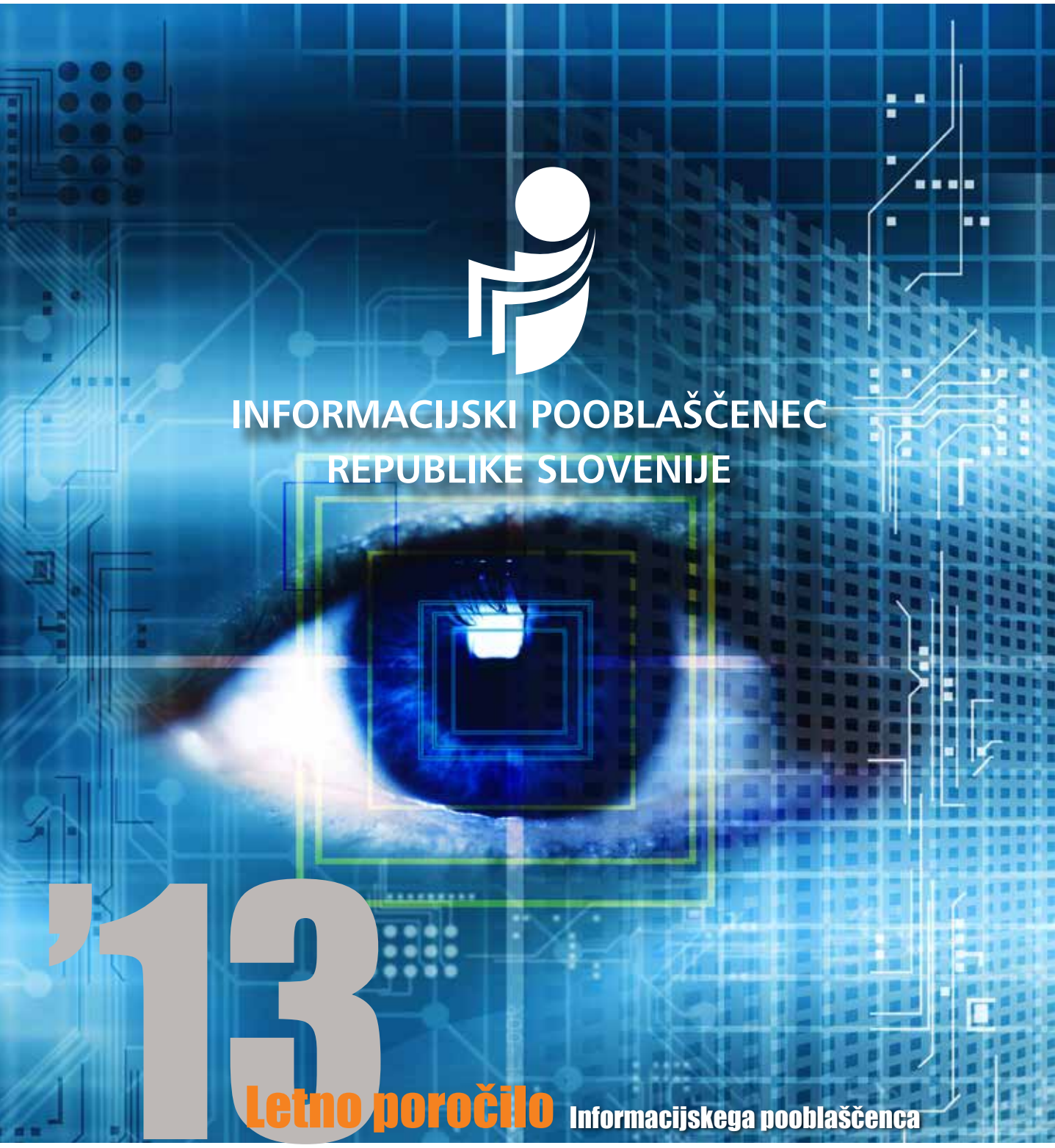


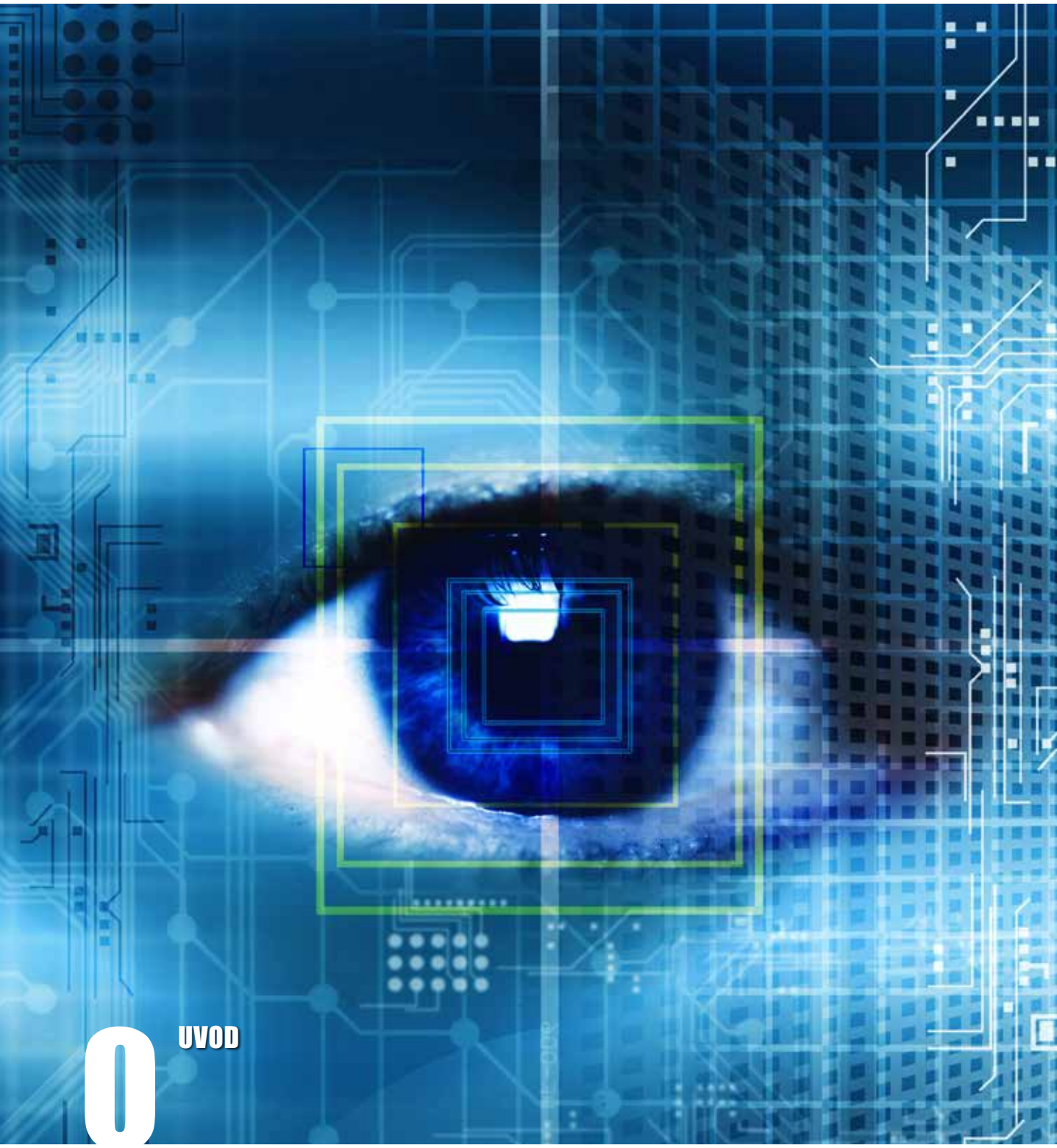
INFORMACIJSKI POOBLAŠČENEC
REPUBLIKE SLOVENIJE

'13 Letno poročilo Informacijskega pooblaščenca

za leto 2013

'13 Letno poročilo

Informacijskega pooblaščenca za leto 2013



0 UVOD

Leto 2013 pomeni deseto obletnico delovanja Informacijskega pooblaščenca, ki je iz Pooblaščenca za dostop do informacij javnega značaja, sprva majhnega pritožbenega organa, prerasel v pomembnega poroka transparentnosti in varuha osebnih podatkov. Prav tako je leto 2013 zadnje polno leto mojega desetletnega mandata informacijske pooblaščenke, ki sem mu posvetila deset čudovitih let svojega življenja, ki se jih bom vedno z veseljem spominjala.

Informacijski pooblaščenec je tudi v preteklem letu na obeh področjih delovanja vnovič prejel (rekordno) veliko število vlog posameznikov, in sicer zaprosil za mnenja, prijav in pritožb. To je sicer po eni strani razveseljujoče, ker nedvomno priča o tem, da posamezniki vse bolj razumejo namen in pomen obeh človekovih pravic v pristojnosti Informacijskega pooblaščenca. Hkrati pa ne smemo spregledati dejstva, da gre tudi v preteklem letu tolikšno povečanje števila pritožbenih in inšpekcijskih zadev pripisati nadaljevanju trenda nekaterih skrb vzbujajočih ravnanj organov zavezancev na področju dostopa do informacij javnega značaja, na drugi strani pa vse manj obvladljivih želja po obdelavi osebnih podatkov najrazličnejših upravljavcev zbirk osebnih podatkov tako v zasebnem kot v javnem sektorju.

Leto 2013 je prineslo pomembne prelomnice, zaradi katerih smo doumeli, kako veliko lahko izgubimo z žrtvovanjem zasebnosti. Odmevne afere, povezane s posegi v zasebnost, so razkrile, kako hudi posegi v zasebnost se nam v resnici dnevno dogajajo in kako šibki smo kot posamezniki, če državi nadzor uide iz rok. S strani Evropske komisije sem bila imenovana v posebno ad hoc skupino EU–ZDA, ki je ugotavljala, kakšne so dejanske aktivnosti ameriške preiskovalne agencije (National Security Agency) glede množičnega zbiranja informacij in osebnih podatkov o državljanih Evropske unije, in na koncu pripravila posebno poročilo. V preteklem letu smo naredili tudi velik korak k boljšemu zagotavljanju transparentnosti delovanja (slovenske) države in najširšega javnega sektorja. Priprava sprememb Zakona o dostopu do informacij javnega značaja in razlogi zanje so pokazali, da država lahko in mora delovati bistveno bolj transparentno. Priprava zadnje novele omenjenega zakona, ki je stopila v veljavo 17. aprila letos in bo veliko pripomogla k večji transparentnosti, je tudi posledica vztrajnih pozivov Informacijskega pooblaščenca k večji preglednosti delovanja podjetij v državni in občinski lasti ter v lasti javnih zavodov. Informacijski pooblaščenec je nosilce oblasti v zadnjih letih večkrat pozval, naj preidejo od besed k dejanjem ter zagotovijo večjo preglednost poslovanja gospodarskih družb v državni ali občinski lasti; ves čas je tudi aktivno sodeloval pri pripravi zakonskih sprememb.

Informacijski pooblaščenec je tako na različnih ravneh vnovič odigral pomembno vlogo pri ukrepanju proti nakazanim pomanjkljivostim v ustroju družbe in države. Informacijski pooblaščenec se je v desetih letih oblikoval v zaupanja vreden in spoštovan državni pritožbeni organ za področje dostopa do informacij javnega značaja ter nadzorni organ za varstvo osebnih podatkov. To si upam trditi tako glede na rezultate javnomnenjskih raziskav kot glede na odziv ljudi, ki se na nas obračajo, glede na odzive kolegov iz tujine ter še posebej glede na sodbe, ki jih izrekajo sodišča, kadar presojajo vložena pravna sredstva zoper naše odločitve in nam pri tem v veliki večini primerov pritrdijo.

Pot, ki smo jo s sodelavci prehodili v teh desetih letih, ni bila lahka. Bila pa je polna izredno zanimivih izzivov, učenja, dobrega sodelovanja in tudi lepih trenutkov v odličnem kolektivu strokovnjakov, ki jim, tako kot meni, vsak dan znova ni vseeno, kako dobro in učinkovito sta uveljavljeni dve pomembni ustavni pravici: pravica do dostopa do informacij javnega značaja ter pravica do varstva osebnih podatkov.

