, in dne 26. januarja 2011 v Koloseju Ljubljana pripravil dogodek, s katerim je želel opozoriti na pomen varstva osebnih podatkov v sodobni, tehnološko vedno bolj razviti družbi. Osrednji del dogodka je bila slovenska premiera britanskega dokumentarnega filma o zasebnosti, nadzoru in vseobsegajočih bazah podatkov Izbrisati Davida. Film odpira mnoga vprašanja o družbi nadzora in izginjajoče zasebnosti. V sodobni družbi se mora namreč zasebnost pogosto boriti z ekonomičnostjo, praktičnostjo ter s zahtevami po večji varnosti. V tem boju je običajno zasebnost tista, ki izgublja. Film pripoveduje zgodbo o Davidu Bondu, ki živi v Veliki Britaniji, eni izmed držav z najbolj invazivnim sistemom nadzorovanja na svetu. Odloči se, da bo izvedel, koliko o njem dejansko vedo zasebna podjetja in vlada, zato se prepusti nadzoru in poskuša izginiti. Za seboj pusti nosečo ženo in majhnega otroka ter prične potovanje v neznano, kjer njegovemu gibanju stalno sledijo preko vseobsegajočih baz podatkov. To strašljivo potovanje ga prisili k premisleku o pomenu zasebnosti in izgubi le-te. Že tradicionalno je Informacijski pooblaščenec ob tej priložnosti dvema upravljavcema podelil nagrado za dobro prakso na področju varstva osebnih podatkov, enemu upravljavcu osebnih podatkov v zasebnem in drugemu v javnem sektorju. V zasebnem sektorju je nagrado prejelo Društvo življenje brez nasilja, ki je odlično poskrbelo za varstvo občutljivih osebnih podatkov njihovih strank, v javnem sektorju pa je bil prejemnik nagrade javni zavod Obalne lekarne Koper, ki si je nagrado prislužil z odličnim varstvom zdravstvenih podatkov strank. Lansko leto je bilo prvič podeljeno posebno priznanje za napore na področju vgrajene zasebnosti (privacy by design) Ambasador zasebnosti 2010. Nagrado je prejel Urad za meroslovje Republike Slovenije za delo na področju sektorskega merjenja hitrosti v prometu, ki dokazuje, da je novo metodo merjenja hitrosti vožnje mogoče izvajati tudi brez nesorazmernih posegov v zasebnost posameznika in z minimalno obdelavo osebnih podatkov. Priznanja so dobila tudi podjetja, ki so v letu 2010 pridobila certifikat po standardu za varovanje informacij ISO/IEC 27000 in s tem izkazala visoko raven zavarovanja osebnih podatkov.

Informacijski pooblaščenec je obeležil tudi Svetovni dan pravice vedeti, ki ga zaznamujemo vsako leto 28. septembra, vse odkar so se leta 2002 različne organizacije civilne družbe iz številnih držav povezale v organizacijo Freedom of Information Advocates Network (FOIAnet). Informacijski pooblaščenec je želel s svojim sporočilom o transparentnosti in pravici do javnih informacij doseči čim širšo javnost. S tem namenom je zasnoval letak s sloganom Radovednost odpira oči. Informacijski pooblaščenec je ugotovil, da je "radovednost" državljanov na zelo zadovoljivi ravni, kar postopoma, a zanesljivo, pripomore k zavedanju celotnega javnega sektorja, da je s svojim delovanjem odgovoren ljudem, ki za njegov obstoj in funkcioniranje plačujejo davke in druge dajatve. Žal pa je opazil, da kljub določenemu napredku na področju zavedanja javnih uslužbencev in funkcionarjev, njihovo delo ni in ne more biti tajno (razen izjemoma in v zakonsko predvidenih okoliščinah). Še naprej narašča število primerov, ko organi prosilcem v zakonskem roku 20 delovnih dni ne posredujejo dokumentov ali z odločbo odločijo o tem, zakaj se pravica do dokumentov zavrne. Takšna praksa je popolnoma nesprejemljiva. V demokratični družbi ima namreč vsakdo pravico, da mu organi oblasti pojasnijo, zakaj so mu omejili z ustavo zagotovljeno temeljno človekovo pravico dostopa do informacij javnega značaja. Informacijski pooblaščenec je opozoril tudi na vedno bolj pogosto prakso organov, da se pri zavrnitvi dostopa do dokumentov sklicujejo na izjemo tajnih podatkov. Mnogo organov "tajnost" dokumentov razume zelo posplošeno; da so to podatki, ki jih javnost ne sme videti ali za katere drugi zakoni določajo, da so »tajni«. Informacijski pooblaščenec pa vedno znova poudarja, da so lahko "tajni" le podatki, ki izpolnjujejo stroge pogoje, določene z Zakonom o tajnih podatkih. Eno od pomembnih načel, ki so jih razvili pri zelo vplivni organizaciji s področja transparentnosti Open Society Justice Iniciative namreč pravi: "Dostop je pravilo – tajnost je izjema!" Vlada Republike Slovenije bi si morala po mnenju Informacijskega pooblaščenca veliko bolj prizadevati za promocijo transparentnosti javnega sektorja, saj je na tem področju popolnoma neaktivna. Jasno je, da se nezanimanje vlade za to temo odraža pri delovanju organov, ki prepogosto državljanom niti ne odgovorijo na njihove vloge. Slovenija dve leti po podpisu še vedno ni ratificirala Konvencije Sveta Evrope o dostopu do uradnih dokumentov, za podpis katere je pohitela med predsedovanjem Sveta Evrope, ni se pridružila Partnerstvu za odprto upravo,

