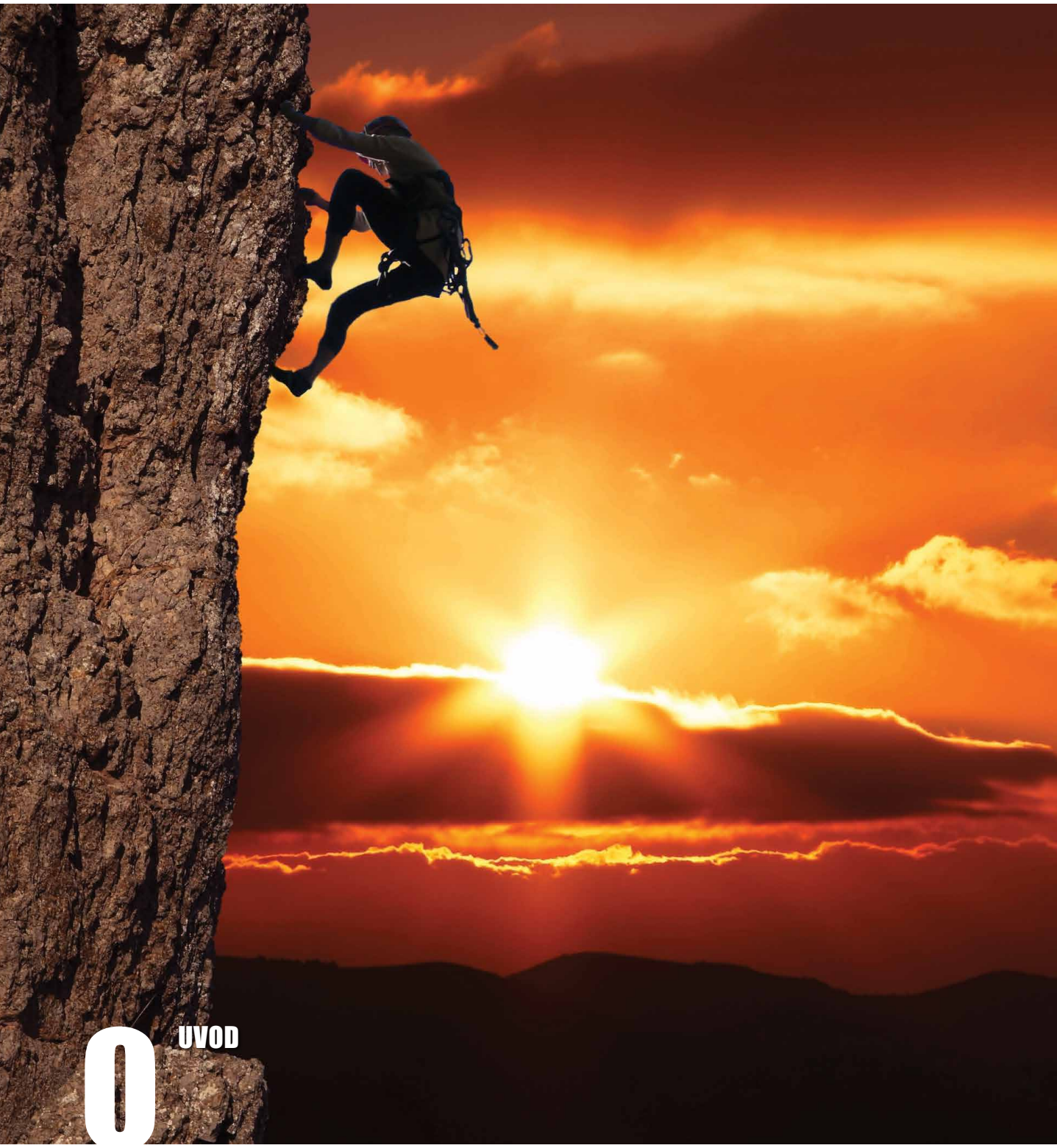
INFORMACIJSKI POOBLAŠČENEC
REPUBLIKE SLOVENIJE

'12 Letno poročilo Informacijskega pooblaščenca

za leto 2012

'12

Letno poročilo Informacijskega pooblaščenca za leto 2012



0 UVOD

Leto 2012 bi lahko označili kot leto velikopoteznih načrtov države v smeri dodatne informatizacije velikih javnih zbirk osebnih podatkov po hitrem postopku in rasti apetitov javnega sektorja po vse obsežnejši obdelavi osebnih podatkov posameznikov. Predvsem je zaskrbljujoče, da država, ki bi v skladu s slovensko ustavo morala varovati zasebnost, začenja najedati njene temelje.

Informacijski pooblaščenec je v letu 2012 obravnaval več kot 80 različnih predlogov sprememb zakonodaje, ki opredeljuje zbiranje in obdelavo osebnih podatkov, kar je za več kot tretjino več kot v letu 2011. Številni med njimi so poskusi uzakonjenja po mnenju Informacijskega pooblaščenca nesorazmernih zahtev po zbiranju in obdelavi osebnih podatkov, ki v zameno za zmanjšan obseg zagotovljene zasebnosti ne bodo prinesli niti poenostavitve postopkov niti varčevanja. Med pomembnejšimi zakoni, ki so doživeli spremembe ali poskuse sprememb v letu 2012, so Zakon o elektronskih komunikacijah, Zakon o nalogah in pooblastilih policije, Zakon o urejanju trga dela, Zakon o dedovanju, Zakon o javnem naročanju, Zakon o državni upravi. V večini teh predlogov sprememb je zaznati tako rekoč popolno odsotnost presoj vplivov posameznih načrtovanih oblik zbiranja in obdelave osebnih podatkov na zasebnost. Vse kaže, da finančna kriza tega področja ni prizadela v tolikšni meri kot druge dele javnega sektorja. Celo nasprotno, številni med temi nas bodo zelo drago stali.

Informacijski pooblaščenec je ob tem v preteklem letu na obeh področjih delovanja ponovno prejel izredno veliko število vlog posameznikov, pa naj gre za zaprosila za mnenja, prijave ali pritožbe. Takšne razmere so sicer po eni strani razveseljujoče, ker nedvomno pričajo o tem, da posamezniki vse bolj razumejo namen in pomen obeh človekovih pravic v pristojnosti Informacijskega pooblaščenca. Hkrati pa ne smemo mimo dejstva, da gre tudi v letu 2012 tolikšno povečanje števila pritožbenih in inšpekcijskih zadev pripisati nekaterim zaskrbljujočim ravnanjem, na eni strani organov zavezancev na področju dostopa do informacij javnega značaja, kot tudi vse težje obvladljivim željam po obdelavi osebnih podatkov najrazličnejših upravljavcev zbirk osebnih podatkov, tako v zasebnem kot tudi v javnem sektorju.

Informacijski pooblaščenec si pri svojem delu kljub izredno velikemu pripadu zadev prizadeva za čim večjo odzivnost in strokovnost, ki pa ob tolikšnem povečevanju obsega zadev v reševanju postajata komajda še dosegljiva cilja. Vesela sem, da nam je to tudi v letu 2012 uspelo in da javnost 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 2013 stopnja zaupanja Informacijskemu pooblaščencu ponovno značilno visoka in celo najvišja med izbranimi šti-

rimi neodvisnimi državnimi nadzornimi organi. Ker tudi predhodne meritve kažejo visoko raven zaupanja in so deleži vselej v zgornji polovici lestvice, lahko govorimo o ohranitvi že v preteklosti izraženega zaupanja, kar me izjemno veseli ter hkrati zavezuje k nadaljevanju dela in iskanju možnosti za izboljšave.

Informacijski pooblaščenec je v letu 2012 izdal 256 odločb v pritožbenih postopkih na področju dostopa do informacij javnega značaja, pri čemer so pritožbeni postopki pravno vse zahtevnejši. Z vsebinskega vidika je porast pritožb glede na 2011 zaznati na področju zaračunavanja stroškov, več je pritožb, ki jih vlagajo mediji, ter pritožb s področja dostopa do dokumentacije iz postopkov javnih naročil. V letu 2012 je Informacijski pooblaščenec glede na leto 2011 prejel tudi precej večje število vlog za pojasnila, mnenja in razlago prakse, tako s strani prosilcev kot s strani zavezanih organov. Po oceni Informacijskega pooblaščenca so prosilci s pravico dostopa do informacij javnega značaja dobro seznanjeni in jo v praksi pogosto uresničujejo, na drugi strani pa je pri organih (tudi zaradi pomanjkanja kadrovskih in finančnih virov) še vedno zaznati nepoznavanje obveznosti, ki jih prinaša Zakon o dostopu do informacij javnega značaja. Ta problematika je prisotna zlasti v organih širšega javnega sektorja (javni zavodi, druge pravne osebe javnega prava, nosilci javnih pooblastil in izvajalci javnih služb). Zato je Informacijski pooblaščenec za te zavezance izvedel več brezplačnih delavnic in predstavitev.

Na področju varstva osebnih podatkov je v letu 2012 Informacijski pooblaščenec obravnaval 725 inšpekcijskih (6% več kot v letu 2011) in 158 prekrškovnih postopkov (16% več kot v letu 2011). Z vidika trendov na tem področju je treba izpostaviti računalništvo v oblaku (angl. cloud computing), ki igra na področju tehnološkega razvoja čedalje pomembnejšo vlogo pri obdelavi osebnih podatkov. Potenciali računalništva v oblaku so izjemni, zato pa zagotovo ne sme priti do nižanja ravni varstva osebnih podatkov kot temeljne človekove pravice. Informacijski pooblaščenec je s ciljem prispevanja k vzpostavitvi ustreznih standardov na tem področju v letu 2012 kot eden prvih nadzornih organov v EU v sodelovanju s Cloud Security Alliance (CSA) - Slovenia Chapter, Slovenskim odsekom ISACA ter Zavodom e-Oblak, Eurocloud Slovenia izdal smernice za varstvo osebnih podatkov pri računalništvu v oblaku[1]*. Namen smernic je dati enotne kontrolne točke, s pomočjo katerih bodo lahko tako uporabniki kot nadzorni organi sprejemali bolj informirane odločitve glede uporabe in nadzora računalništva v oblaku v delu, ki se nanaša na obdelavo osebnih podatkov. Ponudnikom storitev računalništva v oblaku ter iniciativam za varnost in certificiranje tovrstnih storitev pa naj bi smernice ponudile napotke za nadaljnji razvoj s ciljem skladnosti z zakonodajo o varstvu osebnih podatkov. Informacijski pooblaščenec ugotavlja, da številni ponudniki storitev računalništva v oblaku potencialnim uporabnikom trenutno večinoma še ne ponudijo zadostnih informacij za preudarne odločitve in da je treba vzpostaviti mehanizme, ki bodo omogočali razlikovanje med zaupanja vrednimi ponudniki računalništva v oblaku in ponudniki, katerih storitve spremljajo določena tveganja.*

Drug pomemben trend, ki ga je na področju varstva osebnih podatkov v bližnji prihodnosti treba pozorno spremljati, je t.i. koncept »big data«. Gre za zelo velike podatkovne zbirke, ki jih je zaradi obsežnosti težko obvladovati z običajnimi orodji za upravljanje podatkovnih baz. Tovrstne baze omogočajo hiter zajem in obdelavo različnih (ne)struktiriranih podatkovnih virov, kar omogoča, da »vidimo« in »izmerimo« stvari, ki jih prej nismo mogli. Z vzporednim pojavom »interneta stvari« (npr. pametni telefoni, naprave za elektronsko cestninjenje v avtomobilih, pametni števci porabe v gospodinjstvih ipd.), kjer naprava čedalje več podatkov lahko zbira v digitalni obliki, se količine zbranih osebnih podatkov o posameznikih izjemno povečujejo. Količina informacij, ki jo obvladuje upravljavec takšnih tehnologij, je namreč tako velika, da omogoča predvidevanje poslovnih trendov, nakupovalnih navad, prometnih vzorcev vse do napovedovanja izbruhov gripe in verjetnosti kaznivih dejanj na določenem geografskem področju. Omogoča tudi (pravilna ali napačna) sklepanja o posamezniku, njegovi kreditni sposobnosti, zdravstvenem stanju, nakupovalnih navadah in drugih lastnostih, ki mu jih prej ni bilo mogoče enostavno pripisati. Implikacije na varstvo osebnih podatkov so lahko obsežne, zato je »big data« prav gotovo med najpomembnejšimi novimi pojavi, katerega razvoj je, ko govorimo o varstvu zasebnosti, treba spremljati z vso skrbnostjo.

---

[1] https://www.ip-rs.si/varstvo-osebnih-podatkov/iskalnik-po-odlocbah-in-mnenjih/smernice/

Informacijski pooblaščenec je leta 2012 precej pozornosti namenil preventivnemu delovanju. Poleg omenjenih smernic za varstvo osebnih podatkov pri računalništvu v oblaku je z različnimi dejavnostmi zaznamoval dan varstva osebnih podatkov in svetovni dan pravice vedeti. 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 v letu 2012 izpeljal twinning light projekt na področju varstva osebnih podatkov v Srbiji. V okviru mednarodnega sodelovanja na področju dostopa do informacij javnega značaja je sodeloval v projektu LAPSI 1.0, ki se je v letu 2012 zaključil, pridružil pa se je tudi projektu LAPSI 2.0, ki se bo začel izvajati v letu 2013.

Glede na predstavljene trende bi na obeh področjih delovanja Informacijskega pooblaščenca v prihodnje s strani vlade pričakovali aktivnejša prizadevanja za učinkovito zaščito obeh ustavno zagotovljenih pravic. Na področju dostopa do informacij javnega značaja bi si želela aktivnejšega prizadevanja za spodbujanje zavezancev k bolj transparentnemu delovanju, s čimer bi skupaj prispevali tudi k večji integriteti javnega sektorja in zaupanju posameznikov v institucije države. Na tem mestu ponovno ne morem mimo predloga o potrebnosti širitve kroga zavezancev za dostop do informacij javnega značaja na družbe, v katerih imajo država, lokalna skupnost ali javni zavodi prevladujoč vpliv. Minister za notranje zadeve in javno upravo je aprila 2013 obljubil, da bodo naši predlogi naleteli na plodna tla. Držali ga bomo za besedo! Na področju varstva osebnih podatkov pa bi si tako s strani upravljavcev v javnem kot tudi zasebnem sektorju želela, da bi pokazali več skrbi in zavedanja o posledicah na videz nepomembnih ukrepov množičnega in nesorazmernega zbiranja osebnih podatkov, ki so nas pravzaprav že pripeljali v družbo nadzora.

Izzivi, ki so pred nami, niso majhni. Pomembno je, da se z njimi soočimo. Informacijski pooblaščenec bo svoje delo še naprej opravljal po svojih najboljših močeh.

Za konec si želim, da bi o tem, kakšno družbo in državo si želimo, tudi z vidika varstva zasebnosti in transparentnosti, razmišljali vsi, predvsem pa bralci tega poročila v Državnem zboru.

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. Stroški postopka 15
2.6.2. Ponovna uporaba informacij javnega značaja 16
2.6.3. Osebni podatki 17
2.6.4. Mediji, osebni podatki 18
2.6.6. Ali gre za delovno področje organa, poslovna skrivnost 20
2.6.6. Osebni podatki 20
2.6.7. Javna naročila, osebni podatki, poslovna skrivnost 21
2.6.8. Kazenski postopek, notranje delovanje organa, osebni podatek, mediji 22
2.6.9. Osebni podatek, test interesa javnosti 23
2.6.10. Javna naročila, poslovna skrivnost, test interesa javnosti 24
2.7. Splošna ocena in priporočila na področju dostopa do informacij javnega značaja 26

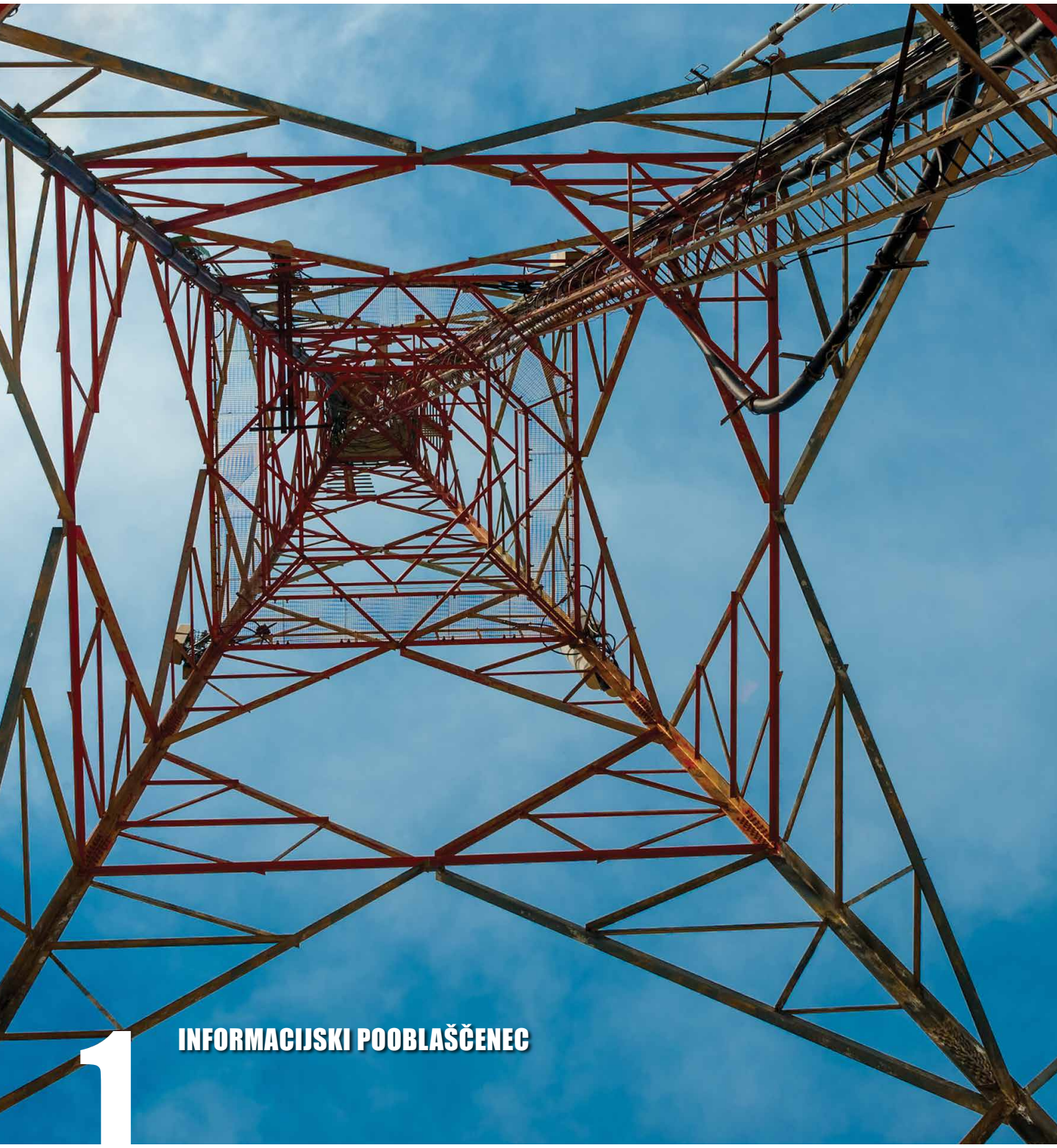
3. DELO NA PODROČJU VARSTVA OSEBNIH PODATKOV

3.1. Koncept varstva osebnih podatkov v Repubiliki Sloveniji 29
3.2. Dejavnost državnih nadzornikov za varstvo osebnih podatkov 30
3.2.1. Pravice in dolžnosti državnega nadzornika 30
3.2.2. Inšpekcijski nadzor 30
3.2.3. Storjeni prekrški 33
3.3. Dajanje pisnih mnenj in pojasnil 35

3.4. Dopustnost izvajanja biometrijskih ukrepov 36
3.5. Ugotavljanje ustrezne ravni varstva osebnih podatkov v tretjih državah 41
3.6. Izdajanje dovoljenj za povezovanje javnih evidenc 44
3.7. Seznanitev z lastnimi osebnimi podatki 47
3.8. Zahteve po presoji ustavnosti zakonov 49
3.8.1. Zahteva za presojo ustavnosti 29. člena Zakona o preprečevanju omejevanja konkurence 50
3.8.2. Zahteva za presojo ustavnosti 45. člena Odloka o cestnoprometni ureditvi Mestne občine Ljubljana 51
3.8.3. Odločitev Ustavnega sodišča v zvezi z zahtevo za presojo ustavnosti Zakona o evidentiranju nepremičnin 53
3.9. Zanimivejše odločitve v inšpekcijskih postopkih 53
na področju varstva osebnih podatkov 53
3.9.1. Nadzor nad delavci v zvezi z uporabo tiskalnika 53
3.9.2. Zbiranje osebnih podatkov za namen neposrednega trženja preko spleta 55
3.9.3. Izvajanje biometrijskih ukrepov in videonadora v fitnes studiu 56
3.9.4. Neustrezno zavarovanje odpadnih (foto-)kopij dokumentov z osebnimi podatki 58
3.9.5. Preusmeritev obiskovalcev strani s spletnimi igrami na srečo na drug naslov in nezakonito zbiranje njihovih osebnih podatkov 59
3.9.6. Obdelava osebnih podatkov uporabnikov storitve BicikeLJ 60
3.10. Splošna ocena stanja varstva osebnih podatkov in priporočila 62

4. DRUGE DEJAVNOSTI INFORMACIJSKEGA POOBLAŠČENCA

4.1. Sodelovanje pri pripravi zakonov in drugih predpisov 67
4.2. Sodelovanje z javnostmi 69
4.3. Mednarodno sodelovanje 72
4.3.1. Sodelovanje na mednarodnih srečanjih 72
4.3.2. Sodelovanje v mednarodnih delovnih telesih 73
4.3.3. Ostale mednarodne dejavnosti 75



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 takšne 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 lastnimi 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 za presojo 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].

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].

---

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.
4 Uradni list RS, št. 94/2007 – uradno prečiščeno besedilo 1; v nadaljevanju ZVOP-1.

Informacijski pooblaščenec ima pristojnosti tudi na podlagi Zakona o elektronskih komunikacijah[5], ki so se s sprejetjem zakona konec leta 2012 povečale, in sicer:

- izvajanje inšpekcijskega nadzora nad izvajanjem določb 149. člena ZEKom-1, ki ureja notranje postopke o odzivanju na zahteve pristojnih organov za dostop do osebnih podatkov uporabnikov na podlagi področnih zakonov,
- najmanj enkrat letno opravljanje inšpekcijskega nadzora nad obdelavo podatkov iz 153. člena ZEKom-1, ki določa pogoje in postopke za posredovanje prometnih in lokacijskih podatkov v primerih varovanja življenja in telesa posameznika,
- izvajanje inšpekcijskega nadzora nad izvajanjem določb 155. člena ZEKom-1, ki ureja sledenje zlonamernih ali nadležnih klicev na pisno zahtevo posameznika, ki klice prejema, in postopke glede posredovanja podatkov, ki razkrijejo identiteto klicočega,
- izvajanje inšpekcijskega nadzora nad izvajanjem določb 157. člena ZEKom-1, ki ureja shranjevanje podatkov ali pridobivanje dostopa do podatkov, shranjenih v terminalski opremi naročnika ali uporabnika s pomočjo piškotkov in podobnih tehnologij,
- izvajanje inšpekcijskega nadzora nad izvajanjem določb 166. člena ZEKom-1, ki ureja posredovanje hranjenih podatkov pristojnim organom.
- izvajanje inšpekcijskega nadzora nad hrambo prometnih in lokacijskih podatkov, pridobljenih ali obdelanih v zvezi z zagotavljanjem javnih komunikacijskih omrežij ali storitev, kot to določajo 162. do 168. člen ZEKom-1, razen določb iz četrtega odstavka 165. člena ZEKom-1 (skladno s 169. členom ZEKom-1),
- na področju, ki ga nadzoruje, Informacijski pooblaščenec odloča o prekrških za kršitve ZEKom-1 in na njegovi podlagi izdanih predpisov kot prekrškovni organ v skladu z zakonom, ki ureja prekrške (232. do 236. člen ZEKom-1).

Z vstopom Republike Slovenije v schengensko območje je Informacijski pooblaščenec prevzel tudi nadzor nad izvajanjem 128. člena Konvencije o izvajanju Schengenskega sporazuma 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[6], Zakonu o potnih listinah državljanov Republike Slovenije[7] in Zakonu o osebni izkaznici[8].

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-1:

- izvajanje nadzora nad 3.a členom ZOIzk-1, 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-1 kot prekrškovni organ odloča o prekršku v skladu z 19.a členom ZOIzk-1.

---

5 Uradni list RS, št. 109/2012; v nadaljevanju ZEKom-1.
6 Uradni list RS, št. 15/2008; v nadaljevanju ZPacP.
7 Uradni list RS, št. 29/2011 – uradno prečiščeno besedilo 4; v nadaljevanju ZPLD-1.
8 Uradni list RS, št. 35/2011; v nadaljevanju ZOIzk-1.

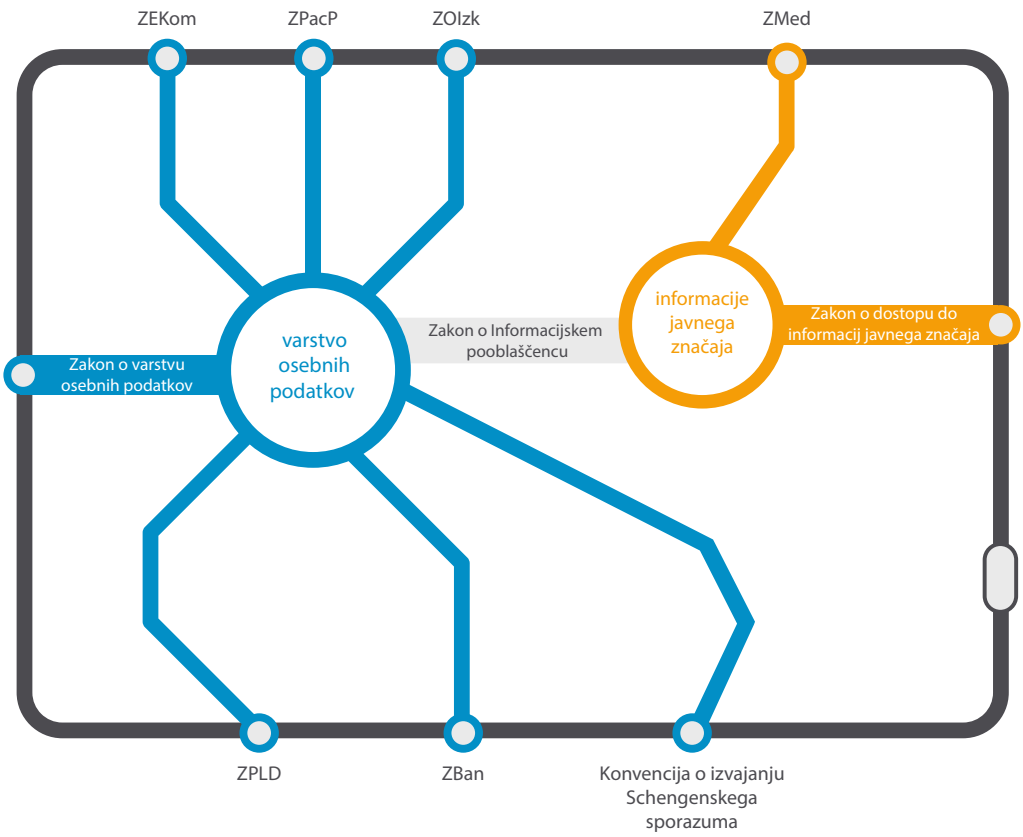
Pristojnosti Informacijskega pooblaščenca na podlagi ZPLD-1:

- izvajanje nadzora nad 4.a členom ZPLD-1, 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-1 kot prekrškovni organ odloča o prekršku v skladu s 34.a členom ZPLD-1.

Leta 2009 je Informacijski pooblaščenec pridobil pristojnosti po Zakonu o bančništvu[9]:

- podaja soglasja upravljavcem sistema SISBON pred začetkom uporabe pravil sistema iz 1. točke trinajstega odstavka 309.a člena ZBan-1, 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-1);
- izvaja nadzor nad 309.a členom ZBan-1, ki ureja zbiranje in obdelovanje ter sistem izmenjave informacij o boniteti strank (sistem SISBON) in skladno s 397. členom ZBan-1 vodi postopke o prekršku zaradi kršitve določb 309.a člena ZBan-1 (deseti do petnajsti odstavek 397. člena ZBan-1).

Slika 1: Pristojnosti Informacijskega pooblaščenca.



1.3. Organiziranost Informacijskega pooblaščenca

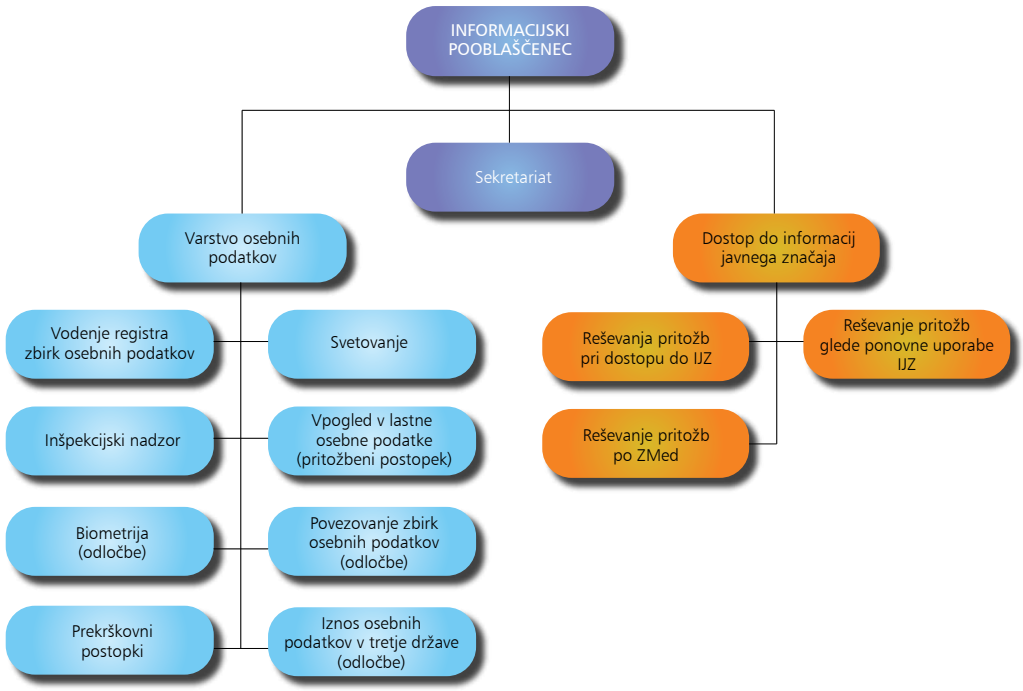
Notranjo organizacijo in sistemizacijo delovnih mest, ki so potrebna za izvajanje nalog pri Informacijskem pooblaščencu, določata Akt o notranji organizaciji in sistematizaciji delovnih mest pri Informacijskem pooblaščencu in njegova priloga Sistemizacija delovnih mest pri Informacijskem pooblaščencu. Sistemizacija delovnih mest je prilagojena nalogam

[9] Uradni list RS, št. 99/2010 – uradno prečiščeno besedilo 5, s spremembami; v nadaljevanju ZBan-1.

Informacijskega pooblaščenca in delovnim procesom, ki potekajo pri njem, ter je oblikovana tako, da zagotavlja čim učinkovitejšo izrabo človeških virov.

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 2012 je imel Informacijski pooblaščenec 33 zaposlenih, od tega tri osebe za določen čas. Število zaposlenih pri Informacijskem pooblaščencu se v primerjavi z letom 2011 ni spremenilo.

Zaposleni so bili:
- informacijska pooblaščenka,
- namestnica za področje varstva osebnih podatkov,
- namestnica za področje dostopa do informacij javnega značaja,
- namestnik za področje informacijskih tehnologij,
- namestnik - vodja državnih nadzornikov za varstvo osebnih podatkov,
- generalna sekretarka,
- osem svetovalcev,
- trije asistenti svetovalca,
- devet državnih nadzornikov za varstvo osebnih podatkov,
- trije raziskovalci,
- informatik,
- tri administrativno-tehnične sodelavke (finančna referentka, poslovna sekretarka, dokumentalistka).

Preglednica 1: Izobrazbena struktura zaposlenih pri Informacijskem pooblaščencu 31. 12. 2012.

	Srednja izobrazba	Višja strokovna šola	Univerzitetna izobrazba	Magisterij	Doktorat	**Skupaj**
Informacijska pooblaščenka			1			1
Namestniki			2	2		4
Generalna sekretarka			1			1
Svetovalci			8			8
Asistenti svetovalca			3			3
Raziskovalci			3			3
Državni nadzorniki za varstvo osebnih podatkov			5	3	1	9
Informatik				1		1
Administrativno-tehnični sodelavci	1	2				3
Skupaj	1	2	23	6	1	**33**

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). Sprejet proračun pri Informacijskem pooblaščencu je v začetku proračunskega leta 2012 znašal 1.487.248,66 EUR.

Na postavko materialni stroški (PP 1271) je bilo dodeljenih 310.000,00 EUR, investicije (PP 1273) 20.000,00 EUR in na plače (PP 1267) 1.136.780,00 EUR. Za sodelovanje Informacijskega pooblaščenca v evropskih projektih je bilo iz preteklega leta prenesenih 17.706,88 EUR, od tega za projekt LAPSI (PP 9586) 441,88 EUR in za projekt Twinning Črna gora (PP 9596) 17.265,00 EUR. V leto 2012 je bilo prenesenih 2.700,00 EUR namenskih sredstev iz naslova sredstev kupnin (PP 7459) in 61,78 EUR iz naslova sredstev odškodnin (PP 7460).

Med letom so se proračunska sredstva pri Informacijskem pooblaščencu povečala za donacije iz naslova sodelovanja v novem projektu Twinning Srbija (PP 9950) za 199.391,20 EUR, projektu LAPSI 6.300,00 EUR, projektu Twining Črna gora 30.589,46 EUR in za donacije za izdelavo in vzdrževanje mednarodne spletne strani pooblaščencev (PP 9958) za 480,00 EUR.

Z rebalansom proračuna v mesecu juniju je bil sprejet proračun na začetku leta znižan za 324.321,00 EUR. Znižana so bila sredstva na postavkah materialni stroški za 59.650,00 EUR, investicije za 3.496,00 EUR in plače za 29.197,14 EUR.

Informacijski pooblaščenec je konec leta 2012 za pokritje stroškov izplačila plač iz sredstev proračunskih rezerv prejel 34.876,14 EUR.

Veljavni proračun je bil tako ob koncu leta 2012 1.666.574,20 EUR: na postavki plače 1.142.459,00 EUR, materialni stroški 253.176,44 EUR, investicije 13.677,56 EUR, namenska sredstva kupnin 2.700,00 EUR, sredstva odškodnin 1.487,84 EUR, preostala evropska sredstva iz sodelovanja v projektu European privacy open space 3,41 EUR, za projekt LAPSI 6.741,88 EUR, za projekt Twining Črna gora 46.456,87 EUR, za projekt Twining Srbija 199.391,20 EUR in za izdelavo in vzdrževanje mednarodne spletne strani pooblaščencev 480,00 EUR.

V letu 2012 je bilo porabljenih 1.610.086,39 EUR, od tega za izplačilo plač 1.138.678,08 EUR, materialne stroške 252.887,49 EUR, investicije 13.677,56 EUR, namenska sredstva odškodnin 1.487,84 EUR, sodelovanje v projektu LAPSI 6.654,64 EUR, v projektu Twinning Črna gora 46.113,99 EUR, v projektu Twining Srbija 150.573,65 EUR, stroški za izdelavo in vzdrževanje mednarodne spletne strani pooblaščencev pa so znašali 13,14 EUR.

Preglednica 2: Poraba proračunskih sredstev leta 2012 (v EUR).

Plače in drugi izdatki zaposlenim	1.138.678,08
Materialni stroški	252.887,49
Pisarniški in splošni material in storitve	35.560,97
Posebni material in storitve	8.178,59
Energija, voda in komunalne storitve	43.007,57
Prevozni stroški in storitve	30.383,97
Izdatki za službena potovanja	20.229,21
Tekoče vzdrževanje	5.053,51
Poslovne najemnine in zakupnine	104.731,42
Drugi operativni odhodki	5.742,25
Investicije in investicijsko vzdrževanje	13.677,56
Nakup opreme	13.167,08
Nakup nematerialnega premoženja	510,48
Projekti	203.342,28
LAPSI	6.654,64
Twinning Črna gora	46.113,99
Twinning Srbija	150.573,65
Ostalo	1.500,98
SKUPAJ	1.610.086,39

Leta 2012 je bilo za plače porabljenih manj sredstev (in sicer 1.138.678,08 EUR) kot leta 2011 (takrat je ta znesek znašal 1.139.495,82 EUR). Tudi za materialne stroške je bilo porabljenih manj sredstev (252.887,49 EUR) kot leta 2011 (302.103,22 EUR), kar pomeni, da se poraba sredstev za materialne stroške že nekaj let stalno zmanjšuje. Materialni stroški so bili potrebni za redno delovanje Informacijskega pooblaščenca (najemnina za poslovne prostore, pisarniški material, potni stroški, čiščenje, obratovalni stroški, poštne storitve, izobraževanje zaposlenih, izdelava brošur ipd.).