Tako osebni podatki kot informacije javnega značaja so valuta informacijske dobe, zato so izzivi, ki čakajo novega pooblaščenca ali pooblaščenko, veliki. Ne dvomim, da mu oziroma ji bo ob podpori odlične ekipe, ki ostaja, kos in da bo Informacijski pooblaščenec svoje delo še naprej opravljal po svojih najboljših močeh, v dobro tistih, ki vladajo, in vseh, ki živimo v Sloveniji.

S spoštovanjem,

Nataša Pirc Musar,
informacijska pooblaščenka

KAZALO

1. PRELOMNIH DESET LET ZA TRANSPARENTNOST IN ZASEBNOST - VLOGA INFORMACIJSKEGA POOBLAŠČENCA

1.1. Ustanovitev in vloga Informacijskega pooblaščenca 1
1.2. Pregled pomembnih sprememb za zagotavljanje večje transparentnosti v Sloveniji 1
1.2.1. Najpomembnejše prelomnice na področju transparentnosti 1
1.2.2. Prelomne odločitve Informacijskega pooblaščenca, ki so vplivale na uveljavljanje transparentnosti v praksi 3
1.3. Pregled pomembnih sprememb za zagotavljanje varstva osebnih podatkov v Sloveniji 5
1.3.1. Najpomembnejše prelomnice na področju varstva osebnih podatkov 5
1.3.2. Prelomne odločitve Informacijskega pooblaščenca, ki so vplivale na zagotavljanje varstva osebnih podatkov v praksi 7
1.4. Druga pomembna področja dela Informacijskega pooblaščenca v preteklih desetih letih 10
1.5. Vpliv Informacijskega pooblaščenca na razvoj področja transparentnosti in varstva osebnih podatkov na mednarodni ravni in na ravni Evropske unije in sodelovanje v mednarodnih projektih 12
1.6. Ključni izzivi v prihodnjih petih letih na področju transparentnosti po oceni Informacijskega pooblaščenca 13
1.7. Ključni izzivi v prihodnjih petih letih na področju zasebnosti po oceni Informacijskega pooblaščenca 14

2. SPLOŠNO O DELU INFORMACIJSKEGA POOBLAŠČENCA

2.1. Pristojnosti Informacijskega pooblaščenca 17
2.2. Organiziranost Informacijskega pooblaščenca 21
2.3. Finančna sredstva Informacijskega pooblaščenca 22

3. DELO NA PODROČJU DOSTOPA DO INFORMACIJ JAVNEGA ZNAČAJA

3.1. Pravna ureditev na področju dostopa do informacij javnega značaja v Republiki Sloveniji 27
3.2. Število vloženih pritožb in število rešenih zadev 27
3.3. Število vloženih tožb na Upravnem sodišču Republike Slovenije, število sodb Upravnega in Vrhovnega sodišča Republike Slovenije 29

3.4.	Statistika po posameznih področjih ZDIJZ	29
3.5.	Storjeni prekrški po ZDIJZ, ZInfP in ZMed	33
3.6.	Predstavitev najodmevnejših in precedenčnih primerov po področjih	33
3.6.1.	Notranje delovanje organa	33
3.6.2.	Ali dokument obstaja	34
3.6.3.	Test javnega interesa, javni uslužbenci, notranje delovanje	35
3.6.4.	Tajni podatki, umik stopnje tajnosti	36
3.6.5.	Notranje delovanje organa	37
3.6.6.	Okoljski podatki	38
3.6.7.	Avtorsko delo	30
3.6.8.	Poslovna skrivnost, test javnega interesa	41
3.6.9.	Davčna tajnost, notranje delovanje, javni uslužbenci	42
3.6.10.	Poslovna skrivnost	43
3.6.11.	Ponovna uporaba informacij javnega značaja	44
3.7.	Splošna ocena in priporočila na področju dostopa do informacij javnega značaja	45

4. DELO NA PODROČJU VARSTVA OSEBNIH PODATKOV

4.1.	Koncept varstva osebnih podatkov v Republiki Sloveniji	49
4.2.	Dejavnost državnih nadzornikov za varstvo osebnih podatkov	50
4.2.1.	Pravice in dolžnosti državnega nadzornika	50
4.2.2.	Inšpekcijski nadzor	50
4.2.3.	Storjeni prekrški	53
4.3.	Dajanje pisnih mnenj in pojasnil	56
4.4.	Dopustnost izvajanja biometrijskih ukrepov	57
4.5.	Ugotavljanje ustrezne ravni varstva osebnih podatkov v tretjih državah	64
4.6.	Izdajanje dovoljenj za povezovanje javnih evidenc	69
4.7.	Seznanitev z lastnimi osebnimi podatki	70
4.8.	Zahteve po presoji ustavnosti zakonov	72
4.9.	Izbrani primeri kršitev varstva osebnih podatkov	78
4.9.1.	Snemanje telefonskih pogovorov s strani javnega zavoda	78
4.9.2.	Pomanjkljivo zavarovanje občutljivih osebnih podatkov s strani zdravstvene ustanove	79
4.9.3.	Policijska pooblastila pri dostopih do podatkov uporabnikov spleta	80
4.9.4.	Izguba podpisov volivcev za razpis zakonodajnega referenduma	81
4.9.5.	Predčasno uničenje zdravstvene dokumentacije	82
4.9.6.	Objava osebnih podatkov strank servisa na "ekranu dobrodošlice"	83
4.9.7.	Zahteva posameznika po prenehanju obdelave osebnih podatkov za namen opravljanja dimnikarskih storitev	84
4.10.	Splošna ocena stanja varstva osebnih podatkov in priporočila	86

5. DRUGE DEJAVNOSTI INFORMACIJSKEGA POOBLAŠČENCA

5.1.	Sodelovanje pri pripravi zakonov in drugih predpisov	93
5.2.	Sodelovanje z javnostmi	96
5.3.	Mednarodno sodelovanje	99
5.3.1.	Sodelovanje v mednarodnih delovnih telesih	99
5.3.2.	Ostale mednarodne dejavnosti	101
5.3.3.	Sodelovanje na mednarodnih srečanjih	101

1 PRELOMNIH DESET LET ZA TRANSPARENTNOST IN ZASEBNOST – VLOGA INFORMACIJSKEGA POOBLAŠČENCA

Ruski borec za transparentnost Ivan Pavlov je ob neki priložnosti dejal: »Človekove pravice so kot mišice, če jih ne uporabljamo, atrofirajo.«

1.1. Ustanovitev in vloga Informacijskega pooblaščenca

Informacijski pooblaščenec deluje od leta 2003; sprva je deloval kot Pooblaščenec za dostop do informacij javnega značaja, torej pritožbeni organ za področje dostopa do informacij javnega značaja s štirimi zaposlenimi. Leta 2006 je s sprejemom Zakona o Informacijskem pooblaščencu ter z združitvijo Pooblaščenca za dostop do informacij javnega značaja in Inšpektorata za varstvo osebnih podatkov nastal Informacijski pooblaščenec, kot ga poznamo danes, ko ima 30 zaposlenih ter združuje pristojnosti pritožbenega organa za dostop do informacij javnega značaja ter nadzornega organa za varstvo osebnih podatkov.

Obseg dela Informacijskega pooblaščenca je od jeseni 2003 strmo naraščal. Že leta 2006 je Informacijski pooblaščenec prejel 504 pritožbe in izdal 101 odločbo na področju dostopa do informacij javnega značaja, prejel je 231 prijav kršitev varstva osebnih podatkov in uvedel 180 inšpekcijskih postopkov. Do leta 2013 je število pritožb, povezanih z zahtevami za dostop do informacij javnega značaja, zraslo na 610 (izdanih je bilo 258 odločb), število inšpekcijskih zadev na področju kršitev varstva osebnih podatkov pa na 712.

Odziv posameznikov kaže, da je Informacijski pooblaščenec svoje delo zastavil dobro, saj je že javnomnenjska raziskava o zaupanju ljudi v institucije Politbarometer leta 2008, ko je v raziskavo prvič uvrstila tudi Informacijskega pooblaščenca, pokazala, da mu zaupa kar 47 % anketiranih, s čimer se je uvrstil na četrto mesto, takoj za predsednika Republike Slovenije (55 %), evro (53 %) in Banko Slovenije (49 %). Podobno visoko se je v isti raziskavi Informacijski pooblaščenec uvrščal tudi pozneje. Tako se je januarja 2013 informacijska pooblaščenka glede na ocene ljudi uvrstila v sam vrh nosilcev vlog v državnih nadzornih organih, izenačeno sta ji sledila varuhinja človekovih pravic Zdenka Čebašek - Travnik in predsednik Računskega sodišča RS Igor Šoltes.

Rezultati dela Informacijskega pooblaščenca se kažejo tudi v visoki stopnji osveščenosti širše javnosti. Javnomnenjska raziskava Eurobarometer o zaznavanju, stališčih in pogledih državljanov v vseh 27 državah članicah glede varstva osebnih podatkov in dojemanja upravljavcev osebnih podatkov, ki jo je konec aprila 2008 objavila Evropska unija (EU), je pokazala, da se Slovenija po poznavanju problematike pri večini merjenih področij uvršča v sam vrh EU.

Na področju dostopa do informacij javnega značaja pa visoko raven varstva pravice do dostopa do informacij javnega značaja dokazuje tudi leta 2013 objavljena raziskava Mednarodnih organizacij Access Info Europe (Španija) in Centre for Law and Democracy (Kanada), ki med 89 državami na področju zakonske ureditve dostopa do informacij javnega značaja Slovenijo uvršča na zavidljivo drugo mesto. Rast števila pritožb na tem področju kaže, da se tudi posamezniki vse bolj zavedajo svojih pravic, s čimer skupaj z Informacijskim pooblaščencem organe zavezance silijo k učinkovitemu izvajanju Zakona o dostopu do informacij javnega značaja (ZDIJZ).

1.2. Pregled pomembnih sprememb za zagotavljanje večje transparentnosti v Sloveniji

1.2.1. Najpomembnejše prelomnice na področju transparentnosti

1. Povečanje transparentnosti na področju porabe javnih sredstev – Tudi kot posledica odločitev Informacijskega pooblaščenca (npr. odločba št. 020-19/2003/19 z dne 17. 8. 2004, s katero je novinar od pisarne bivšega predsednika Republike Slovenije zahteval poimenske podatke o udeležencih, ki jih je bivši predsednik gostil na večerji v vili Podrožnik) je bil leta 2005 noveliran ZDIJZ z določbo 3. odstavka 6. člena, po kateri so podatki o porabi javnih sredstev, ne glede na morebitne izjeme, vedno javno dostopni.

2. Povečanje transparentnosti na področju javnih naročil – Tudi kot posledica prakse Informacijskega pooblaščenca (npr. odločbi št. 021-75/2008/7 in 021-105/2007/9, v

katerih sta prosilca, sicer ponudnika v predmetnih postopkih javnega naročanja, zahtevala seznanitev s podatki iz ponudb v okviru postopkov javnega naročanja ministrstev) je bila leta 2010 novelirana določba 22. člena Zakona o javnem naročanju, ki sedaj izrecno določa, da so javni podatki v postopku javnega naročanja količina iz specifikacije, cena na enoto, vrednost posamezne postavke in skupna vrednost iz ponudbe, če je merilo, katera ponudba je ekonomsko najugodnejša, pa tisti podatki, ki so vplivali na razvrstitev ponudbe v okviru drugih meril.

3. Uvedba testa javnega interesa z novelo ZDIJZ iz leta 2005 – Informacijski pooblaščenec je še pred prvo spremembo ZDIJZ večkrat opozoril na pomen tehtanja med različnimi človekovimi pravicami v postopku v zvezi z zahtevami za dostop do informacij javnega značaja. Test javnega interesa oz. test tehtanja je npr. izvedel leta 2004, in sicer v zadevi št. 020-10/2004/4, v kateri je novinar zahteval podatke o plačah vodilnih zaposlenih na RTV Slovenija.

4. Javnost plač v javnem sektorju – Tudi kot posledica odločitve Informacijskega pooblaščenca v primeru zahteve novinarja po podatku o plačah nekdanjih javnih uslužbencev v zadevi št. 020-10/2004/4 je bil leta 2005 spremenjen 38. člen Zakona o sistemu plač v javnem sektorju (ZSPJS). Dodana je bila določba 6. odstavka 38. člena ZSPJS, ki izrecno določa, da so javnosti po postopku, ki ga ureja ZDIJZ, dostopni individualni podatki o znesku celotne bruto plače vsakega javnega uslužbenca in vsakega funkcionarja brez zmanjšanja za morebitne odbitke zaradi izvršbe, kreditov ali drugih osebnih obveznosti.