ki ga je podpisalo 43 držav po svetu, ne spodbuja nevladnih organizacij, ki se ukvarjajo z vprašanji odprtosti javne uprave, načrtovane spremembe ZDIJZ pa gredo v smeri oženja pravice do dostopa do dokumentov. Informacijski pooblaščenec je organe zavezance in pristojno ministrstvo za javno upravo pozval, naj pri uporabi in razlagi ZDIJZ ter pri načrtovanju morebitnih sprememb zakonodaje sledijo temeljnemu namenu tega zakona, ki je v zagotavljanju javnosti in odprtosti delovanja vseh organov zavezancev. To pomeni, da je prost dostop do informacij pravilo, zakonske izjeme pa je treba razlagati restriktivno.

Mednarodni organizaciji Access Info Europe (Španija) in Centre for Law and Democracy (Kanada) sta v 89 državah izvedli raziskavo o kakovosti zakonodaje s področja dostopa do informacij javnega značaja. Raziskava je bila usmerjena v ustreznost pravnih temeljev zagotavljanja te pravice, ne pa v samo izvajanje zakonov v praksi. Rezultati so pokazali, da stare demokracije, v Evropi zahodne države, nimajo dobre zakonodaje predvsem zato, ker je zakonodaja stara in je ne obnavljajo v skladu s potrebami in razvojem te temeljne človekove pravice in niti ne kažejo nobene želje po prenovi. Slovenija se je z odličnim zakonom uvrstila na zavidljivo drugo mesto, vendar se je treba zavedati, da dobra zakonodaja ni garancija transparentnosti, če se ne izvaja tudi v praksi. Na prvem mestu te raziskave je po kakovosti zakona in ustreznih in učinkovitih pristojnostih Informacijskega pooblaščenca Srbija, ki ji je bila slovenska zakonodaja vzor, in na tretjem mestu Indija, ki je leta 2005 dobila res zelo sodoben in učinkovit zakon o dostopu do javnih informacij. Na zadnjih treh mestih med 89 državami, kjer je bila raziskava izvedena, pa najdemo tri države članice EU, in sicer Grčijo, Avstrijo in Nemčijo.

Center za raziskovanje javnega mnenja Politbarometer je leta 2011 v okviru projekta Javnomnenjske raziskave o odnosu javnosti do aktualnih razmer in dogajanj v Sloveniji izvedel več raziskav. Raziskava iz meseca marca vključuje tudi ocene zaupanja v nadzorne institucije sistema. Navedena meritev je Informacijskega pooblaščenca uvrstila na prvo mesto med institucijami, ki jim Slovenci najbolj zaupajo (51 %). Sledijo Varuh človekovih pravic, Komisija za preprečevanje korupcije, Generalni direktor policije in Generalna državna tožilka. Informacijski pooblaščenec se je med naštetimi institucijami uvrstil najvišje oziroma so mu anketiranci izrazili najvišje zaupanje tudi v raziskavah v letu 2010 in na začetku leta 2012, kar kaže na ustaljeno zaupanje v Informacijskega pooblaščenca.