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[10]. 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[11]. 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 kakršnikoli 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 organ zahtevo zavrnil, ter zoper sklep, s katerim je organ zahtevo zavrgel. O pritožbi odloča

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

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, 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[12] 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 2012 je Informacijski pooblaščenec prejel 519 pritožb, od tega 277 zoper zavrnilne odločbe in 242 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 256 odločb (od tega 53 v zadevah, ki jih je Informacijski pooblaščenec prejel v reševanje pred letom 2012, v osmih primerih pa je po prejeti sodbi Upravnega sodišča v zadevi ponovno odločal), 12 prosilcev je pritožbo umaknilo, v petih primerih je Informacijski pooblaščenec pritožbo s sklepom zavrgel, v dveh primerih pa je združil zadeve.

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 25 primerih je Informacijski pooblaščenec pritožbo zaradi preuranjenosti ali pomanjkljive vloge s sklepom zavrgel, 14 posameznikov je pritožbe umaknilo, ker so prejeli zahtevano dokumentacijo, v osmih primerih pa je Informacijski pooblaščenec prosilcem pojasnil, da za reševanje njihovih vlog ni pristojen in jih odstopil v reševanje pristojnim organom.

[12] Uradni list RS, št. 76/2005 in 119/2007; v nadaljevanju Uredba.

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 2012 je bilo opravljenih 49 takšnih ogledov.

Leta 2012 je Informacijski pooblaščenec prejel 776 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 mnenja na področju dostopa do informacij javnega značaja daje ministrstvo, pristojno 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 2012 je bilo zoper odločbe Informacijskega pooblaščenca na Upravno sodišče vloženih 27 tožb (zoper 10,5 % izdanih odločb), kar je nekoliko manj kot v preteklem letu, ko so bile vložene tožbe zoper 13,1 % odločb. Relativno majhen delež sproženih upravnih sporov kaže na 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 2012 odločilo o 32 tožbah, ki so bile vložene zoper odločbe Informacijskega pooblaščenca:

- tožbo je zavrnilo (16),
- tožbi je ugodilo, izpodbijano odločbo odpravilo in zadevo vrnilo Informacijskemu pooblaščencu v ponovno odločanje (12),
- tožbi je delno ugodilo oziroma je izpodbijano odločbo v delu odpravilo in vrnilo Informacijskemu pooblaščencu v ponovno odločanje, v preostalem delu pa zavrnilo (1),
- tožbo je zavrglo (1),
- postopek je s sklepom ustavilo (2).

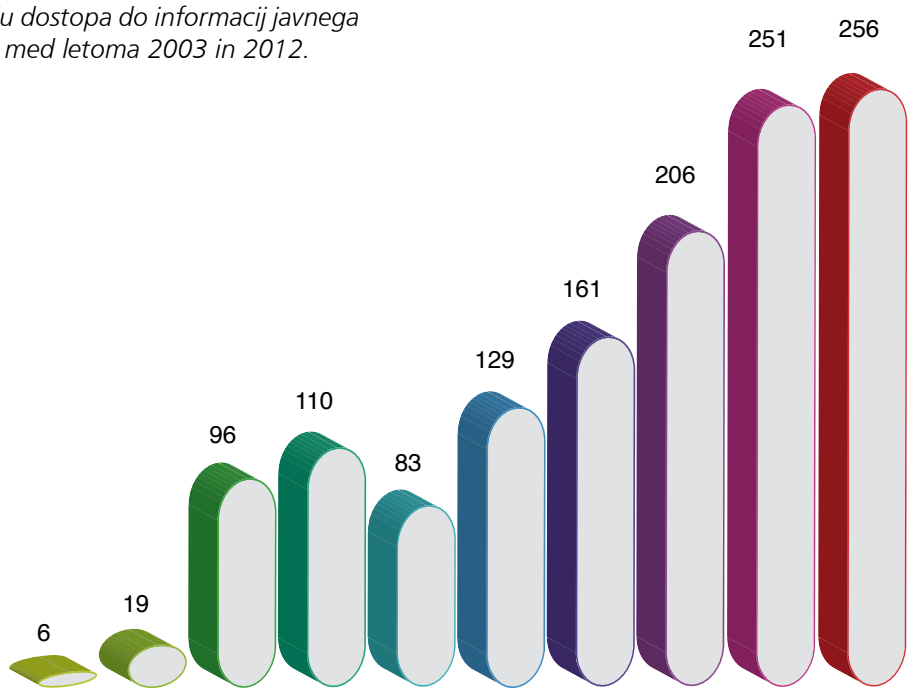
Leta 2012 sta bili zoper sodbe Upravnega sodišča na Vrhovno sodišče vloženi dve reviziji.

Leta 2012 je Vrhovno sodišče odločilo o dveh revizijah, ki sta bili vloženi zoper sodbe Upravnega sodišča. Sodišče je obe zahtevi za revizijo zavrglo.

2.4. Statistika po posameznih področjih ZDIJZ

Število izdanih odločb na področju dostopa do informacij javnega značaja se je v primerjavi s preteklim letom malenkost povečalo. Leta 2011 je bilo izdanih 251 odločb, leta 2012 pa 256.

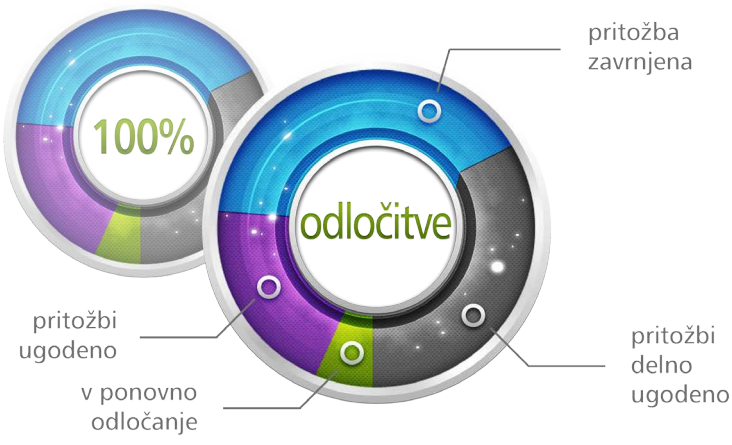
Slika 3: Število izdanih odločb na področju dostopa do informacij javnega značaja med letoma 2003 in 2012.



Informacijski pooblaščenec je v izdanih odločbah:

- v 95 primerih pritožbo zavrnil,
- v 63 primerih pritožbi ugodil in rešil zadevo v korist prosilca,
- v 27 primerih pritožbi ugodil in zadevo vrnil v ponovno odločanje prvostopenjskemu organu,
- v 70 primerih pritožbi delno ugodil, tako da je odobril dostop do informacije le v določenem delu,
- v enem primeru pritožbo zavrgel.

Slika 4: Odločitve Informacijskega pooblaščenca glede prejetih pritožb.



Informacijski pooblaščenec je v odločbah vsebinsko odločal oziroma presojal:

- ali zahtevani dokumenti vsebujejo osebne podatke, katerih razkritje bi pomenilo kršitev varstva osebnih podatkov v skladu z ZVOP-1 (84);
- ali zavezanec sploh ima dokument oziroma informacijo javnega značaja, ki jo je prosilec zahteval (73);
- ali prosilci zahtevajo informacije oziroma podatke, ki so v skladu z zakonom, ki ureja gospodarske družbe, opredeljeni kot poslovna skrivnost (61);
- ali gre za kršitev pravil postopka (34);
- 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 (24);
- ali gre za prosto dostopne informacije iz postopkov javnih naročil (24);
- ali gre za delovno področje organa (17);
- ali je organ pravilno zaračunal stroške posredovanja informacij javnega značaja (16);
- 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 (15);
- ali so zahtevane informacije podatki, ki so na podlagi zakona, ki ureja tajne podatke, opredeljeni kot tajni (10);
- ali je podan javni interes za razkritje zahtevane informacije (7);
- ali so zahtevane informacije podatki, ki so bili pridobljeni ali sestavljeni zaradi upravnega postopka, in bi njihovo razkritje škodovalo njegovi izvedbi (7);
- ali so zahtevane informacije podatki, ki so bili pridobljeni ali sestavljeni zaradi kazenskega pregona ali v zvezi z njim, ali postopka o prekršku in bi njihovo razkritje škodovalo njegovi izvedbi (6);
- ali je zahtevana informacija zavarovana skladno z zakonom, ki ureja avtorsko pravico (5);
- ali je posredovana informacija res tista, ki jo je zahteval prosilec (5);
- ali zahtevani dokument izpolnjuje pogoje za obstoj informacije javnega značaja v skladu s prvim odstavkom 4. člena ZDIJZ (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 so zahtevane informacije podatki, katerih razkritje bi pomenilo kršitev zaupnosti davčnega postopka ali davčne tajnosti skladno z zakonom, ki ureja davčni postopek (4);
- ali so zahtevane informacije podatki, ki so bili pridobljeni ali sestavljeni zaradi pravdnega, nepravdnega ali drugega sodnega postopka, in bi njihovo razkritje škodovalo njegovi izvedbi (3);
- ali gre za ponovno uporabo informacije javnega značaja (2);
- ali sploh gre za pravico po ZDIJZ (2);
- ali mora organ umakniti stopnjo tajnosti zahtevanega dokumenta (2);
- ali je organ kršil materialno pravo (2);
- ali gre za uporabo prava Evropske unije (2);
- ali gre za zlorabo pravice po ZDIJZ (1);
- ali gre za okoljske podatke (1);
- ali gre za dolžnost proaktivne objave informacij (1);
- ali so zahtevane informacije podatki, katerih razkritje bi pomenilo kršitev zaupnosti individualnih podatkov o poročevalskih enotah skladno z zakonom, ki ureja dejavnost državne statistike (1);
- razno (4).

Slika 5: Odločbe na področju ZDIJZ glede na različne izjeme.
(Opomba: ena odločba se lahko nanaša na več izjem.)

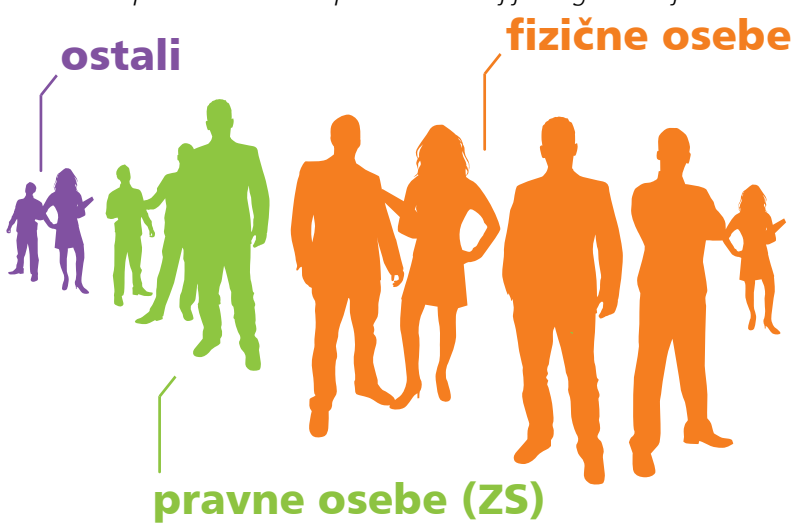
Pritožbe prosilcev zaradi zavrnitve dostopa do informacij javnega značaja, o katerih je Informacijski pooblaščenec odločil z odločbo, so zadevale naslednje skupine zavezancev:

- državne organe (ministrstva in organi v sestavi, upravne enote) (97),
- javne sklade, zavode, agencije, izvajalce javnih služb in nosilce javnih pooblastil (93),
- občine (44),
- sodišča, vrhovno državno tožilstvo, državno pravobranilstvo (19).

Tri pritožbe so se nanašale na pravne osebe iz zasebnega sektorja, za katere pa je bilo ugotovljeno, da niso zavezanci po ZDIJZ.

V 169 primerih so bili prosilci fizične osebe, v 53 primerih so se pritožile pravne osebe iz zasebnega sektorja, novinarji so se pritožili 21-krat, pravne osebe iz javnega sektorja pa 13-krat.

Slika 6: Struktura prosilcev za dostop do informacij javnega značaja.



2.5. Storjeni prekrški po ZDIJZ, ZInfP in ZMed

Leta 2012 so bili uvedeni trije postopki o prekršku, in sicer:

- zaradi storitve prekrška po tretjem odstavku 39. člena ZDIJZ, ker organ kljub pravnomočni odločbi Informacijskega pooblaščenca prosilcu ni posredoval informacij javnega značaja,
- zaradi storitve prekrška po prvem odstavku 15. člena ZInfP, ker organ Informacijskemu pooblaščencu ni posredoval zahtevanih dokumentov, ki so bili potrebni za odločitev v pritožbenem postopku,
- zaradi storitve prekrška po drugem odstavku 39. člena ZDIJZ, ker je organ po prejemu zahteve za posredovanje informacij javnega značaja uničil dokument, v katerem se je nahajala zahtevana informacija javnega značaja.

Vsi postopki so bili zaključeni z izrekom sankcije kršitelju. V dveh postopkih je bil izrečen opomin, v enem pa globa, zoper katero je kršitelj vložil zahtevo za sodno varstvo.

2.6. Predstavitev najodmevnejših in precedenčnih primerov po področjih

V nadaljevanju je predstavljenih nekaj najzahtevnejših in najzanimivejših odločb iz leta 2012, ki so razvrščene po področjih.

2.6.1. Stroški postopka

Z odločbo št. 090-272/2011/4 z dne 6. 2. 2012 je Informacijski pooblaščenec odpravil odločbo Upravne enote Murska Sobota in ji vrnil zadevo v ponovno odločanje.

Prosilec je od organa zahteval skenirane odločbe o denacionalizaciji (z žigom pravnomočnosti), izdane v obdobju od 1. 1. 2006 do 1. 1. 2011.

Organ je prosilcu z dopisom na podlagi 20. člena Uredbe vnaprej sporočil znesek za kritje stroškov posredovanja zahtevanih informacij, in sicer v višini 435,28 EUR za 51 denacionalizacijskih odločb. Ker je organ iz prosilčevega dopisa smatral, da prosi le za prvo stran pravnomočnih odločb, je strošek naknadno znižal na 307,27 EUR.

Prosilec ni založil zahtevanega zneska, zato je organ izdal sklep o ustavitvi postopka, ki ga je prosilec izpodbijal v tem pritožbenem postopku. Informacijski pooblaščenec je pojasnil, da ZDIJZ ne predvideva pritožbe zoper zahtevo za vnaprejšnji polog, možna pa je pritožba zoper sklep, s katerim organ ustavi postopek zaradi neplačila pologa, torej zoper končno odločbo.

Informacijski pooblaščenec je nadalje presojal utemeljenost izdaje sklepa o ustavitvi postopka in posledično zaračunanih stroškov. Ker je organ zaračunal tudi stroške dela javnih uslužbencev, je Informacijski pooblaščenec opozoril, da je zaračunavanje stroškov dela javnih uslužbencev v postopku dostopa do informacij javnega značaja sporno (ker ZDIJZ tega izrecno ne določa, pravi pa, da je vpogled vedno brezplačen). Vendar je možnost zaračunavanja stroškov dela kljub jasni zakonski usmeritvi dopustila Uredba, ki je uvedla možnost določanja stroškov dela s strani organov s sprejemom posebnih stroškovnikov, organ pa je stroške dela v konkretnem primeru zaračunal prav na podlagi Stroškovnika o posredovanju in ponovni uporabi informacij javnega značaja za upravne enote Republike Slovenije. Informacijski pooblaščenec mora pri odločanju v pritožbenem postopku upoštevati veljavni stroškovnik, saj je kot upravni organ vezan na vse veljavne podzakonske predpise in nima pravice do

uporabe instituta exceptio illegalis (izvzetje nezakonitega), torej možnosti, da podzakonskega predpisa, za katerega meni, da ni zakonit, ne uporabi, ampak uporabi neposredno zakon.

Vendar pa je Informacijski pooblaščenec ugotovil, da iz spisovne dokumentacije ni natančno razvidno, zakaj bi stroški organa za posredovanje izrekov 51 denacionalizacijskih odločb znašali 307,27 EUR. Zato je organ pozval, da mu posreduje dodatna pojasnila glede predvidenih stroškov, a ga odgovor organa ni prepričal v utemeljenost zaračunanja stroškov. Informacijski pooblaščenec je zapisal, da zaračunavanje stroškov ne sme biti arbitrarno in odvisno od individualnih sposobnosti javnih uslužbencev, zaposlenih pri določenem organu, oziroma od organizacije dela organa. Prosilec ne sme nositi bremena slabe organizacije dela organa ter posledično dolgotrajnega procesa iskanja in posredovanja zahtevanih informacij javnega značaja. Informacijski pooblaščenec je poudaril, da mora biti arhiv vsakega upravnega organa organiziran skladno z Uredbo o upravnem poslovanju[13], in sicer na način, da se lahko vsak iskan dokument v arhivu (že na podlagi klasifikacijskih znakov posamičnih dokumentov) kar najhitreje locira. Organ pa je za iskanje in odpiranje le 51 dokumentov naračunal več kot 25 ur dela, torej več kot tri delovne dni, kar je po mnenju Informacijskega pooblaščenca vsekakor nesorazmerno. Prav tako ne morejo biti upoštevani stroški dela svetovalke, ki naj bi preverjala pravilnost pripravljenih dokumentov, saj prosilca ni dopustno obremeniti s stroški dela, ki nastanejo zaradi morebitnega nezaupanja nadrejenih v kakovostno delo podrejenih ali zgolj zaradi ponovnega preverjanja kakovosti opravljenega dela.

Informacijski pooblaščenec je opozoril, da zaračunavanje stroškov dela javnih uslužbencev ne sme postati možnost za odvračanje prosilcev od vlaganja zahtev za dostop do informacij javnega značaja. Višina stroškov posredovanja informacij javnega značaja mora biti na najnižji ravni, ki ne ovira nesorazmerno prosilčeve ustavne pravice dostopa do informacij javnega značaja. V konkretnem primeru se je treba zavedati, da je prosilec zahteval le 51 dokumentov, torej zaračunani stroški v višini 307,27 EUR nikakor niso sorazmerni.

2.6.2. Ponovna uporaba informacij javnega značaja

Z odločbo št. 090-8/2012/2 z dne 22. 2. 2012 je Informacijski pooblaščenec odpravil odločbo Uradnega lista in mu zadevo v zvezi s ponovno uporabo informacij javnega značaja vrnil v ponovno odločanje.

Prosilec je na organ naslovil zahtevo za ponovno uporabo objav javnih naročil, ki so brezplačno objavljene na Portalu javnih naročil (www.enarocanje.si). Prosilec bi zahtevane podatke sam prevzemal s spletne strani in jih ponovno uporabil za pridobitne namene. Informacije bi zbral, pregledno razvrstil in omogočil iskanje po imeniku, ki bi ga javno objavil na svoji spletni strani z namenom informiranja javnosti, za iskanje pa bi zaračunal nadomestilo.

Organ je zahteval, da prosilec časovno opredeli informacije, ki jih želi ponovno uporabiti, prosilec pa je odgovoril, da ZDIJZ ne zahteva opredelitve trajanja ponovne uporabe. Ker je navedel, da bo informacije s Portala javnih naročil črpal sam, se zahteva nanaša na vsakokratne podatke, javno in brezplačno objavljene na Portalu javnih naročil. Iz tega je mogoče sklepati, da je njegova zahteva omejena na čas obstoja podatkov, čas delovanja Portala javnih naročil in dodatno na čas, v katerem bodo zahtevani podatki javno in brezplačno objavljeni na Portalu javnih naročil. Organ je prosilca pozval tudi, naj opredeli obliko, v kateri želi prejeti informacije, na to pa je prosilec odgovoril, da ne zahteva informacij v elektronski obliki, pač pa le, da mu organ ponovno uporabo dovoli.

Organ je zavrnil zahtevo prosilca, da bi sam prevzemal informacije s spletnega portala, prav tako je zavrnil ponovno uporabo informacij javnega značaja glede bodočih objav (torej informacij, ki v času odločanja še ne obstajajo). Vendar pa je prosilcu na zgoščenki

[13] Uradni list RS, št. 20/2005, s spremembami.

posredoval vse objave javnih naročil od začetka uporabe portala za tovrstne objave do dneva odločanja organa o zahtevi prosilca. Organ je prosilcu naložil tudi pogoje ponovne uporabe.

Glede zahteve po stalnem ažuriranju informacij je Informacijski pooblaščenec poudaril, da ZDIJZ sicer ne govori o zahtevi, ki predvideva stalno ažuriranje informacij, a takšne primere izrecno predvideva Uredba o posredovanju in ponovni uporabi informacij javnega značaja. Organ bi zato moral upoštevati, da je mogoče zahtevati ponovno uporabo s stalnim ažuriranjem. Bistvo gospodarske funkcije ponovne uporabe informacij javnega značaja se lahko zagotavlja le, če se gospodarskim subjektom omogoča, da od javnega sektorja pridobivajo ažurne, verodostojne in popolne podatke, in ne, da so ponovni uporabniki pri ažurnosti informacij vedno korak za organi javnega sektorja. Glede načina prevzema informacij je Informacijski pooblaščenec opozoril, da ZDIJZ ne izključuje prevzema informacij neposredno s spletne strani. Glede stroškov posredovanja informacij pa je Informacijski pooblaščenec opozoril, da ZDIJZ sicer predvideva zaračunavanje cene za ponovno uporabo v pridobitne namene, vendar pa ta zakon določa tudi, da organ ne zaračuna ponovne uporabe informacij, če jih v svetovni splet posreduje brezplačno.

2.6.3. Osebni podatki

Z odločbo št. 090-80/2012/4 z dne 5. 4. 2012 je Informacijski pooblaščenec odpravil odločbo Javnega sklada RS za razvoj kadrov in štipendije in mu naložil posredovanje zahtevanega seznama prejemnikov Zoisove štipendije s prekritimi varovanimi osebnimi podatki.

Prosilec je zahteval, da mu organ po elektronski pošti posreduje seznam vseh dijakov, ki so v šolskem letu 2011/2012 dijaki prvega letnika in so dobili Zoisovo štipendijo. Prosilec je navedel, da gre pri zahtevanih podatkih za podatke o porabi javnih sredstev in bi mu organ moral razkriti informacijo, za koga se bodo ta javna sredstva porabila.

Organ je prosilčevo zahtevo v celoti zavrnil zaradi varstva osebnih podatkov. Navedel je, da Zakon o štipendiranju[14], na podlagi katerega odloča o dodelitvi Zoisovih štipendij, v prvem odstavku 59. člena (varstvo podatkov) določa, da se za zbiranje, obdelovanje, shranjevanje, posredovanje in uporabo podatkov, vsebovanih v zbirkah podatkov, ter za varstvo informacijske zasebnosti posameznika uporabljajo določbe zakona, ki ureja varstvo osebnih podatkov. Seznami, s katerimi razpolaga organ, vsebujejo poleg imena in priimka tudi enotno matično številko občana in višino dodeljene štipendije. Zaradi navedenega gre po mnenju organa za varovane osebne podatke po ZVOP-1 in posledično za izjemo varstva osebnih podatkov, ki jo določa 3. točka prvega odstavka 6. člena ZDIJZ. Prav tako je organ zapisal, da osebnih podatkov zaradi določbe 24. člena ZVOP-1 ne sme posredovati po elektronski pošti. Podatke bi sicer bilo možno zagotoviti v elektronski obliki, vendar le z osebno vročitvijo. Organ je Informacijskemu pooblaščencu posredoval dva seznama vlagateljev, vendar je navedel, da sistem, v katerem vodi te podatke, za del vlagateljev podatkov o imenu, priimku in EMŠO posameznega vlagatelja ne izpiše, temveč je te podatke možno dobiti le z ročnim vpogledom v vsako zadevo posebej ali od ministrstva proti plačilu stroškov izvajalcu.

Informacijski pooblaščenec je ugotovil, da se želi prosilec seznaniti z elektronskim zapisom, ki pa v določenem delu ne obstaja, saj je organ navedel, da sistem za del vlagateljev podatkov o imenu, priimku in EMŠO posameznega vlagatelja ne izpiše. Glede na to, da je bil organ s pozivom izrecno opozorjen na določbo 10. člena ZInfP (kršitev katere predstavlja prekršek) in izrecno pozvan, da mora posredovati vse podatke, s katerimi razpolaga in so predmet presoje v pritožbenem postopku, Informacijski pooblaščenec ni imel podlage za dvom v resničnost navedb organa, da del zahtevanih podatkov v obliki izpisa iz sistema pri organu ni mogoč. Ker v tem delu ni bil izpolnjen kriterij materializirane oblike iz 4. člena ZDIJZ za obstoj informacije javnega značaja, je bilo treba pritožbo prosilca zavrniti.

[14] Uradni list RS, št. 58/2007, s spremembami; v nadaljevanju ZŠtip.

V delu, ki se nanaša na prejemnike Zoisove štipendije in obstaja elektronski seznam, pa je Informacijski pooblaščenec ugotovil, da gre pri imenih in priimkih prejemnikov štipendij za podatke o porabi javnih sredstev, saj iz ZŠtip izhaja, da se sredstva za te štipendije zagotovijo v proračunu. Informacijski pooblaščenec je poudaril, da vsak osebni podatek nima hkrati statusa t.i. varovanega osebnega podatka oziroma je razkritje osebnega podatka v določenih primerih dopustno, kar velja tudi za razkritje v okviru izvrševanja pravice dostopa do informacij javnega značaja. Tako pravno podlago za razkritje podatkov o prejemnikih Zoisove štipendije predstavlja tretji odstavek 6. člena ZDIJZ, ki določa, da se (ne glede na izjeme od prostega dostopa, tudi če gre za sicer varovane osebne podatke) dostop do zahtevane informacije dovoli, če gre za podatke o porabi javnih sredstev. Na zahtevanih dokumentih predstavljajo varovane podatke podatki o vlagateljih, ki štipendije niso prejeli, ter pri prejemnikih vsi podatki razen imena in priimka, torej rang, točke, višina štipendije in EMŠO. Informacijski pooblaščenec je tako ugotovil, da organ ni presojal možnosti uporabe delnega dostopa iz 7. člena ZDIJZ, ki določa, da če dokument ali njegov del le delno vsebujeta informacije iz 6. člena (npr. varovane osebne podatke) in jih je mogoče izločiti iz dokumenta, ne da bi to ogrozilo njegovo zaupnost, pooblaščena oseba organa izloči te informacije ter seznani prosilca z vsebino preostalega dela dokumenta.

Informacijski pooblaščenec je odpravil odločbo organa in mu naložil, da prosilcu posreduje seznam prejemnikov Zoisove štipendije z imeni in priimki prejemnikov, pri čemer mora prekriti podatke o rangu, točkah, višini štipendije in EMŠO ter podatke o posameznikih, ki niso prejemniki štipendije.

2.6.4. Mediji, osebni podatki

Z odločbo št. 090-74/2012/4 z dne 7. 5. 2012 je Informacijski pooblaščenec odpravil odločbo Zavoda Republike Slovenije za zaposlovanje in mu naložil posredovanje seznama poslovnih subjektov, ki so jim bila izdana raznovrstna delovna dovoljenja za delo državljanom in državljankam Dominikanske republike.

Organ je prosilcu sicer posredoval podatke o izdanih delovnih dovoljenjih po državljanstvu za Dominikansko republiko za razpoložljivo obdobje ter podatek o številu podjetij, od katerih je pridobil vloge za različna dovoljenja za zaposlitev oziroma delo v tem istem obdobju, zavrnil pa je posredovanje podatka o delodajalcu ter izdanih delovnih dovoljenjih pri tem delodajalcu glede na vrsto dela in spol, ker bi s posredovanjem teh podatkov prišlo do razkritja osebnih podatkov. Če bi organ namreč razkril podatek o podjetjih, katerim so bila izdana delovna dovoljenja za državljane Dominikanske republike, podatek o datumu izdaje ter podatek o vrsti izdanega delovnega dovoljenja (tudi glede na spol in vrsto dela), bi lahko ti podatki pokazali točno določenega posameznika – državljana Dominikanske republike, ki je bil oziroma je zaposlen pri določenem podjetju.

Iz pritožbe prosilca je izrecno izhajalo, da se pritožuje le zoper zavrnitev dostopa do podatka o podjetjih, ki so zaprosila in dobila dovoljenja za zaposlitev za državljane Dominikanske republike v zadnjih letih. Zato je bil predmet presoje v pritožbenem postopku samo ta podatek.

Informacijski pooblaščenec je v pritožbenem postopku ugotovil, da seznam, ki mu ga je posredoval organ, vsebuje zahtevane podatke o poslovnih subjektih, ki so jim bila dodeljena razna delovna dovoljenja za državljane Dominikanske republike (naziv subjekta in matična številka), poleg tega pa še podatek o vrsti delovnega dovoljenja, število izdanih delovnih dovoljenj, podatek o času začetka veljavnosti delovnega dovoljenja in podatek o času veljavnosti delovnega dovoljenja.

V zvezi z izjemo varstva osebnih podatkov je Informacijski pooblaščenec ugotovil, da se vsi podatki nanašajo zgolj na pravne osebe in torej ne gre za osebne podatke in posledično tudi ne za izjemo varstva osebnih podatkov. Naziv poslovnega subjekta oziroma firma in matična številka poslovnega subjekta so registrski podatki, ki so javni že po Zakonu o gos-

podarskih družbah[15], Zakonu o Poslovnem registru Slovenije[16] in Zakonu o sodnem registru[17]. Ker torej ne gre za osebne podatke, dostopa do zahtevanih podatkov ni dopustno zavrniti na podlagi te izjeme.

Informacijski pooblaščenec je preveril še, ali zahtevani seznam morda vsebuje kakšno drugo izjemo od prostega dostopa do informacij javnega značaja in ugotovil, da v obravnavanem dokumentu ni zaslediti nobenih drugih izjem. Zato je odločbo organa v delu, ki se nanaša na podatke o podjetjih, na katera so se nanašala delovna dovoljenja za državljane Dominikanske republike v zadnjih letih, odpravil in organu naložil, da mora prosilcu posredovati seznam poslovnih subjektov, katerim so bila izdana raznovrstna delovna dovoljenja za delo državljanov in državljank Dominikanske republike za čas hrambe dokumentarnega gradiva na način, da bosta vidna le podatka o nazivu subjekta in matični številki.

2.6.5. Notranje delovanje organa

Z odločbo št. 090-109/2012/4 z dne 10. 7. 2012 je Informacijski pooblaščenec odpravil odločbo Mestne občine Maribor in ji naložil posredovanje fotokopije zahtevanega revizijskega poročila.

Prosilec je od organa zahteval dostop do revizijskega poročila o obnovi Trga Leona Štuklja, ki naj bi bil označen z oznako »zaupno«. Prosilec je menil, da ima javnost pravico do dostopa do ugotovitev revizije, saj gre za porabo javnega denarja.

Organ je zahtevo prosilca zavrnil zaradi izjeme notranjega delovanja organa iz 11. točke prvega odstavka 6. člena ZDIJZ. Razkritje dokumenta, ki ga je organ označil z oznako "zaupno", bi po mnenju organa pomenilo zlorabo slabosti notranjih kontrol proračunskega porabnika (pri čemer se je organ skliceval na določbo prvega odstavka 100. člena Zakona o javnih financah[18]) in bi negativno vplivalo na njegovo poslovanje. Organ se je skliceval tudi na mnenje Urada Republike Slovenije za nadzor proračuna v dopisu na zaprosilo Skupnosti občin Slovenije o pobudi za dopolnitev ZDIJZ glede notranjerevizijskega poročila kot informacije javnega značaja.

Informacijski pooblaščenec je v pritožbenem postopku najprej ugotovil, da zahtevano poročilo o opravljeni notranji reviziji res predstavlja dokument, ki je nastal v zvezi z notranjim delovanjem organa. Notranje revidiranje namreč zagotavlja neodvisno preverjanje sistemov finančnega poslovodenja (menedžmenta) in kontrol ter svetovanje poslovodstvu za izboljšanje njihove učinkovitosti, pri čemer je za vzpostavitev in delovanje ustreznega sistema finančnega poslovodenja in kontrol ter notranjega revidiranja po prvem odstavku 100. člena ZJF odgovoren predstojnik neposrednega uporabnika. Notranje revidiranje v skladu s četrtim odstavkom 100. člena ZJF izvajajo notranji revizorji.

Organ v izpodbijani določbi ni navedel nobenih razlogov, zakaj bi razkritje zahtevanega revizijskega poročila povzročilo motnje pri njegovem delovanju, kakšne motnje naj bi razkritje povzročilo in s kakšno stopnjo verjetnosti bi do zatrjevanih motenj dejansko lahko prišlo, temveč je možnost nastanka motenj zgolj pavšalno zatrjeval. Informacijski pooblaščenec je zaključil, da razkritje slabosti notranjih kontrol proračunskega uporabnika samo po sebi še ne pomeni zlorabe teh slabosti in da organ ni onkraj dvoma dokazal, da bi razkritje zahtevanega dokumenta povzročilo motnje pri njegovem delovanju.

Informacijski pooblaščenec je v zvezi z označitvijo dokumenta z oznako »zaupno« pojasnil, da oznake, s katero organ lokalne skupnosti sam označi lasten dokument, ni mogoče obravnavati po Zakonu o tajnih podatkih[19], saj ta zakon določa skupne osnove enotnega

[15] Uradni list RS, št. 42/2006, s spremembami; v nadaljevanju ZGD-1.
[16] Uradni list RS, št. 49/2006, s spremembami; v nadaljevanju ZPRS-1.
[17] Uradni list RS, št. 54/2007 – uradno prečiščeno besedilo 2; v nadaljevanju ZSReg.
[18] Uradni list RS, št. 11/2011 – uradno prečiščeno besedilo 4; v nadaljevanju ZJF.
[19] Uradni list RS, št. 50/2006 – uradno prečiščeno besedilo 2, s spremembami; v nadaljevanju ZTP.

sistema določanja, varovanja in dostopa do tajnih podatkov z delovnega področja državnih organov Republike Slovenije, ki se nanašajo na javno varnost, obrambo, zunanje zadeve ali obveščevalno in varnostno dejavnost države, ter prenehanje tajnosti takšnih podatkov. Zato tudi ne pride v poštev izjema od prostega dostopa do informacij javnega značaja po 1. točki prvega odstavka 6. člena ZDIJZ (izjema tajnih podatkov).

2.6.6. Ali gre za delovno področje organa, poslovna skrivnost

Z odločbo št. 090-92/2012/6 z dne 25. 7. 2012 je Informacijski pooblaščenec odpravil odločbo Izvršiteljice Tatjane Krivec Tavčar in ji naložil posredovanje zahtevane zavarovalne police.

Prosilec je zahteval, da mu organ posreduje fotokopijo zavarovalne police, iz katere bo razviden podatek, pri kateri zavarovalnici ima organ sklenjeno škodno zavarovanje za primer povzročene škode pri opravi izvršbe.

Organ je zahtevo prosilca zavrnil s sklicevanjem na prvi odstavek 4. člena ZDIJZ in 7. člen Zakona o izvršbi in zavarovanju[20]. Pojasnil je, da informacija o zavarovalnici, pri kateri ima sklenjeno zavarovanje poklicne odgovornosti, ne predstavlja informacije, ki bi izvirala iz opravljanja neposrednih dejanj izvršitelja v izvršilnih postopkih, torej ne gre za informacijo javnega značaja. Organ zahtevane informacije niti ne more pridobiti v okviru opravljanja svojih temeljnih obveznosti izpolnjevanja odločb sodišč in drugih organov v zvezi z izvršbo in zavarovanjem. Informacijo, ki jo želi pridobiti prosilec, organ pridobi v okviru svojega notranjega poslovnega delovanja in se neposredno ne nanaša na opravljanje njegovih javnih pooblastil. Tudi če bi šlo za informacijo javnega značaja, pa bi zahtevane informacije predstavljale poslovno skrivnost, saj ima organ že od začetka poslovanja s sklepom določeno kot poslovno skrivnost vso računovodsko dokumentacijo ter vse listine in podatke, ki se nanašajo na finančno poslovanje organa ter na poslovne pogodbe organa.

Informacijski pooblaščenec je poudaril, da mora organ informacijo izdelati ali pridobiti pri svojem delu in v postopkih, za katere je pristojen v skladu s splošnimi predpisi, saj obveznost izvršiteljev, da sklenejo zavarovanje za odgovornost, določa 285. člen ZIZ. Pred prisego, s katero izvršitelj nastopi službo, mora skleniti zavarovalno pogodbo za morebitno škodo, za katero je odgovoren po ZIZ. Najnižjo zavarovalno vsoto, za katero mora izvršitelj skleniti zavarovalno pogodbo, je na podlagi drugega odstavka 285. člena ZIZ določil minister, pristojen za pravosodje, s Pravilnikom o najnižji zavarovalni vsoti za izvršitelja[21]. Ker je zavarovanje za odgovornost izvršiteljev za morebitno škodo, za katero so odgovorni po ZIZ, urejeno v zakonu in v podzakonskem aktu, in je v zvezi z izvajanjem javne službe, je Informacijski pooblaščenec v nasprotju z odločitvijo organa ugotovil, da zahtevana informacija v celoti izvira z delovnega področja organa v smislu ZDIJZ.