5. Javnost podatkov o prihodkih notarjev – Informacijski pooblaščenec je leta 2004 v zadevi št. 020-50/2004 obravnaval zahtevo novinarke, naslovljeno na več notarjev, za posredovanje podatkov iz letnih bilanc o prihodkih in dobičku iz javnopravnega dela opravljanja notarske dejavnosti. Zavzel je stališče, da gre za prosto dostopne informacije javnega značaja. V postopku pred Vrhovnim sodiščem RS s tem stališčem sicer ni uspel, vendar je bil leta 2006 posledično spremenjen Zakon o notariatu, ki sedaj v 2. odstavku 2. člena izrecno določa, da so prihodki notarjev kot oseb javnega zaupanja javni, za potrebe varovanja ugleda notariata kot javne službe in za zagotavljanje zaupanja strank glede delovanja notariata kot javne službe.

6. Proaktivna objava podatkov o podeljenih javnih sredstvih – Tudi kot posledica prakse Informacijskega pooblaščenca je npr. Eko sklad začel objavljati prejemnike nepovratnih finančnih spodbud, ministrstva pa prejemnike javnih sredstev, podeljenih na različnih razpisih.

7. Večja transparentnost na področju zaposlovanja javnih uslužbencev in njihovih delovnih razmerij – Informacijski pooblaščenec je v več zadevah (npr. odločba št. 021-70/2005/17 z dne 21. 11. 2005) s široko interpretacijo, ki je v prid transparentnosti, vzpostavil dobro prakso na področju javne dostopnosti dokumentov, ki so povezani z delovnimi razmerji javnih uslužbencev (npr. dokumenti, ki izkazujejo, ali javni uslužbenec izpolnjuje pogoje za zasedbo delovnega mesta).

8. Večja transparentnost delovanja pravnih oseb javnega prava sui generis – Informacijski pooblaščenec je v več zadevah (npr. odločba zoper SOD – št. 020-61/2004/21, KAD – št. 090-108/2009, Študentska organizacija Univerze v Mariboru – št. 021-6/2008/1 ...) opozoril na netransparentnost delovanja pravnih oseb javnega prava sui generis in zavzel stališče, da so tudi te organizacije zavezanke po ZDIJZ. Da je bilo stališče pravilno, je večkrat potrdilo tudi Vrhovno sodišče RS, predmetne odločitve pa so prispevale k bolj transparentnemu delovanju teh zavezancev v praksi.

9. Vzpostavitev dobre prakse na področju presoje izjeme tajnih podatkov – Informacijski pooblaščenec je v več zadevah (npr. odločbe št. 020-44/2004/3, 021-33/2005/5 in 090-157/2010) opozoril, da je izjemo tajnih podatkov treba presojati izjemno restriktivno ter upoštevaje materialni in formalni kriterij, ki ju za tajne podatke določa Zakon o tajnih podatkih (ZTP). Na podlagi odločitve v zadevi št. 090-157/2010 je bila javnosti razkrita večina dokumentov iz t. i. trgovine z orožjem med letoma 1991 in 1994, s katero v glavnem razpolagata Ministrstvo za obrambo in Državni zbor RS.

10. Novela ZDIJZ, s katero se krog zavezanih organov širi tudi na poslovne subjekte, ki so pod prevladujočim vplivom države, lokalnih skupnosti in drugih pravnih oseb javnega prava

– Informacijski pooblaščenec je nosilce oblasti v zadnjih letih večkrat pozval, naj preidejo od besed k dejanjem ter načelne zaveze prelijejo v zakonske rešitve v prid preglednosti poslovanja gospodarskih družb v državni ali občinski lasti, zato zadnjo novelo ZDIJZ v celoti podpira.

11. Sprejem Konvencije Sveta Evrope o dostopu do uradnih dokumentov (Slovenija je bila med prvimi 12 podpisnicami) – Slovenija in kot strokovnjakinja v okviru Sveta Evrope informacijska pooblaščenka Nataša Pirc Musar sta igrali pomembno vlogo pri oblikovanju konvencije, ki postavlja minimalne standarde glede pravice posameznikov do dostopa do uradnih dokumentov. Ta pravica bo po uspešnih ratifikacijah v članicah Sveta Evrope postala tudi mednarodno priznana temeljna človekova pravica. Žal Slovenija konvencije še ni ratificirala.

1.2.2. Prelomne odločitve Informacijskega pooblaščenca, ki so vplivale na uveljavljanje transparentnosti v praksi

Informacijski pooblaščenec je v odločbi št. 020-10/2004/4 v zvezi z zahtevo novinarja časnika Delo, ki je od Javnega zavoda RTV Slovenija zahteval podatke o plačah, izplačilih za delovno uspešnost, nagradah in dodatkih k plači za nekatere vodilne javne uslužbence RTV Slovenija, na podlagi testa tehtanja javnega interesa, ob oceni razmerja med pravico vedeti kot delom pravice do svobodnega izražanja ter pravico do varstva osebnih podatkov, ocenil, da so zahtevani podatki javni, saj prevlada javni interes, ki ima v konkretnem primeru prevladujoč vpliv. Zoper predmetno odločbo je bila sicer vložena tožba, Informacijski pooblaščenec pa s svojimi argumenti na sodišču ni uspel. Je bila pa prav ta odločba povod za široko javno razpravo o pomenu transparentnosti plač v javnem sektorju, posledično pa tudi za spremembo zakona, ki ureja sistem plač v javnem sektorju in po katerem so plače javnih uslužbencev javne.

Informacijski pooblaščenec je v pritožbenem postopku št. 021-75/2008/7 ugodil pritožbi prosilca glede dostopa do ponudbene dokumentacije vseh ponudnikov za javno naročilo čistilnega in toaletnega materiala Ministrstva za obrambo, in sicer v delu, ki se nanaša na ustreznost ponujenega proizvoda posameznega ponudnika glede na zahteve naročnika ter odstotek porabe ponujenega sredstva. Ugotovil je, da gre v omenjenem primeru za prosto dostopne informacije javnega značaja, saj gre za merilo oziroma z merilom neposredno povezan podatek, brez katerega ni mogoče ugotoviti, katera ponudba je najugodnejša oz. najnižja, kar je bil v obravnavanem javnem naročilu ocenjevalni kriterij.

V okviru pritožbenega postopka proti Slovenski odškodninski družbi (SOD) je Informacijski pooblaščenec v odločbi št. 020-61/2004/21 odločil, da je SOD nedvomno zavezanec za dostop do informacij javnega značaja. Edini ustanovitelj in delničar SOD je namreč Republika Slovenija, ki je tudi vplačala z zakonom določen osnovni kapital, Vlada RS pa ima pristojnosti skupščine organa.

V okviru pritožbenega postopka je Informacijski pooblaščenec v odločbi št. 021-33/2005/5, v zvezi z zahtevo prosilca za dostop do analize stanja na slovenskem igralniškem trgu, ki je bila naslovljena na Ministrstvo za finance, odločil, da gre za prosto dostopne informacije javnega značaja. Zahtevani dokument, kljub oznaki zaupno, namreč po vsebini ne predstavlja dokumenta, ki bi v skladu s 5. členom ZTP sploh lahko bil opredeljen kot tajen.

Informacijski pooblaščenec je na podlagi zahteve dveh novinarjev Državnemu zboru RS za dostop do celotne dokumentacije, ki se nanaša na trgovino z orožjem med letoma 1990 in 1994 ter je nastala v okviru dela preiskovalnih parlamentarnih komisij v več pritožbenih postopkih (predvsem pa v pritožbenih postopkih št. 090-157/2010, 090-101/2010 ter 090-32/2009), pregledal nekaj tisoč dokumentov in v dveh letih izdal 11 odločb, s katerimi je prosilcem omogočil dostop do več tisoč dokumentov, povezanih z odmevno orožarsko afero. Ob tem je v okviru pritožbenega postopka posebno pozornost, poleg obsežnosti zahtevane dokumentacije, trejal izjemno velik obseg osebnih podatkov, ki so jih vsebovali dokumenti, ter preverjanje zakonitosti opredelitve posameznih dokumentov za tajne.

Informacijski pooblaščenec je v pritožbenem postopku št. 090-161/2009 odločal o pritožbi prosilca zoper odločbo Ministrstva za zdravje, s katero je to zavrnilo zahtevo

za vpogled v pogodbo med organom in farmacevtsko družbo, ki je dobavljala cepivo proti novi gripi. Informacijski pooblaščenec je zaključil, da je interes javnosti za razkritje informacij, ki se nanašajo na tveganje, jamstvo, odgovornosti za cepivo in odškodnine ter omejitve odgovornosti, močnejši od zasebnopravnega interesa gospodarske družbe, da te informacije varuje kot poslovno skrivnost. Informacijski pooblaščenec je ocenil, da pogodba ne predstavlja poslovne skrivnosti v celoti, ker gre v delu za informacije, ki so javne že na podlagi zakona, oziroma za informacije o porabi javnih sredstev, v delu pa je ugotovil, da javni interes za seznanitev z informacijami prevlada in je treba zahtevane informacije razkriti na podlagi 2. odstavka 6. člena ZDIJZ.

Informacijski pooblaščenec je v zvezi z zahtevo prosilca za posredovanje podatkov o dodeljenih sredstvih humanitarne pomoči po poplavah leta 2007 odločil (odločba št. 0900-23/2008/13), da so prosto dostopne informacije javnega značaja podatki o prejetih donacijah po poplavah po posameznih sklicih, brez poimenskih podatkov prejemnikov, ter poimenski podatki o izplačanih sredstvih po poplavah z naslova humanitarne pomoči fizičnim in pravnim osebam, saj gre v tem delu za podatke o porabi javnih sredstev, ki ne glede na to, da gre za osebne podatke, predstavljajo prosto dostopne informacije javnega značaja.

Informacijski pooblaščenec je v pritožbi (odločba št. 021-54/2006/3) glede zahteve za posredovanje zadnje razpoložljive različice topografskih slojev za celotno Slovenijo, v elektronski obliki, za namene neprofitne ponovne uporabe, odločil, da gre za prosto dostopne informacije javnega značaja, ki jih mora organ prosilcu posredovati brezplačno. Informacijski pooblaščenec je pri tem opozoril, da je za ponovno uporabo informacij ključno, da organi javnega sektorja informacije zbirajo predvsem za izvrševanje svojih javnih nalog, že zbrane informacije pa morajo, če gre za prosto dostopne informacije javnega značaja, posredovati prosilcem za nadaljnjo uporabo za pridobitne ali nepridobitne namene. Informacije javnega sektorja namreč financirajo javna proračunska sredstva in so kot take last plačnikov proračunskih sredstev, torej vseh državljanov, in ne organa, pri katerem so določene informacije nastale. Dejstvo, da je tudi organ lahko ponovni uporabnik informacij, ki nastanejo v okviru izvajanja njegovih javnopravnih funkcij, ne spremeni zahteve zakona, da mora organ pri tem upoštevati načelo prepovedi diskriminacije in ponovno uporabo teh informacij, pod enakimi pogoji, omogočiti vsem zainteresiranim prosilcem. V skladu s 34.a členom ZDIJZ pa lahko organ ponovno uporabo zaračuna le, če gre za ponovno uporabo v pridobitne namene. Upoštevaje dejstvo, da iz prosilčeve zahteve jasno izhaja, da bo zahtevano informacijo uporabil v nepridobitne namene, navedena določba tako ni prišla v poštev.

Informacijski pooblaščenec je na podlagi zahteve novinarja glede posredovanja magnetograma seje Vlade RS, na kateri je ta sprejela sklep o neodplačnem prenosu deleža v Splošni plovbi, d. o. o., na Slovensko odškodninsko družbo, d. d. (odločba št. 090-178/2010/6) v pritožbenem postopku odločil, da gre za prosto dostopno informacijo javnega značaja. Vladi RS namreč ni uspelo izkazati izjeme notranjega delovanja oziroma pojasniti, kako bi s posredovanjem zahtevanega dokumenta prosilcu pri njenem nadaljnjem delu nastale resne motnje.