Skupnost informacijskih pooblaščencev in podobnih institucij, ki skrbijo za transparentnost in varstvo pravice dostopa do informacij, je letos oktobra na 7. mednarodni konferenci informacijskih pooblaščencev v kanadski Ottawi sprejela odločitev, da ustvari in predstavi javnosti skupno spletno stran vseh pooblaščencev. To zahtevno nalogo so informacijski pooblaščenci zaupali slovenskemu Informacijskemu pooblaščencu, ki je tako prevzel iniciativo in ustvaril spletno stran info-commissioners.org ter jo konec novembra predstavil javnosti. Vsebina spletne strani je zanimiva tako za informacijske pooblaščence kot za širšo zainteresirano javnost, saj ponuja osnovne informacije o vseh informacijskih pooblaščencih po svetu, povezave do njihovih spletnih strani, poleg tega pa zajema tudi vse zakone o dostopu do javnih informacij držav, ki so jih do sedaj sprejele, letna poročila pooblaščencev in mnogo drugih informacij. Informacijski pooblaščenci imajo na tej spletni strani priložnost objavljati novice o svojem delovanju, informacije o pomembnih dogodkih, sprejetih prelomnih odločitvah itd. Kmalu bo v celoti začel delovati tudi nejavni del spletne strani (t.i. Skupnost oziroma Community), preko katere bodo informacijski pooblaščenci lahko komunicirali drug z drugim.

4.3. Mednarodno sodelovanje

4.3.1. Sodelovanje na mednarodnih srečanjih

Leta 2011 so se zaposleni pri Informacijskem pooblaščencu udeležili več mednarodnih seminarjev in konferenc. Na nekaterih so sodelovali tudi s svojimi prispevki:

- 26. – 27. januar 2011, Budimpešta, Madžarska. Ob dnevu varstva osebnih podatkov se je konference v organizaciji madžarskega pooblaščenca udeležil mag. Andrej Tomšič, namestnik informacijske pooblaščenke, s predavanjem o spletnih družbenih omrežjih in varstvu osebnih podatkov.
- 18. februar 2011, Berlin, Nemčija. Seminar Evropske platforme za ponovno uporabo informacij javnega značaja (ePSI Platform) z naslovom Open Data: Apps for everyone?, ki se ga je udeležila raziskovalka Tina Kraigher.
- 14. – 18. marec 2011, Den Haag, Nizozemska. Mag. Andrej Tomšič, namestnik informacijske pooblaščenke, je kot član inšpekcijske ekipe JSB sodeloval v nadzoru EUROPOLA.
- 4. – 6. april 2011 Montreal, Kanada. Zasedanja skupine IWGDPT, mednarodne delovne skupine za varstvo osebnih podatkov v telekomunikacijah, se je udeležil mag. Andrej Tomšič, namestnik informacijske pooblaščenke.
- 7. april 2011, London, Velika Britanija. Konference Children & the Web, organizirane s strani DataGuidance, sta se udeležili asistentka svetovalca Eva Kalan in raziskovalka Jelena Burnik.
- 28. – 29. april 2011, Budimpešta, Madžarska. Srečanje skupine CEEDPA, skupine srednjeevropskih in zahodnoevropskih organov za varstvo osebnih podatkov. Zasedanja so se udeležili Jure Logar in Klemen Mišič, državna nadzornika za varstvo osebnih podatkov, in raziskovalec Matic Petek.
- 4. – 6. maj 2011, Milano, Italija. V okviru projekta LAPSI je potekala prva javna konferenca z naslovom PSI at the Crossroads: Current Challenges and New Opportunities o ponovni uporabi informacij javnega sektorja. Dogodka so se udeležile svetovalke Jasna Rupnik, Maja Lubarda, Mojca Komac in Polona Tepina.
- 16. – 18. maj 2011, Podgorica, Črna Gora. Mednarodna konferenca na temo boja proti korupciji in organiziranemu kriminalu, ki jo je organizirala nevladna organizacija MANS. Konference se je udeležila Kristina Kotnik Šumah, namestnica pooblaščenke.
- 20. – 21. maj 2011, Thessaloniki, Grčija. Državni nadzornik Klemen Mišič se je udeležil mednarodnega seminarja o informacijskem pravu, v okviru katerega je predstavil prispevek z naslovom ePrivacy in Practice.
- 30. – 31. maj 2011, Potsdam, Nemčija. Mednarodni simpozij Potrošniške informacije - Regulacija trga s pomočjo transparentnosti. Zasedanja se je udeležila svetovalka Mojca Komac.
- 30. – 31. maj 2011, Beograd, Srbija. Konferenca EuroDIG s področja politične participacije s pomočjo interneta, zasebnosti in varnosti na internetu. Konference sta se udeležila državni nadzornik Jure Logar in informatik mag. Matjaž Drev.
- 8. – 9. junij 2011, Berlin, Nemčija. Konference o dostopu do informacij javnega značaja, Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit, se je s predavanjem udeležil Urban Brulc, svetovalec informacijske pooblaščenke.
- 14. – 15. junij 2011, Varšava, Poljska. Konference BCR in practice – DPA sharing experience se je udeležila razskovalka Jelena Burnik.
- 22. junij 2011, Bruselj, Belgija. Delavnica Workshop with data protection authorities on future options for data retention in the EU. Delavnice se je udeležila raziskovalka Jelena Burnik.
- 11. – 12 julij 2011, Barcelona, Španija. Konferenca 7th International Conference on Internet, Law and Politics. Konference se je udeležila raziskovalka Jelena Burnik s prispevkom in predavanjem na temo bodoče regulacije vedenjskega oglaševanja v elektronskih komunikacijah v EU.
- 12. – 13. september 2011 Berlin, Nemčija. 50. zasedanje skupine IWGDPT, mednarodne delovne skupine za varstvo osebnih podatkov v telekomunikacijah. Zasedanja se je udeležil mag. Andrej Tomšič, namestnik informacijske pooblaščenke.
- 28. september 2011, Bruselj, Belgija. Seminarja z naslovom Svetovni dan pravice vedeti - kaj se EU lahko nauči od drugih, ki ga je organiziral Evropski varuh človekovih pravic, se je udeležila svetovalka Jasna Rupnik.
- 4. – 5. oktober 2011, Ottawa, Kanada. 7. mednarodne konference informacijskih pooblaščencev se je udeležila pooblaščenka Nataša Pirc Musar in njeni namestnici Kris-

tina Kotnik Šumah in Rosana Lemut-Strle. Na konferenci je 23 pooblaščencev sprejelo tudi mednarodno resolucijo.

- 4. – 5. oktober 2011, Varšava, Poljska. 23rd Case Handling Workshop, ki ga je organiziral poljski Pooblaščenec, sta se udeležili raziskovalki Tanja Peršin in Nina Komočar, ki je imela vlogo vodje skupine študije primerov spletnih storitev.
- 19. – 21. oktober 2011, Varšava, Poljska. V okviru projekta LAPSI je potekal peti tematski seminar in druga interna konferenca, v organizaciji Open Knowledge Foundation in Centrum Cyfrowe pa je potekal tudi Open Government Data Camp. Obeh dogodkov so se udeležile svetovalke Mojca Komac, Polona Tepina in Maja Lubarda, ki je predstavila tudi prispevek o pristojnostih in delovanju slovenskega Informacijskega pooblaščenca.
- 31. oktober – 4. november 2011, Mexico City, Mehika. 33. mednarodne konference pooblaščencev za varstvo osebnih podatkov in zasebnosti se je udeležil namestnik informacijske pooblaščenke, mag. Andrej Tomšič.

4.3.2. Sodelovanje v mednarodnih delovnih telesih

Informacijski pooblaščenec kot državni nadzorni organ za varstvo osebnih podatkov sodeluje tudi s pristojnimi organi Evropske unije (EU) in Sveta Evrope za varstvo osebnih podatkov. Sodelovanje na mednarodni ravni in sodelovanje pri zakonodajnih postopkih EU mu narekuje tudi Direktiva 95/46/ES.