Informacijski pooblaščenec je tudi presojal, ali podatki iz pogodbe predstavljajo izjemo poslovne skrivnosti. V postopek je najprej povabil družbo, ki je izdelala zahtevani dokument, a ta ni priglasila udeležbe oziroma na poziv Informacijskega pooblaščenca ni odgovorila. Dokazno breme glede obstoja izjem od prostega dostopa, katerih namen je varovati pravice in pravne koristi stranskega udeleženca, je primarno na subjektu, čigar podatki naj bi se z izjemo varovali. Slednji ima praviloma vsa ustrezna znanja in izkušnje, ki so potrebne za presojo kaj, kako in zakaj bi lahko vplivalo na njegove pravice in pravne koristi. O poslovni skrivnosti omenjene družbe zato v obravnavanem primeru ni mogoče govoriti. V zvezi s subjektivnim kriterijem poslovne skrivnosti po prvem odstavku 39. člena ZGD-1 je organ Informacijskemu pooblaščencu sicer poslal sklep o določitvi poslovnih skrivnosti, vendar je Informacijski pooblaščenec ugotovil, da takšna oznaka ni v skladu s tretjim odstavkom 39. člena ZGD-1. V zavarovalni polici so namreč podatki, ki so po zakonu javni, ker izpolnjujejo pogoj iz 1. alineje tretjega odstavka 6. člena ZDIJZ. Gre za podatke, povezane z opravljanjem javne funkcije. Pojem »javne službe« je namreč

[20] Uradni list RS, št. 3/2007 – uradno prečiščeno besedilo 4, s spremembami; v nadaljevanju ZIZ.
[21] Uradni list RS, št. 95/2002.

treba povezati s pojmom »javna funkcija« iz 1. alineje tretjega odstavka 6. člena ZDIJZ. Pojem javne funkcije ni vezan zgolj na funkcionarje v državnih organih in organih lokalnih skupnosti, ker ne gre za terminus technicus (takšno stališče je zavzelo tudi Upravno sodišče Republike Slovenije v sodbi št. I U 1410/2010-13 z dne 25. 5. 2011). Služba izvršitelja je javna služba, teleološka in sistematična razlaga pa sta Informacijskega pooblaščenca pripeljali do zaključka, da je pojem »javna funkcija« povezan s pojmom »javna služba« v tem smislu, da so dokumenti, ki nastanejo v okviru izvajanja javne službe, dokumenti, ki so povezani z opravljanjem javne funkcije. Izvršitelj, ki opravlja javno službo, torej opravlja javno funkcijo v smislu tretjega odstavka 6. člena ZDIJZ, zato je nadzor javnosti na tem področju izrednega pomena. Informacijski pooblaščenec je zaključil, da je prosilcu le v primeru seznanitve z zavarovalno polico omogočeno doseganje namena nadzora javnosti, ki naj bi ga institut transparentnosti zasledoval, to pa je spodbujanje oziroma zagotavljanje učinkovitega izvajanja javne službe. Slednje je mogoče zagotoviti zgolj s tem, da se javnosti omogoči tudi dostop do podatkov o tem, kaj točno je zajeto z zavarovalno polico. Šele celovita seznanjenost javnosti zagotavlja učinkovit nadzor v zvezi z učinkovitim izvajanjem javne službe.

2.6.7. Javna naročila, osebni podatki, poslovna skrivnost

Z odločbo št. 090-38/2012/14 z dne 13. 8. 2012 je Informacijski pooblaščenec delno odpravil odločbo Slovenskih železnic d.o.o. V enem delu je pritožbo prosilca zavrnil, v drugem delu pa je pritožbi ugodil in organu naložil posredovanje določenih dokumentov s prekritjem varovanih osebnih podatkov.

Prosilec je zahteval vpogled v ponudbeno dokumentacijo izbranega ponudnika GH Holding d.d. in Thales Rail Signalling Solutions GesmbH v postopku javnega naročila »Razvoj ERTMS/ETCS na infrastrukturi koridorja D«.

Zoper izdano odločbo se je prosilec pritožil, saj se ni strinjal z odločitvijo organa, da naj bi bila izpolnjena subjektivni in objektivni kriterij za določitev poslovne skrivnosti po 39. členu ZGD-1. Prosilec se ni strinjal, da je bila dokumentacija pravilno označena kot poslovna skrivnost, ker je ponudnik sklep o poslovni skrivnosti prvič posredoval organu šele skoraj leto dni po oddaji ponudbe na predmetno javno naročilo.

Informacijski pooblaščenec je ugotovil, da organ v določenem delu ne razpolaga z zahtevanimi informacijami in da ne obstaja noben razlog za dvom v njegove navedbe o neobstoju določenih dokumentov. V zvezi z nekaterimi zahtevanimi dokumenti pa je Informacijski poblaščenec ugotovil, da so bili pravilno označeni kot poslovna skrivnost, saj je stranski udeleženec ob predložitvi ponudbe v postopku javnega naročila zahtevane dokumente vidno in nedvoumno označil kot poslovno skrivnost, organu pa je pravočasno predložil tudi pisni sklep o varovanju poslovne skrivnosti, ki je bil sprejet leta 2009. Informacijski pooblaščenec je preveril, ali gre pri teh podatkih za informacije, ki po določbi tretjega odstavka 39. člena ZGD-1 ne morejo biti opredeljene kot poslovna skrivnost, a je ugotovil, da po določbah Zakona o javnem naročanju na vodnem, energetskem, transportnem področju in področju poštnih storitev[22] v konkretnem primeru ni tako. Predmetna dokumentacija tudi ne predstavlja merila za izbiro ponudnika, saj je bila kot edino merilo konkretnega javnega naročila določena najugodnejša cena.

Informacijski pooblaščenec je za nekatere druge dokumente ugotovil, da niso bili pravilno označeni kot poslovna skrivnost po subjektivnem kriteriju. Zato je moral ugotavljati obstoj objektivnega kriterija poslovne skrivnosti. Glede dostopa do certifikatov je ugotovil, da ti izkazujejo, da je določen proizvod skladen z vsemi predpisi, ki se na ta izdelek nanašajo, zato njihovo razkritje zagotovo ne more poslabšati konkurenčne prednosti stranskega udeleženca na trgu ali mu povzročiti škode z vidika drugega odstavka 39. člena ZGD-1, kvečjemu nasprotno. Certifikat namreč odraža kakovostno raven izdelka, skladnost izdelka z normativnimi akti in

[22] Uradni list RS, št. 72/2011 – uradno prečiščeno besedilo 3 s spremembami; v nadaljevanju ZJNVETPS.

standardi, v veliki meri pa prispeva tudi k smotrnemu razvoju izdelka, njegovi tržni uveljavitvi ter ekonomičnosti proizvodnje. Tudi za bančne garancije je Informacijski pooblaščenec ugotovil, da z razkritjem, da je družba dobila potrjeno bančno garancijo, stranskemu udeležencu ne bi mogla nastati občutna škoda. Ravno nasprotno, to je zagotovo eden od kazalnikov, da je družba vredna zaupanja, kar predstavlja prednost na trgu in ne škoduje ugledu.

V delu, ki se nanaša na seznam kadrov in podatke o strokovnjakih ter njihove izkušnje in izobrazbo, je Informacijski poblaščenec ugotovil, da vsebina teh dokumentov utegne vplivati na konkurenčni položaj ponudnika, saj razkriva podrobnosti, ki bi jih konkurenčne družbe lahko uporabile sebi v prid in s tem v škodo stranskega udeleženca. Podatki v dokumentih namreč kažejo na kadrovsko zmogljivost in usposobljenost ponudnika, posledično pa lahko kažejo tudi na način organizacije dela podjetja, zato po mnenju Informacijskega pooblaščenca v skladu z drugim odstavkom 39. člena ZGD-1 ta dokument predstavlja poslovno skrivnost stranskega udeleženca. Ob tem pa Informacijski pooblaščenec ugotavlja, da niso izpolnjeni pogoji, po katerih bi bili zahtevani podatki na podlagi tretjega odstavka 39. člena ZGD-1 javni.

Informacije iz Zapisnika o preverjanju podatkov izbranega ponudnika o njegovi kadrovski, tehnični in finančni usposobljenosti ne predstavljajo poslovne skrivnosti, saj gre za dokument, ki ga je ustvaril organ v postopku javnega naročanja in zgolj po členih Zakona o javnem naročanju[23] povzema izpolnjevanje pogojev in skladnost ponudb z zahtevano vsebino ter ocenitev in rangiranje ponudb in ne razkriva konkretnih kadrovskih, tehničnih in finančnih podatkov.

Nazadnje je Informacijski pooblaščenec ugotovil še, da se v dokumentu Poročilo o odpiranju, pregledi in analize ponudb in v bančnih garancijah nahajajo varovani osebni podatki, saj za njihovo razkritje ne obstaja pravna podlaga (namreč ne gre ne za javne uslužbence ne za zakonite zastopnike gospodarskih družb, katerih imena in priimki so javni na podlagi ZSReg v povezavi z ZGD-1).

2.6.8. Kazenski postopek, notranje delovanje organa, osebni podatek, mediji

Z odločbo št. 090-196/2012/3 z dne 4. 10. 2012 je Informacijski pooblaščenec delno odpravil odločbo Ministrstva za zunanje zadeve in mu naložil posredovanje določenega dela Poročila o nadzoru v veleposlaništvu v Parizu.

Organ je zahtevo prosilke sprva v celoti zavrnil, a je Informacijski pooblaščenec po pritožbi prosilke zadevo vrnil organu v ponoven postopek, ker se organ ni opredelil do vseh vprašanj v zvezi z izjemami od prostega dostopa do informacij javnega značaja in izvedbe delnega dostopa. V ponovljenem postopku je organ pridobil mnenje Okrožnega državnega tožilstva, iz katerega je izhajalo, da bi v primeru razkritja zahtevanega poročila lahko nastale škodljive posledice za izvedbo predkazenskega postopka oziroma morebitnega kazenskega postopka. Tako je organ prosilki omogočil delni vpogled v poročilo o nadzoru, zavrnil pa ji je vpogled v tiste dele, za katere je presodil, da bi njihovo razkritje škodilo izvedbi kazenskega pregona in notranjemu delovanju organa (izjemi po 6. in 11. točki 6. člena ZDIJZ). Organ je upošteval tudi določbo tretjega odstavka 6. člena ZDIJZ, ki določa, da se dostop do zahtevane informacije dovoli, če gre za podatke o porabi javnih sredstev ali za podatke, povezane z opravljanjem javne funkcije ali delovnega razmerja javnega uslužbenca. Tako je ugodil zahtevi za vpogled v poročilo v delu, ki se nanaša na prostore veleposlaništva in rezidence ter druga stanovanja, finančno in materialno poslovanje veleposlaništva in evidence veleposlaništva.

Prosilka je v pritožbi zahtevala, da ji organ izroči fotokopijo poročila, ki bo vseboval dele, za katere ji je organ že odobril vpogled in preostale, zavrnjene dele dokumenta, razen morebitnih delov, ki se nanašajo na medosebne odnose in varnostno delovanje veleposlaništva. Ker je prosilka v zahtevi opredelila, da želi vpogled v dokument, v pritožbi pa je zahtevala

[23] Uradni list RS, št. 12/2013 – uradno prečiščeno besedilo 5; v nadaljevanju ZJN-2.

fotokopijo, je v tem delu (zahteva po fotokopiji) Informacijski pooblaščenec ugotovil, da gre za novo zahtevo in jo je zato odstopil organu v reševanje.

Glede izjeme varstva kazenskega postopka je Informacijski pooblaščenec po pregledu dokumenta in po presoji mnenja tožilstva ocenil, da tožilstvo škodljivega učinka razkritja podatkov iz zahtevanega dokumenta ni argumentiralo prepričljivo in v zadostni meri. Tožilstvo je namreč navedlo, da bi razkritje podatkov iz poročila vplivalo na to, da v (pred)kazenskem postopku zaslišani posamezniki ne bi podali resničnih in točnih informacij o zadevnih dogodkih, pač pa bi v svoja subjektivna zaznavanja dogodkov pomešali informacije, ki bi jih v zvezi s tem pridobili v medijih, saj naj bi bilo splošno znano, da po poteku določenega časa posamezniki ne (pre)poznajo več virov, iz katerih so določene informacije pridobili. Obrazložitev tožilstva po mnenju Informacijskega pooblaščenca ni bila ustrezna, saj takšna domneva ne more biti zadosten razlog za zavrnitev dostopa do zahtevanih informacij. Potrebno je namreč opozoriti na to, da zadevno poročilo ni skupek pričevanj oziroma skupek zgolj subjektivnih zaznav posameznikov, ki so bili neposredno vpleteni v dogodke oziroma dejanja na veleposlaništvu, v zvezi s katerimi je bila podana kazenska ovadba pristojnemu organu, pač pa gre za objektivne ugotovitve strokovnega nadzora na Veleposlaništvu Republike Slovenije v Parizu, izvršenega s strani nepristranskih in v dogodke, ki so predmet kazenske ovadbe, nevpletenih uslužbencev Ministrstva za zunanje zadeve. Nenazadnje pa so od izdaje obravnavanega poročila minila že več kot tri leta, dogodki, ki so predmet poročila, pa so še bolj oddaljeni, zato bodo izjave zaslišanih posameznikov že s časovnega vidika lahko pomanjkljive, kar bo prav tako moral ocenjevati in presojati pristojen organ. Poleg tega pa je Informacijski pooblaščenec po hitrem pregledu svetovnega spleta ugotovil, da v zvezi s konkretnim postopkom nadzora v javnosti že dalj časa kroži množica različnih informacij, s katerimi se je javnost (pa tudi vsi potencialni udeleženci kazenskega postopka) že lahko seznanila, tako da ni mogoče predpostaviti, da bi prav razkritje poročila povzročilo, da tožilstvo oziroma morda kasneje tudi sodišče ne bi moglo pravilno, popolno, objektivno in nepristransko voditi in zaključiti kazenskega postopka. Razkritje obravnavanega poročila kot edinega verodostojnega dokumenta v tej zadevi bi lahko v tem smislu na sam postopek celo ugodno vplivalo.

Informacijski pooblaščenec je po uradni dolžnosti preizkusil še, ali se v dokumentu pojavljajo druge izjeme od prosto dostopnih informacij javnega značaja in ugotovil, da je na dveh mestih sicer zapisana telefonska številka, ki predstavlja varovan osebni podatek, drugi osebni podatki pa niso varovani, saj gre vsebinsko za podatke o porabi javnih sredstev ali za podatke, povezane z opravljanjem javne funkcije ali delovnega razmerja javnega uslužbenca. Poročilo se predvsem v delu, ki je bil kasneje podlaga za kazenske ovadbe, nanaša na nepravilnosti pri opravljanju delovnih nalog javnih uslužbencev ali funkcionarjev oziroma na druge nepravilnosti, do katerih je na veleposlaništvu prišlo v zvezi s porabo javnih sredstev. Na podlagi izrecne določbe tretjega odstavka 6. člena ZDIJZ navedena »izjema od izjem« prevlada nad drugimi morebitnimi izjemami od prostega dostopa do informacij javnega značaja iz prvega odstavka 6. člena ZDIJZ (tudi nad izjemo varstva osebnih podatkov).

2.6.9. Osebni podatek, test interesa javnosti

Z odločbo št. 090-148/2012/8 z dne 19. 10. 2012 je Informacijski pooblaščenec odpravil odločbo Ministrstva za notranje zadeve in mu naložil posredovanje določenega dela mnenja in odločbe organa o pridobitvi slovenskega državljanstva za konkretno posameznico.

Prosilka je od organa zahtevala dokumente o tem, ali je posameznica pridobila slovensko državljanstvo po postopku izredne naturalizacije.

Organ je zapisal, da se vse listine, ki so sestavni del upravnega spisa v postopku sprejema v državljanstvo Republike Slovenije, nanašajo neposredno na določeno fizično osebo. Podatek o državljanstvu posameznika je osebni podatek, ki ga je ministrstvo dolžno posredovati le, če tako določa zakon ali če je podana privolitev posameznika. Zakon o državljanstvu Republike Slovenije[24] pravne podlage za takšno posredovanje ne daje, zato je organ uporabil

[24] Uradni list RS, št. 24/2007-UPB2; v nadaljevanju ZDRS.

3. točko prvega odstavka 6. člena ZDIJZ, ki opredeljuje izjemo varstva osebnih podatkov, in zavrnil dostop do zahtevanih informacij. Nadalje je organ ugotovil, da delni dostop ni mogoč, ker navedeni dokument vsebuje podatke iz dokazil, ki jih je stranka priložila v postopku sprejema v državljanstvo in so bili uporabljeni pri oblikovanju mnenja resornega organa. V kolikor bi jih organ prekril, bi prosilka prejela le dokument z navedbo resornega organa in navedbo kriterijev, ki izhajajo iz Uredbe.

Informacijski pooblaščenec je po pregledu zahtevanih dokumentov sicer ugotovil, da ti vsebujejo osebne podatke fizične osebe in izpolnjujejo kriterije za izjemo od prostega dostopa, vendar je nadalje izvedel tudi test interesa javnosti (drugi odstavek 6. člena ZDIJZ) in presodil, da javni interes za razkritje dokumentov iz postopka izredne naturalizacije pretehta nad interesom konkretne posameznice za omejitev dostopa do zadevnih dokumentov.

Podelitev državljanstva po institutu izredne naturalizacije se namreč že po zakonski dikciji izvaja zaradi posebnih državnih koristi (interesov). Namenjen je posameznikom, ki prinašajo izjemen prispevek k družbenemu, gospodarskemu, znanstvenemu, kulturnemu ali drugačnemu razvoju Republike Slovenije ali k povečanju njenega mednarodnega ugleda oziroma prepoznavnosti. Njihovo delovanje je izjemno pomembno v različnih sferah družbenega (in ne zasebnega) življenja v Republiki Sloveniji, zato se mora njihova pravica do varstva osebnih podatkov v delu, ki se nanaša na izredno naturalizacijo, umakniti javnemu interesu, ki v tem primeru prevlada. V konkretnem primeru bi po presoji Informacijskega pooblaščenca prepoved razkritja takšnih osebnih podatkov onemogočala nadzor javnosti nad tako občutljivim institutom, kot je institut izredne naturalizacije, ki naj bi ga izvršilna oblast uporabljala restriktivno in predvsem z veliko mero premišljenosti. Odprtost teh podatkov po mnenju Informacijskega pooblaščenca vsekakor pripomore zlasti k večji odgovornosti države do državljanov Slovenije in do transparentne politike, ki jo država izvaja na področju podeljevanja državljanstva.

Na koncu je Informacijski pooblaščenec pojasnil, da ni potrebe, da se s testom interesa javnosti odpirajo tudi osebni podatki, ki s samim institutom izredne naturalizacije posameznice niso v bistveni zvezi. Gre za podatke o njenem aktualnem državljanstvu, o datumu in kraju rojstva ter o naslovu bivališča, ki jih mora organ ob posredovanju dokumentacije prekriti.

2.6.10. Javna naročila, poslovna skrivnost, test interesa javnosti

Z odločbo št. 090-190/2012/14 z dne 30. 10. 2012 je Informacijski pooblaščenec delno odpravil odločbo Mestne občine Maribor in ji naložil posredovanje pretežnega dela pogodbe z Iskra sistemi d.d. glede postavitve radarjev.

Novinar je od Mestne občine Maribor zahteval vpogled v razpisno ponudbo in fotokopijo pogodbe iz postopka javno-zasebnega partnerstva »Nadgradnja in avtomatizacija cestnega prometa v Mestni občini Maribor« med Mestno občino Maribor in Iskra sistemi d.d.

Organ je zahtevo v celoti zavrnil s sklicevanjem na izjemo poslovne skrivnosti, saj naj bi bili celotna pogodba in ponudba s strani pogodbenega partnerja označeni kot poslovna skrivnost.

Informacijski pooblaščenec je najprej ugotovil, da so izpolnjeni pogoji za obstoj poslovne skrivnosti po subjektivnem kriteriju iz prvega odstavka 39. člena ZGD-1. Dokument je bil označen kot poslovna skrivnost s pisno odredbo (izrecnim pogodbenim določilom v pogodbi in posebej še v sklepu o varovanju poslovne skrivnosti), s to odredbo so bile seznanjene osebe, ki so dolžne poslovno skrivnost varovati, informacija pa je bila kot poslovna skrivnost določena že pred podpisom pogodbe. Kljub temu pa je bilo treba ugotoviti, da pogodba in ponudba vsebujeta tudi nekatere podatke, ki so javni že na podlagi zakona in zato po določbi tretjega odstavka 39. člena ZGD-1 ne morejo predstavljati poslovne skrivnosti.

Zakon o javno-zasebnem partnerstvu[25] določa, da se javno-zasebno partnerstvo izvaja v javnem interesu in da je njegov namen zagotoviti preglednost, konkurenčnost, nediskriminatornost in poštenost postopkov nastajanja ter sklepanja in izvajanja posameznih oblik javno-zasebnega partnerstva. Vsakdo, ki želi skleniti pogodbo s subjektom javnega prava, se mora podrediti posebnemu načinu sklepanja pravnih poslov, ponudniki pa se morajo zavedati posebnega zakonskega režima glede sklepanja tovrstnih pogodb in ne morejo pričakovati absolutnega varstva svojih podatkov. Javnost podatkov določa tudi ZJN-2, saj drugi odstavek 22. člena določa, da so ne glede na varstvo podatkov (tudi če gre za poslovno skrivnost) vedno javni podatki količina iz specifikacije, cena na enoto, vrednost posamezne postavke in skupna vrednost iz ponudbe, v primeru merila ekonomsko najugodnejše ponudbe pa tisti podatki, ki so vplivali na razvrstitev ponudbe v okviru drugih meril. Po mnenju Informacijskega pooblaščenca podatki, ki izkazujejo, da je izbrani ponudnik izpolnil osnovne pogoje javnega razpisa in da je ponudil rešitev, ki je bila ekonomsko najugodnejša, ne morejo predstavljati poslovne skrivnosti. Upoštevati je treba tudi določbo tretjega odstavka 6. člena ZDIJZ, ki med drugim pravi, da se ne glede na morebitne izjeme (tudi izjemo poslovne skrivnosti) dostop do zahtevane informacije dovoli, če gre za podatke o porabi javnih sredstev. Čeprav organ iz mestnega proračuna zasebnemu partnerju ni neposredno izplačal nobenih sredstev, pa iz sklenjene pogodbe izhaja, da se bo predmet pogodbe nedvomno financiral iz javnih sredstev, in sicer iz sredstev izterjanih glob.

Nenazadnje pa je lahko poslovna skrivnost samo nekaj, kar ni znano širšemu krogu ljudi, ne pa podatki, ki so bili obravnavani na javni seji mestnega sveta in so še vedno prosto dostopni na svetovnem spletu (podatki iz predloga Akta o javno-zasebnem partnerstvu in pravne študije izvedbe partnerstva).

Za določen del dokumentov, za katere zakonodaja ne določa javnosti in so zato veljavno opredeljeni kot poslovna skrivnost, pa je Informacijski pooblaščenec ocenil, da jih je treba razkriti na podlagi drugega odstavka 6. člena ZDIJZ, na podlagi prevladujočega interesa javnosti. Pri uporabi testa interesa javnosti je potrebno presoditi, ali je interes javnosti za razkritje informacije lahko močnejši od potencialno storjene škode, ki bi nastala z razkritjem informacije. V konkretni zadevi je sklenitev javno-zasebnega partnerstva za projekt »Nadgradnje in avtomatizacije cestnega prometa v MO Maribor« v lokalni skupnosti in tudi v širši javnosti sprožila številne dileme in vprašanja, ki so predmet razprav v okviru uradnih institucij (npr. v okviru Mestnega sveta Maribor), v medijih, pa tudi v širši javnosti. Gre za tematiko, ki ni povezana samo z vprašanjem, ali je bila sklenitev predmetnega javno-zasebnega partnerstva transparentna in gospodarna z vidika porabe javnih sredstev, ampak se v javnosti pojavljajo številne dileme in vprašanja v zvezi s pravicami in obveznostmi, ki iz tega javno-zasebnega partnerstva izhajajo za posameznike. Dejstvo je namreč, da predmetno javno-zasebno partnerstvo, katerega temeljni cilj je zvišanje prometne varnosti za vse udeležence v prometu, vključuje tudi postavitev radarjev za nadzor hitrosti, predmet nadzora pa so fizične osebe oziroma udeleženci v prometu. Informacijski pooblaščenec je poudaril, da so pooblastila nadzornih organov in pravice udeležencev prometa urejena že v Zakonu o pravilih cestnega prometa[26], če pa občina sklene javno-zasebno partnerstvo, ki poseže v izvrševanje teh pravic in obveznosti, imajo posamezniki, ki so subjekti tega nadzora, zagotovo pravico do celovitih in popolnih informacij v zvezi s tem. Gre zlasti za informacije o tem, s kakšnimi samodejnimi napravami za nadzor se jih nadzira, kako sistem deluje, kakšne so obveznosti glede vzdrževanja tehnične brezhibnosti, katere podatke sistem zbira in kdo do njih lahko dostopa oziroma jih obdeluje ter kakšne obveznosti ima v zvezi s tem zasebni partner oziroma kakšne pravice je nanj prenesla občina kot javni partner. Prav tako je v javnem interesu vprašanje, kakšne odgovornosti je občina prevzela v okviru javno-zasebnega partnerstva oziroma kakšne pristojnosti je prenesla na subjekt zasebnega prava na tako pomembnem področju, kot je urejanje in varnost cestnega prometa.

Zaradi prevladujočega interesa javnosti je Informacijski pooblaščenec odločil, da mora organ razkriti dele pogodbe, ki predstavljajo obveznosti zasebnega partnerja, obveznosti javnega partnerja, vzdrževanje in upravljanje sistema ter delovanje prekrškovnega sistema. V preostalem delu je Informacijski pooblaščenec odločil, da javni interes ne prevlada in da je treba zavrniti dostop do informacij, ki predstavljajo poslovne skrivnosti.

---

25 Uradni list RS, št. 127/2006; v nadaljevanju ZJZP.

26 Uradni list RS, št. 109/2010, s spremembami; v nadaljevanju ZPrCP.

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

Informacijski pooblaščenec lahko leto 2012 na področju dostopa do informacij javnega značaja oceni kot pozitivno. V letu 2012 je na tem področju v reševanje prejel 1295 zadev, kar je manj kot v letu 2011. Število pritožb se je zmanjšalo zlasti na račun bistveno manjšega števila pritožb zoper molk prvostopenjskih organov. Teh je bilo v letu 2012 242, leto prej pa kar 549. Po večletnem zviševanju pritožb zaradi neodzivnosti zavezancev je tako leto 2012 prvo, ko se je število teh pritožb zmanjšalo, kar kaže na večjo odzivnost organov prve stopnje. Ob tem se je povečalo število vprašanj, pobud in prošenj za pojasnila v zvezi z uporabo ZDIJZ v praksi (skupaj 776 zadev, v letu 2011 699 zadev), število vloženih pritožb zoper zavrnilne odločbe pa je ostalo na primerljivi ravni.

Na podlagi zgoraj navedenih podatkov in izvedenih pritožbenih postopkov Informacijski pooblaščenec ocenjuje, da so tako prosilci kot organi zavezanci bolje seznanjeni z institutom dostopa do informacij javnega značaja, da pa bo v praksi potrebnih še veliko aktivnosti za promocijo te pravice in usposabljanje zavezancev za uporabo zakona. Na to kaže tudi število vprašanj in prošenj za pojasnila v zvezi z uporabo zakona v praksi, ki je tudi v letu 2012 naraslo. Zlasti občine in organi širšega javnega sektorja (javni zavodi s področja šolstva, zdravstva, druge pravne osebe javnega prava), izvajalci javnih služb in nosilci javnih pooblastil, ki so pravne osebe zasebnega prava, so z obveznostmi, ki jim jih nalaga ZDIJZ, še vedno slabo seznanjeni. V zvezi z navedenim Informacijski pooblaščenec poziva resorno ministrstvo (trenutno Ministrstvo za notranje zadeve in javno upravo), 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 so še v postopku reševanja ali se z njimi še ni srečal, pa se kot pritožbeni organ ne sme opredeliti vnaprej.

Ob navedenem velja opozoriti, da se tako organi zavezanci na prvi stopnji kot Informacijski pooblaščenec kot pritožbeni organ na tem področju srečujemo z vse bolj zahtevnimi primeri. V letu 2012 je bistveno naraslo število zadev s področja dostopa do dokumentacije iz postopkov javnega naročanja. Gre za postopke, ki zahtevajo odločanje o obsežni dokumentaciji, vključevanje stranskih udeležencev ter presojo več izjem z vidika porabe javnih sredstev (poslovne skrivnosti, osebnih podatkov). Prav tako je v letu 2012 naraslo število pritožbenih zadev, v katerih so prosilci novinarji oziroma gre za pritožbe po 45. členu ZMed, pri katerih je čim krajši rok reševanja bistvenega pomena. Ob tem Informacijski pooblaščenec ocenjuje, da do pritožbenih postopkov pogosto pride zaradi procesnih napak na strani prvostopenjskega organa (nevključitev stranskih udeležencev, nepravočasno odzivanje na zahteve) ter nepoznavanja zakonskih določb in uporabe zakona v praksi, kar bi bilo mogoče odpraviti z rednim in obveznim usposabljanjem uradnih oseb za dostop do informacij javnega značaja pri organih zavezancih.

Kot že nekaj let zapovrstjo Informacijski pooblaščenec ponovno opozarja na problematiko zaračunavanja stroškov dostopa do informacij javnega značaja v praksi. V letu 2012 se je število vloženih pritožb zaradi visoko zaračunanih stroškov ponovno povišalo, zaskrbljujoče pa je stališče nekaterih zavezancev, da tudi za vpogled v zahtevano informacijo zaračunavajo stroške, čeprav prvi odstavek 34. člena ZDIJZ jasno določa, da je vpogled v zahtevano informacijo brezplačen. Prav tako še vedno ni bila spremenjena Uredba o posredovanju in ponovni uporabi informacij javnega značaja, posledično pa lahko zavezanci prosilcem še naprej arbitrarno zaračunavajo nesorazmerno visoke stroške za delo javnih uslužbencev. Gre za problematiko neusklajenosti med predmetno Uredbo in ZDIJZ, na katero Informacijski pooblaščenec opozarja že od leta 2009.

Tudi v letu 2012 je Informacijski pooblaščenec večkrat javno opozoril na potrebo po širjenju kroga zavezanih organov, in sicer na vse pravne osebe, katerih ustanovitelj je ali ima v njih država, lokalna skupnost ali druga pravna oseba javnega prava prevladujoč vpliv. Praksa je

namreč pokazala, da gre za subjekte, katerih poslovanje je lahko neposredno ali posredno v javnem interesu, javnost pa na podlagi veljavnega ZDIJZ nima dostopa do nobenih informacij o njihovem poslovanju, ker gre za subjekte zasebnega prava.

V letu 2012 je Informacijski pooblaščenec prejel dve pritožbi 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 informacij javnega značaja ima pomemben gospodarski potencial, ki pa v praksi ostaja premalo izkoriščen. Na to opozarja tudi Evropska komisija, pri kateri je tudi v letu 2012 potekala razprava o predlogu sprememb Direktive Evropskega parlamenta in Sveta z dne 17. 2. 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 2012 sodeloval v mednarodnem konzorciju pri projektu LAPSI (Legal Aspects of Public Sector Information), 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 pojavljajo 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 ena izmed zagotovljenih človekovih pravic in temeljnih svoboščin v državi. Navedena določba 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. Zato je tak poseg dopusten, če je v zakonu določno opredeljeno, kateri osebni podatki se smejo obdelovati, namen njihove obdelave, zagotovljeno pa mora biti tudi 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 tega 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 v zvezi z zavarovanjem osebnih podatkov, katalogi zbirk osebnih podatkov in registracijo zbirk osebnih podatkov, pravice 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 rok hrambe osebnih podatkov.

Zakon o varstvu osebnih podatkov[27], 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[28].

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, iznosa osebnih podatkov v tretje države 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,

27 Uradni list RS, št. 86/2004; v nadaljevanju ZVOP-1.
28 Uradni list Evropskih skupnosti, št. L 281, 23. 11. 1995.

ki je bila ratificirana in objavljena leta 1994[29]. 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 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[30]. ZVOP-1A je uvedel dve pomembni novosti – poleg določenih olajšav z vidika oblik dostopa posameznikov do njihovih osebnih podatkov je novela bistveno zožila krog zavezancev za vpis zbirk osebnih podatkov v register, kar predstavlja administrativno in s tem posledično tudi finančno razbremenitev upravljavcev osebnih podatkov.

Določbe ZVOP-1A so bile usklajene s spremembami Zakona o prekrških[31] iz leta 2006 ter so upoštevale uvedbo evra kot plačilnega sredstva v Republiki Sloveniji s 1. 1. 2007.

Uradno prečiščeno besedilo Zakona o varstvu osebnih podatkov je bilo izdano septembra 2007 (Uradni list RS, št. 94/2007).

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, pravice, dolžnosti in pooblastila državnih nadzornikov, postopek inšpekcijskega nadzora, inšpekcijski ukrepi in druga vprašanja, povezana z inšpekcijskim nadzorom, so določeni v Zakonu o inšpekcijskem nadzoru[32], 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:

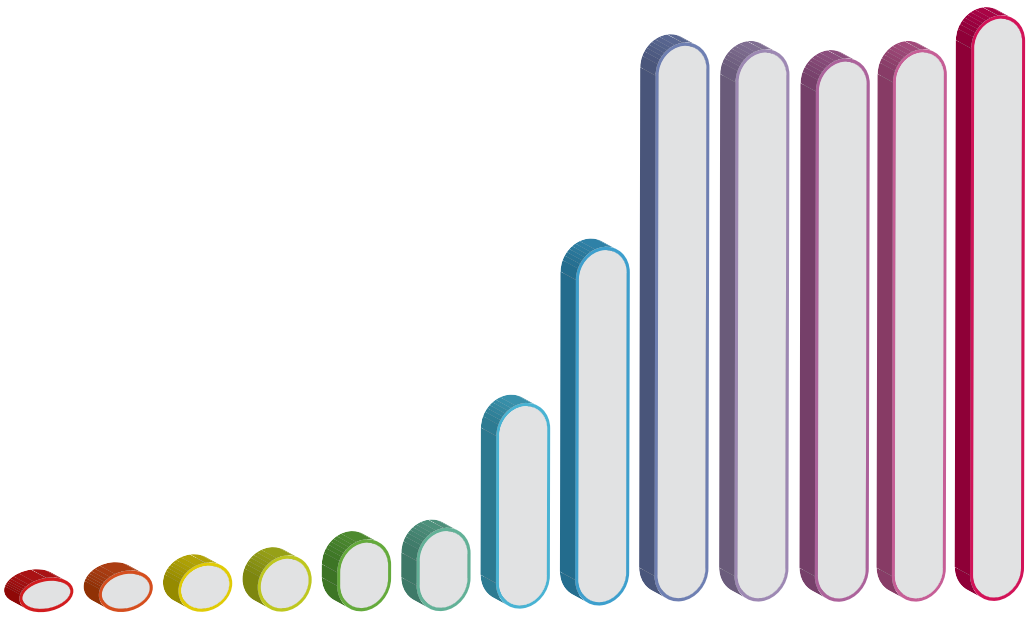
- nadzor zakonitosti obdelave osebnih podatkov;
- nadzor ustreznosti in izvajanja postopkov in ukrepov za zavarovanje osebnih podatkov;
- nadzor nad izvajanjem določb ZVOP-1, ki urejajo katalog zbirke osebnih podatkov, register zbirk osebnih podatkov in evidentiranje posredovanja osebnih podatkov posameznim uporabnikom osebnih podatkov;
- nadzor nad izvajanjem določb ZVOP-1 v zvezi z iznosom osebnih podatkov v tretje države in njihovim posredovanjem tujim uporabnikom.

Informacijski pooblaščenec je leta 2012 zaradi suma kršitev določb ZVOP-1 vodil 725 inšpekcijskih zadev, 245 v javnem in 480 v zasebnem sektorju. Zoper pravne osebe javnega sektorja je na podlagi prijav vodil 212 inšpekcijskih zadev, 33 inšpekcijskih postopkov pa je uvedel po uradni dolžnosti, če je npr. na podlagi objav v medijih zaznal sum kršitve varstva osebnih podatkov. Zoper zavezance v zasebnem sektorju je na podlagi prijav vodil 446 inšpekcijskih zadev, 34 inšpekcijskih postopkov je začel po uradni dolžnosti. Število prijav in pritožb zaradi

[29] Uradni list RS, št. 11/1994 – Mednarodne pogodbe št. 3/1994.
[30] Uradni list RS, št. 67/2007; v nadaljevanju ZVOP-1A.
[31] Uradni list RS, št. 40/2006.
[32] Uradni list RS, št. 43/2007 – uradno prečiščeno besedilo 1; v nadaljevanju ZIN.

suma kršitev določb ZVOP-1 se je v primerjavi s statističnimi podatki za preteklo leto ponovno nekoliko povečalo. Število prijav, ki jih je prejel Informacijski pooblaščenec, je nekoliko večje od števila vodenih inšpekcijskih zadev oziroma uvedenih inšpekcijskih postopkov, saj je zoper določene zavezance prejel več prijav v zvezi z istimi sumi kršitev določb ZVOP-1. Večje število prijav zoper posamezne zavezance je opaznejše v zasebnem sektorju, zlasti zoper zavezance, ki izvajajo neposredno trženje in svoje ponudbe pošiljajo velikemu številu posameznikov. Tako je Informacijski pooblaščenec v letu 2012 zoper zavezance v javnem sektorju prejel 237 prijav, zoper zavezance v zasebnem sektorju pa 510 prijav.