Informacijski pooblaščenec je v pritožbenem postopku glede posredovanja pogodbe o javno-zasebnem partnerstvu med Mestno občino Maribor in družbo Iskra sistemi, d. d., pri projektu »Nadgradnje in avtomatizacije cestnega prometa v Mestni občini Maribor« glede postavitve radarjev (odločba št. 090-190/2012/14) odločil, da del zahtevanih dokumentov predstavlja prosto dostopne informacije javnega značaja. Čeprav organ iz mestnega proračuna zasebnemu partnerju ni neposredno izplačal nobenih sredstev, namreč iz sklenjene pogodbe izhaja, da se bo predmet pogodbe nedvomno financiral iz javnih sredstev, in sicer iz sredstev, pridobljenih z izterjanimi globami. Poleg tega podatki, ki kažejo na to, ali je organ sledil zastavljenemu okviru javno-zasebnega partnerstva in ali je izbral ustrezno ponudbo ter posledično sklenil pogodbo, ki ustreza določilom podzakonskega akta, ki to ureja, ne morejo predstavljati poslovne skrivnosti. Prav tako ne morejo biti kot poslovna skrivnost varovani deli ponudbe in pogodbe, v katerih gre za podatke o količini iz specifikacije, ceni na enoto, vrednosti posameznih postavk in skupni vrednosti iz ponudbe, pa tudi podatki, ki izkazujejo izpolnjevanje pogojev, in tisti podatki, ki so vplivali na razvrstitev ponudbe v okviru ocenjevanja le-te na podlagi postavljenih meril, saj so ti javni že po zakonu. Za dele pogodbe, ki predstavljajo obveznosti zasebnega partnerja, obveznosti javnega partnerja, vzdrževanje in upravljanje sistema ter delovanje prekrškovnega sistema, ki so bili sicer

veljavno opredeljeni kot poslovna skrivnost, pa je Informacijski pooblaščenec ocenil, da jih je treba razkriti na podlagi 2. odstavka 6. člena ZDIJZ, na podlagi prevladujočega interesa javnosti. Ocenil je namreč, da je interes javnosti za razkritje informacije močnejši od škode, ki bi lahko nastala z razkritjem informacije. Vprašanje, kakšne odgovornosti je občina prevzela v okviru javno-zasebnega partnerstva oz. katere pristojnosti je prenesla na subjekt zasebnega prava (na stranskega udeleženca), na tako pomembnih področjih, kot sta urejanje in varnost cestnega prometa, namreč nikoli ne more biti izven javnega interesa. V preostalem delu je Informacijski pooblaščenec odločil, da javni interes ne prevlada in da je treba dostop do informacij, ki predstavljajo poslovne skrivnosti, zavrniti.

1.3. Pregled pomembnih sprememb za zagotavljanje varstva osebnih podatkov v Sloveniji

1.3.1. Najpomembnejše prelomnice na področju varstva osebnih podatkov

1. Omejevanje prekomerne javne objave osebnih podatkov posameznikov prek registra nepremičnin – Kot posledica zahteve za oceno ustavnosti, ki jo je Informacijski pooblaščenec (ponovno) vložil leta 2011, je Ustavno sodišče RS razveljavilo določbi 1. in 2. odstavka 114. člena Zakona o evidentiranju nepremičnin, ki določata javnost zemljiškega katastra in katastra stavb, in sicer v delu, ki se nanaša na podatke o lastniku, če gre za fizično osebo. Ustavno sodišče je s tem jasno izrazilo stališče, da javna objava osebnih podatkov za določen namen (kot npr. v zemljiški knjigi) ne pomeni absolutne javnosti teh podatkov in ne dopušča njihove nadaljnje obdelave za kakršen koli namen. Z navedeno določbo so geodeti obšli odločbo Ustavnega sodišča RS iz leta 2007, ko so ustavni sodniki na zahtevo Informacijskega pooblaščenca že razveljavili del istega zakona, ki je določal javnost registra nepremičnin v delu, ki se nanaša na podatke o fizičnih osebah.

2. Zagotavljanje zakonitosti posegov v zasebnost in varstvo osebnih podatkov s strani Slovenske obveščevalno-varnostne agencije – Informacijski pooblaščenec je z leta 2008 vloženo zahtevo za oceno ustavnosti Zakona o Slovenski obveščevalno-varnostni agenciji (ZSOVA) opozoril na protiustavno določbo 21. člena ZSOVA, na podlagi katere nastaja zbirka osebnih podatkov v zvezi z izvajanjem strateškega nadzora telekomunikacij. Ustavno sodišče RS je zahtevo zavrglo iz procesnih razlogov in o zadevi ni meritorno določilo. Zato ostajamo brez nujno potrebne opredelitve najvišjega sodišča do pomembnega pravnega vprašanja o dopustnosti ravnanja Slovenske obveščevalno-varnostne agencije z vidika poseganja v ustavno varovano pravico do komunikacijske zasebnosti posameznikov.

3. Omejevanje poseganja nadzornih organov v (elektronsko) komunikacijsko zasebnost posameznikov – Informacijski pooblaščenec je z zahtevo za presojo ustavnosti določb 29. člena Zakona o preprečevanju omejevanja konkurence (ZPOmK-1) opozoril na vprašanje dopustnosti ravnanja nadzornih organov, ki svoje pristojnosti izvršujejo v okviru upravnih – inšpekcijskih in/ali prekrškovnih postopkov, ter na podlagi zakonske določbe, vendar brez odredbe sodišča in izven namenov, ki jih določa 37. člen Ustave RS, posežejo v (elektronsko) komunikacijo. Ustavno sodišče RS se je v preteklosti do vsebine komunikacijske zasebnosti že opredeljevalo, vendar še nikoli glede pooblastil nadzornih – upravnih organov. V okviru inšpekcijskega postopka zoper Urad za varstvo konkurence (zdaj Javna agencija RS za varstvo konkurence) zaradi pregledovanja in izpisovanja elektronske pošte zaposlenih v družbi Produkcija Plus, d. o. o., (št. 0612-166/2011) je Informacijski pooblaščenec ocenil, da je Urad za varstvo konkurence pregledoval elektronsko pošto zaposlenih na način, ki ni združljiv z ustavno zaščiteno komunikacijsko zasebnostjo, zato je vložil zahtevo za oceno ustavnosti določb 29. člena ZPOmK-1. Ustavno sodišče RS je zahtevo zavrglo iz procesnih razlogov, zaradi česar ostajamo brez nujno potrebne opredelitve najvišjega sodišča do vprašanja o dopustnosti poseganja nadzornih organov v ustavno varovano pravico do komunikacijske zasebnosti posameznikov.

4. Zagotavljanje sorazmernosti posegov v zasebnost posameznikov v okviru davčnega postopka – javna objava davčnih neplačnikov – Informacijski pooblaščenec je z zahtevo za presojo ustavnosti določb opozoril na morebitno neustavnost nekaterih določb 20. člena Zakona o davčnem postopku (ZDavP-2), ki se nanašajo na ukrep javne objave davčnih

neplačnikov. Ukrep po mnenju Informacijskega pooblaščenca ni nujen in primeren za dosego namenov, zaradi katerih je bil sprejet, hkrati pa ni sorazmeren z (neobstoječimi) pozitivnimi učinki, ki naj bi jih dosegel. Seznam neplačnikov namreč zelo raznovrstne življenjske zgodbe posameznikov izrazito nesorazmerno postavlja na isti »sramotilni steber«, medtem ko javnosti ostaja skrito bistvo – kaj je država storila za to, da bi davčni dolg izterjala. Ustavno sodišče RS o zahtevi še ni odločilo.

5. Nedopustnost prekomernega zakonskega ukrepa obvezne hrambe podatkov o prometu elektronskih komunikacij – Informacijski pooblaščenec je z zahtevo za oceno ustavnosti nekaterih določb XIII. poglavja Zakona o elektronskih komunikacijah (ZEKom-1) o obvezni hrambi podatkov o prometu in lokaciji ter z njimi povezanih podatkov, ki določajo naročnika ali uporabnika javne komunikacijske storitve, opozoril, da ti ukrepi niso v skladu z načelom sorazmernosti in z vsebino Direktive 2006/24/ES z dne 15. 3. 2006. Zatrjujoč kršitve določenih pravic in svoboščin posameznikov so ustavna sodišča Nemčije, Romunije, Češke ter Višje sodišče Irske tovrsten ukrep obvezne hrambe podatkov o prometu elektronskih komunikacij že prepoznala kot spornega. Sodišče EU je na podlagi pobude Avstrije in Irske za presojo skladnosti Direktive z Evropsko konvencijo o temeljnih pravicah in svoboščinah Direktivo razveljavilo. Ustavno sodišče RS o zahtevi še ni odločilo.

6. Vzpostavitev dobre prakse glede zbiranja osebnih podatkov v zvezi z izpolnjevanjem pogodbe – Informacijski pooblaščenec je z odločitvijo v inšpekcijskem postopku (št. 0613-144/2011) v zvezi s storitvijo izposoje mestnih koles BicikeLJ zoper Europlakat, d. o. o., opozoril na dopustne meje obdelave osebnih podatkov za sklenitev in izpolnjevanje pogodbe med zavezancem in uporabnikom. Informacijski pooblaščenec je zavezancu z odločbo odredil, da neha zbirati osebne podatke (med drugim podatek o spolu in številko mobilnega telefona), za zbiranje katerih nima ustrezne pravne podlage (pogodbo je namreč mogoče skleniti in izvajati tudi brez njih, zavezanec pa za obdelavo teh podatkov tudi ni pridobil veljavne osebne privolitve uporabnikov). Informacijski pooblaščenec je v odločbi jasno razmejil med osebnimi podatki, ki so potrebni (npr. ime in priimek, naslov, datum rojstva, elektronski naslov, PIN koda, številka plačilnega računa ter identifikacijska oznaka banke, podatki o kreditni kartici), ter podatki, ki za izpolnjevanje pogodbe niso potrebni. Opozoril je tudi na dejstvo, da gre za javno-zasebno partnerstvo med zavezancem, podjetjem Europlakat, d. o. o., in Mestno občino Ljubljana, zaradi česar 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. Upravno sodišče RS je potrdilo odločbo Informacijskega pooblaščenca in v sproženem upravnem sporu tožbo zavezanca zavrnilo.

7. Vzpostavitev ustrezne prakse glede posegov v osebne podatke o telefonskih pogovorih zaposlenih – Informacijski pooblaščenec je v dveh odmevnih inšpekcijskih postopkih – v postopku na Okrožnem sodišču v Ljubljani (zadeva št. 0603-154/2009) ter na Ministrstvu za zunanje zadeve (zadeva št. 0612-19/2008) – opozoril na pereč problem zakonske neurejenosti področja zasebnosti na delovnem mestu v Republiki Sloveniji ter s svojo prakso prispeval k izboljšavam. Sodišče je odločitve Informacijskega pooblaščenca v obeh primerih potrdilo. Poleg tega je Informacijski pooblaščenec večkrat pozval k sprejemu zakona, ki bi jasno urejal to področje, ter pristojnemu ministrstvu celo poslal predlog osnutka Zakona o zasebnosti na delovnem mestu.

8. Vzpostavitev ustrezne prakse glede zavarovanja zdravstvene dokumentacije – Informacijski pooblaščenec je z več inšpekcijskimi postopki opozoril na pomen in nujnost ustreznega zavarovanja občutljivih osebnih podatkov v večjih bolnišnicah in zdravstvenih domovih. V vseh primerih je Informacijski pooblaščenec odredil vzpostavitev ustreznih ukrepov fizičnega in tehničnega zavarovanja osebnih podatkov, med katere sodi tudi zagotavljanje dnevnikov sledljivosti obdelave osebnih podatkov ter nujnost sklenitve pisne pogodbe o pogodbeni obdelavi osebnih podatkov in ustreznega dodatnega nadzora, kadar izvajalci zdravstvenih storitev za posamezne naloge obdelave osebnih podatkov pooblastijo zunanje izvajalce (npr. za prevoz, uničenje zdravstvene dokumentacije).