Informacijski pooblaščenec je leta 2011 aktivno sodeloval v šestih delovnih telesih EU, ki se ukvarjajo z nadzorom nad izvajanjem varstva osebnih podatkov v okviru posameznih področij EU, in sicer:

- v Delovni skupini za varstvo osebnih podatkov po 29. členu Direktive 95/46/ES ter štirih njenih podskupinah (v tehnološki podskupini, podskupini Future of Privacy, podskupini BCR in podskupini BTLE),
- v Skupnem nadzornem organu za Europol,
- v Skupnem nadzornem organu za Schengen,
- v Skupnem nadzornem organu za carino,
- na skupnih koordinacijskih sestankih Evropskega nadzornika za varstvo osebnih podatkov in nacionalnih organov za varstvo osebnih podatkov za nadzor nad CIS,
- na koordinacijskih sestankih Evropskega nadzornika za varstvo osebnih podatkov in državnih organov za varstvo osebnih podatkov za nadzor EURODAC.

Delovna skupina po 29. členu (Article 29 Data Protection Working Party) je lani sprejela več pomembnih mnenj, med drugim mnenje o privolitvi; o spremenjenem predlogu industrije glede okvira ocene učinka na varstvo zasebnosti in podatkov za aplikacije radiofrekvenčne identifikacije (RFID); o predlogu Direktive o uporabi podatkov iz evidence podatkov o potnikih za preprečevanje, odkrivanje, preiskovanje in pregon terorističnih in hudih kaznivih dejanj; o inteligentnih merilnih sistemih; o geolokacijskih storitvah na pametnih prenosnih napravah; o varstvu podatkov v zvezi s preprečevanjem pranja denarja in bojem proti financiranju terorizma ter o priporočilu najboljše prakse EASA/IAB v zvezi s spletnim vedenjskim oglaševanjem. Med pomembnejše aktivnosti delovne skupine je sodilo spremljanje in priprava odzivov na predlog nove Uredbe o varstvu osebnih podatkov, ki naj bi prvič v zgodovini poenotila režim varstva osebnih podatkov v vseh državah članicah. Delovna skupina se je pri tem sestala tudi s komisarko za pravosodje Viviane Reding. Člani so si izmenjevali podatke o preiskavah pomembnejših primerov domnevnih kršitev varstva osebnih podatkov, predvsem tistih, ki so vplivali na posameznike po vsej Evropi, in so bili povezani z velikimi upravljavci osebnih podatkov – multinacionalnih korporacij.

V okviru delovne skupine po 29. členu je Informacijski pooblaščenec aktivno sodeloval tudi v štirih njenih podskupinah, in sicer v (1) podskupini za internet in informacijske tehnologije, t. i. Tehnološki podskupini, (2) v podskupini Future of Privacy, (3) v podskupini BCR (glede zavezujočih poslovnih pravil, ki so podlaga za iznos podatkov v tretje države) ter (4) v podskupini BTLE (za varstvo osebnih podatkov na področju nadzora mej, transporta in organov pregona). Tehnološka podskupina se je v letu 2011 ukvarjala predvsem s pametnimi števci, samo-regulativnim kodeksom za vedenjsko oglaševanje, ki ga je predlagala industrija, s pametnimi telefoni, ki omogočajo oddajanje geolokacije, orodji za spletno analitiko, piškotki, orodji za prepoznavo obraza in računalništvom v oblaku. Podskupina Future of Privacy se je osredotočala na prenovo Direktive 95/46/ES o varstvu osebnih

podatkov, pri čemer je veliko pozornosti namenila predvsem pristojnostim nacionalnih nadzornih organov, konceptu občutljivih osebnih podatkov ter učinkovitosti nekaterih elementov obstoječe direktive, kot so centralni registri zbirk osebnih podatkov. V okviru podskupine BCR je Informacijski pooblaščenec sodeloval pri pripravi okvirja za instrument zavezujočih poslovnih pravil za pogodbene obdelovalce, ki se predvsem kažejo kot možno učinkovito orodje pri iznosu osebnih podatkov v tretje države v okviru računalništva v oblaku. Podskupina BTLE, ki se je kot taka formirala šele v letu 2011, pa se je osredotočala na evidence podatkov o potnikih v letalskem prometu, na telesne skenerje na letališčih, na evropski sistem za sledenje financiranja terorističnih dejavnosti (TFTS) ter na predlog nove Direktive o varstvu posameznikov pri obdelavi osebnih podatkov, ki jih pristojni organi obdelujejo za namene preprečevanja, preiskovanja, odkrivanja ali pregona kaznivih dejanj ali izvrševanja kazenskih sankcij, in o prostem pretoku takih podatkov.