Slika 8: Število inšpekcijskih zadev, ki jih je zaradi suma kršitev določb ZVOP-1 vodil Informacijski pooblaščenec med letoma 2000 in 2012.



Informacijski pooblaščenec je zaradi suma kršitev določb ZVOP-1 zoper pravne osebe javnega sektorja na podlagi prijav vodil 212 inšpekcijskih zadev. V 53 primerih je bilo že iz samih prijav razvidno, da opisano dejanje ne pomeni kršitve določb ZVOP-1, zato je državni nadzornik prijaviteljem pisno pojasnil, zakaj uvedba postopka inšpekcijskega nadzora ne bi bila smiselna. Leta 2012 je bilo izdanih še devet obvestil o neuvedbi inšpekcijskega postopka za prijave, prejete konec leta 2011. Informacijski pooblaščenec je pet prijav odstopil v reševanje pristojnim institucijam. Po preučitvi prejetih prijav je bilo v letu 2012 začetih 154 inšpekcijskih postopkov, 33 pa še po uradni dolžnosti, skupaj torej 187. V okviru inšpekcijskih postopkov v javnem sektorju je bilo opravljenih 62 inšpekcijskih pregledov. Za odpravo ugotovljenih nepravilnosti je bilo izrečenih pet opozoril v zapisniku o inšpekcijskem nadzoru in izdanih 24 odločb, od tega 13 v postopkih, začetih pred letom 2012. Šest zavezancev je na Upravno sodišče Republike Slovenije vložilo tožbe zoper odločbe Informacijskega pooblaščenca, navedeno sodišče pa je odločilo v upravnem sporu v zvezi z odločbo Informacijskega pooblaščenca iz leta 2011. Sodišče je postopek ustavilo, ker je tožeča stranka tožbo umaknila. Leta 2012 je bilo zaključenih 140 inšpekcijskih postopkov. S sklepom o ustavitvi postopka jih je bilo zaključenih 120, od tega 42 iz preteklih let. Z odločbo se je zaključilo 18 postopkov (zoper šest odločb so zavezanci namreč vložili tožbe), od tega 10 iz preteklih let, z zaznamkom v zapisniku o inšpekcijskem nadzoru pa sta bila ustavljena dva postopka. V 52 inšpekcijskih postopkih, ki so bili uvedeni in zaključeni v letu 2012, Informacijski pooblaščenec ni zaznal kršitev določb ZVOP-1.

Informacijski pooblaščenec je v javnem sektorju vodil zadeve v zvezi z naslednjimi sumi kršitev določb ZVOP-1:

- 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 - 96,
- nezakonito zbiranje oziroma zahtevanje osebnih podatkov - 65,
- neustrezno zavarovanje osebnih podatkov - 21,
- nezakonito izvajanje videonadzora - 16,
- neposredno trženje - 1,
- razno: pogodbena obdelava osebnih podatkov, nezakonito uničenje osebnih podatkov, obdelava netočnih in neažurnih osebnih podatkov, obdelava osebnih podatkov v nasprotju z namenom njihovega zbiranja, v okviru inšpekcijskih postopkov po uradni dolžnosti je Informacijski pooblaščenec preverjal izvajanje določb ZVOP-1 v celoti - 46.

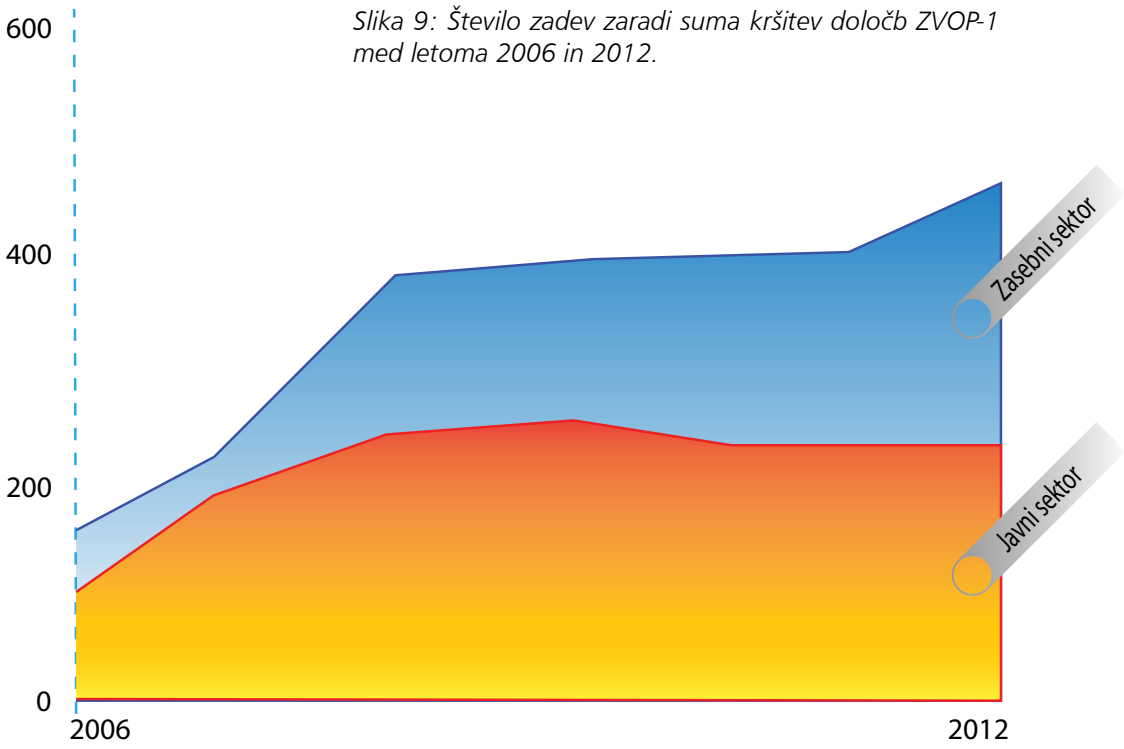
Prijave so bile vložene in postopki po uradni dolžnosti uvedeni zoper naslednje skupine zavezancev v javnem sektorju:

- javne sklade, zavode, agencije in druge osebe javnega prava - 104, od tega zoper vzgojno-izobraževalne ustanove 28 in 23 zoper zdravstvene ustanove,
- državne organe 97, od tega sodišča 16,
- občine 44.

Informacijski pooblaščenec je leta 2012 zoper zavezance v zasebnem sektorju vodil 480 zadev, od tega 446 na podlagi prijav in 34 po uradni dolžnosti. Kar v 143 primerih so bili prijavitelji obveščeni, da Informacijski pooblaščenec postopka inšpekcijskega nadzora ne bo uvedel, ker iz njihove prijave ni izhajal sum kršitev določb ZVOP-1 ali ker tudi po pozivu Informacijskega pooblaščenca niso posredovali dovolj podatkov za uvedbo inšpekcijskega postopka. Informacijski pooblaščenec je 15 prijaviteljev napotil na pravico do seznanitve z lastnimi osebnimi podatki in na pravico zahtevati prenehanje uporabe osebnih podatkov za namen neposrednega trženja s pojasnilom, da mu v primeru zavrnitve zahteve lahko podajo pritožbo ali prijavo. 12 prijav je posredoval v reševanje pristojnim institucijam. Izdal je še 14 obvestil o neuvedbi inšpekcijskega postopka, ki so se nanašale na prijave, prejete konec leta 2011. Tako je bilo leta 2012 na podlagi prejetih prijav začetih 276 postopkov inšpekcijskega nadzora, 34 jih je bilo uvedenih po uradni dolžnosti, skupaj torej 310. Državni nadzorniki za varstvo osebnih podatkov so v zasebnem sektorju opravili 115 inšpekcijskih pregledov. Zaradi ugotovljenih nepravilnosti so izrekli 13 opozoril v zapisniku o inšpekcijskem nadzoru in izdali 50 ureditvenih odločb, od tega polovico v postopkih, začetih pred letom 2012. Leta 2012 sta dva zavezanca zoper prejeto odločbo sprožila upravni spor z vložitvijo tožbe na Upravno sodišče Republike Slovenije. En zavezanec je kasneje tožbo umaknil. Sodišče je odločilo v treh upravnih sporih iz preteklih let - dve tožbi je zavrnilo, eno pa zavrglo. Informacijski pooblaščenec je prejel tudi sodbo Vrhovnega sodišča Republike Slovenije, ki je odločalo o reviziji tožeče stranke zoper sodbo Upravnega sodišča iz leta 2010. Vrhovno sodišče je revizijo zavrnilo in potrdilo sodbo Upravnega sodišča, ki je potrdilo odločbo Informacijskega pooblaščenca. Leta 2012 je bilo izdanih 181 sklepov o ustavitvi inšpekcijskega postopka, od tega 76 v postopkih, ki so bili začeti pred letom 2012, trije postopki so bili ustavljeni z zaznamkom v zapisniku o inšpekcijskem nadzoru. V 54 inšpekcijskih postopkih, ki so bili začeti in zaključeni v letu 2012, Informacijski pooblaščenec ni zaznal kršitev določb ZVOP-1.

Sumi kršitve določb ZVOP-1 v zasebnem sektorju so se nanašali na:

- nezakonito razkrivanje 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 - 130,
- zlorabe osebnih podatkov za namene neposrednega trženja - 118,
- nezakonito zbiranje oziroma zahtevanje osebnih podatkov - 79,
- nezakonito izvajanje videonadzora - 56,
- neustrezno zavarovanje osebnih podatkov - 23,
- ostalo: predčasno uničenje osebnih podatkov, zavrnitev posredovanja osebnih podatkov, obdelava netočnih in neažurnih osebnih podatkov, obdelava osebnih podatkov v nasprotju z namenom njihovega zbiranja, pogodbena obdelava - 74.



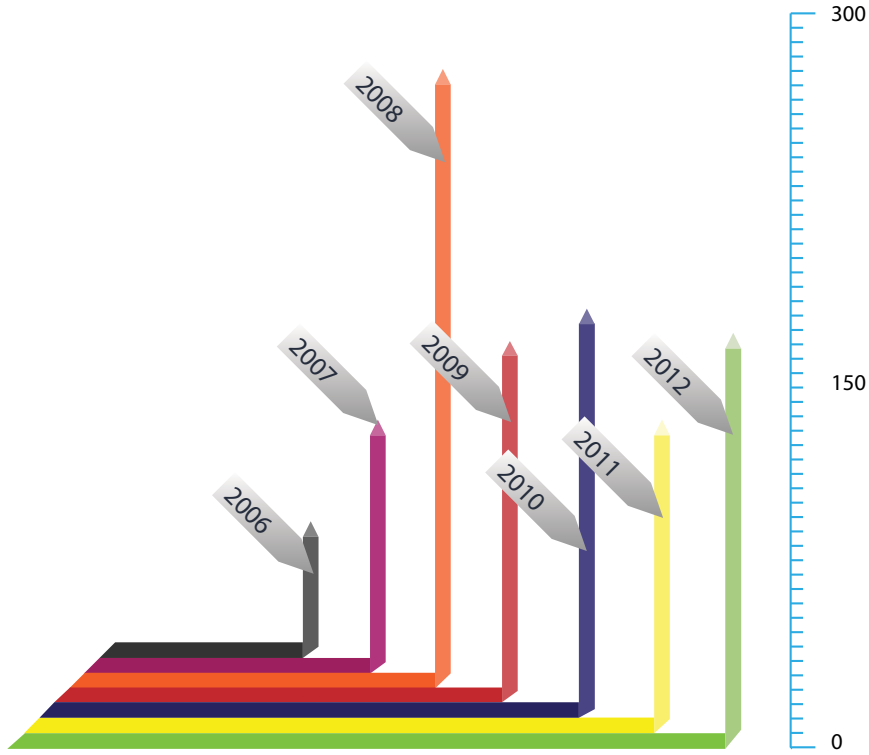
Slika 9: Število zadev zaradi suma kršitev določb ZVOP-1 med letoma 2006 in 2012.

3.2.3. Storjeni prekrški

Zaradi kršitev določb ZVOP-1 je bilo leta 2012 začetih 158 postopkov o prekršku, 29 postopkov zoper pravne osebe javnega sektorja in njihove odgovorne osebe, 78 postopkov zoper pravne osebe zasebnega sektorja in njihove odgovorne osebe ter 51 postopkov zoper posameznike in odgovorne osebe državnih organov in samoupravnih lokalnih skupnosti. Za ugotovljeni prekršek lahko prekrškovni organ v skladu s 53. členom Zakona o prekrških[33] izreče opozorilo, če je storjeni prekršek neznatnega pomena 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.

33 Uradni list RS, št. 29/2011 - uradno prečiščeno besedilo 8; v nadaljevanju ZP-1.

Slika 11: Število uvedenih postopkov o prekršku med letoma 2006 in 2012.



V prekrškovnih postopkih je Informacijski pooblaščenec leta 2012 izdal:
- 17 opozoril,
- 119 odločb o prekršku (61 opominov in 58 glob, od tega sedem plačilnih nalogov).

Število izdanih odločb o prekršku se je v primerjavi z letom 2011 močno povečalo, veliko večje je bilo tudi število izrečenih glob. Leta 2011 je Informacijski pooblaščenec namreč izdal 71 odločb o prekršku in izrekel 19 glob.

Informacijski pooblaščenec je v skladu z načelom ekonomičnosti v okviru postopkov inšpekcijskega nadzora izrekel tudi 87 opozoril po 53. členu ZP-1 (leta 2011 75), 24 v javnem in 63 v zasebnem sektorju.

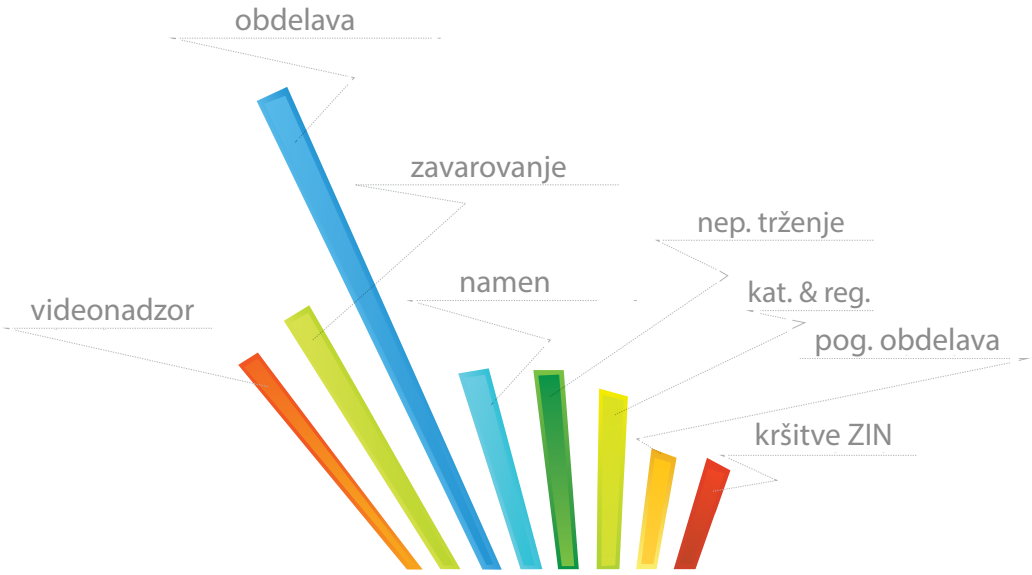
Kršitelji so zoper izdane odločbe o prekršku vložili 30 zahtev za sodno varstvo, od tega 28 zoper globe in dve zoper opomine.

Leta 2012 je Informacijski pooblaščenec ustavil šest postopkov o prekršku, 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 (88),
- zavarovanje osebnih podatkov: 24. in 25. člen ZVOP-1 (54),
- videonadzor: 74., 75., 76. in 77. člen ZVOP-1 (45),
- namen zbiranja in nadaljnje obdelave osebnih podatkov: 16. člen ZVOP-1 (32),
- neposredno trženje: 72. in 73. člen ZVOP-1 (27),
- vzpostavitev katalogov zbirk osebnih podatkov in posredovanje podatkov v register zbirk osebnih podatkov: 26. in 27. člen ZVOP-1 (25),
- pogodbeno obdelavo osebnih podatkov: 11. člen ZVOP-1 (23),
- neizpolnjevanje ukrepov, izrečenih v postopkih inšpekcijskega nadzora: 29. člen ZIN (11),
- sledljivost posredovanja osebnih podatkov: tretji odstavek 22. člena ZVOP-1 (8),
- obveščanje posameznika o obdelavi osebnih podatkov: 19. člen (4),

- rok hrambe osebnih podatkov: 21. člen ZVOP-1 (2),
- zavarovanje občutljivih osebnih podatkov: 14. člen ZVOP-1(2),
- obdelava občutljivih osebnih podatkov: 13. člen ZVOP-1 (2),
- vpogled v lastne osebne podatke: 30. in 31. člen ZVOP-1(1),
- iznos osebnih podatkov v tretje države: 63. člen ZVOP-1 (1).

Slika 12: Najpogostejše kršitve določb ZVOP-1 leta 2012.



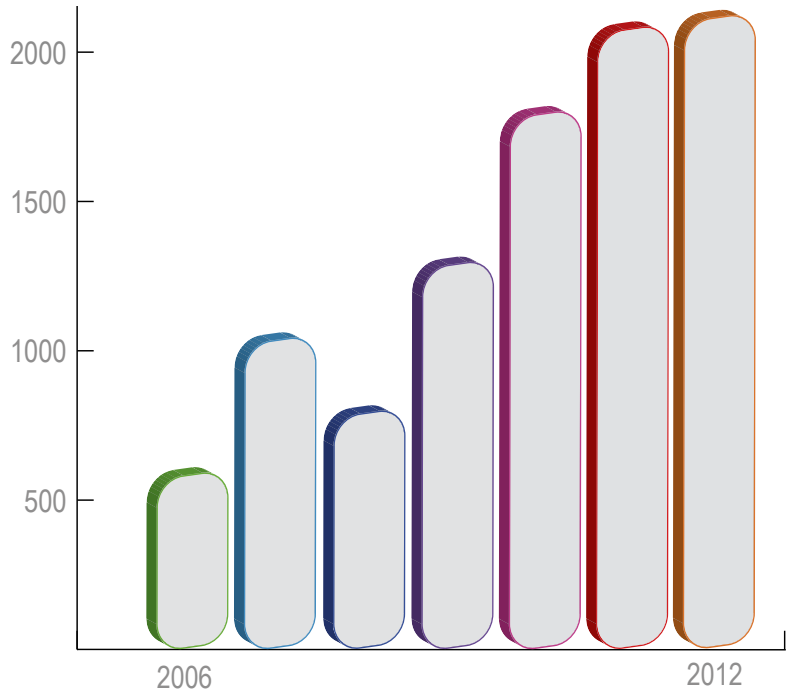
Leta 2012 je Informacijski pooblaščenec prejel 17 odločitev (sodba ali sklep), s katerimi so okrajna sodišča odločila o vloženih zahtevah za sodno varstvo zoper odločbe o prekrških, ki jih je izdal Informacijski pooblaščenec v preteklih letih:

- zahteva za sodno varstvo je bila zavrnjena kot neutemeljena, odločba Informacijskega pooblaščenca pa potrjena - 10,
- zahtevi za sodno varstvo je bilo ugodeno v delu, ki se nanaša na izrečeno sankcijo, tako da se je storilcem za prekršek spremenila sankcija ali višina globe, sicer je bila zahteva za sodno varstvo zavrnjena kot neutemeljena - 4,
- zahtevi za sodno varstvo je bilo ugodeno, odločba Informacijskega pooblaščenca odpravljena, postopek o prekršku pa ustavljen - 3.

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 2012 prejel 2.191 prošenj za podajo pisnega pojasnila ali mnenja v zvezi s konkretnimi vprašanji, kar je malenkost več kot prejšnje leto, ko jih je prejel 2.143. 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 izdal 143 mnenj in pojasnil, medtem ko je 2.048 posameznikom, ki so zastavili vprašanja, na katera je v preteklosti že odgovarjal, posredoval le kratek odgovor oziroma jih le napotil na že izdelano mnenje. Informacijski pooblaščenec je dajal tudi ustna mnenja in pojasnila. V uradu je namreč vsak dan na voljo dežurni državni nadzornik, ki na vprašanja odgovarja po telefonu.

Slika 13: Število zaprosil za mnenja med letoma 2006 in 2012.



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, vrtci, zavarovalništvo, zavarovanje osebnih podatkov, zdravstveni osebni podatki). Velik del izdanih mnenj je objavljen na spletni strani www.ip-rs.si.

3.4. Dopustnost izvajanja biometrijskih ukrepov

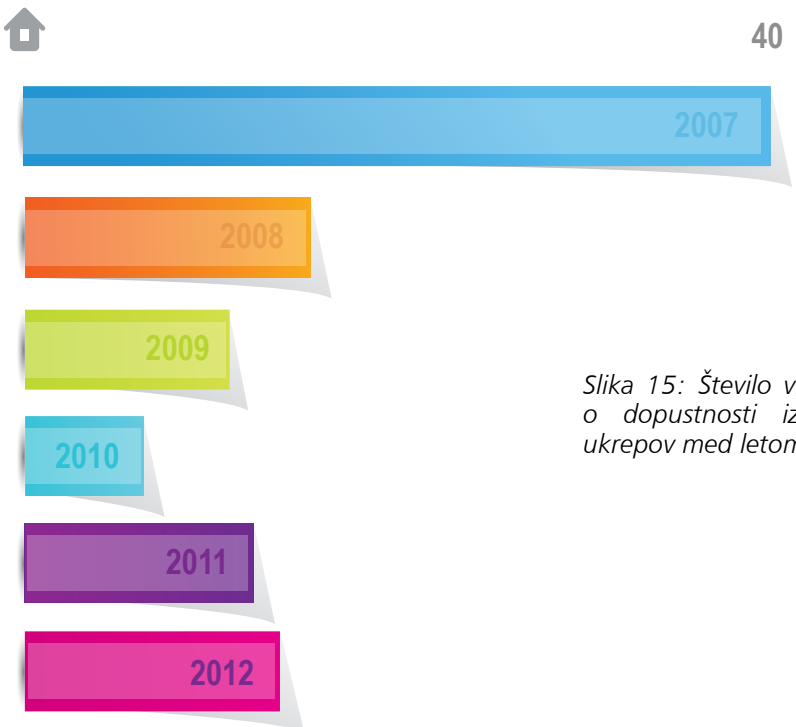
Informacijski pooblaščenec je po določbi 80. člena ZVOP-1 pristojen za vodenje upravnih postopkov za izdajo odločb o tem, ali je nameravano izvajanje biometrijskih ukrepov v skladu z določbami ZVOP-1 ali ne. Biometrijski ukrepi so kot posebna oblika obdelave osebnih podatkov opredeljeni v tretjem poglavju VI. dela ZVOP-1, v 78.–81. členu.

Po določbi tretjega odstavka 80. člena ZVOP-1 mora Informacijski pooblaščenec odločiti, ali je nameravana uvedba biometrijskih ukrepov v skladu z določbami ZVOP-1, predvsem, ali je izvajanje biometrijskih ukrepov nujno potrebno za opravljanje dejavnosti, za varnost ljudi ali premoženja ali za varovanje tajnih podatkov ali poslovne skrivnosti. Z določitvijo teh pogojev je zakonodajalec sledil načelu sorazmernosti (3. člen ZVOP-1) ter s tem omejil možnosti prekomernih in neupravičenih posegov v zasebnost in dostojanstvo posameznika. Pri presoji, ali so biometrijski ukrepi nujno potrebni za dosego namena, Informacijski pooblaščenec ugotavlja, ali bi namen, ki ga zasleduje vlagatelj, lahko dosegel z načini obdelave osebnih podatkov, ki manj posegajo v zasebnost zaposlenih oziroma ne vključujejo biometrijskih ukrepov. Pri uvajanju biometrijskih ukrepov je namreč treba upoštevati, da njihovo izvajanje predstavlja neprimerno večji poseg v informacijsko zasebnost posameznika,

saj gre za obdelavo tistih značilnosti, 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 (ali se bodo uporabljali za preverjanje identitete – avtentikacija ali za ugotavljanje identitete – identifikacija).

Biometrijske ukrepe je torej upravičeno uvesti le, če to terja nek resen in utemeljen razlog oziroma če je to nujno potrebno za dosego katerega od v ZVOP-1 določenih namenov. Razlog za uvedbo ni utemeljen in tudi ne nujno potreben, če vlagatelj uvaja biometrijske ukrepe zgolj zaradi priročnosti oziroma odsotnosti skrbi nad npr. karticami oziroma kot alternativno rešitev za preprečitev vstopov nepooblaščenih oseb v svoje prostore.

Informacijski pooblaščenec je leta 2012 prejel 11 vlog za izdajo dovoljenja za uvedbo biometrijskih ukrepov. Izdal je sedem odločb o dopustnosti izvajanja biometrijskih ukrepov, od tega dve za vlogi, ki jih je prejel v reševanje v letu 2011. V petih odločbah je Informacijski pooblaščenec uvedbo biometrijskih ukrepov dovolil, v dveh je njihovo izvajanje zavrnil, eno vlogo pa je s sklepom zavrgel.



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

Informacijski pooblaščenec je ugodil petim zahtevam za izvajanje biometrijskih ukrepov:

1. zahtevi vlagatelja za namen nadzora dostopa v strežniško sobo z uporabo čitalnika prstnih odtisov. Informacijski pooblaščenec je ugotovil, da vlagatelj z uvedbo biometrijskih ukrepov zasleduje cilj nadzora dostopa do sobe, kjer se nahaja strežnik, na katerem so za vlagateljevo poslovanje pomembni podatki, tudi podatki, ki v skladu z 39. členom ZGD-1 predstavljajo poslovne skrivnosti, in osebni podatki. Vlagatelj z izvajanjem biometrijskih ukrepov varuje tudi svoje premoženje večje vrednosti, saj je omenjeni strežnik visokega cenovnega razreda. Informacijski pooblaščenec je zaključil, da je vlagatelj upravičen sprejeti in izvajati ukrepe – tudi biometrijske, s katerimi bo kar najučinkoviteje zavaroval prej navedene dobrine. Z biometričnim varovanjem bo vlagatelj dostop do strežniške sobe omogočil samo dvema pooblaščenima zaposlenima in tako zagotovil najstrožji režim varovanja.

2. zahtevi vlagatelja za namen varovanja premoženja in varovanja poslovnih skrivnosti z uporabo čitalnika prstnih odtisov nad tistimi zaposlenimi, ki vstopajo v naslednje prostore na sedežu vlagatelja:

- prostor predaje plemenitih kovin kupcem,
- prostor priprave blaga,

- trezor,
- arhiv,
- skupni prostor priprave blaga oziroma plemenitih kovin.

Informacijski pooblaščenec je zaključil, da je vlagatelj izkazal nujnost uvedbe biometrijskih ukrepov. Strogo nadzorovanje vstopa v navedene prostore je potrebno, ker vlagatelj v njih hrani in drugače obdeluje plemenite kovine (zlate investicijske palice in kovance). Vlagatelj je podobno kot banke izpostavljen visokemu varnostnemu tveganju, saj bi dostop nepooblaščene osebe do velike količine plemenitih kovin in njihova potencialna odtujitev pomenila veliko škodo za premoženje vlagatelja. Poleg tega so vlagateljevi zaposleni zaradi narave njegove dejavnosti (trgovanje na debelo s kovinami in rudami) izpostavljeni tveganju ropa, napadov, izsiljevanja in ugrabitve. Vlagatelj je izkazal tudi, da razpolaga s poslovnimi skrivnostmi v smislu določb ZGD-1, saj se v prostorih, ki jih bo varoval z biometrijskimi ukrepi, nahaja informacijski sistem, ki ga je razvil sam in je po njegovih navedbah edini sistem take vrste v Sloveniji, preko katerega je nenehno povezan s svetovno borzo. Na osnovi teh podatkov vlagatelj generira cenike in ostale podatke, nujno potrebne za poslovni proces. Vlagatelj v teh prostorih hrani tudi vso dokumentacijo, povezano s svojim poslovanjem, trgovanjem s plemenitimi kovinami, dokumentacijo z oznako davčne tajnosti in zahteve Urada za preprečevanje pranja denarja. V skladu z načelom sorazmernosti bo vlagatelj izvajal biometrijske ukrepe le nad tistimi zaposlenimi, ki morajo zaradi opravljanja svojih delovnih nalog vstopati v varovane prostore, ostale osebe bodo v te prostore lahko vstopale le v spremstvu zaposlenega z dostopnimi pravicami. Čitalniki prstnih odtisov bodo uporabljeni zgolj za avtentikacijo uporabnika in bodo delovali le kot mehanizem za proženje stikal, ki omogočajo odpiranje vrat.

3. zahtevi vlagatelja (banke) za namen varovanja poslovne skrivnosti z uporabo dveh čitalnikov prstnih odtisov, nameščenih na obeh vhodih v pisarno predsednika uprave. Biometrijski ukrepi se bodo izvajali nad tremi zaposlenimi (predsednik uprave in člana uprave), ki imajo pooblastilo za vstop v varovan prostor. Beležil se bo čas vstopa, pri čemer bo zavedeno samo, kateri vzorec je bil preverjen. Odpiranje vrat v varovano območje bo namreč potekalo po sistemu primerjanja zajetega s shranjenim podatkovnim vzorcem prstnega odtisa, tako da se ne bo izvajal postopek identifikacije, ampak zgolj postopek preverjanja istovetnosti (avtentikacije) osebe, ki bo vstopala v prostor. Informacijski pooblaščenec je ugotovil, da bo vlagatelj z uvedbo biometrijskih ukrepov nadziral dostop do pisarne, v kateri se nahaja dokumentacija, ki vsebuje podatke različnih vrst in stopenj tajnosti, med katerimi so tudi podatki, ki v skladu z 39. členom ZGD-1 predstavljajo poslovno skrivnost vlagatelja. V skladu z ZBan-1 naj bi se tudi vsi podatki o komitentih banke obravnavali kot zaupni podatki. Informacijski pooblaščenec je zaključil, da je v konkretnem primeru pomembno tudi dejstvo, da se bodo biometrijski ukrepi izvajali izključno nad ozkim krogom vodstvenih delavcev vlagatelja, ki so hkrati tudi sprejeli odločitev o uvedbi biometrijskih ukrepov.

4. zahtevi vlagatelja za namen opravljanja dejavnosti in varovanje premoženja. Biometrijski ukrepi bodo temeljili na prepoznavi obraza in se bodo izvajali nad zaposlenimi, ki so pooblaščeni za vstopanje v t. i. čiste prostore laboratorijev. Informacijski pooblaščenec je ugotovil, da je vlagatelj izkazal nujnost uvedbe biometrijskih ukrepov za namen opravljanja dejavnosti, saj v varovanih prostorih proizvaja celične izdelke za zdravljenje različnih poškodb in bolezni. Strogo nadzorovanje vstopa v te čiste prostore laboratorija pa je nujno potrebno, saj bi v primeru nepooblaščenega dostopa v te prostore obstajala velika možnost porušitve kontrolnega okolja in uničenja celičnih kultur v proizvodnem procesu. To bi resno ogrozilo opravljanje dejavnosti vlagatelja, ki temelji na zaupanju posameznikov, da je njihov biološki material pri vlagatelju varen. Informacijski pooblaščenec je zaključil, da dejavnost vlagatelja zahteva najvišje standarde varovanja in da je vlagatelj izkazal tudi nujnost uvedbe biometrijskih ukrepov za namen varovanja premoženja. Vlagatelj bo izvajal biometrijske ukrepe le nad tistimi zaposlenimi, ki so izrecno pooblaščeni za vstopanje v prostore, za katere morajo tudi z vidika regulacije takšne dejavnosti veljati najstrožja pravila dostopa in sledljivosti dostopa.

5. zahtevi vlagatelja za namen varovanja premoženja, ki se nahaja v najetih prostorih v objektu telefonske centrale telekomunikacijskega operaterja. Vlagatelj je navedel, da bo za izvajanje biometrijskih ukrepov nad svojima zaposlenima (direktor, vodja projektov) uporabil čitalnik prstnih odtisov operaterja, s katerim bo sklenil pogodbo o obdelavi osebnih podat-

kov (o izvajanju biometrijskih ukrepov). Informacijski pooblaščenec je v postopku ugotovil, da je operater zaradi varovanja premoženja že dovolil izvajanje biometrijskih ukrepov za vstopanje v objekt telefonske centrale. Čeprav izvajanje biometrijskih ukrepov na način, kot ga je želel vlagatelj - na glavnem vhodu v objekt telefonske centrale, ne predstavlja enako učinkovitega zavarovanja prostorov in premoženja, kot bi ga predstavljalo izvajanje biometrijskih ukrepov za vstopanje zgolj v njegove prostore, je Informacijski pooblaščenec ocenil, da je takšno izvajanje biometrijskih ukrepov mogoče opredeliti kot nujno potrebno za varovanje premoženja, ki se nahaja v prostorih vlagatelja. Glede na to, da lahko s strani operaterja v varovani objekt vstopajo samo posebej pooblačeni zaposleni in da so vstopi v prostore vlagatelja še dodatno zavarovani s ključavnicami, izvajanje biometrijskih ukrepov na vhodu v telefonsko centralo v konkretnem primeru ne zagotavlja bistveno nižje stopnje zavarovanja prostorov vlagatelja, kot bi ga izvajanje teh ukrepov izključno za vstopanje v njegove prostore. Zaposleni, ki so pooblaščeni za vstopanje v telefonsko centralo, po oceni Informacijskega pooblaščenca ne predstavljajo realne nevarnosti za premoženje vlagatelja in njegovih strank, saj gre za posameznike, ki naj bi bili zanesljivi in vredni zaupanja, zlasti glede na dejstvo, da lahko dostopajo do občutljive opreme operaterja, ki po vrednosti in občutljivosti znatno presega premoženje, ki se nahaja v prostorih vlagatelja. Vlagatelj z izvajanjem biometrijskih ukrepov zasleduje cilj nadzora dostopa do svojih prostorov, v katerih so njegove naprave in oprema ter naprave njegovih strank, ki jih hrani za namene izvajanja naročenih preizkusov za potrebe certifikacije. Dejavnost vlagatelja so raziskave in razvoj na področju internetnih tehnologij. Naprave predstavljajo že vsaka zase premoženje precejšnje vrednosti, ob upoštevanju dejstva, da se bo v teh prostorih vlagatelja nahajalo večje število takih naprav, pa je Informacijski pooblaščenec zaključil, da bo vlagatelj razpolagal s premoženjem večje vrednosti, ki je tudi po naravi tako, da zahteva dodatno in strožje zavarovanje.

Kot izhaja iz odločb, s katerimi je Informacijski pooblaščenec dovolil izvajanje biometrijskih ukrepov, se bodo ti 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 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 njihovo uvedbo in odtehtajo tudi poseg v informacijsko zasebnost zaposlenih.