9. Zagotavljanje zakonite obdelave osebnih podatkov pobudnikov za razpis občinskega referenduma – Informacijski pooblaščenec je v inšpekcijskem postopku proti Občini Borovnica in odvetniku Andreju Dolesu (št. 0612-54/2008 in 0603-36/2008) ugotovil nezakonito obdelavo osebnih podatkov, in sicer s strani župana ter odvetnika Andreja Dolesa. Župan je namreč Pobudo volivcem za vložitev zahteve za razpis referenduma glede gradnje stanovanjskih objektov v občini s priloženim seznamom 420 podpisnikov z

njihovimi osebnimi podatki posredoval odvetniku kot pooblaščencu družbe Orbital, d. o. o., ta pa je nato vse podpisnike še isti dan po pošti pozval, naj takoj prekličejo svoj podpis in jim zagrozil, da bo v nasprotnem primeru proti njim vložen odškodninski zahtevek. Niti župan niti odvetnik za opisano obdelavo osebnih podatkov podpisnikov pobude nista imela ustrezne pravne podlage, zato je Informacijski pooblaščenec v okviru prekrškovnega postopka zaradi kršitev oba oglobil. Zakon o odvetništvu odvetnikom namreč nikakor ne daje splošnega pooblastila za pridobivanje in uporabo vseh osebnih podatkov. Sodišče je odločitev Informacijskega pooblaščenca potrdilo in zavrnilo zahtevi za sodno varstvo.

10. Prepoved nezakonitega nadzora elektronske pošte zaposlenih – Informacijski pooblaščenec je v okviru inšpekcijskega postopka pri Javni agenciji za raziskovalno dejavnost RS (št. 0612-81/2008) ugotovil nezakonito pregledovanje in nadaljnjo obdelavo prometnih podatkov o prejeti elektronski pošti zaposlenih na poštnih strežnikih zavezanca z namenom razbremenjevanja poštnega strežnika (z omejevanjem zasebne elektronske pošte z večjimi priponkami). Zavezancu je Informacijski pooblaščenec naložil, da popravi pravilnik, ki to dopušča, in preneha opisan nadzor elektronske pošte na svojih poštnih strežnikih. Odločitev Informacijskega pooblaščenca je potrdilo tudi sodišče.

1.3.2. Prelomne odločitve Informacijskega pooblaščenca, ki so vplivale na zagotavljanje varstva osebnih podatkov v praksi

V primeru kršitve na Okrožnem sodišču v Ljubljani (zadeva št. 0603-154/2009) je Informacijski pooblaščenec ugotovil nezakonito zbiranje in uporabo podatkov o opravljenih klicih s službenega mobilnega telefona sodnice (datum in čas klica, klicana telefonska številka oz. številka prejemnika SMS-ja/MMS-ja, trajanje klica, znesek in vrsta opravljene storitve). Zavezanec je podatke pridobil z namenom dokumentiranja poteka medsebojnega obveščanja v zvezi z eksplozijo bombe na stanovanjski hiši sodnice Katarine Turk Lukan ter ugotavljanja, katera oseba na sodišču je po službenem mobilnem telefonu komunicirala z novinarjem. Prav tako je šlo v primeru ugotovljenih kršitev s strani Ministrstva za zunanje zadeve (zadeva št. 0612-19/2008) za nezakonito uporabo izpiskov telefonskih pogovorov v stacionarnem telefonskem omrežju ministrstva (seznama vseh približno 110.000 vhodnih in izhodnih klicev), tokrat za namen izvedbe notranjega nadzora na ministrstvu – odkrivanja osebe, ki naj bi novinarju posredovala dokument veleposlaništva RS v Washingtonu. Komisija je s ciljem nadaljnjega ukrepanja v okviru predmetnega notranjega nadzora pregledala seznam in iskala uporabnike, ki so po telefonu kontaktirali določeno časopisno hišo. Nezakonito je bilo tako samo pridobivanje seznama kot tudi t. i. podatkovno rudarjenje po nezakonito pridobljeni zbirki s pomočjo iskalnika. Podatki o klicanih in klicočih številkah namreč uživajo varstvo tako v skladu z 38. kot tudi s 37. členom Ustave RS. Sodišče je odločitve Informacijskega pooblaščenca v obeh primerih potrdilo.

Informacijski pooblaščenec je v okviru postopka inšpekcijskega nadzora obravnaval primer neustreznega zavarovanja občutljivih osebnih podatkov (zadevi št. 0612-1/2008 in 0603-4/2008) pri prevozu na uničenje oz. termično odstranitev, ko je iz tovornjaka izpadlo neugotovljeno število kartonskih škatel z internimi naročilnicami za laboratorijske preiskave Zdravstvenega doma Celje. Poleg tega je Informacijski pooblaščenec ob pregledu prostorov Onkološkega inštituta Ljubljana (zadeva št. 0612-48/2008) ugotovil, da je bila medicinska dokumentacija (kartoteke umrlih pacientov) shranjena v več kot sto odprtih kartonastih škatlah na hodniku, ki je bil v času gradbenih del oziroma delovnega časa gradbenih delavcev odklenjen. Informacijski pooblaščenec je izvedel tudi preventivne inšpekcijske pobude ex-offo (več zadev, npr. št. 0612-81/2007) v vseh večjih bolnišnicah in zdravstvenih domovih zaradi preverjanja postopkov in ukrepov za zavarovanje osebnih podatkov.

Informacijski pooblaščenec je v okviru postopka inšpekcijskega nadzora pri Uradu RS za nadzor prirejanja iger na srečo (št. 0612-11/2012) opozoril, da ni dopustno omogočanje javnega dostopa do spletne statistike s podatki o obiskih spletne strani zavezanca (podatkov o datumu in času obiska, IP-naslovu obiskovalca, o brskalnem okolju, napotiteljih in drugih podatkih spletne strani). Zavezanec je s tem neprimerno zavaroval navedene osebne podatke. Poleg tega je Informacijski pooblaščenec opozoril, da brez ustrezne pravne podlage (zakona ali osebne privolitve posameznika) ni dopustna samodejna preusmeritev obiskovalcev strani (www.infounpis.si) na druge naslove ter posledična vzpostavitev zbirke osebnih podatkov o osebah, ki so želele obiskati druge spletne strani. V konkretnem primeru

gre namreč za preusmeritev, s katero je zavezanec zbiral osebne podatke posameznikov, ki niso želeli obiskati njegove spletne strani, ampak spletne strani s spletnimi igralnicami, prek katerih se prirejajo spletne igre na srečo brez koncesije vlade (npr. strani blokiranih spletnih stavnic). Zavezanec je po odredbi Informacijskega pooblaščenca preprečil javno dostopnost podatkov, poskrbel za tako nastavitev strežnika, ki ne beleži IP-naslovov, ter iz dnevniških datotek nepovratno izbrisal podatke, ki predstavljajo osebne podatke posameznikov, ki so bili z drugih spletnih strani preusmerjeni na spletno stran zavezanca. Zavezanec je hkrati zoper odločbo Informacijskega pooblaščenca vložil tožbo na Upravno sodišče RS, ker se ni strinjal s tem, da so podatki, katerih izbris in ukinitev beleženja je zahteval Informacijski pooblaščenec, osebni podatki. Sodišče v upravnem sporu še ni odločilo.

Konec leta 2011 je Okrajno sodišče v Novem mestu potrdilo doslej najvišjo globo, ki jo je izrekel Informacijski pooblaščenec zavarovalnici zaradi nezakonite obdelave osebnih podatkov (zadeve št. 0613-178/2009, 0603-111/2009 in 0603-112/2009). V postopku o prekršku je namreč ugotovil, da so bili z ene zavarovalnice na drugo posredovani osebni podatki o 2.382 nekdanjih zavarovancih prve brez podlage v zakonu ali v osebni privolitvi posameznika, na katere se osebni podatki nanašajo, ti podatki pa so bili nato s strani druge zavarovalnice uporabljeni za neposredno trženje. Sodišče je zahtevo za sodno varstvo, ki sta jo vložila kršitelja, zavrnilo in potrdilo odločbo z izrečeno globo pravni osebi v višini 112.590 evrov, odgovorni osebi pa v višini 20.000 evrov.

Informacijski pooblaščenec je prek izvedbe postopka inšpekcijskega nadzora na Davčni upravi RS (št. 0612-91/2008) zaradi preverjanja zakonitosti vpogledov v davčni register s strani zaposlenih na DURS opozoril na obveznosti vseh upravljavcev glede zagotavljanja spoštovanja določb Zakona o varstvu osebnih podatkov v praksi (ZVOP-1). Informacijski pooblaščenec je na podlagi načela sledljivosti preverjal, kako javni uslužbenci spoštujejo varstvo osebnih podatkov v različnih registrih javne uprave, in sicer upravičenost dostopa do registra davčnih zavezancev. Informacijski pooblaščenec je od vsakega zaposlenega zahteval navedbo razloga za vpogled. V postopku je bilo ugotovljeno, da je od preverjanih 200 uslužbencev 47 uslužbencev v dokumentacijo vpogledalo zaradi edinega po zakonu dovoljenega razloga, to je vodenja davčnega postopka. Ostalih 153 uslužbencev za vpogled ni imelo utemeljenega razloga. Najpogostejši razlog za vpogled je bila radovednost. Informacijski pooblaščenec je zaradi obdelave osebnih podatkov brez ustrezne pravne podlage in s tem kršitve 8. člena ZVOP-1 kršiteljem izdal opomin, v poduk ostalim državnim uslužbencem, da po osebnih podatkih ne morejo "brskati" kar tako.

Davčna uprava RS (DURS) je prek pogodbenega obdelovalca podjetja KRO, d. o. o., (zadeva št. 0612-52/2007) leta 2007 na neustrezen način pošiljala predizpolnjene dohodninske napovedi, zaradi česar je Informacijski pooblaščenec v okviru prekrškovnega postopka ugotovil kršitev predpisov glede zavarovanja osebnih podatkov s strani obeh zavezancev. Dohodninske napovedi so bile namreč neustrezno zaprte, saj so bile zlepljene le točkovno in ne po celotni dolžini, zaradi česar je bilo mogoče vpogledati v tajne davčne podatke, nekateri prejemniki pa so predizpolnjene dohodninske napovedi prejeli celo odprte. Zavezanec je napako takoj odpravil in ustavil nadaljnje razpošiljanje predizpolnjenih dohodninskih napovedi. Vse nadaljnje pošiljke predizpolnjenih napovedi so bile vložene v plastično folijo, ki je bila zaprta, poleg tega so bile pošiljke še dodatno, močneje zalepljene. Dokumentacija z osebnimi podatki davčnih zavezancev mora biti glede na njihovo občutljivost (davčna tajnost) med prenosom podatkov po pošti shranjena v takšnih ovojnicah, da se z vsebino podatkov ne bi bilo mogoče seznaniti brez vidne poškodbe ovojnice, poleg tega mora biti tako zaprta ovojnica zaščitena tudi z zaščitnim tiskom, da ob običajni svetlobi ali pri osvetlitvi ovojnic z običajno lučjo vsebina ovojnice oziroma osebni podatki, ki jih odločba vsebuje, niso vidni.

Informacijski pooblaščenec je v svoji odločbi (zadeva št. 0613-4/2006), ki jo je potrdilo tudi Okrajno sodišče v Ljubljani, ugotovil, da je objava imen in priimkov prejemnikov najvišjih bruto in neto izplačanih plač zaposlenih v časopisni družbi v tedniku Demokracija nezakonita. Za objavo osebnih podatkov 86 zaposlenih v časopisni družbi namreč tednik ni imel zakonske podlage, prav tako ni imel osebnih privolitvev posameznikov, višina plač pa je javni podatek le za javni sektor. Pravica do svobode izražanja, na katero se je tednik skliceval, je omejena že z Zakonom o medijih, po katerem bi bil tednik upravičen pridobiti in objaviti sporne podatke le takrat, ko bi s tem preprečil hujše kaznivo dejanje ali neposredno nevarnost za življenje ljudi in njihovo premoženje, o čemer pa v obravnavanem primeru ni bilo mogoče govoriti. Objava podatkov je posegla v ustavne pravice do osebnega dostojanstva, varstva zasebnosti in osebnostnih pravic ter pravico do varstva osebnih podatkov. Pravica do svobode izražanja

v tem »trku« pravic ni prevladala.

Informacijski pooblaščenec je leta 2009 izvedel sistematičen nadzor nad zavarovanjem osebnih podatkov v bančnem sektorju (zadeva št. 0613-336/2009) zaradi preverjanja zakonitosti obdelave osebnih podatkov pri medbančni izmenjavi podatkov o boniteti komitentov v okviru novo uvedenega sistema SISBON ter zakonitosti dostopanja do podatkov na računih komitentov. Ugotovljeno je bilo, da pri medbančni izmenjavi podatkov o boniteti komitentov do nezakonitih dostopov do podatkov ni prihajalo. Pri preverjanju dostopov do podatkov nekaterih znanih slovenskih posameznikov, ki ga je izvedel pri šestih največjih slovenskih bankah, pa je ugotovil, da je pri dveh bankah prišlo do nezakonitih vpogledov v podatke. Zoper uslužbence bank, ki so nezakonito dostopali do podatkov na osebnih računih komitentov, je Informacijski pooblaščenec izrekel sankcije.