Informacijski pooblaščenec je aktivno sodeloval tudi pri pripravi in izvedbi dveh delavnic na temo obveznega poročanja o incidentih, ki zadevajo varstvo osebnih podatkov, v okviru delovne skupine Implementation of e-Privacy Directive.

Informacijska pooblaščenka je v lanskem letu nadaljevala z delom podpredsednice Skupnega nadzornega organa za Europol. Pod gostiteljstvom Informacijskega pooblaščenca so se člani skupnih nadzornih organov za Europol, Eurojust, Schengen in carine konec januarja 2011 na skupnem zasedanju zbrali v Ljubljani, kjer so na dvodnevnem zasedanju razpravljali o načinu organizacije in delovanja skupnih nadzornih organov v prihodnje.

Marca 2011 je namestnik informacijske pooblaščenke sodeloval v mednarodni inšpekcijski skupini, ki je na sedežu v Haagu opravila nadzor nad varstvom osebnih podatkov na Europolu.

Informacijski pooblaščenec se je redno udeleževal tudi sestankov Delovne skupine za varstvo osebnih podatkov v okviru policijskega in pravosodnega sodelovanja (WPPJ), ki kot specifična delovna skupina že od leta 2007 deluje na podlagi mandata Konference evropskih organov za varstvo osebnih podatkov in je zadolžena za spremljanje razvoja glede varstva osebnih podatkov na področju policije in pravosodnega sodelovanja. V letu 2011 se je WPPJ posvečala predvsem obdelavi podatkov o DNK s strani organov pregona, spremljanju implementacije Okvirnega sklepa Sveta 2008/977/JHA o varstvu osebnih podatkov, ki se obdelujejo v okviru policijskega in pravosodnega sodelovanja v kazenskih zadevah, ter nadaljevanju sodelovanja s Svetom Evrope, zlasti v zvezi z revizijo Konvencije Sveta Evrope o varstvu posameznikov glede na avtomatsko obdelavo osebnih podatkov (Konvencija št. 108) in Priporočila R(87)15 o obdelavi policijskih podatkov.

Informacijski pooblaščenec je aktivno sodeloval tudi v Mednarodni delovni skupini za varstvo osebnih podatkov v telekomunikacijah (IWGDPT – International Working Group on Data Protection in Telecommunications), v okviru katere se srečujejo predstavniki informacijskih pooblaščencev in organov za varstvo osebnih podatkov in zasebnosti s celega sveta. Delovna skupina je na zasedanjih v Montrealu in Berlinu sprejela naslednje dokumente: Privacy by Design and Smart Metering: Minimize Personal Information to Maintain Privacy, Working Paper on Privacy and Electronic Micropayment on the Internet, Working Paper: Event Data Recorders on Vehicles - Privacy and data protection issues for governments and manufacturers.

V okviru Sveta Evrope je predstavnik Informacijskega pooblaščenca tudi v letu 2011 sodeloval v Posvetovalnem odboru (T-PD) po Konvenciji Sveta Evrope o varstvu posameznikov glede na avtomatsko obdelavo osebnih podatkov (Konvencija št. 108). Odbor T-PD je na edinem lanskem plenarnem zasedanju (v začetku decembra) razpravljal predvsem o predlogih sprememb Konvencije št. 108 iz javne razprave, ki je o tem potekala od začetka leta 2011, obravnavo predlaganih sprememb z namenom posodobitve te konvencije pa Odbor nadaljuje v letu 2012. Odbor T-PD je obravnaval še dve priporočili Sveta Evrope, ki sta v postopku spreminjanja oz. posodabljanja, in sicer o varstvu osebnih podatkov na področju zaposlovanja in na policijskem področju. Kot vsako leto, so bila obravnavana tudi poročila o

mednarodnem in globalnem sodelovanju Sveta Evrope v zvezi z varstvom osebnih podatkov ter poročila nadzornih organov za varstvo osebnih podatkov iz držav članic Sveta Evrope o novostih in dosežkih na tem področju, ter še posebej informacije o obeležitvi Dneva varstva osebnih podatkov.