Informacijski pooblaščenec je zavrnil dve vlogi za izdajo dovoljenja za uvedbo biometrijskih ukrepov:

1. vlogo vlagatelja (vrtca), ki je navedel, da bi biometrijske ukrepe uvedel za namene opravljanja dejavnosti, varnosti ljudi in premoženja ter varovanja poslovnih skrivnosti in tajnih podatkov z uporabo čitalca prstnih odtisov na glavnem vhodu, ki bi ga uporabljal za odpiranje vrat in registracijo prihoda in odhoda zaposlenih. Vlagatelj po presoji Informacijskega pooblaščenca ni izkazal nujne potrebnosti uvedbe biometrijskih ukrepov za varovanje poslovne skrivnosti in tajnih podatkov, saj je kot podatke, ki jih je treba varovati z navedenimi ukrepi, zgolj na splošno opredelil svoje metode pedagogike skupnosti in različne projekte, ki naj bi predstavljali njegovo intelektualno lastnino in avtorsko delo. Informacijski pooblaščenec je v zvezi s tem pojasnil, da sprejema navedbe vlagatelja, da razpolaga z različnimi podatki, metodami in projekti, ki lahko predstavljajo njegova avtorska dela in intelektualno lastnino, ki jih mora ustrezno zavarovati, vendar je hkrati poudaril, da 80. člen ZVOP-1 kot varovane dobrine izrecno našteva tajne podatke in poslovne skrivnosti, kar pomeni, da je avtorska dela in intelektualno lastnino mogoče varovati z biometrijskimi ukrepi samo, če jih je mogoče hkrati opredeliti tudi kot tajne podatke oziroma poslovne skrivnosti po ZTP in ZGD-1. Podatki, ki jih je navedel vlagatelj, pa tem kriterijem ne ustrezajo. V zvezi z izvajanjem biometrijskih ukrepov za vstopanje v objekt vlagatelja in evidentiranje delovnega časa, ki jih je vlagatelj želel izvajati nad vsemi zaposlenimi, je Informacijski pooblaščenec ugotovil, da izvajanje teh ukrepov ni nujno potrebno za dosego navedenih namenov (opravljanje dejavnosti, varnost ljudi in premoženja), saj lahko vlagatelj povsem primerljivo stopnjo zavarovanja teh pravnih dobrin zagotovi tudi z drugimi načini vstopanja v objekt, ki ne

posegajo ali pa v dosti manjši meri posegajo v informacijsko zasebnost zaposlenih. Informacijski pooblaščenec je ob tem poudaril, da je ob ustrezni uporabi ključev in brezkontaktnih kartic s strani zaposlenih tudi s takim načinom vstopanja mogoče v veliki meri zavarovati objekt pred nepooblaščenim vstopanjem, hkrati pa je opozoril na možnost vstopanja s pomočjo gesel, ki zagotavlja praktično enako stopnjo zavarovanja vstopanja v prostore in za razliko od biometrijskih ukrepov ne posega v informacijsko zasebnost zaposlenih. Tak sistem vstopanja je mogoče zlorabiti zgolj s sodelovanjem zaposlenega, ki je pooblaščen za vstop, ob čemer pa velja poudariti, da je s sodelovanjem zaposlenih mogoče zlorabiti tudi biometrijske ukrepe, saj lahko pooblaščena oseba, potem ko s pomočjo svoje biometrijske značilnosti odpre vrata v prostor, omogoči vstop v prostor tudi eni ali več nepooblaščenim osebam. Pri presoji potrebnosti izvajanja biometrijskih ukrepov za varovanje premoženja je Informacijski pooblaščenec ugotovil, da premoženje, ki ga je želel vlagatelj varovati (didaktični pripomočki, nekaj osebnih računalnikov, fotokopirni stroj), ni take narave ali take vrednosti, da bi odtehtalo izvajanje biometrijskih ukrepov. V zvezi z zagotavljanjem varnosti otrok je Informacijski pooblaščenec poudaril, da se ta v prvi vrsti zagotavlja z ustreznim nadzorom vzgojiteljic in drugimi varnostnimi ukrepi ter da je omejitev vstopanja v objekt z biometrijskimi ukrepi zgolj eden od ukrepov za zagotavljanje varnosti otrok. Sicer pa je bilo ugotovljeno, da je vlagatelj zunanjim obiskovalcem že omejeval vstop v objekt, tako da so lahko vanj vstopali le, če jih je tja po poprejšnji identifikaciji preko domofona spustila pooblaščena oseba vlagatelja. Tudi z uvedbo biometrijskih ukrepov se način vstopanja za zunanje obiskovalce ne bi spremenil.

2. vlogo vlagatelja, ki je želel biometrijske ukrepe izvajati nad štirinajstimi zaposlenimi za namene opravljanja dejavnosti ter zagotavljanja varnosti ljudi in premoženja s čitalcem prstnih odtisov, ki bi omogočal tudi registracijo delovnega časa. Informacijski pooblaščenec je po proučitvi vlagateljevih navedb zaključil, da ni ustrezno opredelil dobrin, ki jih je želel varovati z biometrijskimi ukrepi, da ni izkazal, v čem je njihova ogroženost, da ni opredelil, na kakšen način naj bi izvajanje biometrijskih ukrepov znižalo ogroženost oziroma povečalo stopnjo varovanja takih dobrin, poleg tega pa ni izkazal, zakaj objektov svojega varovanja ne more zavarovati z drugimi ukrepi, ki bi v manjši meri posegali v informacijsko zasebnost zaposlenih.

Informacijski pooblaščenec je zavrgel ponovno zahtevo vlagatelja, ki mu je v letu 2011 že izdal zavrnilno odločbo, ker je po preučitvi vloge in izdane odločbe ugotovil, da je dejansko stanje nespremenjeno oziroma da vlagatelj ni navedel nobenega novega dejstva, ki bi lahko vplivalo na drugačno odločitev. Vlagatelj je želel biometrijske ukrepe z uporabo čitalca prstnih odtisov uvesti za dostop do posebnih blagajn, 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. Izvajanje biometrijskih ukrepov pa pooblaščenim osebam ne more preprečiti, da ne bi dostopa do blagajn omogočile drugim nepooblaščenim osebam ali da ne bi same zlorabile dostopa. Vlagatelj je želel izvajati biometrijske ukrepe tudi za registracijo delovnega časa nad vsemi zaposlenimi in študenti, ker v praksi občasno prihaja do nenatančnosti, popravljanja in ročnega spreminjanja podatkov o prihodih in odhodih ter prilagajanja urnikov s strani odgovornih oseb. 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.

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 ugotovil, da tretja država ustrezno raven varstva osebnih podatkov zagotavlja le delno, v seznamu navede 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 mora kot pristojni nadzorni organ za varstvo osebnih podatkov glede na določbe 7. točke prvega odstavka 70. člena ZVOP-1 v postopku odločanja o dovolitvi iznosa osebnih podatkov v tretjo državo preveriti, ali upravljavec osebnih podatkov (izvoznik podatkov) zagotavlja ustrezne postopke in ukrepe zavarovanja osebnih podatkov ter preveriti, ali je v določbah pogodb ali v splošnih pogojih poslovanja navedel ustrezne možnosti njihovega uresničevanja in varstva. Poleg tega mora Informacijski pooblaščenec pri odločanju o izdaji odločbe glede iznosa osebnih podatkov v tretje države opraviti tudi vsebinski preizkus o tem, ali za posredovanje oziroma za razkrivanje, širjenje in dajanje določenih osebnih podatkov na razpolago drugi pravni osebi obstaja ustrezna pravna podlaga. Slednje namreč izhaja iz dolžnosti nadzora nad zakonitostjo in poštenostjo obdelave osebnih podatkov, ki jo Informacijskemu pooblaščencu nalagata ZVOP-1 in ZInfP.

Informacijski pooblaščenec je leta 2012 prejel pet vlog za iznos osebnih podatkov v tretje države. Izdal je pet odločb, od tega tri odločbe v zadevah, ki jih je prejel v reševanje v letu 2011. Vsem vlagateljem je iznos osebnih podatkov dovolil:

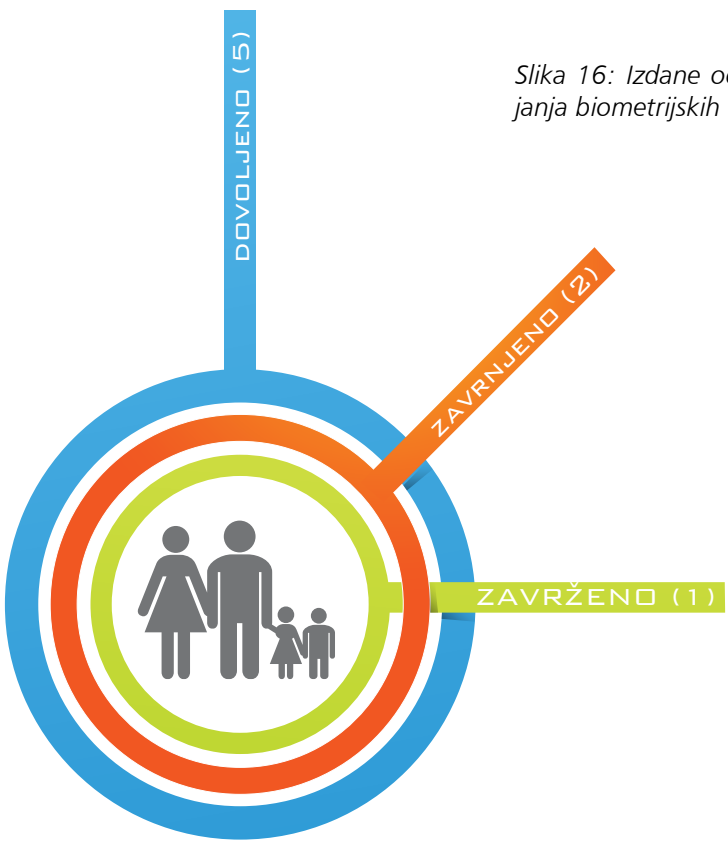
1. trgovski družbi (izvoznik podatkov) je dovolil, da po prejemu odločbe svojemu pogodbenemu obdelovalcu osebnih podatkov v Indiji (uvozniku podatkov) iznaša in posreduje osebne podatke zaposlenih in kontaktnih oseb pri dobaviteljih in strankah. Uvoznik podatkov bo za izvoznika podatkov izvajal opravila v zvezi z izvrševanjem plačil zaposlenim, kontaktiranjem zaposlenih v zvezi s stroški ter kontaktiranjem dobaviteljev in strank. Osebni podatki, ki se bodo iznašali v okviru zgoraj naštetih aktivnosti in se nanašajo na zaposlene pri izvozniku, so: ime, fotografija, telefonska številka znotraj družbe, elektronski naslov znotraj družbe, osebna telefonska številka, podatki o bančnem računu, domač naslov. Osebni podatki, ki se nanašajo na dobavitelje in stranke in bodo predmet iznosa, so: ime, podrobnosti o poslovnem kontaktu.

2. družbi, ki se ukvarja s trženjem farmacevtskih izdelkov (izvoznik podatkov), je dovolil, da po prejemu odločbe svojemu pogodbenemu obdelovalcu osebnih podatkov v Indiji (uvoznik podatkov) iznaša in posreduje osebne podatke zaposlenih pri izvozniku podatkov. Uvoznik podatkov bo za izvoznika podatkov izvajal opravila v zvezi z opravljanjem storitev informacijske tehnologije za skupino družb na podlagi oddaljenega dostopa do podatkov. Podatki, ki se bodo iznašali, zadevajo zaposlene pri izvozniku podatkov, in sicer: EMŠO, začetnice, ime, vzdevek, datum začetka zaposlitve, opis delovnega mesta, ime delovnega mesta, organizacijska dodelitev, državljanstvo, jezik komuniciranja, rojstni datum, kraj dela, naslov kraja dela, telefon kraja dela, zasebni naslov, plača, plačilna struktura, vrsta pogodbe, jubilejni datum, rezultati testa (zaposlitveni in osebnostni test, ki se nanaša zgolj na delo delavca), odsotnost z dela zaradi bolezni. Po navedbah izvoznika se bodo podatki obdelovali izključno za potrebe delovnega razmerja in za izpolnjevanje zahtev veljavne zakonodaje, npr. izplačilo plače.

3. trgovskemu in storitvenemu podjetju (izvoznik podatkov) je dovolil, da po prejemu odločbe svojemu pogodbenemu obdelovalcu osebnih podatkov v Indiji (uvoznik podatkov) iznaša in posreduje osebne podatke zaposlenih pri izvozniku podatkov, posameznikov, ki izvajajo poslovanje v lastnem imenu, in kontaktnih oseb, ki nastopajo v imenu poslovnih partnerjev. Uvoznik podatkov bo za izvoznika podatkov izvajal opravila v zvezi z opravljanjem računovodskih storitev. Osebni podatki, ki se bodo iznašali, so: osebna številka, identifikacija obdelovalca podatkov, podatki o izvedbi naročil, čas zastoja oziroma izpada v proizvodnji, ime, priimek, naslov, e-naslov, podatki o bančnem računu, dejavnosti na računu, številka kupca, številka prodajalca.

4. družbi, katere osnovna dejavnost je montaža industrijskih strojev in naprav (izvoznik podatkov) je dovolil, da po prejemu odločbe svojemu pogodbenemu obdelovalcu osebnih podatkov v Indiji (uvozniku podatkov) iznaša in posreduje osebne podatke zaposlenih in kontaktnih oseb pri dobaviteljih in strankah. Uvoznik podatkov bo za izvoznika podatkov izvajal opravila v zvezi z izvrševanjem plačil zaposlenim, kontaktiranjem zaposlenih v zvezi s stroški ter kontaktiranjem dobaviteljev in strank. Osebni podatki, ki se bodo iznašali v okviru zgoraj naštetih aktivnosti in se nanašajo na zaposlene pri izvozniku, so: ime, fotografija, telefonska številka znotraj družbe, elektronski naslov znotraj družbe, osebna telefonska številka, podatki o bančnem računu, domač naslov. Osebni podatki, ki se nanašajo na dobavitelje in stranke in so predmet iznosa, so: ime, podrobnosti o poslovnem kontaktu.

Informacijski pooblaščenec je pri presoji pravne podlage za nameravano posredovanje osebnih podatkov ugotovil, da gre v vseh štirih zgoraj navedenih primerih za posredovanje osebnih podatkov pogodbenim obdelovalcem (uvoznikom podatkov), ki bodo osebne podatke obdelovali v imenu in za račun upravljavcev osebnih podatkov (izvoznikov podatkov). Pravno podlago za posredovanje osebnih podatkov predstavlja 11. člen ZVOP-1, ki določa, da lahko upravljavec osebnih podatkov posamezna opravila v zvezi z obdelavo osebnih podatkov s pogodbo zaupa pogodbenemu obdelovalcu, ki je registriran za opravljanje takšne dejavnosti in zagotavlja ustrezne postopke in ukrepe iz 24. člena ZVOP-1. Pogodbeni obdelovalec sme

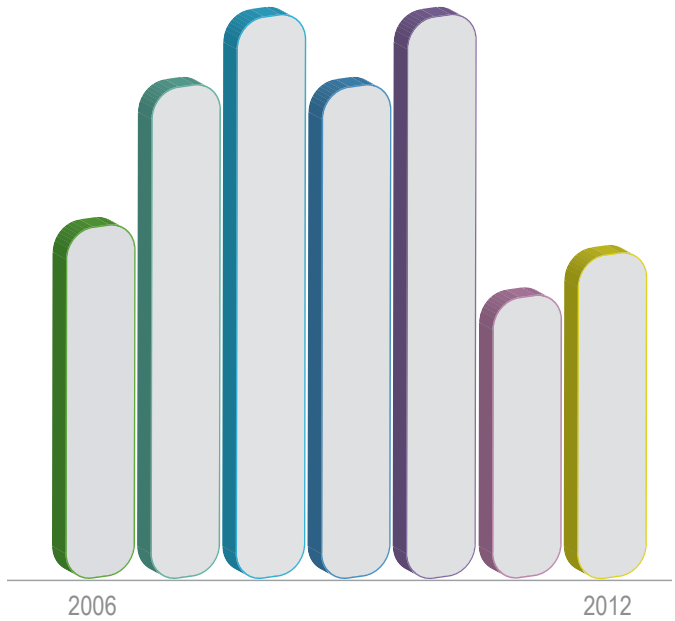


Slika 16: Izdane odločbe o dopustnosti izvajanja biometrijskih ukrepov leta 2012.

opravljati posamezna opravila v zvezi z obdelavo osebnih podatkov v okviru naročnikovih pooblastil in osebnih podatkov ne sme obdelovati za noben drug namen. Medsebojne pravice in obveznosti se uredijo s pogodbo, ki mora biti sklenjena v pisni obliki in mora vsebovati tudi dogovor o postopkih in ukrepih iz 24. člena tega zakona. Informacijski pooblaščenec je po pregledu pogodb s standardnimi pogodbenimi klavzulami, ki so jih predložili izvozniki podatkov, ugotovil, da so izvozniki in uvozniki podatkov uporabili in sprejeli model standardnih pogodbenih klavzul in oba dodatka iz Sklepa Komisije z dne 5. februarja 2010 o standardnih pogodbenih klavzulah za prenos osebnih podatkov obdelovalcem s sedežem v tretjih državah v skladu z Direktivo 95/46/ES (notificirana pod dokumentarno številko C(2010) 593 (2010/87/ES). Uporabljene standardne pogodbene klavzule zagotavljajo primerne zaščitne ukrepe glede varstva zasebnosti ter temeljnih pravic in svoboščin posameznikov in njihovega uresničevanja, kot to zahteva drugi odstavek 26. člena Direktive 95/46/ES Evropskega Parlamenta in Sveta z dne 24. oktobra 1995 o zaščiti posameznikov pri obdelavi osebnih podatkov in o prostem gibanju takih podatkov. Sprejete standardne pogodbene klavzule hkrati zadostijo tudi vsem zahtevam iz 11. člena ZVOP-1, saj štejejo kot pisna pogodba med upravljavcem osebnih podatkov in pogodbenim obdelovalcem, iz katere so razvidne medsebojne pravice in obveznosti, poleg tega pa sprejete klavzule skupaj z obema dodatkoma in prej navedeno pogodbo vsebujejo tudi dogovor o postopkih in ukrepih za zavarovanje osebnih podatkov iz 24. člena ZVOP-1.

Informacijski pooblaščenec je na predlog družbe, ki se ukvarja z grafičnimi in dokumentacijskimi storitvami (izvoznik podatkov) uvedel postopek ugotavljanja ustrezne ravni varstva osebnih podatkov v Republiki Makedoniji. Izvoznik podatkov in družba v tretji državi, ki je delno v njegovi lasti (uvoznik podatkov), sodelujeta na precej področjih, pri čemer je za opravljanje posameznih poslov nujno potreben in neizogiben tudi prenos osebnih podatkov iz ene družbe v drugo. Družbi želita v bodoče uvesti novosti in delitev dela tudi na področju tiskanja dokumentov, ki vsebujejo osebne podatke, ti pa uživajo posebno varstvo in jih je dovoljeno iznašati le v tiste tretje države, za katere je ugotovljeno, da zagotavljajo ustrezno raven varstva osebnih podatkov ali pa na podlagi posebnega dovoljenja Informacijskega pooblaščenca, ki pa bi ga bilo potrebno izdati za vsakega upravljavca osebnih podatkov posebej. Po tako utemeljenem pravnem interesu je Informacijski pooblaščenec na Ministrstvo za zunanje zadeve Republike Slovenije naslovil zahtevo, da od pristojnega organa Republike Makedonije, to je Direktorata za varstvo osebnih podatkov Republike Makedonije, pridobi dokumentacijo in informacije, ki so potrebne za odločanje o iznosu osebnih podatkov v navedeno državo. Po določbah 63. člena ZVOP-1 je iznos oziroma posredovanje osebnih podatkov v tretjo državo namreč dopustno v skladu z določbami tega zakona in pod pogojem, da državni nadzorni organ izda odločbo, da država, v katero se osebni podatki iznašajo, zagotavlja ustrezno raven varstva osebnih podatkov. Odločba ni potrebna, če je država že na seznamu tistih držav, za katere je državni nadzorni organ že ugotovil, da imajo zagotovljeno ustrezno raven varstva osebnih podatkov. Pri odločanju o ustrezni ravni varstva osebnih podatkov v tretji državi je Informacijski pooblaščenec po določbah prvega odstavka 68. člena ZVOP-1 dolžan ugotoviti vse okoliščine v zvezi z iznosom osebnih podatkov. Predvsem mora upoštevati vrsto osebnih podatkov, namen in trajanje predlagane obdelave, pravno ureditev v državi izvora in v državi prejemnici, vključno z ureditvijo varstva osebnih podatkov tujih državljanov, ter ukrepe zavarovanja osebnih podatkov, ki se v njih uporabljajo. Po določbah 67. člena ZVOP-1 je Informacijski pooblaščenec pri odločanju o ustrezni ravni varstva osebnih podatkov v tretji državi vezan na odločitve pristojnega organa Evropske unije. Informacijski pooblaščenec je ugotovil, da Republike Makedonije ni na seznamu iz 66. člena ZVOP-1, niti ni na seznamu držav, za katere je ustrezno raven varstva osebnih podatkov ugotavljala Komisija Evropskih Skupnosti. Zaradi tega je uvedel postopek ugotavljanja ustrezne ravni varstva osebnih podatkov v Republiki Makedoniji. Po proučitvi prejete dokumentacije je zaključil, da pravna ureditev v Republiki Makedoniji zajema vsa načela, ki so nujna za zagotovitev ustrezne ravni varstva osebnih podatkov v tej državi, ter da se sprejeti Zakon o varstvu osebnih podatkov v Republiki Makedoniji tudi dejansko izvaja in preko projektov tesnega medinstitucionalnega sodelovanja z nadzornimi organi iz držav članic Evropske unije še krepi pristojnosti Direktorata za varstvo osebnih podatkov. Zato je Informacijski pooblaščenec odločil, da se za namene 63. člena ZVOP-1 šteje, da Republika Makedonija v celoti zagotavlja ustrezno raven varstva osebnih podatkov.

Slika 17: Število vlog za izdajo odločbe glede iznosa osebnih podatkov med letoma 2006 in 2012.



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 (pozitivne odločbe) Informacijskega pooblaščenca ni dovoljeno. Ta povezavo dovoli na podlagi pisne vloge upravljavca osebnih podatkov, če ugotovi, da zagotavlja ustrezno zavarovanje osebnih podatkov. Postopki in ukrepi za zavarovanje morajo biti ustrezni glede na tveganje, ki ga predstavljata obdelava in narava osebnih podatkov, ki se obdelujejo. 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. V okviru povezave zbirk osebnih podatkov se lahko posredujejo oziroma obdelujejo le tiste vrste osebnih podatkov, ki jih določa veljavna zakonodaja.

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

Informacijski pooblaščenec je leta 2012 prejel devet vlog za pridobitev dovoljenja za povezovanje zbirk osebnih podatkov. Izdal je 12 odločb (od tega sedem za vloge, prejete leta 2011), s katerimi je vlagateljem dovolil povezovanje z drugo ali drugimi zbirkami osebnih podatkov. Poleg teh je izdal delno zavrnilno odločbo, s katero je na podlagi sodbe Upravnega sodišča popravil odločbo iz leta 2011. Eno vlogo je s sklepom zavrgel, ker je o isti upravni zadevi že pravnomočno odločil. Dva upravljavca (ena vloga iz leta 2011 in ena iz 2012) sta svoji vlogi umaknila, Informacijski pooblaščenec pa je oba postopka ustavil, ker njuno nadaljevanje ni bilo v javnem interesu.

Informacijski pooblaščenec je dovolil povezovanje naslednjih zbirk osebnih podatkov:

1. Zavodu za zdravstveno zavarovanje Slovenije in Ministrstvu za izobraževanje znanost, kulturo in šport je dovolil vzpostavitev neposredne računalniške povezave med Evidenco o zavarovanih osebah obveznega zdravstvenega zavarovanja in Evidenčnim in analitskim in-

formacijskim sistemom visokega šolstva v Republiki Sloveniji (eVŠ). Povezava med zbirkama se lahko izvede na način, da se kot povezovalni znak uporabi enotna matična številka občana (EMŠO).

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

- zbirko osebnih podatkov eVŠ - Evidenčni in analitski informacijski sistem visokega šolstva v Republiki Sloveniji, katere upravljavec je Ministrstvo za visoko šolstvo, znanost in tehnologijo;
- zbirko osebnih podatkov Centralna evidenca udeležencev vzgoje in izobraževanja, katere upravljavec je Ministrstvo za šolstvo in šport.

Povezava med zbirkami se lahko izvede z uporabo EMŠO ali davčne številke.

3. Ministrstvu za finance, Carinski upravi Republike Slovenije, je dovolil, da Evidenco o davčni izvršbi poveže z Davčnim registrom, katerega upravljavec je Ministrstvo za finance, Davčna uprava Republike Slovenije. Kot povezovalni znak se uporabi davčna številka.

4. Ministrstvu za visoko šolstvo, znanost in tehnologijo je dovolil, da eVŠ - Evidenčni in analitski informacijski sistem visokega šolstva v Republiki Sloveniji poveže s Centralnim registrom prebivalstva, katerega upravljavec je Ministrstvo za notranje zadeve. Kot povezovalni znak se uporabi EMŠO.

5. Ministrstvu za izobraževanje, znanost, kulturo in šport je dovolil, da Evidenco študentov in diplomantov ter Evidenco izvajalcev visokošolske dejavnosti, ki ju vodi v okviru zbirke eVŠ - Evidenčni in analitski informacijski sistem visokega šolstva v Republiki Sloveniji, poveže z zbirkami osebnih podatkov, ki jih kot upravljavci osebnih podatkov vodijo akreditirani visokošolski zavodi v Republiki Sloveniji, in sicer z njihovimi:

- evidencami z osebnimi podatki študentov in vpisanih na študijske programe za izpopolnjevanje ter
- evidencami z osebnimi podatki izvajalcev visokošolske dejavnosti.

Povezava med zbirkami osebnih podatkov se lahko izvede z uporabo EMŠO.

6. Državnemu pravobranilstvu Republike Slovenije je dovolil, da Zbirko vpisnikov za evidentiranje zadev, ki jih obravnava Državno pravobranilstvo, in sicer

- P vpisnik za pravdne zadeve,
- PP vpisnik za predhodne postopke po 214. členu ZP-1,
- PK vpisnik za predhodne postopke po 539. členu Zakona o kazenskem postopku[34],
- PRR vpisnik po Zakonu o pravici do sojenja brez nepotrebnega odlašanja[35],
- I vpisnik za izvršilne zadeve,
- St. vpisnik za prijave v stečajne postopke, likvidacijske postopke in postopke prisilne poravnave ter
- E vpisnik za zadeve, ki se obravnavajo pred mednarodnimi sodišči

poveže s Centralnim registrom prebivalstva, katerega upravljavec je Ministrstvo za notranje zadeve. Kot povezovalni znak se uporabi EMŠO.

7. Vrhovnemu sodišče Republike Slovenije je dovolil, da Informacijski sistem za vodenje kazenskih postopkov poveže s Centralnim registrom prebivalstva, katerega upravljavec je Ministrstvo za notranje zadeve. Kot povezovalni znak se uporabi EMŠO.

8. Državnemu tožilstvu Republike Slovenije je dovolil, da Zbirko vpisnikov državnega tožilstva, in sicer:

- Kt vpisnik – kazenski postopki zoper znane polnoletne in pravne osebe,
- Ktm vpisnik – kazenski postopki zoper mladoletnike,
- Ktpp vpisnik – obvestila in usmerjanje v predkazenskem postopku ter pritožbe zoper delo policije in

[34] Uradni list RS, št. 32/2012 - uradno prečiščeno besedilo 8, s spremembami.
[35] Uradni list RS, št. 67/2012 - uradno prečiščeno besedilo 2.

- KpPo vpisnik – policijsko preiskovanje na Posebnem oddelku

poveže s Centralnim registrom prebivalstva, katerega upravljavec je Ministrstvo za notranje zadeve. Povezava med zbirkami se lahko izvede na način, da se kot povezovalni znak uporabi EMŠO.

9. Ministrstvu za delo, družino in socialne zadeve in Vrhovnemu sodišču Republike Slovenije je dovolil povezavo med Centralno zbirko podatkov o pravicah iz javnih sredstev in Informatizirano glavno knjigo zemljiške knjige. Povezava med zbirkama se lahko izvede na način, da vlagatelj poizvedbe v Informatizirani glavni knjigi zemljiške knjige opravlja po ID znaku nepremičnine.

10. Zavodu za zdravstveno zavarovanje Slovenije (ZZZS) in Agenciji Republike Slovenije za javnopravne evidence in storitve (AJPES), je dovolil vzpostavitev neposredne računalniške povezave med Evidenco o zavarovanih osebah obveznega zdravstvenega zavarovanja (Evidenca OZZ) in Poslovnim registrom Slovenije (PRS). Povezava med zbirkama se lahko izvede na način, da se ZZZS omogoči, da iz PRS pridobi EMŠO, če teh ni, pa davčne številke ustanoviteljev posameznega poslovnega subjekta ter tako pridobljene osebne podatke vključi v Evidenco OZZ, pri čemer pa mora biti povezava zbirk osebnih podatkov izvedena na način, ki ZZZS onemogoča iz PRS pridobiti podatke o tem, v katerih poslovnih subjektih se določen posameznik pojavlja kot ustanovitelj poslovnega subjekta.

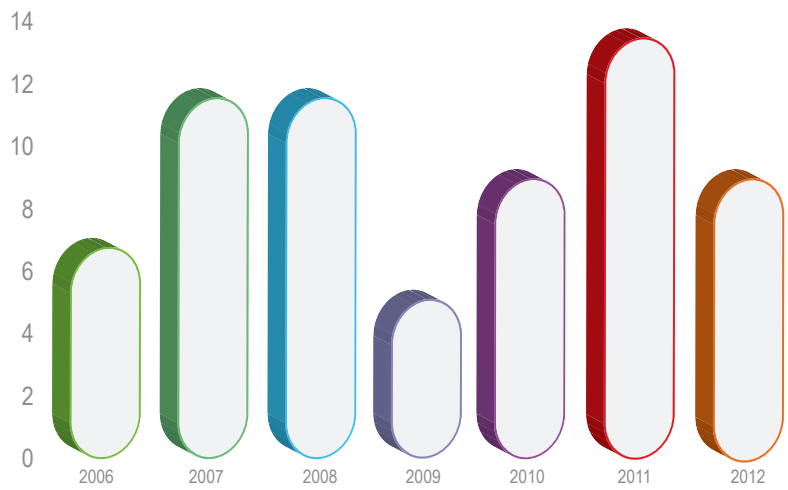
11. Zavodu za zdravstveno zavarovanje Slovenije in Ministrstvu za izobraževanje znanost, kulturo in šport je dovolil vzpostavitev neposredne računalniške povezave med Evidenco o zavarovanih osebah obveznega zdravstvenega zavarovanja in Centralno evidenco udeležencev vzgoje in izobraževanja. Kot povezovalni znak se uporabi EMŠO.

12. Splošni bolnišnici Jesenice in Ministrstvu za notranje zadeve je dovolil, da v okviru aplikacije e-Rojstva povežeta naslednje zbirke osebnih podatkov:

- Osnovno medicinsko dokumentacijo,
- Centralni register prebivalstva ter
- Matični register.

Povezava med zbirkami se lahko izvede z uporabo EMŠO.

Slika 18: Število vlog za izdajo odločbe glede povezljivosti zbirk osebnih podatkov med letoma 2006 in 2012.



Informacijski pooblaščenec je zavrnil zahtevek Ministrstva za delo, družino in socialne zadeve (MDDSZ) z dne 31. 1. 2011 za izdajo odločbe oziroma dovoljenja za povezavo zbirk osebnih podatkov v delu, ki se nanaša na povezavo Centralne zbirke podatkov o pravicah iz javnih sredstev z Informatizirano glavno knjigo zemljiške knjige, katere upravljavec je Vrhovno sodišče Republike Slovenije. MDDSZ je Informacijskega pooblaščenca zaprosil, da

mu za namene izvajanja Zakona o uveljavljanju pravic iz javnih sredstev[36] izda odločbo oziroma dovoli, da Centralno zbirko podatkov o pravicah iz javnih sredstev poveže z več drugimi zbirkami različnih upravljavcev, med drugim tudi z Zemljiško knjigo. Informacijski pooblaščenec je v upravnem postopku z odločbo št. 0602-2/2011/38 z dne 1. 9. 2011 dovolil povezovanje zbirk. Vrhovno sodišče Republike Slovenije je zoper omenjeno odločbo preko Državnega pravobranilstva Republike Slovenije vložilo tožbo. Upravno sodišče je v sodbi opr. št. I U 1715/2011-9 z dne 18. 4. 2012 tožbi ugodilo, točko I/14 izpodbijane odločbe odpravilo in zadevo v tem delu vrnilo Informacijskemu pooblaščencu v ponovni postopek, v katerem je moral upoštevati stališča sodišča glede uporabe materialnega prava. Če bi MDDSZ povezalo centralno zbirko podatkov z zbirko podatkov o lastništvu nepremičnin posamezne osebe, bi pristojne osebe lahko zaradi te povezave prišle do podatkov o lastništvu nepremičnine posamezne osebe, kar pa je v nasprotju z 199. členom Zakona o zemljiški knjigi [37]. Po določbi tega člena ima državni organ pravico do vpogleda in izpisa podatkov o tem, ali je določena oseba lastnik oziroma imetnik drugih pravic na katerikoli nepremičnini, če to potrebuje zaradi postopka, ki ga vodi, le na način, da o dostopu odloči zemljiškoknjižni sodnik na podlagi obrazložene pisne zahteve, kateri so priložene listine in drugi dokazi o obstoju okoliščin, zaradi katerih je dostop do podatkov dopusten. Po določbi 51. člena ZUPJS pa bi zaradi povezave centralne zbirke podatkov s podatki o lastništvu nepremičnin posamezne osebe MDDSZ lahko prišel do takih podatkov brez odločitve zemljiškoknjižnega sodnika. Kot je ugotovilo sodišče, sta si določbi 199. člena ZZK-1 in 51. člena ZUPJS v nasprotju, zato je presojalo, kateremu zakonu dati prednost. ZUPJS je bil sprejet kasneje kot ZZK-1, vendar pa se sodišče ne strinja, da je ZUPJS lex specialis glede na ZZK-1. ZUPJS ureja pravico MDDSZ do pridobivanja osebnih podatkov le na splošno, povezovanje se nanaša na veliko število zbirk podatkov, ki jih je mogoče povezovati in s tem pridobiti dostop do osebnih podatkov, medtem ko je ZZK-1 področni zakon, ki se nanaša le na vprašanje zemljiške knjige in pri tem samostojno ureja, na kakšen način je možno dostopati do posameznih podatkov v zemljiški knjigi. Zato je sodišče zaključilo, da je ZZK-1 specialnejši predpis. Poleg tega četrti odstavek 51. člena ZUPJS MDDSZ daje zgolj možnost povezave, ne navaja pa, da se zbirke morajo povezati. Ker v konkretnem primeru obstaja zadržek pri povezovanju zbirk osebnih podatkov - 199. člen ZZK-1, je Informacijski pooblaščenec v ponovnem postopku odločil, da za povezavo Centralne zbirke podatkov o pravicah iz javnih sredstev z Informatizirano glavno knjigo zemljiške knjige ni ustrezne zakonske podlage.

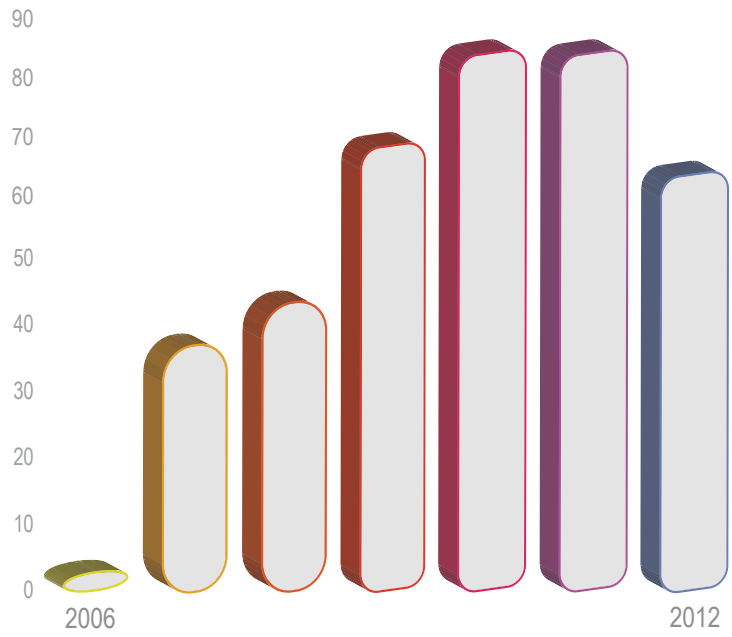
3.7. Seznanitev z lastnimi osebnimi podatki

V skladu s tretjim odstavkom 38. člena Ustave je posamezniku zagotovljena pravica do seznanitve z zbranimi osebnimi podatki, ki se nanašajo nanj. Navedena pravica posameznika do seznanitve z lastnimi osebnimi podatki je konkretizirana v 30. in 31. členu ZVOP-1. 30. člen določa vsebino pravice, 31. člen pa postopek seznanitve.

Informacijski pooblaščenec je leta 2012 vodil 63 pritožbenih postopkov v zvezi s pravico do seznanitve z lastnimi osebnimi podatki. Število pritožb se je v primerjavi s preteklimi leti nekoliko zmanjšalo (leta 2011 in 2010 jih je bilo 85). V okviru navedenih pritožbenih postopkov je Informacijski pooblaščenec reševal tudi pritožbe, ko posamezniki niso pridobili zdravstvene dokumentacije po ZPacP. Te so bile leta 2010 štiri, leta 2011 jih je bilo 18, leta 2012 pa deset.
Informacijski pooblaščenec opaža, da je v primerjavi z letom 2011 delež molkov upravljavcev osebnih podatkov, ko upravljavci na zahtevo posameznika v zvezi s seznanitvijo z lastnimi osebnimi podatki sploh niso odgovorili, ostal na isti ravni (52 %). Posameznik lahko v primeru molka upravljavca, pa tudi v primeru zavrnitve seznanitve vloži pritožbo Informacijskemu pooblaščencu.

[36] Uradni list RS, št. 62/2010, s spremembami; v nadaljevanju ZUPJS.
[37] Uradni list RS, št. 58/2003, s spremembami; v nadaljevanju ZZK-1.

Slika 19: Število pritožb v zvezi s pravico do seznanitve z lastnimi osebnimi podatki med letoma 2006 in 2012.