Informacijski pooblaščenec je na podlagi prijave ugotovil nezakonito pridobivanje osebnih podatkov lastnikov psov s strani nekaterih veterinarskih ambulant za namen neposrednega trženja (več zadev, npr. št. 0603-38/2011). Na podlagi dnevnikov sledljivosti obdelav osebnih podatkov lastnikov psov v Centralnem registru psov (katerega upravljavec je bila takrat Veterinarska uprava RS, danes Uprava RS za varno hrano, veterinarstvo in varstvo rastlin) je Informacijski pooblaščenec ugotovil, da veterinarske ambulante z uporabo osebnih podatkov navedenega registra lastnikom psov pošiljajo obvestila o cepljenju psov proti steklini, v katerih jih obveščajo, da v določenem obdobju razpisujejo splošno cepljenje psov proti steklini, večkrat pa lastnikom psov hkrati ponujajo tudi druge storitve (npr. cepljenje proti kužnim boleznim, sterilizacijo, kastracijo). Navedena oblika uporabe podatkov iz registra, ki nima statusa javnega registra, ni dopustna. Podatki namreč niso javno dostopni, zato jih je dopustno obdelovati zgolj v zakonsko opredeljene namene, med katere pa ne sodi uporaba za namene neposrednega trženja. Veterinarske ambulante lahko za namen neposrednega trženja uporabljajo le osebne podatke tistih lastnikov psov, ki so njihove stranke, oziroma tiste osebne podatke, ki jih pridobijo v okviru zakonitega opravljanja dejavnosti, in podatke, ki jih dobijo iz javno dostopnih virov.

Informacijski pooblaščenec je Državni volilni komisiji odredil brisanje osebnih podatkov kandidatov na volitvah v Državni zbor RS leta 2008, 2004 in 2000 ter na lokalnih volitvah leta 2010, 2006 in 1998 (osebno ime, datum rojstva, kraj rojstva, naslov prebivališča, poklic in delo, ki ga opravlja) s spletnih strani komisije (zadeva št. 0612-192/2011). Področni Zakon o volitvah v Državni zbor, ki določa oblikovanje seznamov potrjenih list kandidatov v volilni enoti in seznamov kandidatov, o katerih se glasuje v posameznih volilnih okrajih, ter njihovo objavo, namreč določa takšno obliko obdelave osebnih podatkov kandidatov samo za čas pred volitvami, ne ureja pa objave osebnih podatkov v času po volitvah. Namen obdelave osebnih podatkov – njihova objava na spletnih staneh – je bil s tem dosežen, prav tako izida volitev ni mogoče izpodbijati z nobenim pravnim sredstvom več, zato je Informacijski pooblaščenec odločil, da zavezanec nima več zakonske podlage za njihovo (nadaljnjo) obdelavo.

Informacijski pooblaščenec je podjetju Ljubljanski potniški promet, d. o. o., prepovedal zbiranje lokacijskih podatkov uporabnikov neprenosljivih terminskih vozovnic Urbana, saj je v inšpekcijskem postopku (zadeva št. 0613-246/2009) ugotovil, da je podjetje zbiralo in hranilo podatke o času, kraju in liniji vstopa (lokacijski podatki) neselektivno, tj. za vse potnike, ki so prevoz plačali z neprenosljivo terminsko vozovnico Urbana, čeprav za obdelavo teh podatkov potnikov niso imeli pravne podlage. Podjetje LPP, d. o. o., je moralo tako na podlagi odločbe Informacijskega pooblaščenca nehati zbirati lokacijske podatke potnikov, ki so prevoz plačali z neprenosljivimi terminskimi vozovnicami, ter omenjene podatke izbrisati iz vseh svojih zbirk osebnih podatkov. Informacijski pooblaščenec je v inšpekcijskem postopku ugotovil, da je do obdelave osebnih podatkov prihajalo le pri kartici Urbana zelene barve, ki je imenska in neprenosljiva, medtem ko kartico Urbana rumene barve posameznik lahko uporablja povsem anonimno, ne da bi pri tem prišlo do obdelave njegovih osebnih podatkov.

Informacijski pooblaščenec je v okviru inšpekcijskega postopka (št. 0613-263/2010) odločil, da pomeni objava obtožnega predloga v zadevi Patria na Facebook profilu Janeza Janše nezakonito obdelavo osebnih podatkov oseb, zoper katere je omenjeni obtožni predlog podan. Zato je zavezancu kot upravljavcu svojega spletnega profila odredil umik navedenega obtožnega predloga s spletne strani. V predmetni zadevi je Informacijski pooblaščenec podal tudi kazensko ovadbo, ki pa jo je Okrožno državno tožilstvo v Ljubljani zavrglo, ker je bila

podana nesorazmernost med majhnim pomenom kaznivega dejanja ter posledicami, ki bi jih povzročil kazenski pregon.

Informacijski pooblaščenec je v okviru inšpekcijskega postopka zoper Mestno občino Ljubljana in zoper Listo Zorana Jankovića – Pozitivna Slovenija zaradi suma nezakonite obdelave osebnih podatkov otrok Osnovne šole Koseze, ki so se fotografirali z ljubljanskim županom Zoranom Jankovićem, njihova fotografija pa je bila za tem novembra 2011 objavljena v časopisu Pozitivne Slovenije Bolje (za namene predvolilne kampanje za predčasne volitve v Državni zbor RS 2011), ugotovil, da so bili osebni podatki otrok iz zbirke fotografij Mestne občine Ljubljana nezakonito posredovani in uporabljeni za namene predvolilne propagande Pozitivne Slovenije. Pozitivna Slovenija je namreč v svojem časopisu objavila fotografijo, ki jo je posnel uradni (pogodbeni) fotograf Mestne občine Ljubljana z namenom dokumentiranja obiska župana na osnovni šoli. Informacijski pooblaščenec je zaradi tega Pozitivni Sloveniji in njeni odgovorni osebi izrekel globo, prav tako je sankcijo izrekel fotografu, ki je fotografijo nezakonito posredoval agenciji, ki je oblikovala časopis.

Informacijski pooblaščenec je v okviru inšpekcijskega postopka ocenil, da je neustaven del določb 128. člena Zakona o letalstvu, ki ureja gibanje in zadrževanje na javnem letališču ter v objektu navigacijskih služb zračnega prometa. Zato je leta 2006 vložil zahtevo za oceno ustavnosti. Z izpodbijanim členom se namreč po oceni Informacijskega pooblaščenca grobo posega v informacijsko zasebnost kot ustavno pravico posameznika, saj se predvideva prekomerno zbiranje osebnih podatkov, ki ni sorazmerno s koristjo skupnosti in splošno varnostjo v državi, ki bi bila nujna v demokratični družbi. Poleg tega z izpodbijano določbo zakon osebne podatke, ki naj bi se zbirali, našteva le eksemplifikativno in ne določno, kot zahteva Ustava RS. Ustavno sodišče RS je v pretežnem delu ugodilo zahtevi Informacijskega pooblaščenca.

Informacijski pooblaščenec je z vložitvijo zahteve za oceno ustavnosti 45. člena Odloka o cestnoprometni ureditvi Mestne občine Ljubljana, ki določa, da lahko občina javne ceste in druge javne površine na območju občine opremi z video nadzornim sistemom zaradi spremljanja prometnih razmer, nadzora spoštovanja prometnih predpisov, izboljšanja pretočnosti prometa in prometne varnosti ter s tem zbira osebne podatke. Informacijski pooblaščenec je 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. Po oceni Informacijskega pooblaščenca temu ni tako. Od odgovora na to vprašanje je namreč odvisno ravnanje vseh lokalnih skupnosti v prihodnje na eni strani ter nivo varstva osebnih podatkov v Republiki Sloveniji na drugi strani. Ustavno sodišče RS o zadevi še ni odločilo.

1.4. Druga pomembna področja dela Informacijskega pooblaščenca v preteklih desetih letih

Informacijski pooblaščenec je vsa leta veliko pozornosti posvečal dvigovanju ozaveščenosti o pomenu zasebnosti in varstva osebnih podatkov. Zasnoval je široko paleto aktivnosti, s katerimi se je trudil delovati preventivno in izobraževalno.

Med najpomembnejše aktivnosti na tem področju sodi izdajanje neobveznih mnenj glede številnih vprašanj varstva osebnih podatkov. Večina mnenj je dostopnih na spletni strani in predstavlja obsežen korpus znanja, ki je v veliko pomoč upravljavcem osebnih podatkov. Upamo si trditi, da takšnega obsega objavljenih mnenj ni mogoče najti pri nobenem drugem nadzornem organu za varstvo osebnih podatkov v EU.

Poleg mnenj Informacijski pooblaščenec pripravlja tudi smernice, ki podajajo odgovore na najpogosteje zastavljena vprašanja z določenega tematskega področja. Informacijski pooblaščenec je bil v kar nekaj primerih med prvimi v EU, ki so izdali smernice za določeno področje (npr. računalništvo v oblaku, digitalna televizija, inteligentna video analitika). Ob smernicah je pripravil tudi poročila, kot je na primer Poročilo o varstvu osebnih podatkov pri klubih zvestobe.

Informacijski pooblaščenec je ves čas močno prisoten na spletu, ki ga izkorišča za učinkovito komuniciranje s svojimi ciljnimi publikami. Veliko je vlagal v svojo spletno podobo – leta 2008 je prejel priznanje Netko za najboljšo spletno stran v kategoriji javne uprave. Ima tudi svoj profil na družabnem omrežju Facebook, informacijska pooblaščenka pa je tudi med najbolj znanimi in vplivnimi uporabniki omrežja Twitter.

Informacijski pooblaščenec je izoblikoval tudi nagrade za dobre prakse, s katerimi se spodbuja dobre rešitve na področju varstva osebnih podatkov. Informacijski pooblaščenec tako vsako leto podari posebno priznanje predstavniku iz javnega in zasebnega sektorja, ki se je izkazal z doslednim spoštovanjem zakona ali uspešnimi prijemi za varstvo osebnih podatkov. Prvič je nagrado podelil leta 2008 Zavodu za zdravstveno zavarovanje Slovenije za prizadevanja za zagotovitev ustrezne informacijske rešitve na področju zavarovanja zbirk osebnih podatkov ob uvedbi nekaterih sistemov za obdelavo osebnih podatkov ter družbi Livar, d. d., iz Ivančne Gorice za zgledno ureditev zavarovanja osebnih podatkov, ki so jo izkazali ob nenapovedanem inšpekcijskem obisku. Nagrajeni so bili še: leta 2009: podjetje Cetis, d. d., za izredno dodelan in učinkovit sistem organizacijskih, tehničnih in logično-tehničnih postopkov in ukrepov za zavarovanje osebnih podatkov ter Ministrstvo za obrambo RS za izredno natančno zastavljen sistem pristojnosti obdelave osebnih podatkov, ki se z vojaško skrbnostjo tudi izvaja; leta 2010: Dom dr. Janka Benedika iz Radovljice za dodelan in učinkovit sistem postopkov in ukrepov za zavarovanje osebnih podatkov v zvezi z izvajanjem videonadzora ter družba Iskraemeco, merjenje in upravljanje energije, d. d., za izdelan sistem pristojnosti obdelave osebnih podatkov; leta 2011: Društvo življenje brez nasilja, ki je odlično poskrbelo za varstvo občutljivih osebnih podatkov svojih strank ter javni zavod Obalne lekarne Koper za odlično varstvo zdravstvenih podatkov strank; leta 2012 nagrade Informacijski pooblaščenec ni podelil, leta 2013 pa sta jo prejela Vrhovno sodišče RS za e-Zemljiško knjigo ter Zavarovalnica Maribor, d. d., za ustrezno zavarovanje osebnih podatkov, ugotovljeno v okviru inšpekcijskega nadzora.