4.3.3. Ostale mednarodne dejavnosti

Z vstopom Republike Slovenije v schengensko območje je Informacijski pooblaščenec pristojen tudi za nadzor nad izvajanjem 128. člena Schengenske konvencije ter predstavlja neodvisen organ za nadzor prenosa osebnih podatkov za namene te konvencije. Leta 2011 Informacijski pooblaščenec ni prejel nobene pritožbe glede izvajanja te pravice na prvi stopnji.

V okviru nacionalnih pristojnosti nadzora varstva osebnih podatkov je Informacijski pooblaščenec izvedel inšpekcijski nadzor na veleposlaništvu Republike Slovenije v Prištini in v Kairu, kjer je med drugim preverjal tudi zakonitost obdelave osebnih podatkov v okviru postopkov za pridobitev Schengenskega vizuma ter v okviru vizumskega informacijskega sistema (VIS).

Informacijski pooblaščenec je v letu 2011 gostil predstavnike sorodnih institucij iz nekaterih evropskih držav, kot so Hrvaška, Srbija, Kosovo, Črna gora in Makedonija in jim predstavil svoje delovanje ter dobre prakse s področij, za katere je pristojen.

Informacijski pooblaščenec je v letu 2011 pripravil odgovore na 24 vprašalnikov tujih organov za varstvo osebnih podatkov, mednarodnih organizacij in tujih nevladnih organizacij.

V letu 2011 je Informacijski pooblaščenec kot Junior Partner nadaljeval z izvedbo projekta tesnega medinstitucionalnega sodelovanja IPA 2009, št. MN/09/IB/JH/03 – »Implementation of Personal Data Protection Strategy« v Črni gori, za katerega je bil leta 2010 izbran skupaj z nosilcem projekta Ludwig Boltzmann Institute for Human Rights iz Avstrije, in ki se osredotoča na vzpostavitev nacionalnega organa za varstvo osebnih podatkov v Črni gori, izobraževanje kadrov, izgradnjo in implementacijo pravnega okvira za varstvo osebnih podatkov v državi ter tesnejše sodelovanje Črne gore z EU na tem področju. Projekt se nadaljuje tudi v letu 2012.

Novembra 2011 je bil Informacijski pooblaščenec s strani Evropske komisije izbran za izvedbo twinning light projekta SR/2009/IB/JH/01 – »Improvement of Personal Data Protection« v Srbiji. Projekt se osredotoča na izboljšanje varstva osebnih podatkov v Srbiji in krepitev nacionalnega nadzornega organa za varstvo osebnih podatkov, izobraževanje kadrov nadzornega organa, analizo in predloge sprememb pravnega okvira za varstvo osebnih podatkov v državi, pripravo kampanj osveščanja o varstvu osebnih podatkov, izobraževanje izbranih skupin upravljavcev in obdelovalcev osebnih podatkov ter tesnejše sodelovanje Srbije z EU na tem področju. Projekt se izvaja v letu 2012.

Informacijski pooblaščenec je v lanskem letu nadaljeval z delom na evropskem projektu LAPSI, namenjenemu izgradnji tematske mreže strokovnjakov na področju ponovne uporabe informacij javnega značaja, s ciljem odprave ovir v praksi za njeno izvajanje. Projekt se nadaljuje tudi v letu 2012.

Odgovorna urednica:

Nataša Pirc Musar

Avtorji besedil:

dr. Monika Benkovič Krašovec, državna nadzornica za varstvo osebnih podatkov
Jože Bogataj, vodja državnih nadzornikov za varstvo osebnih podatkov
Alenka Jerše, generalna sekretarka
Eva Kalan, svetovalka
Polona Tepina, svetovalka
Kristina Kotnik Šumah, namestnica informacijske pooblaščenke
mag. Andrej Tomšič, namestnik informacijske pooblaščenke

Oblikovanje:

Bons d.o.o. in Klemen Mišič

Lektorirala:

Vesna Veingerl, univ. dipl. nov.

Informacijski pooblaščenec Republike Slovenije
Vošnjakova 1
1000 Ljubljana

www.ip-rs.si
gp.ip@ip-rs.si

Ljubljana, maj 2012

ISSN 1854-9500