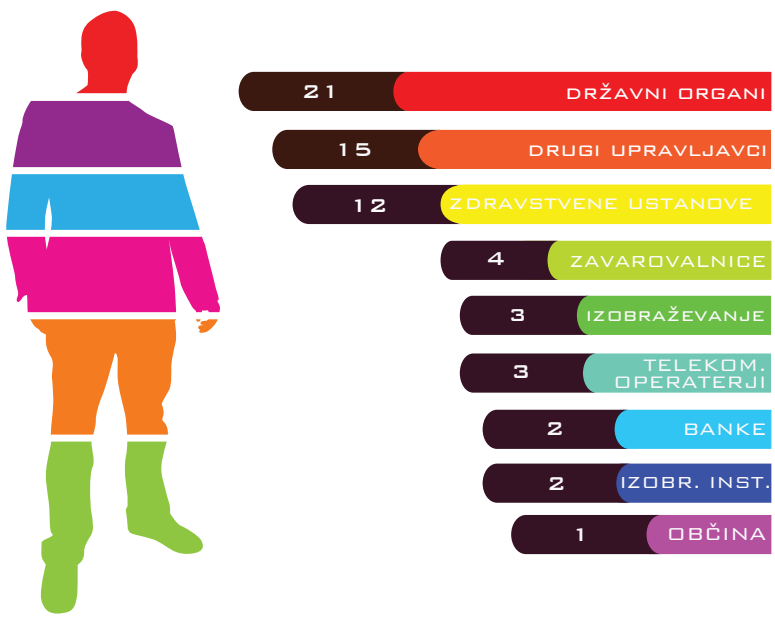


Vložene pritožbe zaradi zavrnitve seznanitve z lastnimi osebnimi podatki ali molka upravljavcev so zadevale naslednje skupine upravljavcev osebnih podatkov:

- ministrstva in organi v njihovi sestavi - 21,
- zdravstvene ustanove - 12,
- zavarovalnice - 4,
- izobraževalne institucije - 3,
- telekomunikacijski operaterji - 3,
- banke - 2,
- sodišča - 2,
- občina - 1,
- drugi upravljavci, npr. društva, javna komunalna podjetja - 15.

V 11 izmed zgoraj navedenih primerov 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 skupine upravljavcev osebnih podatkov leta 2012.



Informacijski pooblaščenec je po prejemu pritožbe upravljavca osebnih podatkov vedno najprej pozval, da pojasni, zakaj posamezniku ni odgovoril ali zakaj mu ni omogočil seznanitve z osebnimi podatki. V 19 primerih so upravljavci posameznikom omogočili vpogled v zahtevane podatke ali pa so jim posredovali odgovor in zahtevane dokumente takoj po pozivu Informacijskega pooblaščenca, v enem primeru pa je upravljavec osebnih podatkov zahtevi posameznika ugodil delno. Razlog za molk upravljavcev osebnih podatkov je bil v večini primerov nepoznavanje pravice do seznanitve z lastnimi osebnimi podatki in njihovih dolžnosti v zvezi z njenim izvrševanjem. Če upravljavci osebnih podatkov posameznikom niso omogočili seznanitve, je Informacijski pooblaščenec o pravici posameznika odločil z odločbo. Tako je izdal 14 odločb, s katerimi je upravljavcem naložil, da morajo posameznikom omogočiti seznanitev z njihovimi osebnimi podatki (od tega je bilo osem odločb izdanih v pritožbenih postopkih, začetih pred letom 2012). V treh odločbah zahtevam posameznikov ni ugodil v celoti, ampak delno. Zaradi potrebe po popolni ugotovitvi dejanskega stanja (ogled razpoložljivega dokumentarnega gradiva) je Informacijski pooblaščenec v prostorih upravljavcev osebnih podatkov opravil šest ogledov, na katere so bili vabljeni tudi prosilci oziroma posamezniki, ki so vložili pritožbe. Informacijski pooblaščenec je z odločbo zavrnil 16 pritožb posameznikov (od tega pet vlog, prejetih leta 2011), eno pritožbo pa je s sklepom zavrgel. Pritožbe je zavrnil, če vsebinsko niso predstavljale pritožbe zaradi zavrnitve seznanitve z lastnimi osebnimi podatki ali niso bile utemeljene, zavrgel pa, ker je bila vloga preuranjena. Informacijski pooblaščenec je trem posameznikom svetoval, kako naj postopajo, dva posameznika sta svoji pritožbi umaknila. Informacijski pooblaščenec je 13 pritožb odstopil v reševanje pristojnim organom.

V enem postopku je Informacijski pooblaščenec reševal pritožbo zaradi nepravilnega zaračunavanja stroškov, ki so nastali kot posledica seznanitve z lastno zdravstveno dokumentacijo. V postopku je bilo ugotovljeno, da interni akt upravljavca ni bil usklajen s Pravilnikom o zaračunavanju stroškov pri izvrševanju pravice posameznika do seznanitve z lastnimi osebnimi podatki[38]. Upravljavec je posamezniku vrnil previsoko zaračunani znesek, saj so bile cene kopij bistveno višje od tistih, ki jih določa navedeni pravilnik in jih morajo upravljavci osebnih podatkov upoštevati.

V letu 2012 so bile zoper odločitve Informacijskega pooblaščenca vložene tri tožbe na Upravno sodišče Republike Slovenije. Dve tožbi sta vložila upravljavca osebnih podatkov, en upravni spor pa je sprožil prosilec zaradi sklepa o zavrženju pritožbe. V letu 2012 je Upravno sodišče odločilo v treh upravnih sporih, od tega sta bila dva sprožena v letu 2011. Sodišče je vse tri tožbe kot neutemeljene zavrnilo.

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[39], če se pojavi vprašanje ustavnosti ali zakonitosti v zvezi s postopkom, ki ga vodi. Pri vlaganju zahtev po presoji ustavnosti je torej omejen, saj ne gre za splošno pooblastilo za vlaganje zahtev na Ustavno sodišče, ampak se mora zahteva nanašati na konkreten postopek.

Leta 2012 je Informacijski pooblaščenec vložil dve zahtevi za oceno ustavnosti.

[38] Uradni list RS, št. 85/2007 in 5/2012.
[39] Uradni list RS, št. 64/2007 – uradno prečiščeno besedilo 1, s spremembami.

3.8.1. Zahteva za presojo ustavnosti 29. člena Zakona o preprečevanju omejevanja konkurence[40]

Izpodbijana določba ZPOmK-1 daje Uradu Republike Slovenije za varstvo konkurence (UVK) med drugim pooblastila za pregled poslovnih knjig, pogodb, listin, poslovne korespondence, poslovnih evidenc in drugih podatkov, ki so v zvezi s poslovanjem podjetja, ne glede na nosilec, na katerem so zapisani ali shranjeni, in za odvzem ali pridobitev kopij ali izvlečkov iz poslovnih knjig in druge dokumentacije v kakršni koli obliki z uporabo fotokopirnih sredstev ter računalniške opreme podjetja ali agencije. Izrecno določa še, da mora podjetje pooblaščenim osebam omogočiti dostop do prostorov ter do poslovnih knjig in druge dokumentacije ter da lahko pooblaščene osebe opravljajo preiskavo tudi proti njegovi volji.

Informacijski pooblaščenec je v inšpekcijskem postopku ugotovil, da UVK zakonska pooblastila iz 29. člena ZPOmK-1 v praksi izvaja tako, da od delavcev pridobi gesla za dostop do predala elektronske pošte. Po predalu elektronske pošte potem išče s pomočjo ključnih besed in odpira elektronska sporočila, za katera oceni, da bi bila lahko povezana s prepovedanim omejevanjem konkurence. Sporočila prebere, določena pa kot dokazilo natisne in odvzame. Posredovanja gesla za dostop do predala elektronske pošte med izvajanjem nadzora po mnenju Informacijskega pooblaščenca ni mogoče šteti za prostovoljnega v smislu svobodne volje delavca. V situaciji, ko UVK vodi preiskavo zoper delavčevega delodajalca, je delavec namreč kar v dvakrat podrejenem položaju - v odnosu do delodajalca in do preiskovalca. Če delavec gesla ne bi posredoval, bi lahko šlo za oviranje postopka preiskave, pri čemer bi potencialno škodo utrpel delodajalec, odgovornost zanjo pa bi pripisal delavcu in nanjo navezal za delavca neprijetne ukrepe. Informacijski pooblaščenec je poudaril, da UVK na podlagi izpodbijanih zakonskih določb nasproti zavezancem in njihovim delavcem nastopa z močjo oblastne avtoritete in v tem svojstvu ravna na način, ki se kaže kot nezdružljiv z eno temeljnih ustavnih vrednot – komunikacijsko zasebnostjo.

Uporaba informacijsko-komunikacijske tehnologije je dandanes pravilo, tako v poslovnem kot zasebnem življenju. Kako (predvsem zasebnopravni) poslovni subjekti ravnajo s poslovno korespondenco, je predmet ureditve v njihovih internih pravilih. Ravnanje posameznika z zasebno komunikacijo je seveda prepuščeno njegovi lastni presoji. Posledično tako poslovna kot zasebna komunikacija, ki se odvija po elektronski poti, ostaja v elektronskih poštnih predalih posameznih delavcev. Elektronski predali se praviloma glasijo na ime delavca in so sestavljeni iz njegovega osebnega imena in kratice firme delodajalca. Na takšen način sestavljen naslov elektronske pošte ustreza definiciji osebnega podatka. Z izmenjavo elektronskih sporočil v elektronskem poštnem predalu nastaja zbirka osebnih podatkov (t.i. inbox/outbox), sestavljena iz elektronskih naslovov, ki ustrezajo definiciji osebnega podatka, kratkega opisa zadeve, označbe ali gre za prejeto ali poslano sporočilo, časom prejema/pošiljanja in velikostjo sporočila. Navedeni podatki so po razlogovanju iz razsodbe Up-106/05 neločljivo povezani s komunikacijo in uživajo enak nivo varstva kot komunikacija sama. Zbirka osebnih podatkov v elektronskem poštnem predalu zaradi vezi s komunikacijo ni varovana zgolj po 38. členu[41] Ustave, določbah ZVOP-1 in področnih zakonov, ampak je skupaj z vsebino komunikacije varovana tudi po 37. členu[42] Ustave. Informacijski pooblaščenec je poudaril, da pravnega temelja za obdelavo (pridobitev, uporabo…) teh osebnih podatkov ne more dati zgolj zakonska določba, ki jo Ustava zahteva v 38. členu, temveč je poseg dopusten le, če je po zakonu odrejen z odločbo sodišča in namenjen uvedbi ali poteku kazenskega postopka ali varnosti države.

Informacijski pooblaščenec je Ustavnemu sodišču predlagal, da določbo 29. člena ZPOmK-1 spozna za neskladno s 37. členom Ustave (varstvo tajnosti pisem in drugih občil).

---

40 Uradni list RS, št. 36/2008, 40/2009, 26/2011 in 87/2011; v nadaljevanju ZPOmK-1.

41 Drugi odstavek 38. člena Ustave določa, da zbiranje, obdelovanje, namen uporabe, nadzor in varstvo tajnosti osebnih podatkov določa zakon.

42 37. člen Ustave določa: Zagotovljena je tajnost pisem in drugih občil. Samo zakon lahko predpiše, da se na podlagi odločbe sodišča za določen čas ne upošteva tajnost pisem in drugih občil in nedotakljivost človekove zasebnosti, če je to nujno za uvedbo ali potek kazenskega postopka ali za varnost države.

Gre za vprašanje dopustnosti ravnanja nadzornih organov, ki svoje pristojnosti izvršujejo v okviru upravnih – inšpekcijskih in/ali prekrškovnih postopkov, da na podlagi zakonske določbe, vendar brez odredbe sodišča in izven namenov, ki jih določa Ustava, posežejo v (elektronsko) komunikacijo. Dilema o tem, ali lahko področni zakon (v konkretnem primeru ZPOmK-1) dopusti poseg v komunikacijsko zasebnost (npr. pregled elektronske pošte, SMS ali MMS sporočil, poslušanje posnetkov telefonskih pogovorov) brez odredbe sodišča in ne le za namene kazenskega postopka ali zaradi varnosti države, je glede na uporabo modernih tehnologij v vsakodnevni zasebni in poslovni praksi aktualna pri delu vseh nadzornih organov. Informacijski pooblaščenec meni, da stroga določba 37. člena Ustave upravnim organom ne daje temelja za poseg v komunikacijsko zasebnost, saj se mora cilj učinkovitega izvajanja zakonskih pristojnosti upravnih organov umakniti pred pravicami, ki jih posameznikom daje Ustava. Ni zanemarljivo tudi dejstvo, da izpodbijana določba ZPOmK-1 kaže (le) na voljo zakonodajalca, da v škodo komunikacijske zasebnosti regulira razmere na trgu, pri čemer prezre druge temeljne človekove pravice in svoboščine. Ustavno sodišče se še nikoli ni opredelilo glede pooblastil nadzornih – upravnih organov. Informacijski pooblaščenec je prepričan, da gre za pomembno pravno vprašanje, ki ga brez intervencije Ustavnega sodišča ni mogoče rešiti, zato mu je predlagal, da zadevo obravnava absolutno prednostno. Ustavno sodišče do izdaje letnega poročila odločitve še ni sprejelo.

3.8.2. Zahteva za presojo ustavnosti 45. člena Odloka o cestnoprometni ureditvi Mestne občine Ljubljana[43]

45. člen Odloka določa: Zaradi spremljanja prometnih razmer, nadzora nad spoštovanjem prometnih predpisov, izboljšanja pretočnosti prometa in prometne varnosti so javne ceste in druge javne površine na območju MOL lahko opremljene z video nadzornim sistemom. Z video nadzornim sistemom zbrani podatki so last MOL. Z njimi se razpolaga skladno z določili zakona, ki ureja varstvo osebnih podatkov.

Informacijski pooblaščenec je v zahtevi za presojo ustavnosti navedel, da izpodbijana določba 45. člena Odloka ni v skladu z 38. členom (varstvo osebnih podatkov), 140. členom (delovno področje samoupravnih lokalnih skupnosti) in 15. členom (uresničevanje in omejevanje pravic) Ustave.

Zakon o lokalni samoupravi[44] v 13. alineji drugega odstavka 21. člena določa, da občina za zadovoljevanje potreb svojih prebivalcev gradi, vzdržuje in ureja lokalne javne ceste, javne poti, rekreacijske in druge javne površine, v skladu z zakonom ureja promet v občini ter opravlja naloge občinskega redarstva. Dopustna ravnanja ne vključujejo izvajanja videonadzora. Ta je vsebinsko urejen v 2. poglavju VI. dela ZVOP-1, v členih 74 do 77. Informacijski pooblaščenec je zato poudaril, da je po ZVOP-1 za namene, ki jih taksativno določajo prej navedeni členi, dopusten videonadzor le nad dostopom v uradne službene oziroma poslovne prostore (75. člen), dostopom do vhodov in izhodov večstanovanjskih stavb ter njihovimi skupnimi prostori (76. člen) ter nad delovnimi prostori (77. člen). Osnovno načelo obdelave osebnih podatkov določa, da je zaradi varstva človekove pravice dopustno le tisto, kar je izrecno dovoljeno z zakonom, vse ostale oblike obdelave osebnih podatkov pa so prepovedane. ZVOP-1 ne ureja videonadzora nad javnimi površinami (cestami, križišči, trgi, parki ipd.), kar po prepričanju Informacijskega pooblaščenca pomeni, da ta oblika videonadzora ni dopustna, njeno uvajanje z odlokom lokalne skupnosti pa je v nasprotju z 38. členom Ustave. Določba Odloka namreč ni in ne more biti enakovredna v zakonodajnem postopku sprejeti normi.

Informacijski pooblaščenec je v zahtevi poudaril, da urejanje obdelave osebnih podatkov (izvajanje videonadzora je eden izmed načinov obdelave osebnih podatkov) ne sodi med t.i. izvirne naloge lokalne skupnosti, ki jih te lahko urejajo samostojno. To pomeni, da občina ne sme vzpostavljati zbirk osebnih podatkov brez temelja v zakonu oziroma ne da bi bila

[43] Uradni list RS, št. 122/2007, 101/2009, 31/2010, 76/2010, 48/2011 in 57/2011, v nadaljevanju Odlok.
[44] Uradni list RS, št. 94/2007, uradno prečiščeno besedilo 2, s spremembami; v nadaljevanju ZLS.

zbirka osebnih podatkov posledica odločanja lokalne skupnosti o posameznikovi pravici ali obveznosti. Občina lahko izvaja le tiste oblastne naloge, ki jih nanjo prenese država, v preostalem gre za izvajanje servisa za občane – za zadovoljevanje njihovih potreb. Te potrebe se nanašajo zlasti na urejanje rabe občinskega prostora, zagotavljanje gospodarskih javnih služb, gradnjo in vzdrževanje lokalne infrastrukture, zagotavljanje zdravstvene oskrbe na primarni ravni, varstva in osnovnega šolanja otrok, osnovno socialno pomoč, zagotavljanje neprofitnih stanovanj, pa tudi urejanje lokalnega prometa in drugih področij življenja, kadar gre za zadeve lokalnega pomena. Videonadzor javnih površin po svoji naravi ni »lokalna zadeva« in ne zadeva le prebivalcev občine, ampak že v izhodišču cilja na vse. Vzpostavljanje zbirk posnetkov videonadzornih sistemov nad javnimi površinami, iz katerih bo razvidno gibanje vsakega posameznika, prinaša s seboj veliko skušnjav, s tem pa veliko odgovornost. Vprašanje je, kako lahko občine zagotovijo primerno varstvo in zavarovanje osebnih podatkov v zbirkah posnetkov, še posebej v primerih, ko se zdi, da glede na število zaposlenih niso kos niti osnovnim nalogam občine. Občine so namreč različnih velikosti, temu primerno imajo številčno in po strokovni zasedbi različno občinsko upravo. Informacijski pooblaščenec tudi meni, da to ni v korist lokalnega prebivalstva. Stalen videonadzor javnih površin prinaša družbo popolnega nadzora, v kateri so trditve o morebitni lažji izsleditvi posameznika, ki je poškodoval betonsko korito za rože, potopni stebriček, smetnjak ipd. za namen izterjave škode, le slepilo. Verjetnost, da bo pristojni občinski delavec lahko na podlagi posnetka prepoznal tistega, ki je npr. vrgel kamen v svetilko javne razsvetljave ali polomil gugalnico na otroškem igrišču, je namreč zelo majhna, v večjih občinah pa neznatna. Tako je očitno, da iz videonadzora nad javnimi površinami ne more iziti nobena korist za lokalno prebivalstvo, pač pa gre za nadzor lokalne oblasti nad vsemi na javnih površinah v občini. Takšno ravnanje pa ni več odraz nudenja servisa za občane, ampak izraz oblastne moči, ki si jemlje pravico videti in nadzirati vse.

Po mnenju Informacijskega pooblaščenca poseg v zasebnost in pravico do varstva osebnih podatkov z videonadzorom po izpodbijani določbi ni sorazmeren z zasledovanim ciljem (spremljanja prometnih razmer, nadzor nad spoštovanjem prometnih predpisov, izboljšanje pretočnosti prometa in prometne varnosti). Očitno je, da MOL s posegom v navedeno pravico ne varuje nobene druge človekove pravice, ki jo zagotavlja Ustava. Izpodbijana določba po prepričanju Informacijskega pooblaščenca tudi bistveno presega pooblastila, ki jih občinskemu redarstvu daje Zakon o pravilih cestnega prometa[45], in uvaja splošen nadzor nad gibanjem na javnih površinah torej nad vsemi, ki so na pločniku, cesti, v parku, na trgu, ne glede na dejstvo, da ničesar ne kršijo. Dopuščanje videonadzora na katerihkoli javnih površinah bi bistveno preseglo namen varnosti v cestnem prometu, ki jo je mogoče zagotavljati na drugačne, za posameznike (še posebej tiste, ki ničesar ne kršijo) manj invazivne načine. Ob tem Informacijski pooblaščenec poudarja še, da občinsko redarstvo, tako kot ostali represivni organi, ne sme omejevati posameznikovih pravic, dokler ne obstaja določena stopnja verjetnosti, da je posameznik prekršil zakonsko zapoved. Tudi takrat pa lahko ravna le v skladu s pooblastili, ki mu jih je podelil zakonodajalec.

Informacijski pooblaščenec je v predmetni zahtevi za presojo ustavnosti kot ključno izpostavil vprašanje, ali obdelavo osebnih podatkov posameznikov lahko prepoznamo kot izvirno nalogo lokalne skupnosti, torej kot nalogo oziroma pristojnost, o kateri lahko lokalna skupnost odloča povsem samostojno, z odloki določa nove zbirke osebnih podatkov, njihovo vsebino ipd. Od odgovora na to vprašanje je namreč odvisno ravnanje vseh lokalnih skupnosti v prihodnje na eni strani in raven varstva osebnih podatkov v Republiki Sloveniji na drugi strani. Ustavno sodišče je zahtevo prevzelo v absolutno prednostno obravnavo, vendar do izdaje letnega poročila odločitve še ni sprejelo.

[45] Uradni list RS, št. 109/2010; v nadaljevanju ZPrCP.

3.8.3. Odločitev Ustavnega sodišča v zvezi z zahtevo za presojo ustavnosti Zakona o evidentiranju nepremičnin[46]

Informacijski pooblaščenec je v letu 2012 prejel sodbo Ustavnega sodišča, v kateri je odločilo o zahtevi za presojo ustavnosti, ki jo je vložil leta 2011 v zvezi s prvim in drugim odstavkom 114. člena ZEN, 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. členom 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 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 prikazal, da navedene zakonske določbe ne prestanejo ustavnega testa sorazmernosti, ki se zahteva za poseg v človekove pravice.

Ustavno sodišče je razveljavilo določbi prvega in drugega odstavka 114. člena ZEN, ki določata javnost zemljiškega katastra in katastra stavb, v delu, ki se nanaša na podatke o lastniku, če gre za fizično osebo. S tem je pritrdilo stališču Informacijskega pooblaščenca, da podatki o lastnikih nepremičnin, če so ti fizične osebe, sodijo med varovane osebne podatke, ki ne smejo biti javno objavljeni brez v zakonu jasno določenega namena. Prav tako je Ustavno sodišče jasno izrazilo stališče, da kljub javnosti osebnih podatkov za določen namen (kot so npr. v zemljiški knjigi), to še ne pomeni absolutne javnosti teh podatkov in ne dopušča njihove nadaljnje obdelave za kakršenkoli namen. Ustavno sodišče je razveljavilo javnost osebnih podatkov lastnikov nepremičnin v obeh katastrih, zato ni bilo potrebe po razveljavitvi drugih določb ZEN in Pravilnika o vrstah in vsebini potrdil iz zbirk geodetskih podatkov ter o načinu izkazovanja podatkov[47], ki jih je Informacijski pooblaščenec še izpodbijal.

3.9. Zanimivejše odločitve v inšpekcijskih postopkih na področju varstva osebnih podatkov

V nadaljevanju je predstavljenih šest zanimivejših odločitev Informacijskega pooblaščenca v inšpekcijskih postopkih, ki jih je vodil leta 2012.

3.9.1. Nadzor nad delavci v zvezi z uporabo tiskalnika

Informacijski pooblaščenec je prejel prijavo, iz katere je izhajalo, da je bilo s strani vodstva državnega organa (zavezanec) odrejeno, da se pripravi poimenski seznam zaposlenih glede njihove uporabe tiskalnika. Seznam je poleg imena in priimka vseboval tudi podatek o tem, koliko tiskalnih poslov je posamezen delavec naredil in imena natisnjenih dokumentov.

V postopku inšpekcijskega nadzora je bilo ugotovljeno, da se je zavezanec soočil s potrebo po nadzoru oziroma omejevanju stroškov iz naslova tiskanja (stroški tiskalnikov in papirja). Ker so komercialna orodja za to predraga, je uporabil brezplačno aplikacijo Printcut logger, ki o tiskalniških opravilih zbira naslednje podatke: čas tiskanja, uporabniško ime osebe, ki tiska, število natisnjenih strani/izvodov, ime tiskalnika, naslov natisnjenega dokumenta, klient, velikost papirja, (tiskalniški) jezik, višina (izpisa), širina (izpisa), dvostransko tiskanje, črno-belo/barvno tiskanje, velikost dokumenta v kilo bajtih. Zavezanec je na podlagi zbranih podatkov ugotovil, da se zaposleni pri tiskanju dokumentov obnašajo neracionalno

[46] Uradni list RS, št. 47/2006; v nadaljevanju ZEN.
[47] Uradni list RS, št. 22/2007 in 33/2009.

in neekološko, saj tiskajo dokumente, ki so objavljeni in stalno dostopni na intranetu ali internetu, obrazce v večjem številu in dokumente za svoje privatne potrebe (npr. študijsko gradivo).

Osebni podatek je katerikoli podatek, ki se nanaša na posameznika, ne glede na obliko, v kateri je izražen, pri tem pa je posameznik določena ali določljiva fizična oseba, na katero se nanaša osebni podatek (1. in 2. točka 6. člena ZVOP-1). Informacijski pooblaščenec je ugotovil, da se podatki o tiskalniških opravilih zaposlenega zapišejo poleg njegovega uporabniškega imena. Zaposleni je s tem, ko se prijavi v komunikacijsko omrežje, enolično identificiran in s tem tudi določen. Glede na široko definicijo osebnega podatka so navedeni podatki o posameznem tiskalniškem poslu osebni podatki, saj jih je mogoče uvrstiti pod katerekoli podatke, ki se nanašajo na določeno fizično osebo.

Informacijski pooblaščenec je nadalje obravnaval zakonitost obdelave osebnih podatkov. V konkretnem primeru je bilo ugotovljeno, da so se osebni podatki zaposlenih obdelovali na način, da so bili najprej zbrani oziroma pridobljeni s pomočjo aplikacije Printcut logger, nato razvrščeni v tabele, v enem primeru pa še posredovani na vse notranje organizacijske enote zavezanca.

ZVOP-1 v 8. členu določa, da se lahko osebni podatki 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. Zavezanec osebnih privolitev vseh zaposlenih, ki uporabljajo tiskalnike, ni izkazal. Pa tudi sicer je osebna privolitev zaposlenega kot pravna podlaga za obdelavo njegovih osebnih podatkov v zvezi z delovnim razmerjem redko upoštevana. Privolitev posameznika v skladu z načelom svobodne izbire v razmerju do delodajalca po mnenju Informacijskega pooblaščenca ni takšna izbira, da bi jo lahko zaradi socialnih ali ekonomskih okoliščin, ali celo kakšnih drugih osebnih okoliščin, v katerih se znajde zaposleni, ki da osebno privolitev, praviloma upoštevali kot dovolj svobodno in s tem veljavno, kot to zahteva 14. točka 6. člena ZVOP-1. Pravno podlago za obdelavo osebnih podatkov v obravnavanem primeru bi lahko predstavljal 46. člen Zakona o delovnih razmerjih[48]. Zato je Informacijski pooblaščenec presojal, ali je potrebno osebne podatke zaposlenih o njihovih tiskalniških poslih obdelovati zaradi uresničevanja pravic in obveznosti iz delovnega razmerja, ali v zvezi z delovnim razmerjem oziroma zaradi nadzora nad uporabo tiskalnikov in s tem povezanimi stroški. V postopku je bilo ugotovljeno, da se je zavezanec celotnega podjema z nadzorom tiskanja lotil zaradi bolj racionalnega nabavljanja tiskalniških strojev glede na njihovo predvideno obremenitev, in zaradi ugotovitev, da materialni stroški, povezani s tiskanjem, naraščajo. Informacijski pooblaščenec ne dvomi, da je obvladovanje materialnih stroškov skrb vsakega delodajalca na eni strani, na drugi pa tudi, da mora zaposleni službena sredstva uporabljati za službene namene. Vendar ugotovitev delodajalca avtomatično še ne upravičuje, da bi lahko zaradi nadzora nad stroški tiskanja osebne podatke, ki so v zvezi s tem na voljo, neomejeno obdeloval.

Informacijski pooblaščenec je zaključil, da je v konkretnem primeru sporno zbiranje podatka o imenu datoteke, ki se tiska in naslovu natisnjene spletne strani. Z ostalimi podatki o posameznem tiskalniškem opravilu se lahko ugotovi, koliko posamezna oseba porabi papirja in barve ter koliko obrabi tiskalniški stroj. Delodajalec lahko nato določi, koliko listov sme vsak zaposleni natisniti in kako se ravna, če se ta meja prekorači pred pretekom nekega časovnega obdobja, npr. meseca.

Glede na to, da se lahko zasledovan namen nadzora nad tiskanjem in tiskalniki doseže tudi brez obdelave podatka o imenu datoteke oziroma spletne strani, ki se tiska, je obdelava tega podatka po mnenju Informacijskega pooblaščenca nesorazmerna in nezakonita, saj zavezanec nima pravne podlage za obdelavo tega podatka v smislu 9. člena ZVOP-1, ki določa pravne podlage za obdelavo osebnih podatkov v javnem sektorju. Zato mu je Infor-

[48] Uradni list RS, št. 42/2002 s spremembami in dopolnitvami; v nadaljevanju ZDR.

macijski pooblaščenec odredil, da mora prenehati zbirati podatke o tem, katero datoteko oziroma spletno stran je natisnil posamezen uporabnik, in že zbrane podatke uničiti. To ni pomenilo, da bi moral zavezanec prenehati uporabljati aplikacijo Papercut logger, ampak bi jo lahko spremenil oziroma prilagodil tako, da ne bi več zbiral podatka o imenu datoteke. Če bi zavezanec prilagodil aplikacijo, bi moral o nadzoru skladno z 19. členom ZVOP-1 seznaniti zaposlene (kateri podatki se zbirajo, namen zbiranja, omejitve uporabe in kaj pomeni prekoračitev teh omejitev). Če bi zavezanec obdržal nesporne podatke o tiskalniških poslih, bi upravljal z novo zbirko osebnih podatkov, ki bi jo moral prijaviti Informacijskemu pooblaščencu in spoštovati tudi vse obveznosti, ki izvirajo iz naslova njenega zavarovanja ter beleženja zunanjih in notranjih revizijskih sledi.

Zavezanec se je odločil, da podatkov o tiskalniških poslih ne bo več zbiral, kar pomeni, da je prenehal uporabljati aplikacijo Papercut logger in da je izbrisal vse z njo pridobljene osebne podatke zaposlenih.

3.9.2. Zbiranje osebnih podatkov za namen neposrednega trženja preko spleta

Informacijski pooblaščenec je na podlagi več prijav pri zavezancu, ki se ukvarja z izvajanjem neposrednega trženja po elektronski pošti, uvedel postopek inšpekcijskega nadzora z namenom preveriti zakonitost obdelave osebnih podatkov, ki jih uporablja za izvajanje neposrednega trženja.

V postopku inšpekcijskega nadzora je bilo ugotovljeno, da zavezanec v svojih zbirkah obdeluje osebne podatke več kot sto tisoč posameznikov, ki so registrirani uporabniki njegove spletne strani (ime, priimek, elektronski naslov, spol, datum registracije, datum in čas aktivacije uporabniškega računa) ali uporabniki določenih Facebook aplikacij (npr. elektronski naslov, datum sodelovanja, ime in priimek, ID številka uporabnika na facebooku).

Iz določb ZVOP-1 (8. in 10. člen) jasno izhaja, da se lahko osebni podatki v zasebnem sektorju obdelujejo le, če obdelavo osebnih podatkov določa zakon ali če se obdelujejo na podlagi podane osebne privolitve posameznika, na katerega se nanašajo osebni podatki. V obravnavanem primeru, kjer posebna zakonska podlaga ne obstaja, se lahko osebni podatki obdelujejo le na podlagi osebne privolitve posameznika.

Glede osebnih podatkov iz zbirke registriranih uporabnikov je Informacijski pooblaščenec ugotovil, da so v tej zbirki tudi podatki o tem, kdaj naj bi posameznik podal osebno privolitev (datum in čas aktivacije uporabniškega računa). Navedene podatke je sicer možno potvoriti, vendar je Informacijski pooblaščenec zaključil, da ne obstajajo indici ali dokazi, ki bi izkazovali, da se je to dejansko tudi zgodilo. Registracija posameznika na spletni strani zavezanca, v okviru katere posameznik sprejme splošne pogoje, ki vsebujejo določilo glede privolitve za obdelavo njegovih osebnih podatkov, vsaj nakazuje na podajo osebne privolitve. Zato je Informacijski pooblaščenec zaključil, da pri posameznikih, za katere zavezanec razpolaga s podatki o tem, kdaj so opravili postopek registracije, ni mogoče v zadostni meri očitati neobstoj pravne podlage za obdelavo njihovih osebnih podatkov.

V nasprotju z navedenim pa pri posameznikih, katerih osebni podatki so bili v zbirkah uporabnikov različnih Facebook aplikacij, zavezanec ni razpolagal z nobenim dokazilom, da so opravili postopek registracije ali dejansko s klikom potrdili seznanjenost in strinjanje s splošnimi pogoji uporabe določene aplikacije, v okviru katerega bi podali svojo osebno privolitev za obdelavo osebnih podatkov. 14. točka 6. člena ZVOP-1 določa, da je osebna privolitev posameznika prostovoljna izjava volje posameznika, da se lahko njegovi osebni podatki obdelujejo za določen namen, in je dana na podlagi informacij, ki mu jih mora zagotoviti upravljavec. Osebna privolitev posameznika je lahko pisna, ustna ali druga ustrezna privolitev. Zavezanec osebnih podatkov uporabnikov različnih spletnih aplikacij ni pridobil na podlagi ustne ali pisne privolitve, temveč naj bi bila privolitev pridobljena po elektronski poti. ZVOP-1 sicer dopušča, da je privolitev podana tudi na druge načine, ki pa morajo biti ustrezni, da lahko zadostijo kriteriju »druga ustrezna privolitev posameznika«. Zato je Informacijski pooblaščenec

moral presoditi, ali je bila privolitev po elektronski poti takšna, da jo lahko štejemo za ustrezno. V skladu s 16. točko 6. člena ZVOP-1 je ustna ali druga ustrezna privolitev posameznika tista, ki je dana ustno ali s telekomunikacijskim ali drugim ustreznim sredstvom ali na drug ustrezen način, iz nje pa je mogoče nedvomno sklepati na posameznikovo privolitev. Pri tem je treba upoštevati, da elektronsko podana privolitev, ki se lahko udejanja npr. s klikom na določeno povezavo, z izpolnitvijo potrditvenega okenca, izbiro ponujenih možnosti na (spustnem ali drugačnem) seznamu in (praviloma, ne pa nujno) tudi s klikom na določen gumb (označen s tekstom, kot je »Sprejemam pogoje«, »Registriraj se« ipd.) ali ustrezno povezavo, generira ukaz oziroma zahtevek spletnemu strežniku. Ta ukaz, ki je opremljen tudi z datumom in časom, IP naslovom uporabnika in drugimi podatki, se privzeto zabeleži v dnevniških datotekah spletnega strežnika. Iz tovrstnih podatkov je mogoče naknadno razbrati, kdaj in iz katerega naslova je bil poslan zahtevek spletnemu strežniku in na ta način naknadno ugotoviti, ali je bila in kdaj je bila elektronsko podana privolitev posameznika v obdelavo osebnih podatkov. Tovrstno beleženje je privzeto nastavljeno v najbolj pogostih spletnih strežnikih in ga je - če obstaja potreba po izključitvi – potrebno posebej izključiti, privzeto pa te podatke beležijo vsi spletni strežniki.

Zavezanec v postopku inšpekcijskega nadzora ni predložil nobenih podatkov in dokazov, iz katerih bi bilo razvidno, da so uporabniki različnih Facebook aplikacij dejansko podali svojo privolitev, čeprav bi glede na domnevni način podaje privolitve s temi podatki (privzeto) moral razpolagati. Zatrjeval je, da sam obstoj podatkov v njegovih zbirkah osebnih podatkov dokazuje, da je bila za vnos osebnih podatkov podana privolitev posameznikov. Informacijski pooblaščenec je zaključil, da zgolj iz obstoja osebnih podatkov v bazah zavezanca ni mogoče nedvoumno sklepati na posameznikovo privolitev. Zavezanec bi moral predložiti podatke o tem, kdaj so bili osebni podatki posameznikov vneseni v zbirko osebnih podatkov, uporabljeni ali drugače obdelani, ker jih je pri pridobivanju privolitev po elektronski poti mogoče enostavno zagotoviti. Informacijski pooblaščenec je ob tem poudaril, da obratna interpretacija, češ da že sam obstoj osebnih podatkov v zbirki osebnih podatkov dokazuje, da so bili podatki zbrani zakonito, ne vzdrži strokovne presoje. Takšna interpretacija bi zavezancem namreč omogočila, da v svojih zbirkah osebnih podatkov obdelujejo izjemne količine osebnih podatkov, za katere bi trdili, da so jih pridobili s privolitvijo, podano po elektronski poti, ne da bi razpolagali s kakršnimikoli dokazi o tem, kako in ali so jih zakonito pridobili.

Glede na to, da zavezanec za obdelavo osebnih podatkov uporabnikov Facebook aplikacij ni izkazal ustrezne pravne podlage (osebne privolitve), je Informacijski pooblaščenec zaključil, da nima pravne podlage za njihovo hrambo, uporabo za namen neposrednega trženja ali kakršnokoli drugačno obdelavo in mu je odredil, da jih mora iz svojih zbirk nepovratno izbrisati. Zavezanec je izvršil odrejeni ukrep.

3.9.3. Izvajanje biometrijskih ukrepov in videonadora v fitnes studiu

Informacijski pooblaščenec je uvedel inšpekcijski postopek zoper zavezanca, ki naj bi po navedbah v prijavi za vstopanje v prostore fitnes studia nad svojimi člani izvajal biometrijske ukrepe, poleg tega pa naj bi v garderobi fitnes studia izvajal videonadzor.