Informacijski pooblaščenec od leta 2008 podeljuje tudi priznanja za pridobitev certifikata po standardu za sistem vodenja varovanja informacij ISO/IEC 27001:2005 in tako promovira uporabo tega mednarodnega standarda, ki omogoča celovito upravljanje informacijske varnosti, ki je pomemben del varstva osebnih podatkov. Leta 2011 je Informacijski pooblaščenec prvič podelil nagrado ambasador zasebnosti, ki predstavlja posebno priznanje za napore na področju t. i. vgrajene zasebnosti (angl. Privacy by Design), ki poudarja proaktivno varstvo osebnih podatkov in izkazuje, da je legitimne cilje pogosto mogoče doseči ob minimalnih ali celo ničelnih posegih v zasebnost. Prvi ambasador zasebnosti je leta 2011 postal Urad za meroslovje RS, za napore, vložene v varstvo osebnih podatkov na področju t. i. sektorskega merjenja hitrosti v prometu. Leta 2012 so ambasadorji postali: Stanka Šalamun, Renata Stupar, ekipa podjetja Acros, d. o. o., za delo pri Projektu SLED, s katerim so marsikaterega upravljavca zbirk osebnih podatkov opomnili na pravice posameznika glede seznanitve z lastnimi osebnimi podatki ter opozorili na pomen proaktivnega delovanja v duhu koncepta vgrajene zasebnosti. Leta 2013 je ambasador zasebnosti postal Direktorat za informatiko in e-storitve, Ministrstvo za javno upravo in pravosodje ter zaposlena mag. Aleš Pelan in dr. Alenka Žužek Nemec za upoštevanje vgrajene zasebnosti pri uspešnem delu na evropskih projektih STORK, SPOCS, STORK 2.0 in drugih ter pri izdelavi Analize možnosti za uvedbo varnejših in uporabniku prijaznejših e-identitet.

Informacijski pooblaščenec je veliko pozornosti posvečal tudi predhodnim presojam vplivov na zasebnost (angl. Privacy Impact Assesment). Strokovnjaki Informacijskega pooblaščenca so številnim organizacijam iz javnega in zasebnega sektorja odgovorili na marsikatero dilemo, s katero so se srečali pri uvajanju novih sistemov, zakonodajnih rešitev, spremembah poslovnih procesov in tolmačenju zahtev zakonodaje. Prepričani smo, da smo s takšnim preventivnim delovanjem preprečili marsikatero kršitev in pomagali pri oblikovanju boljših rešitev.

Informacijski pooblaščenec je aktivno sodeloval v številnih skupinah, med katerimi velja izpostaviti medresorsko delovno skupino, ki se je ukvarjala z uvedbo varnejših in uporabniku prijaznejših e-identitet, pri katerih je bila v sodelovanju z Ministrstvom za javno upravo, Ministrstvom za notranje zadeve in Ministrstvom za visoko šolstvo, znanost in tehnologijo pripravljena celovita analiza stanja e-identitet v Sloveniji, analiza možnih pravnih in izvedbenih možnosti ter primerjalna analiza z drugimi državami. Izvedene so bile ankete in posveti z deležniki, kot so ponudniki storitev, overitelji, državljani ter zaposleni v javni upravi. Prenova sistema e-identitet omogoča boljše in učinkovitejše storitve e-uprave z večjo stopnjo

uporabe pri ciljnih skupinah, obenem pa prenova ob ustreznih odločitvah omogoča tudi višjo raven varovanja osebnih podatkov, kot jo nudijo trenutna sredstva za identifikacijo in avtentikacijo posameznika v virtualnem svetu.

Informacijski pooblaščenec od svoje ustanovitve izjemno pozornost posveča spremljanju premikov in sprememb na področju zakonodaje na področju dostopa do informacij javnega značaja ter še posebej na področju varstva osebnih podatkov, kjer so prav področni predpisi tisti, ki opredeljujejo posamezne zbirke osebnih podatkov, načine obdelave, hrambe in druge vidike posegov v zasebnost posameznikov v zvezi z obdelavo osebnih podatkov. Informacijski pooblaščenec je pri tem pogosto zelo kritičen do lahkotnosti, nepremišljenosti in nedoslednosti, s katero skušajo predlagatelji zakonov velikokrat brez tehtanja nujnosti posegov glede na njihove koristi, brez tehtnih premislekov in temeljitega preigravanja posledic posameznih zakonskih rešitev uvesti različne nove oblike in načine zbiranja osebnih podatkov, povezovati obstoječe velike zbirke osebnih podatkov ali uvajati nove zbirke osebnih podatkov brez občutljivosti za posledice takšnih zakonskih rešitev ter predvsem brez razmisleka o tem, do kakšnih zlorab bi lahko zato prišlo. Informacijski pooblaščenec se je tako med drugim z opozorili aktivno vključil v postopek spreminjanja Zakona o elektronskih komunikacijah, Zakona o nalogah in pooblastilih policije ter Zakona o kazenskem postopku. Informacijski pooblaščenec pripombe sicer poda na okoli 50 predlogov predpisov na leto (leta 2013 jih je bilo več kot 100), pripravljavci in predlagatelji predpisov pa jih zelo različno upoštevajo. Še vedno se zgodi, da se nekateri na opozorila z vidika varstva osebnih podatkov ne ozirajo oziroma podcenjujejo pomembnost področja posameznikove zasebnosti. Posledica tega je tudi sprejem predpisov, ki nesorazmerno posegajo v zasebnost posameznikov – torej na način, ki državi ali družbi ne prinaša koristi, ki bi odtehtale ne dovolj premišljene in za zasebnost invazivne zakonske rešitve. Prav na pobudo Informacijskega pooblaščenca so se s spremembami ustreznih zakonskih določb razrešile pobude za oceno ustavnosti določb 62. ter 62.d člena Zakona o zdravstvenem varstvu in zdravstvenem zavarovanju, določb 390. člena Zakona o bančništvu ter določb 47., 58., 123., 165., 247., 334., 432. in 543. člena Zakona o trgu finančnih instrumentov, ki so bile po oceni Informacijskega pooblaščenca neustavne.

Ureditev pooblastil za lociranje mobilnih telefonov v primerih, ko sta ogrožena življenje in telo posameznika (104.a oz. novi 153. člen Zakona o elektronskih komunikacijah), je lep primer povezovalne vloge Informacijskega pooblaščenca. Predvsem na njegovo pobudo in z njegovim sodelovanjem so nastale skrbno pripravljene pravne podlage in natančno opredeljeni postopki, ki so v praksi stanje od pravne negotovosti in zamudnih postopkov premaknili k učinkovitemu izvajanju pooblastil ter s tem k uspešnemu reševanju človeških življenj. S posebnim angažmajem strokovnjakov Informacijskega pooblaščenca bodo prenovljeni postopki še hitrejši, podatki uporabnejši, nadzor pa okrepljen. Gre za lep primer, kako je lahko sicer zelo invazivno pooblastilo podrobno urejeno in redno nadzorovano ter tako sorazmerno in učinkovito.

Kot eden prvih in še vedno redkih organov javne uprave je Informacijski pooblaščenec leta 2011 s strani Arhiva RS dobil potrjena notranja pravila, ki predstavljajo formalne pogoje za prehod na sistem e-hrambe dokumentarnega in arhivskega gradiva.

1.5. Vpliv Informacijskega pooblaščenca na razvoj področja transparentnosti in varstva osebnih podatkov na mednarodni ravni in na ravni Evropske unije ter sodelovanje v mednarodnih projektih

Informacijski pooblaščenec si je od svoje ustanovitve pridobil precejšen ugled in zaupanje tudi pri kolegih iz drugih držav EU. Mednarodna delovna skupina za varstvo osebnih podatkov v telekomunikacijah (IWGDPT ali t. i. Berlinska skupina) je tako sprejela Sofia memorandum, ki temelji na delu Informacijskega pooblaščenca in predstavlja mejnik pri vprašanjih varstva osebnih podatkov na področju satelitskega cestninjenja. Informacijski pooblaščenec v okviru mednarodnih aktivnosti s pripombami aktivno sodeluje tudi pri pripravi nove uredbe glede varstva osebnih podatkov v EU.

Informacijska pooblaščenka Nataša Pirc Musar je bila leta 2013 s strani Evropske komisije imenovana v posebno ad hoc skupino EU–ZDA, ki je ugotavljala dejansko stanje aktivnosti ameriške preiskovalne agencije (National Security Agency, NSA) glede množičnega zbiranja informacij in osebnih podatkov o državljanih EU ter o tem pripravila posebno poročilo.

Delovanje Informacijskega pooblaščenca je bilo zelo visoko ocenjeno tudi v procesu vključevanja Slovenije v OECD.

Poleg sodelovanja na zasedanjih in delovnih podskupinah Delovne skupine po 29. členu (Article 29 Data Protection Working Party) ter v Posvetovalnem odboru (T-PD) po Konvenciji Sveta Evrope o varstvu posameznikov glede na avtomatsko obdelavo osebnih podatkov (Konvencija št. 108) Informacijski pooblaščenec od svojega nastanka aktivno sodeluje tudi v organih za nadzor evropskih 'mega zbirk' osebnih podatkov, kot so: Schengenski informacijski sistem, Europol, Vizni informacijski sistem in sistem Eurodac. Informacijski pooblaščenec je med drugim sodeloval v Skupni nadzorni akciji glede implementacije direktive o obvezni hrambi podatkov v prometu elektronskih komunikacij. Slovenska informacijska pooblaščenka Nataša Pirc Musar od leta 2012 predseduje skupnemu nadzornemu organu za Europol (pred tem je bila njegova podpredsednica). Informacijski pooblaščenec je imel ob tem z vidika zagotavljanja ustrezne ravni varstva osebnih podatkov pomembno vlogo pri vstopu Slovenije v schengensko območje, prek sodelovanja pooblaščenke in drugih zaposlenih pa tudi pri evalvacijah ustreznosti ravni varstva osebnih podatkov v drugih državah (npr. Švica, Romunija, Bolgarija).

Informacijski pooblaščenec je leta 2012 s srbskim Informacijskim pooblaščencem uspešno izpeljal tudi mednarodni t. i. Twinning Light Projekt, ki se je osredotočal na izboljšanje varstva osebnih podatkov v Srbiji in krepitev nacionalnega nadzornega organa za varstvo osebnih podatkov. Strokovnjaki Informacijskega pooblaščenca so uspešno sodelovali tudi pri podobnem projektu v Črni gori ter v evropskem projektu LAPSI (Legal Aspects of Public Sector Information), namenjenem izgradnji tematske mreže strokovnjakov na področju ponovne uporabe informacij javnega značaja.

V sodelovanju z resornim ministrstvom je Informacijski pooblaščenec na področju e-uprave uspešno predstavil model za čezmejne storitve e-uprave, pri katerem posameznik ohranja nadzor nad svojimi osebnimi podatki. T. i. pristop STORK, ki temelji na pravici posameznika do dostopa do lastnih osebnih podatkov, je prepričal tudi druge države EU, ki se trudijo z vzpostavljanjem čezmejnih storitev e-uprave.

Predstavniki Informacijskega pooblaščenca so z vsebinskimi prispevki vsako leto nastopili na številnih mednarodnih konferencah in dogodkih (npr. na evropski in svetovni konferenci Informacijskih pooblaščencev). V okviru aktivnosti ozaveščanja javnosti Informacijski pooblaščenec vsako leto obeleži 28. januar, evropski dan varstva osebnih podatkov, ter 28. september, mednarodni dan pravice vedeti.

1.6. Ključni izzivi v prihodnjih petih letih na področju transparentnosti po oceni Informacijskega pooblaščenca

1. Med ključne izzive na področju dostopa do informacij javnega značaja v prvi vrsti sodi implementacija zadnje novele ZDIJZ, s katero se krog zavezanih organov širi tudi na poslovne subjekte, ki so pod prevladujočim vplivom države, lokalnih skupnosti in drugih pravnih oseb javnega prava, v praksi.

2. Prav tako med ključne izzive sodijo vprašanja prenosa sprememb direktive o ponovni uporabi informacij javnega značaja v slovensko zakonodajo in njena učinkovita implementacija v praksi. Sprememba direktive 2013/37/EU Evropskega parlamenta in Sveta z dne 26. 6. 2013 o spremembi Direktive 2003/98/ES o ponovni uporabi informacij javnega značaja namreč omejuje možnost zaračunavanja ponovne uporabe, širi krog zavezancev za ponovno uporabo (tudi npr. na muzeje, knjižnice in arhive), določa obvezen okvir zagotavljanja pravnega varstva ter spodbuja zagotavljanje informacij v strojno berljivih in odprtih formatih. Zaradi teh sprememb bo v prihajajočem letu treba prilagoditi slovenski

zakonodajni okvir (novela ZDIJZ), nato pa te spremembe še uspešno udejaniti v praksi.