V postopku inšpekcijskega nadzora je bilo ugotovljeno, da je zavezanec izvajal biometrijske ukrepe s čitalcem prstnih odtisov na vhodu v vadbene prostore fitnes studia. Biometrijske ukrepe je izvajal nad večino članov fitnes studia za namene nadzora vstopov v te prostore, pri čemer se je član fitnes studia lahko sam odločil, ali bo v fitnes vstopal s pomočjo posebne čip kartice, na kateri ni biometričnih podatkov, ali pa z izvajanjem biometrijskih ukrepov. Zavezanec je članu, ki se je odločil za slednji način vstopanja, odčital prstni odtis, ki se je pretvoril v kombinacije številk (t.i. template) in se shranil na posebnem strežniku. Ob vstopanju v navedene prostore zavezanca z biometrijskimi ukrepi je sistem zabeležil ime in priimek člana, ki je vstopil in čas vstopa.

Zavezanec je menil, da pri opisanem sistemu vstopanja v vadbene prostore fitnes studia ne gre za izvajanje biometrijskih ukrepov, saj v svoji bazi ni hranil posnetkov prstnih odtisov,

ampak zgolj na njihovi podlagi ustvarjene unikatne številke, ki jih je sistem ob sami registraciji prepoznaval. Informacijski pooblaščenec je v zvezi z navedenim pojasnil, da ZVOP-1 pod pojmom »biometrijskih ukrepov« zajema dva različna načina (postopka) prepoznave posameznika: postopek, s katerim se ugotavljajo lastnosti posameznika, tako da se lahko izvrši njegova identifikacija (prepoznava), in postopek, s katerim se primerjajo lastnosti posameznika, tako da se lahko preveri njegova identiteta oziroma istovetnost (avtentikacija). Sistem vstopanja v prostore na način, kot ga je izvajal zavezanec, je v celoti ustrezal definiciji biometrijskih ukrepov. Naprava je omogočala povezovanje prstnega odtisa, ki ga je »prebral« čitalec prstnih odtisov, z izvedenim podatkom, ki je bil shranjen v bazi. Na podlagi take povezave je sistem preveril identiteto posameznika in posledično odprl ali ni odprl vrat oziroma je člana registriral ali ne. Dejstvo, da iz številke, ki jo na podlagi prstnega odtisa generira in hrani naprava, ni mogoče rekonstruirati prstnega odtisa, je za definicijo biometrijskih ukrepov popolnoma nepomembno.

Informacijski pooblaščenec je zavezancu odredil, da mora prenehati izvajati biometrijske ukrepe, ki jih je za vstopanje v prostore fitnes studia izvajal nad člani tega studia, ker za takšno obdelavo osebnih podatkov ni imel pravne podlage. V skladu z 80. členom ZVOP-1 je izvajanje biometrijskih ukrepov v zasebnem sektorju, kamor sodi tudi zavezanec, dopustno na podlagi zakona ali odločbe Informacijskega pooblaščenca, s katero je dovolil izvajanje biometrijskih ukrepov. Ker izvajanje biometrijskih ukrepov v zvezi z dejavnostjo zavezanca ni določeno v zakonu, bi zavezanec moral pred uvedbo ukrepov posredovati zahtevo Informacijskemu pooblaščencu, česar pa ni storil. V konkretnem primeru je bilo pomembno tudi, da je zavezanec izvajal biometrijske ukrepe nad člani fitness studia in ne nad svojimi zaposlenimi. V skladu z 80. členom ZVOP-1 namreč lahko zasebni sektor biometrijske ukrepe izvaja le nad svojimi zaposlenimi, če so bili predhodno o tem pisno obveščeni, in sicer, če so nujno potrebni za opravljanje dejavnosti, za varnost ljudi ali premoženja ali za varovanje tajnih podatkov ali poslovne skrivnosti.

V zvezi z izvajanjem videonadzora je bilo v inšpekcijskem postopku ugotovljeno, da zavezanec izvaja videonadzor delovnih prostorov (recepcija) in tistih delovnih prostorov izven delovnega mesta (garderoba), kjer je z določbo tretjega odstavka 77. člena ZVOP-1 izrecno prepovedan. Zavezanec je z eno kamero snemal celotno območje recepcije, ki se nahaja ob vhodu v prostore fitnes studia, dve kameri pa sta bili nameščeni v moški garderobi oziroma slačilnici.

Izvajanje videonadzora znotraj delovnih prostorov se lahko izvaja le v izjemnih primerih, pod pogoji, ki jih določa 77. člen ZVOP-1, tj. kadar je to nujno potrebno za varnost ljudi ali premoženja ali za varovanje tajnih podatkov ter poslovne skrivnosti, tega namena pa ni možno doseči z milejšimi sredstvi. Videonadzor se lahko izvaja le glede tistih delov prostorov, kjer je potrebno varovati naštete interese. Prepovedano je izvajati videonadzor v delovnih prostorih izven delovnega mesta, zlasti v garderobah, dvigalih in sanitarnih prostorih.

Videonadzor delovnih prostorov predstavlja po mnenju Informacijskega pooblaščenca dokaj velik poseg v informacijsko zasebnost zaposlenih, zato je zakonodajalec v prvem odstavku 77. člena ZVOP-1 za izvajanje takega videonadzora določil stroge pogoje in njegovo izvajanje omejil na izjemne primere, ko je varovanju taksativno naštetih pravnih dobrin potrebno dati prednost pred varstvom osebnih podatkov zaposlenih. Zavezanec je navedel, da želi z izvajanjem videonadzora delovnih prostorov zagotavljati varnost premoženja, pri tem pa ni natančneje pojasnil, katero premoženje želi z videonadzorom celotne recepcije varovati, na kakšen način in kdo ogroža to premoženje. Zato je Informacijski pooblaščenec glede videonadzora recepcije zaključil, da bi bil dopusten omejen videonadzor, ki bi ga zavezanec izvajal tako, da bi z videokamero snemal zgolj tisto območje recepcije, kjer se nahaja blagajna. Blagajno zavezanca je v konkretnem primeru mogoče opredeliti kot premoženje, ki ga je dopustno zavarovati z videonadzorom, hkrati pa je tak videonadzor mogoče opredeliti kot sorazmeren, saj zavezanec z njim nadzor omeji na objekt varstva. Poleg tega zavezanec s takim videonadzorom v manjši meri poseže v informacijsko zasebnost zaposlenih, saj snema zgolj majhen del območja znotraj njihovega delovnega prostora.

Glede na navedene določbe ZVOP-1 je Informacijski pooblaščenec zavezancu odredil, da mora prenehati izvajati videonadzor moške garderobe v prostorih fitnes studia ali pa obiskovalcem fitnes studia zagotoviti ločene prostore za preoblačenje, v katerih ne bo izvajal videonadzora. Odredil mu je tudi, da mora prenehati izvajati videonadzor recepcije fitnes studia ali pa obstoječi videonadzor recepcije spremeniti, tako da bo videokamera snemala zgolj območje blagajne, ki se nahaja v tej recepciji. Informacijski pooblaščenec je zavezancu tako v obeh primerih izvajanja videonadzora prepustil odločitev, ali bo z njegovim izvajanjem v celoti prenehal ali pa ga bo prilagodil in spremenil tako, da bo v skladu z določbami ZVOP-1.

3.9.4. Neustrezno zavarovanje odpadnih (foto-)kopij dokumentov z osebnimi podatki

Informacijski pooblaščenec je prejel tudi prijavo, iz katere je izhajalo, da so otroci v popoldanskem varstvu v določenem vrtcu od vzgojiteljice prejeli za namen likovnega ustvarjanja liste, ki so na hrbtni strani vsebovali fotokopije različnih dokumentov z osebnimi podatki določenih posameznikov (npr. fotokopije fotografij, dokumentov iz sodnih spisov in kazenskih ovadb, podanih pri policiji in tožilstvu). Na tak način se je z osebnimi podatki seznanil širši krog ljudi, ki do teh podatkov ni bil upravičen.

V postopku inšpekcijskega nadzora je bilo ugotovljeno, da se na hodniku vrtca še vedno nahajajo identične odpadne fotokopije, kakršne je ob prijavi prejel Informacijski pooblaščenec, ter da je navedene odpadne fotokopije z osebnimi podatki v vrtec za namen likovnega ustvarjanja otrok prinesla oseba, ki ima v tem vrtcu otroka, doma pa tiskarno in fotokopirnico. Informacijski pooblaščenec je v vrtcu pridobljeno dokumentacijo skladno z določbami ZIN zasegel in uvedel inšpekcijski nadzor pri zavezancu, ki je fotokopije vrtcu posredoval. Zavezanec je pojasnil, da je deloval v dobri veri in je želel le pomagati vrtcu oziroma otrokom priskrbeti papir za risanje. V postopku je bilo ugotovljeno, da je zavezanec odpadno dokumentacijo metal v koš za smeti, kasneje pa koš izpraznil v zabojnik na ulici, ki je namenjen odlaganju odpadnega papirja. Zavezanec je sicer razpolagal s strojem za razrez papirja, vendar ga je uporabil le v primeru, če ga je stranka opozorila, da fotokopije vsebujejo osebne podatke, ki jih je potrebno uničiti.

Informacijski pooblaščenec je zaključil, da zavezanec nima urejenega ustreznega zavarovanja osebnih podatkov, s katerimi upravlja pri opravljanju svoje dejavnosti, t. j. pri procesu tiskanja, fotokopiranja ali drugačnega reproduciranja dokumentacije, ki take podatke vsebuje. Zavezanec je pri reprodukciji dokumentacije dolžan ustrezno zavarovati tako izvirno (originalno) dokumentacijo in reprodukcije te dokumentacije, kakor tudi odpadne ali odvečne izvode, ki nastanejo ob fotokopiranju, izpisovanju ali tiskanju, če ti vsebujejo osebne podatke. Zavarovanje osebnih podatkov v skladu s 24. členom ZVOP-1 vključuje tudi njihovo ustrezno uničenje, zato bi zavezanec moral poskrbeti, da bi se odpadne fotokopije oziroma dokumentacija, ki vsebuje osebne podatke, uničila na način, da osebnih podatkov ne bi bilo več mogoče razbrati ali nadaljnje uporabiti oziroma zlorabiti. Tako je bil zavezanec dolžan neprevzeto dokumentacijo stranke (ugotovljeno je bilo, da je oseba, katere osebni podatki so se med drugim nahajali na fotokopijah, ki jih je prejel vrtec, izvirno dokumentacijo prinesla k zavezancu z namenom fotokopiranja, a je ni nikoli prišla iskat), ki je vsebovala osebne podatke, do izročitve stranki ustrezno zavarovati in v skrajnem primeru po določenem času ustrezno uničiti, nikakor pa te dokumentacije ne bi smel odvreči v koše za smeti, jo oddati kot odpadni papir ali jo posredovati vrtcu za namene likovnega ustvarjanja otrok, saj je s takšnim malomarnim ravnanjem omogočil nepooblaščeno obdelavo osebnih podatkov.

Zaradi ugotovitev v postopku inšpekcijskega nadzora je Informacijski pooblaščenec zavezancu odredil, da mora zagotoviti zavarovanje osebnih podatkov, ki jih vsebuje dokumentacija, ki mu jo stranke izročijo za namene reproduciranja. To mora storiti na način, da prejeto dokumentacijo in izdelane reprodukcije te dokumentacije, kot so fotokopije, izpisi in ponatisi, hrani v omarah do izročitve stranki. Prostori in omare v njih morajo biti

izven delovnega časa in medtem ko v prostorih ni njegovih zaposlenih, obvezno zaklenjeni. Prav tako pa mora sproti uničiti odpadne izvode reproducirane dokumentacije, ki vsebujejo osebne podatke.

V zvezi z zgoraj opisanim primerom in drugimi podobnimi primeri je Informacijski pooblaščenec pripravil obvestilo za javnost, v katerem je opozoril fotokopirnice, tiskarne in druge subjekte, ki se ukvarjajo z reprodukcijo dokumentacije, ki lahko vsebuje tudi osebne podatke, da poskrbijo za ustrezno uničenje tistega dela nastalih odpadnih dokumentov, ki vsebujejo osebne podatke in tako preprečijo nepooblaščeno seznanjanje s temi podatki ter morebitne zlorabe tako pridobljenih osebnih podatkov, do katerih bi zaradi neustreznega zavarovanja lahko prišlo. Če podjetja, ki se ukvarjajo z reprodukcijo dokumentov, ne poskrbijo za ustrezno uničenje odpadnih fotokopij z osebnimi podatki in če zaradi tega pride do nezakonitega razkrivanja osebnih podatkov ali do njihove zlorabe, so odgovorna tako za prekršek po ZVOP-1 zaradi neustreznega zavarovanja osebnih podatkov kot tudi za nastalo materialno ali/in nematerialno škodo.

3.9.5. Preusmeritev obiskovalcev strani s spletnimi igrami na srečo na drug naslov in nezakonito zbiranje njihovih osebnih podatkov

Informacijski pooblaščenec je uvedel postopek inšpekcijskega nadzora zoper Urad Republike Slovenije za nadzor prirejanja iger na srečo, v katerem je ugotovil, da je zavezanec registriral domeno www.infounpis.si in vzpostavil spletni strežnik, na katerega so bili preusmerjeni obiskovalci spletnih strani, na katerih se prirejajo spletne igre na srečo brez koncesije vlade.

Informacijski pooblaščenec je v inšpekcijskem postopku ugotovil, da 107.a člena Zakona o igrah na srečo[49], ki ga je kot pravno podlago za svoje ravnanje navedel zavezanec, ne daje podlage za preusmeritev obiskovalcev strani s spletnimi igrami na srečo na druge naslove in ne zavezancu ne drugemu organu ali inštituciji ne dajejo pravne podlage za vzpostavitev zbirke osebnih podatkov o osebah, ki so takšne spletne strani želele obiskati. Določbe navedenega člena namreč opredeljujejo možnost omejitev dostopa do spletnih strani, česar pa ni dopustno razširiti s preusmerjanjem na druge spletne strani in zbiranjem osebnih podatkov o tistih osebah, katerih zahtevki so bili preusmerjeni. Zlasti je pomembno, da v konkretnem primeru zavezanec ni zbiral podatkov o obiskovalcih svoje spletne strani, temveč osebne podatke posameznikov, ki niso želeli obiskati njegove spletne strani, ampak spletne strani s spletnimi igralnicami (npr. blokiranih spletnih stavnic). Obiskovalci spletnih igralnic so, misleč, da bodo pristali na zahtevani spletni strani, s svojim brskalnikom posredovali veliko podatkov, ki so bili namenjeni zahtevani spletni strani, ne pa zavezancu, in za katere zavezanec nima nobene pravne podlage za pridobitev, beleženje ali kakršnokoli drugačno obdelavo. Zavezanec je tako brez pravne podlage vzpostavil zbirko osebnih podatkov, ki vsebuje osebne podatke o IP naslovu, datumu in času obiska, verziji operacijskega sistema, verziji brskalnika ter druge podatke, ki so se zabeležili v dnevniških datotekah spletnega strežnika, za posameznike, ki so bili preusmerjeni na spletno stran www.infounpis.si. Informacijski pooblaščenec je ugotovil, da je zavezanec podatke v tej zbirki tudi obdeloval, kar je razvidno iz komunikacije zavezanca z mediji, ki so poročali, koliko obiskov je zabeležila preusmeritvena spletna stran www.infounpis.si v nekaj tednih, pri čemer do teh podatkov ni mogoče priti brez obdelave podatkov o posameznih zahtevkih.

Informacijski pooblaščenec je zavezancu naložil, da mora iz dnevniške datoteke za spletno stran www.infounpis.si izbrisati osebne podatke posameznikov, ki so bili z drugih spletnih strani preusmerjeni na to spletno stran. Informacijski pooblaščenec je v odločbi pojasnil, da je podatke o IP številkah praviloma treba obravnavati kot osebne podatke (IP naslovi omogočajo natančno identifikacijo internetnih uporabnikov), podobno je treba obravnavati podatke o obiskanih spletnih straneh, tehničnih značilnostih uporabnikovega brskalnega okolja, morebitne podatke o uporabniških imenih in piškotke ter podatke o tem, s katere

[49] Uradni list RS, št. 14/2011, uradno prečiščeno besedilo 3; v nadaljevanju ZIS.

spletne strani je bil posameznik napoten na zadevno spletno stran. Ti podatki se skupaj ali posamič nanašajo na konkreten posamezen obisk in s tem na posameznika, ki je lahko določljiv, tudi če dnevniške datoteke ne vsebujejo podatkov o IP naslovu. Zgolj brisanje najbolj določljivih podatkov, kot je v tem primeru IP naslov, še ne more zagotoviti, da posameznik iz množice drugih podatkov ne bo določljiv, saj je določljivost odvisna od entropije informacij, ki jih vsebujejo dnevniški zapisi. Dovolj veliko število raznovrstnih podatkov lahko tvori enoličen podpis brskalnega okolja posameznika (angl. »browser fingerprinting«), ki omogoča razlikovanje med posameznimi obiski in posledično med posameznimi obiskovalci.

Informacijski pooblaščenec je zavezancu odredil tudi, da mora tvorjenje dnevniških datotek spletne strani www.infounpis.si nastaviti tako, da se ne bodo hranili podatki, iz katerih je določljivost posameznika neprimerno lažja, in sicer: obiskana vsebina (cs-uri-stem), poizvedba odjemalca (cs-uri-query), uporabniško ime avtenticiranih uporabnikov (cs-username), vrsta in verzija uporabljenega protokola (cs-version), podatki o brskalnem okolju (cs(User-Agent)). V zvezi s tem je Informacijski pooblaščenec zavezanca opozoril, da bi ob morebitnem zbiranju teh podatkov moral razpolagati s pravno podlago za njihovo obdelavo, posameznikom pa bi moral ob tem v skladu s prvim in drugim odstavkom 19. člena ZVOP-1 podati ustrezne informacije.

Zavezanec je izvršil odločbo Informacijskega pooblaščenca, hkrati pa je zoper njo vložil tožbo na Upravno sodišče Republike Slovenije, ker se ne strinja s tem, da so podatki, katerih izbris in ukinitev beleženja je zahteval Informacijski pooblaščenec, osebni podatki. Sodišče do izdaje letnega poročila v upravnem sporu še ni odločilo.

3.9.6. Obdelava osebnih podatkov uporabnikov storitve BicikeLJ

Informacijski pooblaščenec je na podlagi prejetih prijav uvedel postopek inšpekcijskega nadzora zoper ponudnika storitve Bicikelj. Prijavitelji so navajali, da zavezanec pri registraciji, ki jo mora posameznik opraviti, če želi koristiti njegovo storitev izposoje mestnih koles Bicikelj, od posameznika zahteva veliko osebnih podatkov, med njimi tudi podatke, ki za koriščenje take storitve po njihovem mnenju sploh niso potrebni.

V postopku inšpekcijskega nadzora je bilo ugotovljeno, da pri zavezancu obstajajo štiri različice koriščenja storitev sistema Bicikelj (Prijava na tedensko naročnino, Prijava na letno naročnino prek spleta in plačilo s kreditno kartico, Prijava na letno naročnino prek spleta in plačilo z direktno obremenitvijo, Prijava na letno naročnino po pošti in plačilo z direktno obremenitvijo), ki se medsebojno razlikujejo glede na čas koriščenja storitve (tedenska ali letna naročnina na storitev), način prijave v sistem koriščenja storitve (preko spleta ali po pošti) in način plačila storitve (z direktno obremenitvijo ali s kreditno kartico). Zavezanec pri vsaki od teh različic zbira različen nabor osebnih podatkov uporabnikov storitve izposoje koles.

Informacijski pooblaščenec je moral v inšpekcijskem postopku najprej ugotoviti, ali za vse osebne podatke, ki jih od posameznika, ki želi uporabljati storitev izposoje mestnih koles Bicikelj, zahteva zavezanec, obstaja katera od pravnih podlag iz 10. člena ZVOP-1. Navedeni člen namreč določa dopustne pravne podlage za obdelavo osebnih podatkov v zasebnem sektorju, kamor se uvršča zavezanec. Ugotovil je, da kot pravna podlaga za obdelavo osebnih podatkov v tem primeru pridejo v poštev le drugi odstavek 10. člena (izpolnjevanje pogodbe) ter 8. člen in prvi odstavek 10. člena ZVOP-1 (privolitev uporabnikov). Informacijski pooblaščenec je pri vsaki različici koriščenja storitev zavezanca presojal, ali je obdelava vseh osebnih podatkov uporabnikov, ki jih od njih zahteva zavezanec, potrebna in primerna za sklenitev in izvajanje pogodbe, ki nastane med njim in uporabniki, ali pa za obdelavo osebnih podatkov potrebuje njihovo osebno privolitev.

Informacijski pooblaščenec je zaključil, da zavezanec za obdelavo nekaterih osebnih podatkov uporabnikov nima ustrezne pravne podlage, saj jih ni mogoče opredeliti kot potrebnih za sklenitev in izpolnjevanje pogodbe med zavezancem in uporabnikom (pogodbo je

namreč mogoče skleniti in izvajati tudi brez njih), zavezanec pa za obdelavo teh podatkov tudi ni pridobil osebne privolitve uporabnikov, ker so mu jih morali za koriščenje njegovih storitev obvezno posredovati. Zato je Informacijski pooblaščenec zavezancu z odločbo odredil, da mora v določenem roku pri izvajanju storitev izposoje koles v okviru sistema Bicikelj od posameznikov, ki želijo koristiti te storitve in se v sistem registrirajo preko Prijave na letno naročnino prek spleta in plačila s kreditno kartico, kot pogoj za koriščenje storitev izposoje koles prenehati zbirati podatek o spolu, domačem naslovu (naslov, poštna številka, mesto) in številki mobilnega telefona. Od posameznikov, ki se v sistem registrirajo preko Prijave na letno naročnino prek spleta in plačila z direktno obremenitvijo in Prijave na letno naročnino po pošti in plačila z direktno obremenitvijo, pa mora zavezanec prenehati zbirati podatek o spolu in številki mobilnega telefona.

V odločbi je Informacijski pooblaščenec jasno razmejil med osebnimi podatki, ki so potrebni, to so: ime in priimek, naslov (ulica, mesto, poštna številka, država), datum rojstva, elektronski naslov, PIN koda (geslo, ki si ga uporabnik izbere oziroma izmisli sam), številka plačilnega računa - IBAN ter identifikacijska oznaka banke (BIC koda), podatki o kreditni kartici (številka kartice, varnostna koda in datum veljavnosti) in podatki (npr. spol in številka mobilnega telefona), ki niso potrebni za izpolnjevanje pogodbe. Informacjski pooblaščenec je kot potrebne opredelil podatke, s katerimi se zavezanec zavaruje pred oškodovanjem (podatki o kreditni kartici, podatki o plačilnem računu), in kontaktne podatke, ki strankama omogočajo komunikacijo preko izbranega komunikacijskega sredstva (npr. elektronski naslov, ime in priimek, naslov, poštna številka, mesto). Podatkov o spolu in številki mobilnega telefona uporabnika ni mogoče opredeliti kot primernih in potrebnih za izpolnjevanje pogodbe. V pogodbenem razmerju namreč nobena pravica ali obveznost ni odvisna od spola uporabnika, komunikacija med zavezancem in uporabnikom za potrebe izpolnjevanja pogodbe pa lahko poteka po elektronski pošti ali preko naslova bivališča, odvisno od načina registracije.

Informacijski pooblaščenec je v postopku poudaril, da je kljub načelu pogodbene svobode, na podlagi katerega naj bi bilo izvajalcu storitve prepuščeno, katere podatke bo zahteval od svojega pogodbenika, potrebno upoštevati omejitve iz 10. člena ZVOP-1 in obdelavo vsakega osebnega podatka, ki ga od uporabnika zahteva kot obveznega, izkazati kot potrebno za izvajanje medsebojne pogodbe. Informacijski pooblaščenec je pri predmetni zadevi opozoril tudi na dejstvo, da sta zavezanec Europlakat d.o.o. in Mestna občina Ljubljana (MOL) sklenila pogodbo o javno-zasebnem partnerstvu, s katero se je zavezanec zavezal izvajati storitev Bicikelj, MOL pa je prispevala zemljišča za postavitev točk za izposojo koles. Iz navedenega izhaja, da je izvajanje storitve mestnega kolesa Bicikelj mogoče opredeliti kot javni projekt, storitve, ki jih pri tem izvaja zavezanec, pa kot javne storitve. Zaradi tega ni mogoče govoriti o pogodbeni svobodi zavezanca, v okvir katere naj bi spadalo tudi svobodno odločanje o tem, katere osebne podatke bo zahteval od uporabnikov storitve. Za izvajanje storitev, ki jih nudi zavezanec, namreč obstaja interes, ki je širši od ozkega zasebnega interesa udeležencev, tj. javni interes. Zavezanec po prepričanju Informacijskega pooblaščenca ne sme pogojevati nudenja javnih storitev s posredovanjem širšega nabora osebnih podatkov, kot je potreben za izvajanje same pogodbe, s sklicevanjem na to, da se posameznik lahko sam odloča, ali bo uporabljal njegove storitve in posredoval svoje osebne podatke ali ne. Če je posameznik postavljen pred izbiro, ali bo posredoval vse osebne podatke, ki jih ponudnik javne storitve zahteva, ali pa take storitve ne bo mogel koristiti, ni mogoče govoriti o osebni privolitvi, kot jo definira 14. točka 6. člena ZVOP-1 (prostovoljna izjava volje posameznika). Ta v skladu z 10. členom ZVOP-1 predstavlja pravno podlago za obdelavo osebnih podatkov. Informacijski pooblaščenec je s svojo odločitvijo želel doseči, da bo uporabnik svoje osebne podatke, ki niso potrebni za izvajanje pogodbe med njim in zavezancem, posredoval prostovoljno in da bo njegove javne storitve lahko koristil tudi, če se za posredovanje dodatnih osebnih podatkov ne bo odločil.

V zaključku odločbe je Informacijski pooblaščenec navedel še, da lahko zavezanec vse osebne podatke, ki bi jih od uporabnikov želel zbirati in ki jih ni mogoče opredeliti kot potrebne za samo izvrševanje pogodbe (podatek o spolu, domačem naslovu in številki mobilnega telefona), zbira in nadalje obdeluje na podlagi osebne privolitve posameznikov. To pomeni, da mora zavezanec pri zbiranju osebnih podatkov uporabnikov jasno razmejiti med osebnimi podatki,

ki jih lahko zbira in nadalje obdeluje, ker so potrebni za izvajanje pogodbe in mu jih morajo uporabniki obvezno posredovati, če hočejo koristiti njegovo storitev izposoje koles, in med osebnimi podatki, ki za samo izvajanje pogodbe sicer niso potrebni, lahko pa v določeni meri olajšujejo in poenostavljajo njeno izpolnjevanje, saj lahko prispevajo k boljši in hitrejši komunikaciji med strankama. Posredovanje slednjih osebnih podatkov mora biti prepuščeno svobodni volji uporabnika in s strani zavezanca ne sme biti opredeljeno oziroma na obrazcih označeno kot obvezno. Zavezanec mora uporabnika seznaniti tudi z nameni, za katere namerava njegove osebne podatke (torej tiste, ki jih bo uporabnik posredoval le, če bo to želel) obdelovati.

Zavezanec je ukrepe iz odločbe izvršil, a odločba Informacijskega pooblaščenca še ni pravnomočna, ker je zavezanec z vložitvijo tožbe na Upravno sodišče Republike Slovenije sprožil upravni spor.

3.10. Splošna ocena stanja varstva osebnih podatkov in priporočila

Informacijski pooblaščenec je podobno kot v preteklih letih tudi v letu 2012 največ pritožb prejel zaradi nezakonitega razkrivanja osebnih podatkov oziroma posredovanja osebnih podatkov nepooblaščenim osebam ali objave osebnih podatkov na internetu in v drugih medijih, sledijo prijave v zvezi z nezakonitim zbiranjem osebnih podatkov in uporabo osebnih podatkov za namene neposrednega trženja ter izvajanjem videonadzora.

Informacijski pooblaščenec je v letu 2012 na področju varstva osebnih podatkov vodil skupaj 725 inšpekcijskih zadev, od tega 245 na področju javnega sektorja in 480 na področju zasebnega sektorja (leta 2011 jih je bilo skupaj 682, leta 2010 pa 599) ter 158 prekrškovnih postopkov (leta 2011 jih je bilo 136, leta 2010 pa 179). Navedene številke kažejo, da se število inšpekcijskih zadev iz leta v leto še vedno rahlo povečuje, pri čemer pa je potrebno omeniti, da se v inšpekcijskih postopkih, ki so uvedeni zaradi prejetih prijav, pri obravnavi prijav v mnogih primerih izkaže, da zakon ni bil kršen in da so bile prijave vložene z željo po nagajanju oziroma maščevanju določeni pravni ali fizični osebi.

Poleg inšpekcijskih in prekrškovnih postopkov je Informacijski pooblaščenec v letu 2012 prejel še 2.191 zaprosil za mnenja in pojasnila s področja varstva osebnih podatkov (leta 2011 jih je bilo 2.143, leta 2010 pa 1.859), devet vlog za izdajo dovoljenja za povezovanje zbirk osebnih podatkov (leta 2011 jih je bilo 14, leta 2010 pa devet), 11 vlog za izdajo dovoljenja za izvajanje biometričnih ukrepov (leta 2011 jih je bilo devet, leta 2010 pa šest), pet vlog za izdajo dovoljenja za iznos osebnih podatkov (leta 2011 so bile štiri, leta 2010 pa osem), 63 pritožb zaradi zavrnitve zahteve za seznanitev z lastnimi osebnimi podatki (leta 2011 in 2010 jih je bilo po 85). Iz navedenih podatkov je tako razvidno, da pri vlogah, z izjemo pritožb zaradi zavrnitve zahteve za seznanitev z lastnimi osebnimi podatki, katerih število se je glede na prejšnja leta zmanjšalo, ni zaznati bistvenih sprememb.

Pri obdelavi osebnih podatkov za namene neposrednega trženja prevladujejo prijave zaradi nezakonitega pridobivanja naslovov elektronske pošte za te namene, pri čemer bi kazalo izpostaviti zlasti zbiranje elektronskih naslovov s strani pravnih in fizičnih oseb, ki ponujajo tako imenovane skupinske nakupe in s tem povezane popuste, saj se je število takšnih ponudnikov v zadnjem času zelo povečalo. Ponudniki skupinskih nakupov (pa tudi drugi izvajalci neposrednega trženja) v mnogih primerih 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 uporabo osebnih podatkov za namene neposrednega trženja je potrebno ponovno opozoriti, da izvajalci neposrednega trženja z njegovim izvajanjem v mnogih primerih ne prenehajo niti potem, ko je posameznik že zahteval prenehanje uporabe svojih osebnih podatkov za ta namen, zaradi česar je Informacijski pooblaščenec takšnim izvajalcem v prekrškovnih postopkih dosledno izrekal sankcije za prekršek po 94. členu ZVOP-1.

Informacijski pooblaščenec je v preteklosti javnost in upravljavce osebnih podatkov vseskozi opozarjal na nujnost zavarovanja osebnih podatkov, ki so dostopni preko spletnih strani ali ki se uporabljajo za namene pošiljanja elektronskih sporočil, ter v zvezi s tem upravljavcem osebnih podatkov dosledno izrekal sankcije. Vendar pa se v obravnavanem obdobju število prijav in ugotovljenih kršitev kljub temu ni zmanjšalo. Še vedno so bili pogosto ugotovljeni primeri, ko so bili pri uporabi naslovov elektronske pošte za namene izvajanja neposrednega trženja, ali npr. za namene obveščanja o neizbiri kandidata na prijavljeno delovno mesto, prejemnikom takšnega elektronskega sporočila razkriti naslovi elektronske pošte vseh ostalih prejemnikov, saj pošiljatelj 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«). Odkriti so bili tudi primeri, ko upravljavci osebnih podatkov pri zbiranju osebnih podatkov preko spletnih strani in pri shranjevanju osebnih podatkov, ki bi smeli biti preko spletnih strani dostopni samo določenim pooblaščenim osebam, niso izvedli ustreznih tehničnih in logično-tehničnih postopkov in ukrepov, s katerimi bi zavarovali dostop do podatkov, kar je imelo za posledico, da so lahko posamezniki ob pomoči spletnih iskalnikov po njihovi spletni strani prosto, nepooblaščeno in nekontrolirano dostopali do osebnih podatkov.

Z uporabo Zakona o uveljavljanju pravic iz javnih sredstev[50] je Informacijski pooblaščenec pričel prejemati prijave zoper centre za socialno delo, ki odločajo o teh pravicah. Prijave so bile vložene iz razloga, ker je center za socialno delo v obrazložitvi odločbe, s katero je odločil o pravici iz javnih sredstev, razkril dohodke in premoženje vseh oseb, katerih dohodke in premoženje je upošteval pri svojem odločanju. Informacijski pooblaščenec je v zvezi z navedenimi prijavami v večini primerov ugotovil, da takšna navedba osebnih podatkov ne pomeni kršitve zakona, saj gre za pridobivanje in uporabo osebnih podatkov, ki so potrebni za odločanje o pravici iz javnih sredstev, pri čemer je potrebno v obrazložitvi odločbe, s katero se odloči o pravici, navesti vrsto in višino dohodkov ter vrsto in vrednost premoženja vseh oseb, katerih dohodke in premoženje je center za socialno delo upošteval pri svojem odločanju. Nezakonito pridobivanje in navajanje osebnih podatkov v odločbah, s katerimi so centri za socialno delo odločali o pravici do javnih sredstev, je bilo ugotovljeno le v primerih ugotavljanja in navajanja dohodkov in premoženja tistih oseb, katerih dohodki in premoženje se skladno z 11. členom ZUPJS ne upoštevajo pri ugotavljanju materialnega stanja vlagatelja. Na področju tehnološkega razvoja igra z vidika osebnih podatkov čedalje pomembnejšo vlogo računalništvo v oblaku (angl. cloud computing). Potenciali računalništva v oblaku so izjemni, ne sme pa to povzročiti nižanja ravni varstva osebnih podatkov kot temeljne človekove pravice, kar je tudi eno temeljnih priporočil mednarodne delovne skupine IWGDPT v t.i. Sopot Memorandumu o varstvu osebnih podatkov pri računalništvu v oblaku[51]. Informacijski pooblaščenec je pomembno prispeval k sprejemu omenjenega memoranduma, ki kaže konsenz varuhov zasebnosti na svetovni ravni, aktiven pa je bil tudi na nacionalni ravni.

Informacijski pooblaščenec je tako v letu 2012 v sodelovanju s Cloud Security Alliance (CSA) Slovenia Chapter, Slovenskim odsekom ISACA ter Zavodom e-Oblak, Eurocloud Slovenia kot eden prvih nadzornih organov v Evropski uniji izdal smernice za varstvo osebnih podatkov pri računalništvu v oblaku[52]. Namen smernic je podati enotne kontrolne točke, s pomočjo katerih bodo lahko tako uporabniki kot nadzorni organi sprejemali bolj informirane odločitve glede uporabe in nadzora računalništva v oblaku v delu, ki se nanaša na obdelavo osebnih podatkov, ponudnikom storitev računalništva v oblaku ter iniciativam za varnost in certificiranje tovrstnih storitev pa naj bi ponudile napotke za nadaljnji razvoj s ciljem skladnosti z zakonodajo o varstvu osebnih podatkov. Smernice pojasnjujejo minimalne zahteve zakonodaje in na preprost način z uporabo kontrolnega seznama pojasnijo upravljavcem osebnih podatkov, na kaj morajo paziti, preden se odločijo za ponudnika storitev v oblaku. Pogosto se upravljavci osebnih podatkov namreč ne zavedajo, da so oni odgovorni za podatke, pa čeprav jih

[50] Uradni list RS, št. 62/2010, s spremembami; v nadaljevanju ZUPJS.

[51] IWGDPT: Working Paper on Cloud Computing - Privacy and data protection issues - "Sopot Memorandum" - 51st meeting, 23-24 April 2012, Sopot (Poland): http://www.datenschutz-berlin.de/content/europa-international/international-working-group-on-data-protection-in-telecommunications-iwgdpt/working-papers-and-common-positions-adopted-by-the-working-group.

[52] https://www.ip-rs.si/varstvo-osebnih-podatkov/iskalnik-po-odlocbah-in-mnenjih/smernice/.

zaupajo v obdelavo nekomu tretjemu, npr. večjemu ponudniku iz Združenih držav Amerike. Informacijski pooblaščenec ugotavlja, da številni ponudniki storitev računalništva v oblaku potencialnim uporabnikom trenutno večinoma še ne ponudijo zadostnih informacij za preudarne odločitve in da je treba vzpostaviti mehanizme, ki bodo omogočali ločevanje zaupanja vrednih ponudnikov računalništva v oblaku od tistih tveganih. Medtem ko potekajo številne aktivnosti za izgradnjo zaupanja v računalništvo v oblaku, naj bi smernice pripomogle k večji ozaveščenosti na tem področju in predstavljajo obvezno branje za vsako organizacijo, veliko ali malo, ki se odloča za katero od oblačnih storitev, kot so pisarniški paketi, rešitve za upravljanje odnosov s strankami (CRM), poštni strežniki ter druge poslovne aplikacije, infrastruktura in platforme.

Drug pomemben trend, ki bo igral čedalje večjo vlogo na področju varstva osebnih podatkov v bližnji prihodnosti, je t.i. koncept »big data«. Poenostavljeno povedano, gre za zelo velike podatkovne zbirke, ki jih je zaradi obsežnosti težko obvladovati z običajnimi orodji za upravljanje podatkovnih baz, a z ustreznimi orodji omogočajo hiter zajem in obdelavo različnih (ne)struktiriranih podatkovnih virov, kar omogoča, da »vidimo« in »izmerimo« stvari, ki jih prej nismo mogli. Z vzporednim pojavom interneta stvari (npr. pametni telefoni, elektronika v avtomobilih, pametni števci porabe v gospodinjstvih ipd.), kjer čedalje več naprav lahko zbira podatke v digitalni obliki, nizi podatkov izjemno naraščajo. Predstavljajte si, koliko podatkov ima Facebook, Amazon ali Google (Walmart npr. obdela milijon transakcij na sekundo) in kaj vse bi se dalo iz teh podatkov ugotoviti. Količina informacij, ki jo obvladujejo, je namreč tako velika, da omogoča ugotavljanje poslovnih trendov, nakupovalnih navad, prometnih vzorcev vse do napovedovanja izbruhov gripe in verjetnosti kaznivih dejanj na določenem območju. Kakor tudi (pravilnih ali napačnih) sklepanj in ugotovitev o posamezniku, njegovi kreditni sposobnosti, zdravstvenem stanju, nakupovalnih navadah in drugih lastnostih – podatkov, ki jih predhodno ni bilo mogoče razbrati. Implikacije na varstvo osebnih podatkov so lahko obsežne, zato je »big data« prav gotovo med najpomembnejšimi trendi, ko govorimo o varstvu zasebnosti.

Informacijski pooblaščenec ves čas posebno pozornost namenja spremljanju področja elektronskih komunikacij in podobno, kot je ugotavljal leto poprej, opozarja, da prihaja do povečanih teženj po nadzorovanju uporabe elektronskih komunikacij, pri čemer prihaja do trenj med različnimi interesi in pravicami.

V letnem poročilu za leto 2011 je Informacijski pooblaščenec izpostavil neprimernost ureditve omejevanja dostopnosti spletnih vsebin v določbah Zakona o igrah na srečo[53], ki ponudnikom dostopa do interneta nalaga blokiranje dostopa do spletnih iger na srečo in poskus širjenja pooblastil organov pregona v zvezi z uporabo podatkov, ki so jih dolžni hraniti operaterji elektronskih komunikacij (t.i. data retention). Vlada je predlagala spremembe 149.b člena Zakona o kazenskem postopku[54], ki bi omogočile ne le pridobivanje podatkov za določeno telefonsko številko, temveč za celotno bazno postajo mobilne telefonije. Zaskrbljujoč trend se je nadaljeval v letu 2012, zlasti v procesu usklajevanja novega ZEKom-1, v katerega je Informacijski pooblaščenec vložil ogromno napora in kjer so nekatere dobre rešitve zaradi načina in vsebine nekaterih zelo spornih predlogov ostale neopažene. Organi pregona so si ponovno poskušali olajšati režim za dostop do podatkov o identiteti komunicirajočih posameznikov, in sicer je določba 166. člena predvidevala, da je za pridobitev podatkov o identiteti komunicirajočih posameznikov dovolj pisna zahteva državnega organa in ne sodna odredba, kot je to določal veljavni zakon, ki je sledil zahtevam 37. člena Ustave. Ta določa, da je zagotovljena tajnost pisem in drugih občil in da samo zakon lahko predpiše, da se na podlagi odločbe sodišča za določen čas ne upošteva varstva tajnosti pisem in drugih občil in nedotakljivosti človekove zasebnosti, če je to nujno za uvedbo ali potek kazenskega postopka ali za varnost države. Ustava tako za posege v komunikacijsko zasebnost postavlja stroge pogoje, med katerimi je tudi sodni nadzor, in povsem očitno je šlo za ponoven poskus, kako se temu izogniti. Po posebnih naporih Informacijskega pooblaščenca, sporočilih za javnost in večkratnemu predstavljanju svojih stališč je bila predlagana določba vendarle deležna

[53] Uradni list RS, št. 14/2011 - uradno prečiščeno besedilo 3 in 108/2012; v nadaljevanju ZIS.
[54] Uradni list RS, št. 32/2012 - uradno prečiščeno besedilo 8; v nadaljevanju ZKP.

kritike javnosti in umaknjena iz predloga zakona. Ne glede na navedeno, pa mora Informacijski pooblaščenec opozoriti, da gre za že skoraj simptomatične in vztrajne poskuse organov pregona, ki poskušajo z nepreprečljivimi obrazložitvami in z različnimi zakoni znižati raven komunikacijske ter informacijske zasebnosti na način, da bi si olajšali dostop do identitete komunicirajočih. Čedalje bolj pogosto se kaže, kako se pri teh podatkih vse začne in da je včasih to, kdo je kdaj in s kom komuniciral, pomembnejše kot vsebina komunikacije. Oboje po sodbi Ustavnega sodišča uživa ustavno varstvo.

Informacijski pooblaščenec prav tako ugotavlja, da policija vztrajno poskuša povečati svoja pooblastila, ne da bi te ukrepe argumentirala z analizami, ki bi utemeljile, da so dodatna pooblastila:

1. nujna (kriminalitete se ne da omejiti na kakšen drug, manj invaziven način),
2. učinkovita (tehnično sredstvo v resnici omogoča dosego cilja) in
3. sorazmerna s posegi v temeljne človekove pravice (cilja se ne da doseči na manj invaziven način, npr. s klasičnim policijskim delom).

Tovrstne analize učinka (angl. Impact Assesment) bi morale biti izvedene pred uvedbo novih pooblastil - zakonodajnih predlogov predvidenih sprememb, ki bistveno povečujejo tveganja za zlorabe osebnih podatkov. Nujnost in učinkovitost ukrepov pa bi morali tudi naknadno redno presojati (angl. Regulatory Impact Assesment). Žal ne predhodne ne naknadne analize pri nobenem od predlaganih ukrepov niso bile izdelane, temveč so bile vsakič ponujene le kratke, neargumentirane in s podatki nepodprte obrazložitve.

Informacijski pooblaščenec je v letu 2012 nadaljeval s preventivnim delom in presojami vplivov na zasebnost. Nanj se je 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 podal svoje presoje glede zelo različnih projektov, kot so uporaba pametnih tabel in RDFID oznak na urgentnem oddelku bolnice, uporaba GPS sledilnikov za nadzor nad kurirskimi pošiljkami, izvedba elektronskih volitev znotraj organizacije, uporaba storitev računalništva v oblaku, vzpostavitev evidence visokega šolstva, uporaba mestne kartice Urbana v knjižnicah, spletne DNK analize, prenova splošnih aktov informacijsko varnostnih politik, sledenje aktivnosti uporabnikov z zajemalniki zaslona, uporaba pametnih števcev porabe v gospodinjstvih, izvajanje centralnega nadzora po kontrolnikih kakovosti, sistem ocenjevanja kreditne sposobnosti posameznikov, kriptiranje podatkov pri posredovanju po elektronskih omrežjih, povezljivost evidence pripornikov, sledljivost in arhiviranje elektronske pošte ter uporaba spletnih piškotkov.

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 obdelavo osebnih podatkov.

Informacijski pooblaščenec je v letu 2012 zaznal zaskrbljujoče veliko število predlogov sprememb zakonov oziroma predlogov novih zakonov, ki vsebujejo resne posege v zasebnost posameznikov z vidika obdelave osebnih podatkov, a se sprejemajo po hitrem postopku brez ustreznih analiz in ocen o njihovih posledicah za zagotavljanje ustavno zagotovljenega varstva zasebnosti in osebnih podatkov posameznikov.

Leta 2012 je Informacijski pooblaščenec s podajo mnenj sodeloval pri pripravi naslednjih zakonov in drugih predpisov:

- Predlog Zakona o spremembah in dopolnitvah Zakona o izvrševanju kazenskih sankcij (mnenje z dne 6. 2. 2012),
- Predlog Uredbe o evidencah na področju odvzema premoženja nezakonitega izvora (mnenje z dne 10. 2. 2012),
- Predlog Uredbe Sveta o upravnem sodelovanju na področju trošarin (mnenje z dne 16. 2. 2012),
- Predlog Zakona o spremembah in dopolnitvah Zakona o varstvu pravice do sojenja brez nepotrebnega odlašanja (mnenje z dne 23. 2. 2012),
- Predlog Uredbe o varstvu osebnih podatkov (mnenje z dne 27. 2. 2012),
- Predlog Uredbe o izvajanju Uredbe (EU) o državljanski pobudi (mnenje z dne 9. 3. 2012),
- Predlog Pravilnika o spremembah in dopolnitvah Pravilnika o pravosodnem nadzoru nad državnimi tožilstvi (mnenje z dne 25. 3. 2012),
- Predlog sprememb in dopolnitev letnega programa statističnih raziskovanj 2012 (mnenje z dne 26. 3. 2012),
- Predlog Zakona za uravnoteženje javnih financ (mnenje z dne 25. 4. 2012),
- Predlog Uredbe o spremembah Uredbe o evidencah na področju odvzema premoženja nezkonitega izvora (mnenje z dne 11. 5. 2012),
- Predlog Zakona o spremembah in dopolnitvah Zakona o cestah (mnenje z dne 17. 5. 2012),
- Predlog Zakona o spremembah in dopolnitvah Zakona o prevozih v cestnem prometu (mnenje z dne 24. 5. 2012),
- Predlog Uredbe o formalnostih poročanja v pomorskem prometu (mnenje z dne 11. 6. 2012),
- Predlog Uredbe o izvajanju Uredbe (ES) o prodaji na kratko in določenih vidikih poslov kreditnih zamenjav (mnenje z dne 3. 6. 2012),
- Predlog Konvencije o policijskem sodelovanju v Jugovzhodni Evropi (mnenje z dne 17. 6. 2012),
- Predlog Zakona o spremembah in dopolnitvah Zakona o prevozih v cestnem prometu (mnenje z dne 26. 6. 2012),
- Predlog Zakona o fitofarmacevtskih sredstvih (mnenje z dne 29. 6. 2012),
- Predlog Zakona o spremembah in dopolnitvah Zakona o izvajanju rejniške dejavnosti (mnenje z dne 29. 6. 2012),
- Predlog Zakona o elektronskih komunikacijah ZEKom-1 (mnenje z dne 2. 7. 2012),
- Dodatni predlog za spremembo 139. člena predloga ZEKom-1 (mnenje z dne 3. 7. 2012),
- Predlog Zakona o spremembah in dopolnitvah Zakona o splošnem upravnem postopku ZUP-H (mnenje z dne 3. 7. 2012),
- Predlog Zakona o spremembah in dopolnitvah Zakona o davčnem postopku (mnenje z dne 16. 7. 20112),
- Predlog Pravilnika o vodenju podatkov evidence trga nepremičnin ter načinu pošiljanja podatkov (mnenje z dne 18. 7. 2012),
- Predlog Zakona o spremembah in dopolnitvah Zakona o notariatu (mnenje z dne 18. 7. 2012),

- Predlog nove določbe 398. člena Zakona o spremembah in dopolnitvah Zakona o davčnem postopku v zvezi s predlogom novega osmega in devetega odstavka (mnenje z dne 25. 7. 2012),
- Predlog Zakona o spremembah in dopolnitvah Zakona o kazenskem postopku (mnenje z dne 27. 7. 2012),
- Predlog Zakona o spremembah in dopolnitvah Zakona o davčnem postopku (166. člena ZDavP-2F) (mnenje z dne 30. 7. 2012),
- Predlog Zakona o spremembah in dopolnitvah Zakona o davčnem postopku (398.a člena ZDavP-2F) (mnenje z dne 2. 8. 2012),
- Predlog Zakona o elektronskih komunikacijah (mnenje z dne 13. 8. 2012),
- Predlog Zakona o Agenciji za nadzor finančnih trgov (mnenje z dne 13. 8. 2012),
- Predlog Zakona o spremembah in dopolnitvah Zakona o zaščiti živali (mnenje z dne 20. 8. 2012),
- Predlog spremembe 20. člena ZDavP-2 (mnenje z dne 21. 8. 2012),
- Predlog Uredbe o spreminjanju ulova in prodaji ribiških proizvodov (mnenje z dne 28. 8. 2012),
- Predlog Zakona o spremembah in dopolnitvah Zakona o zaščiti živali (mnenje z dne 31. 8. 2012),
- Predlog Srednjeročnega programa statističnih raziskovanj 2013-2017 – medresorsko usklajevanje (mnenje z dne 31. 8. 2012),
- Predlog Zakona o nalogah in pooblastilih policije (mnenje z dne 3. 9. 2012),
- Predlog Zakona o spremembah in dopolnitvah Zakona o kazenskem postopku (mnenje z dne 24. 9. 2012),
- Predlog Zakona o spremembah in dopolnitvah Zakona o volilni in referendumski kampanji (mnenje z dne 25. 9. 2012),
- Predlog Zakona o nalogah in pooblastilih policije (mnenje z dne 2. 10. 2012),
- Predlog Zakona o spremembah in dopolnitvah Zakona o državni upravi – nujni postopek (mnenje z dne 17. 10. 2012),
- Predlog Zakona o spremembah in dopolnitvah Zakona o urejanju trga dela (mnenje z dne 26. 10. 2012),
- Predlog Zakona o spremembah in dopolnitvah Zakona o verski svobodi – predlog ZVS-A (mnenje z dne 29. 10. 2012),
- Predlog Zakona o spremembah in dopolnitvah Zakona o javnem naročanju (mnenje z dne 29. 10. 2012),
- Predlog Zakona o spremembah in dopolnitvah Zakona o kazenskem postopku, predlog ZKP-L (mnenje z dne 6. 11. 2012,
- Predlog Zakona o spremembah in dopolnitvah Zakona o igrah na srečo (mnenje z dne 4. 11. 2012),
- Predlog Zakona o spremembah in dopolnitvah Zakona o urejanju trga dela (mnenje z dne 14. 11. 2012),
- Predlog Zakona o spodbujanju razvoja turizma (mnenje z dne 19. 11. 2012),
- Predlog Zakona o štipendiranju (mnenje z dne 29. 11. 2012),
- Osnutek Pravilnika o izvajanju nujne medicinske pomoči na smučiščih (mnenje z dne 3. 12. 2012),
- Predlog Zakona o spremembah in dopolnitvah Zakona o državnem tožilstvu (mnenje z dne 4. 12. 2012),
- Predlog Zakona o spremembah in dopolnitvah Zakona o inšpekcijskem nadzoru (mnenje z dne 12. 12. 2012),
- Predlog Zakona o sodelovanju v kazenskih zadevah z državami članicami Evropske unije (mnenje z dne 14. 12. 2012),
- Predlog Zakona o spremembah in dopolnitvah Zakona o notariatu – ZN-G (mnenje z dne 28. 12. 2012).

4.2. Sodelovanje z javnostmi

Informacijski pooblaščenec je tudi v letu 2012 skrbel za javnost svojega dela in obveščanje pravnih in fizičnih oseb s sporočili za javnost, komentarji, intervjuji pooblaščenke, novinarskimi konferenceami in objavami na svoji spletni strani.

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

- predstavitev zgodovine Informacijskega pooblaščenca in 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 osebnih podatkov) 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, aktualno letno poročilo),
- domače in tuje članke z obeh področij,
- 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 kot pomoč 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, vzorci katalogov zbirk osebnih podatkov, vzorec pravilnika o zavarovanju osebnih podatkov, vzorec pogodbe za potrebe pogodbene obdelave osebnih podatkov po 11. členu ZVOP-1, primeri opozoril in obvestil ob neposrednem trženju),
- izdana mnenja s področja varstva osebnih podatkov in vse odločbe, 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,
- sodbe 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,
- register zbirk osebnih podatkov, katalog informacij javnega značaja Informacijskega pooblaščenca, poveyCentralni katalog informacij javnega značaja in register zbirk osebnih podatkov,
- e-novice, na katere se lahko posamezniki, ki želijo biti seznanjeni z dogajanjem na obeh področjih v Sloveniji in tujini, prijavijo.

Informacijski pooblaščenec je tudi leta 2012 obeležil Evropski dan varstva osebnih podatkov, ki je 28. januarja, in v ta namen organiziral dogodek, s katerim je želel opozoriti na varstvo osebnih podatkov pri uporabi družbenih omrežij na spletu. Pripravil je javni natečaj za srednješolce, na katerem je izbral najboljši kratki film na temo Varstvo osebnih podatkov in spletna družbena omrežja. Med prijavljenimi kratkimi filmi je natečajna komisija izbrala tri najboljše:

1. nagrado za kratki film z naslovom Varstvo osebnih podatkov in družbena omrežja so prejeli dijaki z Gimnazije in ekonomske srednje šole Trbovlje;
2. nagrado za kratki film z naslovom Nepovabljeni je prejela dijakinja iz Srednje ekonomske šole Kamnik;

3. nagrado za kratki film z naslovom WTF (Welcome to Facebook) pa so prejeli dijaki iz Šolskega centra Celje.

Spletna družbena omrežja so namreč fenomen, ki je v zadnjih letih dodobra spremenil naša življenja, načine komunikacije in preživljanje prostega časa. Kljub nespornim prednostim, ki jih ta omrežja imajo, so vse pogosteje v ospredju tudi njihove temne plati. Mladi družbena omrežja pogosto uporabljajo nekritično in odprto delijo velike količine svojih podatkov, temu pa nemalokrat sledijo mnoge neprijetnosti: zlorabe vsebin, nadlegovanja, kraje profilov in neprimerna uporaba osebnih podatkov. Mladi so tudi tisti, ki pogosto vodijo pri udejstvovanju na spletu in pri navdušenju nad sodobnimi komunikacijskimi sredstvi, a so hkrati bolj ranljivi. Ravno zato se je Informacijski pooblaščenec odločil, da dan varstva osebnih podatkov posveti njim. Sporočilo dogodka je bilo, da so družbena omrežja na spletu enaka tistim v realnem svetu, zato naj veljajo enaka pravila obnašanja, odgovornosti in previdnosti.

Ob tej priložnosti je Informacijski pooblaščenec drugič zapored podelil posebno priznanje za napore na področju vgrajene zasebnosti (privacy by design) Ambasador zasebnosti 2011. Nagrado je prejela ekipa podjetja Acros d.o.o. za Projekt SLED. Sodelujoči v projektu so na naslove številnih organizacij na podlagi zakonske pravice posameznika do seznanitve z lastnimi osebnimi podatki poslali obrazec z zahtevo po seznanitvi z lastnimi osebnimi podatki. Spraševali so jih, katere osebne podatke hranijo in v katerih zbirkah, komu in zakaj so jih posredovali, zakaj jih zbirajo, do kdaj jih bodo hranili, kako jih varujejo in obdelujejo ter ali so jih izvažali. Rezultat projekta je v duhu koncepta vgrajene zasebnosti z vidika proaktivnega delovanja marsikateremu upravljavcu osebnih podatkov pokazal njegove dolžnosti. Potencialne težave z vidika varstva osebnih podatkov in zasebnosti naj bi upravljavci osebnih podatkov namreč pravočasno predvideli in poslovne prakse vnaprej prilagodili na način, ki zmanjšuje tveganja za zlorabe, namesto da bi čakali, da se ta tveganja uresničijo.

Priznanja je dobilo še devet podjetij, ki so v letu 2011 pridobila certifikat po standardu za varovanje informacij ISO/IEC 27000 in s tem izkazala visoko raven zavarovanja osebnih podatkov: SmartIS d.o.o., Elektro energija d.o.o., Miška d.o.o., Mikrografija d.o.o., Dravske elektrarne Maribor d.o.o., Športna loterija d.d., ČETRTA POT d.o.o., GVA7 d.o.o. in Salviol d.o.o.

Svetovni dan pravice vedeti 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). Ob svetovnem dnevu pravice vedeti organizacije javnega in nevladnega sektorja, ki se ukvarjajo s tem področjem, opozarjajo na pomembnost transparentnosti in odgovornosti delovanja javnega sektorja ter zagotavljanja pogojev za bolj učinkovito participacijo državljanov pri odločanju o skupnih zadevah. Tudi Informacijski pooblaščenec že devet let s svojim delom opozarja na pomembnost pravice vedeti in pravice do dostopa do informacij javnega značaja. Žal je mnogo organov širšega javnega sektorja, ki jim ZDIJZ nalaga obveznost zagotavljanja dostopa do dokumentov, še vedno neodzivnih ali neupravičeno zavračajo zahteve prosilcev po dostopu do dokumentov. Kljub temu da je raziskava dveh nevladnih organizacij pokazala, da ima Slovenija enega najkvalitetnejših zakonov na področju dostopa do informacij javnega značaja z močnimi pritožbenimi mehanizmi, je dejstvo, da praksa dostopa do informacij v Sloveniji vseeno še ni tako učinkovita, kot bi lahko bila. Problem je namreč v slabi praksi nekaterih organov, ki ne odgovarjajo na zahteve prosilcev, se izmikajo odločanju ali zavračajo dostop do dokumentov iz razlogov, ki jih zakon sploh ne predvideva. Poleg tega je Informacijski pooblaščenec že ob mnogih priložnostih izpostavil problem, da družbe, v katerih ima država ali lokalna skupnost prevladujoč vpliv, niso zavezane k enaki stopnji transparentnosti svojih dokumentov. Informacijski pooblaščenec meni, da takšne gospodarske družbe, ki jih vse pogosteje ustanavljajo subjekti javnega prava, poslujejo z javnim denarjem in/ali pod vplivom javne oblasti, zato bi morala biti njihova odgovornost do javnosti toliko večja. Zaenkrat posluha za spremembo zakonodaje še ni bilo.

Informacijski pooblaščenec tako želi, da bi v praksi še bolj zaživelo pravilo, da morajo biti dokumenti javnega sektorja prosto dostopni kot pravilo, dostop do dokumentov pa se lahko zavrne le izjemoma. Navedeno se učinkoviteje doseže z aktivno oziroma proaktivno objavo informacij na svetovnem spletu, saj organi na ta način zelo pozitivno prispevajo k izboljšanju transparentnosti svojega dela. V Evropi je poleg zahtev po proaktivni objavi vedno večje količine dokumentov vedno bolj razširjen tudi institut t.i. ponovne uporabe informacij javnega značaja, za katerega je spletna objava informacij (predvsem v digitalnih in strojno berljivih formatih) še toliko pomembnejša. Podatki javnega sektorja, ki jih zasebni sektor pridobi, obdela in obogati, lahko namreč služijo kot surovina za ustvarjanje različnih proizvodov in storitev, predvsem na digitalnem trgu različnih aplikacij. Organi javnega sektorja pa žal še vedno ne vidijo makro ekonomskih učinkov ponovne uporabe (zaposlovanje v zasebnem sektorju in večji davčni prihodki) in gledajo le na svoje mikro okolje.

V zvezi s ponovno uporabo informacij javnega značaja je Informacijski pooblaščenec pripravil zloženko z naslovom Podatki – neusahljivi viri poslovnih idej!, ki jo je predstavil prav ob Svetovnem dnevu pravice vedeti. Z zloženko je Informacijski pooblaščenec želel tudi kot partner v projektu LAPSI (Legal Aspects of Public Sector Information) opozoriti na velik potencial ponovne uporabe informacij in pokazati, da obstaja v Evropi živahen trg s takšnimi informacijami. V zgibanki so prikazani različni primeri ponovne uporabe (npr. vremenskih, prometnih, nepremičninskih, finančnih in podobnih podatkov) in izpostavljeni trendi, ki so zavladali na tem področju.

Informacijski pooblaščenec je z izvajanjem različnih delavnic in seminarjev skrbel za stalno izobraževanje zavezancev, sodeloval je na različnih izobraževalnih konferencah, delavnicah in okroglih mizah. Prisoten je bil na spletnem družbenem omrežju Facebook, kjer s svojim profilom skrbi za dvig ozaveščenosti glede pomena varstva osebnih podatkov. Aktivno sodeluje tudi v projektih na področju varne rabe interneta SAFE-SI in Spletno oko. V okviru te dejavnosti je izvedel številna predavanja o varstvu osebnih podatkov na internetu za šolarje, učitelje in starše.

Informacijski pooblaščenec je tudi leta 2012 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 2012 je izdal Smernice glede iznosa osebnih podatkov v tretje države in Smernice za varstvo osebnih podatkov in računalništvo v oblaku.

V letu 2012 je Informacijski pooblaščenec zaradi ukrepov varčevanja zelo omejil tisk svojih publikacij in je izdal zgolj Letno poročilo Informacijskega pooblaščenca za leto 2011 v slovenščini ter v okviru sodelovanja v projektu LAPSI zloženko z naslovom Podatki – neusahljivi viri poslovnih idej!, ki jo je objavil tudi na spletni strani. Letno poročilo Informacijskega pooblaščenca za leto 2011 v angleščini je bilo objavljeno zgolj v elektronski obliki. Zgolj v elektronski obliki na spletni strani Informacijskega pooblaščenca so bile objavljene tudi zgoraj navedene smernice.

Center za raziskovanje javnega mnenja Politbarometer je tudi leta 2012 v okviru projekta Javnomnenjske raziskave o odnosu javnosti do aktualnih razmer in dogajanj v Sloveniji izvedel več raziskav. Raziskava iz meseca januarja 2012 vključuje tudi ocene zaupanja v nadzorne institucije sistema. Navedena raziskava je Informacijskega pooblaščenca uvrstila na prvo mesto med osrednjimi državnimi in družbenimi ustanovami, ki jim Slovenci najbolj zaupajo (52 %). Sledijo predsednik republike, zdravstvo, vojska, šolstvo. Informacijski po-

oblaščenec se je uvrstil najvišje oziroma so mu anketiranci izrazili najvišje zaupanje tudi v raziskavah v letu 2010 in 2011. To kaže na ustaljeno zaupanje ljudi v njegovo delovanje.

Skupnost informacijskih pooblaščencev in podobnih institucij, ki skrbijo za transparentnost in varstvo pravice dostopa do informacij, je oktobra leta 2011 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 ustvaril spletno stran info-commissioners.org. 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, novice o njihovem delovanju, informacije o pomembnih dogodkih, sprejetih prelomnih odločitvah itd. Informacijski pooblaščenec je tudi v letu 2012 skrbel za delovanje navedene spletne strani.

4.3. Mednarodno sodelovanje

4.3.1. Sodelovanje na mednarodnih srečanjih

Leta 2012 so se zaposleni pri Informacijskem pooblaščencu udeležili več mednarodnih seminarjev in konferenc. Na nekaterih so sodelovali tudi s svojimi prispevki:

- 22. – 24. februar 2012, Haag, Nizozemska - namestnik informacijske pooblaščenke mag. Andrej Tomšič je kot član mednarodne inšpekcijske ekipe sodeloval pri inšpekcijskem nadzoru Urada za evropsko pravosodno sodelovanje (Eurojust).
- 22. – 23. marec 2012, Budimpešta, Madžarska - v okviru projekta LAPSI v zvezi s ponovno uporabo informacij javnega sektorja sta potekala 6. tematski seminar in 3. interna konferenca. Dogodka sta se udeležili svetovalka Mojca Komac in raziskovalka Tina Kraigher.
- 23. – 24. april 2012, Sopot, Poljska - zasedanja skupine IWGDPT, mednarodne delovne skupine za varstvo osebnih podatkov v telekomunikacijah, sta se udeležila mag. Andrej Tomšič, namestnik informacijske pooblaščenke in Jure Logar, državni nadzornik za varstvo osebnih podatkov. Med drugim je bil na zasedanju sprejet Sopot Memorandum, ki obravnava varstvo osebnih podatkov pri računalništvu v oblaku.
- 3. – 4. maj 2012, Luksemburg - spomladanske konference evropskih pooblaščencev za varstvo osebnih podatkov 2012 so se udeležili državna nadzornika za varstvo osebnih podatkov Klemen Mišič in Jernej Dirnbek ter raziskovalka Tina Kraigher. Klemen Mišič je predstavil prispevek o pristojnostih in delovanju slovenskega Informacijskega pooblaščenca.
- 9. – 10. maj 2012, Dunaj, Avstrija - mag. Andrej Tomšič, namestnik informacijske pooblaščenke, se je udeležil tretjega simpozija o varstvu osebnih podatkov v organizaciji Evropske agencije za temeljne človekove pravice (European Union Agency for Fundamental Rights - FRA) in v panelu o neodvisnosti nadzornih organov za varstvo osebnih podatkov predstavil izkušnje Informacijskega pooblaščenca.
- 14. – 15. maj 2012, Bruselj, Belgija - pod okriljem Mednarodne zveze za informatiko v medicini (International Medical Informatics Association) je potekalo srečanje z naslovom Summit on Trustworthy Reuse of Health Data. Srečanja se je udeležila raziskovalka Tina Kraigher.
- 20. – 22. maj 2012, Kijev, Ukrajina - srečanja skupine CEEDPA, skupine srednjeevropskih in vzhodnoevropskih organov za varstvo osebnih podatkov, sta se udeležila državni nadzornik za varstvo osebnih podatkov Blaž Pavšič in raziskovalec Matic Petek.
- 28. 9. 2012, Zagreb, Hrvaška - svetovalec Urban Brulc se je s predavanjem o izkušnjah Informacijskega pooblaščenca na področju dostopa do tajnih podatkov in na področju proaktivne objave informacij udeležil konference Informacijama do demokracije, ki jo je v hrvaškem saboru pripravila hrvaška organizacija GONG. Ugleden in medijsko pokrit dogodek je bil organiziran ob Svetovnem dnevu pravice vedeti.
- 14. 11. 2012, Priština, Kosovo - državni nadzornik za varstvo osebnih podatkov

Klemen Mišič je na mednarodni okrogli mizi o dostopu do informacij, njihovi klasifikaciji (tajnost podatkov) in o varstvu osebnih podatkov, ki jo je organiziral Ženevski Center za demokratični nadzor nad oboroženimi silami (DCAF), predstavil pristojnosti Informacijskega pooblaščenca in pomen neodvisnega državnega organa pri varstvu podatkov.

4.3.2. Sodelovanje v mednarodnih delovnih telesih

Informacijski pooblaščenec kot državni nadzorni organ za varstvo osebnih podatkov sodeluje 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.

Zaradi znižanja proračunskih sredstev se je Informacijski pooblaščenec v letu 2012 na EU ravni udeležil le najnujnejših plenarnih sestankov ter občasno še sestankov štirih izmed številnih podskupin Delovne skupine po 29. členu Direktive 95/46/ES. Skupaj je tako Informacijski pooblaščenec 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 podskupini Future of Privacy, Tehnološki podskupini, 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), ki Evropski komisiji daje strokovna mnenja s področja varstva osebnih podatkov, je lani sprejela več pomembnih mnenj, med drugim mnenje o računalništvu v oblaku, o piškotkih, ki so izvzeti iz zahteve po soglasju, o razvoju na področju biometričnih tehnologij ter o prepoznavanju obrazov v spletnih in mobilnih storitvah. Delovna skupina je nadaljevala z obravnavo različnih delov predloga reforme varstva osebnih podatkov – Uredbe o varstvu osebnih podatkov in Direktive o varstvu podatkov, ki se obdelujejo v okviru policijskega in pravosodnega sodelovanja v kazenskih zadevah. Skupina se je sestala s poročevalcema Evropskega parlamenta za reformni paket. Predvsem pa se je delo skupine osredotočilo na v predlogu Uredbe predvidene mehanizme sodelovanja med nadzornimi organi, da se zagotovi najvišja raven zaščite posameznikovih pravic, povezanih z varstvom osebnih podatkov. V praksi pa takšni mehanizmi sodelovanja že potekajo, kar se je v letu 2012 najbolj pokazalo na primeru Googla, ko je francoski nadzorni organ v imenu in ob sodelovanju vseh nadzornih organov držav članic začel postopek ugotavljanja skladnosti Googlove nove politike zasebnosti z evropskimi predpisi o varstvu osebnih podatkov. Delovna skupina je spremljala tudi priprave v Združenih državah Amerike na sprejem Zakona o pravici do zasebnosti potrošnikov, ki naj bi predstavljal velik napredek glede obravnave varstva osebnih podatkov v Združenih državah Amerike ter zaradi globalizacije in elektronskih poti posledično tudi po celem svetu.

V okviru delovne skupine po 29. členu je Informacijski pooblaščenec aktivno sodeloval tudi v štirih njenih podskupinah, in sicer v (1) podskupini Future of Privacy, (2) v podskupini za internet in informacijske tehnologije, t.i. Tehnološki podskupini, (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). Podskupina Future of Privacy je v letu 2012 nadaljevala z delom na temo prenove Direktive 95/46/ES o varstvu osebnih podatkov in prispevala stališča evropskih nadzornih organov na reformne predloge Evropske komisije. Glede tega je izdala dve mnenji, ki sta bili sprejeti na plenarnih zasedanjih Delovne skupine po 29. členu. Tehnološka podskupina

se je v letu 2012 ukvarjala predvsem z mnenjem o tehnologijah za prepoznavo obrazov v spletnem in mobilnem okolju, mnenjem o izjemah pri piškotkih in mnenjem o računalništvu v oblaku, veliko časa je posvetila temi pametnih naprav in mobilnih aplikacij, nadzoru nad obdelavo osebnih podatkov s strani družbenega omrežja Facebook, ki ga je izvajal irski organ za varstvo osebnih podatkov, novim politikam zasebnosti, ki jih je objavil Google, in novim določbam o obveznem poročanju o kršitvah varstva osebnih podatkov pri operaterjih elektronskih komunikacij. V okviru podskupine BCR je Informacijski pooblaščenec nadaljeval z delom pri pripravi potrebnih podlag 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. Pripravljena je bila tabela z glavnimi elementi in načeli ter vzorec prijave. Informacijski pooblaščenec je sodeloval tudi v podskupini BTLE, ki se je formirala v letu 2011 ter prevzela in deloma razširila vsebino, s katero se je pred tem ukvarjala Delovna skupina za varstvo osebnih podatkov v okviru policijskega in pravosodnega sodelovanja (WPPJ), ki je s tem prenehala delovati. Podskupina BTLE se je v letu 2012 osredotočala na evidence podatkov o potnikih v letalskem prometu, iznos API podatkov v tretje države, t.i. EU Smart Border Programme, predlog Uredbe o uvedbi evropskega sistema nadzorovanja meja (EUROSUR), predlog Direktive o evropskem preiskovalnem nalogu, predlog Uredbe o Eurodacu, sporazum EU-US TFTP2 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.

Poleg sodelovanja v navedenih štirih delovnih podskupinah je Informacijski pooblaščenec v lanskem letu začel sodelovati v delovni podskupini e-Government, in sicer glede priprave mnenja o ponovni uporabi informacij javnega značaja z vidika obdelave osebnih podatkov.

Informacijska pooblaščenka je v lanskem letu nadaljevala svoj drugi mandat kot podpredsednica Skupnega nadzornega organa za Europol.

Februarja 2012 je namestnik informacijske pooblaščenke sodeloval v mednarodni inšpekcijski skupini, ki je na sedežu v Haagu opravila nadzor nad varstvom osebnih podatkov v Uradu za evropsko pravosodno sodelovanje (Eurojust).

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 se je v letu 2012 ukvarjala predvsem z vprašanjem pravice do pozabe, na svojem zasedanju v Sopotu na Poljskem pa je sprejela t.i. Sopot memorandum (Cloud Computing – Privacy and data protection issues).

V okviru Sveta Evrope je predstavnik Informacijskega pooblaščenca tudi v letu 2012 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 dveh plenarnih zasedanjih, v juniju in novembru, obravnaval predvsem predloge sprememb v tako imenovanem procesu posodabljanja Konvencije št. 108, ki poteka od začetka leta 2011. Na zadnjem plenarnem zasedanju je Odbor končal ta projekt v okviru svoje pristojnosti s sprejetjem delovnega besedila. Odbor je obravnaval tudi proces sprememb in posodabljanja priporočil Sveta Evrope o varstvu osebnih podatkov na področju zaposlovanja in na policijskem področju, ki poteka že drugo leto. Kot vsako leto je Odbor obravnaval poročila o mednarodnem in globalnem sodelovanju Sveta Evrope v zvezi z varstvom osebnih podatkov in 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 Evropskega 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 2012 Informacijski pooblaščenec ni prejel nobene pritožbe glede izvajanja te pravice na prvi stopnji.

Informacijski pooblaščenec je v letu 2012 gostil predstavnike sorodnih institucij iz nekaterih evropskih in drugih držav, kot so Srbija, Gruzija, Makedonija, Albanija in jim predstavil svoje delovanje ter dobre prakse s področij, za katere je pristojen.

Informacijski pooblaščenec je v letu 2012 pripravil odgovore na 62 vprašanj in vprašalnikov tujih organov za varstvo osebnih podatkov, mednarodnih organizacij in tujih nevladnih organizacij.

V letu 2012 je Informacijski pooblaščenec kot Junior Partner uspešno zaključil projekt tesnega medinstitucionalnega sodelovanja IPA 2009, št. MN/09/IB/JH/03 – Implementation of Personal Data Protection Strategy v Črni gori, samostojno pa je začel izvajati twinning light projekt SR/2009/IB/JH/01 – Improvement of Personal Data Protection v Srbiji.

Informacijski pooblaščenec je v lanskem letu nadaljeval in septembra zaključil 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.

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:

Klemen Mišič in Bons, d. o. o.

Fotografije:

Fotolia in Klemen Mišič

Lektorirala:

Vesna Veingerl, univ. dipl. nov.

Informacijski pooblaščenec Republike Slovenije
Zaloška cesta 59
1000 Ljubljana

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

Ljubljana, maj 2013