3. Država bo morala več pozornosti nameniti spodbujanju povečanja proaktivne transparentnosti in dobrih praks na področju ponovne uporabe t. i. »open data« (več informacij bi moralo biti na voljo in posredovanih brez zahtev prosilcev, s čimer bi omogočili pogostejšo ponovno uporabo), saj sta razvoj in polno izkoriščenje možnosti, ki jih prinaša ponovna uporaba takih informacij, v Sloveniji še vedno premalo izkoriščen (tudi gospodarski) potencial.

4. Razviti bi morali smernice in dobre prakse na področju upravljanja z avtorskimi pravicami v javnem sektorju ter posledično spodbujati dobre prakse na področju dostopa do informacij javnega značaja in ponovne uporabe le-teh.

5. Zelo pomembno področje pa ostaja krepitev sodelovanja z nevladnimi organizacijami in organi zavezanci ter s tem širjenje zavesti o pomenu pravice dostopa do informacij javnega značaja. Zgolj učinkovito in v transparentnost usmerjeno delovanje organov zavezancev ob aktivnem sodelovanju z nevladnimi organizacijami, ki morajo odigrati vlogo lakmusovega papirja ter na ključnih področjih delovanja družbe opozarjati na pomanjkljivosti, lahko Slovenijo na področju transparentnosti države in javne uprave pripelje na naslednjo raven razvoja. To pomeni, da bi postalo omogočanje čim lažjega dostopa do čim širšega kroga prosto dostopnih informacij javnega značaja v zavesti vseh, tako prosilcev kot organov zavezancev, primarni cilj sam po sebi in ne zgolj zakonska obveza.

1.7. Ključni izzivi v prihodnjih petih letih na področju zasebnosti po oceni Informacijskega pooblaščenca

1. Med ključne izzive na področju varstva osebnih podatkov v prvi vrsti sodi prenova evropskega zakonodajnega okvira. Direktiva iz leta 1995 prav gotovo ne nudi več pravega odgovora na izzive, ki jih predstavljajo internet in globalna izmenjava podatkov ter trendi, ki vključujejo »internet stvari«, računalništvo v oblaku in »big data«. Od tega, kakšna bodo nova pravila, bo v veliki meri odvisno tudi delovanje Informacijskega pooblaščenca.

2. Med ključne izzive sodijo tudi težka vprašanja glede varovanja osebnih podatkov in javne dostopnosti osebnih podatkov. Z digitalizacijo arhivov medijev se ob možnostih, ki jih nudijo spletni iskalniki in računalništvo v oblaku, odpirajo velike dileme glede dopustnosti (namenov) uporabe podatkov na spletu ter pravice do pozabe oziroma izbrisa.

3. Profiliranje bo v prihodnosti gotovo področje, ki bo terjalo večjo pozornost varuhov zasebnosti. Tako zasebni kot javni sektor zbirata vse več podatkov, ki lahko z avtomatizirano obdelavo vodijo v sprejem odločitev z resnimi posledicami za posameznika. Lahko se zgodi, da bodo naša življenja vse bolj usmerjali algoritmi ter bo polje naše zasebnosti in s tem svobode vedno ožje.

4. Pomembno področje bo ostalo vprašanje ravnovesja med svobodo in nadzorom, ki se udejanja v številnih trenjih med uvajanjem novih nadzorovalnih tehnologij in pooblastil, ki močno posegajo v temeljne človekove pravice. Iskanje pravega ravnovesja bo ob uveljavljanju novih tehnologij, kot so biometrijska prepoznava obrazov, avtomatska prepoznava registrskih tablic, RFID-čipi, brezpilotni letalniki itd., terjalo ustrezen angažma varuhov zasebnosti. Omeniti velja, da bo zelo pomembno, kako uspešno bodo slednji znali pokazati in zagovarjati povezavo med zasebnostjo in svobodo.

5. Morda najbolj ključen izziv pa bo, kako iz osebnih podatkov izvleči družbeno korist, a ob tem ohraniti varstvo osebnih podatkov. Obdelava zdravstvenih, lokacijskih, transakcijskih in drugih osebnih podatkov lahko pomembno pripeva k reševanju številnih težav, s katerimi se soočamo (npr. onesnaževanje okolja, reševanje prometnih težav ipd.), bistveno pa bo izvleči največ iz teh podatkov na način, ki ohranja njihov zasebni značaj. Tako osebni podatki kot informacije javnega značaja so namreč valuta informacijske dobe.

2 INFORMACIJSKI POOBLAŠČENEC

2.1. Pristojnosti Informacijskega pooblaščenca

Državni zbor RS 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 status neodvisnega organa, in Inšpektorat za varstvo osebnih podatkov, ki je deloval kot organ v sestavi Ministrstva za pravosodje. Ob uveljavitvi ZInfP je Pooblaščenec za dostop do informacij javnega značaja nadaljeval delo kot Informacijski pooblaščenec, ki je prevzel inšpektorje in druge uslužbence Inšpektorata za varstvo osebnih podatkov, pripadajočo opremo in sredstva. Hkrati je prevzel tudi vse nedokončane zadeve, arhive in evidence, ki jih je vodil Inšpektorat za varstvo osebnih podatkov. S tem so se pristojnosti organa, ki je skrbel za nemoteno izvajanje dostopa do informacij javnega značaja, močno spremenile in se razširile še na pravno področje varstva osebnih podatkov. Informacijski pooblaščenec je tako postal tudi državni nadzorni organ za varstvo osebnih podatkov. Delo je začel 1. 1. 2006.

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

Neodvisnost Informacijskega pooblaščenca je zagotovljena na dva načina. Prvi je postopek imenovanja pooblaščenca kot funkcionarja, ki ga na predlog predsednika Republike Slovenije imenuje Državni zbor Republike Slovenije. Drugi način, ki omogoča predvsem finančno neodvisnost, pa je, da se sredstva za delo Informacijskega pooblaščenca zagotovijo v proračunu Republike Slovenije, tako da o tem odloča Državni zbor na predlog Informacijskega pooblaščenca.

Državni zbor RS je 21. 5. 2009 na predlog predsednika republike dr. Danila Türka informacijski pooblaščenki Nataši Pirc Musar podelil še en mandat, ki se bo iztekel julija 2014.

Informacijski pooblaščenec svoje z zakonom določene naloge in pristojnosti opravlja na dveh področjih:
1. na področju dostopa do informacij javnega značaja,
2. na področju varstva osebnih podatkov.

Informacijski pooblaščenec ima na področju dostopa do informacij javnega značaja pristojnosti pritožbenega organa, ki je 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 (pristojnost je določena v 2. členu ZInfP).

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].

Na področju varstva osebnih podatkov ima Informacijski pooblaščenec pristojnosti, ki mu jih dajeta Zakon o varstvu osebnih podatkov[4] in 2. člen ZinfP, in sicer:
1. opravlja inšpekcijski nadzor nad izvajanjem določb ZVOP-1 in drugih predpisov, ki urejajo varstvo ali obdelavo osebnih podatkov (obravnava prijave, pritožbe, sporočila in druge vloge, v katerih je izražen sum kršitve zakona, ter opravlja načrtovani preventivni inšpekcijski nadzor pri upravljavcih osebnih podatkov s področja javnega in zasebnega sektorja) (pristojnost je določena v 2. členu ZInfP);
2. odloča o pritožbi posameznika, kadar upravljavec osebnih podatkov ne ugodi njegovi

[1] Uradni list RS, št. 113/2005, 51/2007 – ZUstS-A; v nadaljevanju ZInfP.
[2] Uradni list RS, št. 110/2006-UPB1, s spremembami; v nadaljevanju ZMed.
[3] Uradni list RS, št. 51/2006-UPB2, s spremembami; v nadaljevanju ZDIJZ.
[4] Uradni list RS, št. 94/2007-UPB1; v nadaljevanju ZVOP-1.

zahtevi glede pravice posameznika do seznanitve z zahtevanimi podatki, do izpisov, seznamov, vpogledov, potrdil, informacij, pojasnil, prepisovanja ali kopiranja po določbah zakona, ki ureja varstvo osebnih podatkov (pristojnost je določena v 2. členu ZInfP);
3. vodi postopke o prekrških s področja varstva osebnih podatkov (hitri postopek);
4. vodi in vzdržuje register zbirk osebnih podatkov in skrbi, da je slednji ažuren ter javno dostopen prek svetovnega spleta (28. člen ZVOP-1);
5. omogoča vpogled in prepis podatkov iz registra zbirk osebnih podatkov, praviloma isti dan, najpozneje pa v osmih dneh (29. člen ZVOP-1);
6. odloča o ugovoru posameznika glede obdelave osebnih podatkov na podlagi 4. odstavka 9. člena in 3. odstavka 10. člena ZVOP-1;
7. izdaja odločbe o zagotavljanju ustrezne ravni varstva osebnih podatkov v tretjih državah (63. člen ZVOP-1);
8. vodi postopke ugotavljanja ustrezne ravni varstva osebnih podatkov v tretjih državah na podlagi ugotovitev inšpekcijskega nadzora in drugih informacij (64. člen ZVOP-1);
9. vodi seznam tretjih držav, za katere je ugotovil, da imajo v celoti ali delno zagotovljeno ustrezno raven varstva osebnih podatkov ali da te nimajo zagotovljene; če je ugotovljeno, da tretja država le delno zagotavlja ustrezno raven varstva osebnih podatkov, je v seznamu navedeno tudi, v katerem delu je ustrezna raven zagotovljena (66. člen ZVOP-1);
10. vodi upravne postopke za izdajo dovoljenj o iznosu osebnih podatkov v tretjo državo (70. člen ZVOP-1);
11. vodi upravne postopke za izdajo dovoljenj za povezovanje javnih evidenc in javnih knjig, kadar katera od zbirk osebnih podatkov, ki naj bi se jih povezovalo, vsebuje občutljive osebne podatke ali je za izvedbo povezovanja potrebna uporaba istega povezovalnega znaka (npr. EMŠO ali davčna številka) (84. člen ZVOP-1);
12. vodi upravne postopke za izdajo ugotovitvenih odločb o tem, ali je nameravana uvedba izvajanja biometrijskih ukrepov v zasebnem sektorju v skladu z določbami ZVOP-1 (80. člen ZVOP-1);
13. sodeluje z državnimi organi, pristojnimi organi Evropske unije za varstvo posameznikov pri obdelavi osebnih podatkov, mednarodnimi organizacijami, tujimi nadzornimi organi za varstvo osebnih podatkov, zavodi, združenji ter drugimi organi in organizacijami glede vseh vprašanj, ki so pomembna za varstvo osebnih podatkov;
14. daje in objavlja predhodna mnenja državnim organom ter nosilcem javnih pooblastil o usklajenosti določb predlogov predpisov z zakoni in drugimi predpisi, ki urejajo osebne podatke;
15. daje in objavlja neobvezna mnenja o skladnosti kodeksov poklicne etike, splošnih pogojih poslovanja oziroma njihovih predlogih s predpisi s področja varstva osebnih podatkov;
16. pripravlja, daje in objavlja neobvezna navodila in priporočila glede varstva osebnih podatkov na posameznem področju;
17. na spletni strani in na drug ustrezen način objavlja predhodna mnenja o usklajenosti predlogov zakonov in drugih predpisov z zakonom in drugimi predpisi s področja varstva osebnih podatkov ter zahtev za oceno ustavnosti predpisov (48. člen ZVOP-1), objavlja odločbe in sklepe sodišč, ki se nanašajo na varstvo osebnih podatkov ter neobvezna mnenja, pojasnila, stališča in priporočila glede varstva osebnih podatkov na posameznih področjih (49. člen ZVOP-1);
18. daje izjave za javnost o opravljanih nadzorih in pripravlja letna poročila o svojem delu;
19. sodeluje v delovnih skupinah za varstvo osebnih podatkov, oblikovanih znotraj EU, ki združujejo neodvisne institucije za varstvo osebnih podatkov držav članic (v Delovni skupini po 29. členu Direktive 95/46/EC in v nadzornih organih, ki se ukvarjajo z nadzorom obdelave osebnih podatkov v Schengenskem informacijskem sistemu, v informacijskem sistemu za carino, v okviru Europola ter v skupini za nadzor Eurodaca).

Informacijski pooblaščenec je tudi prekrškovni organ, pristojen za nadzor nad izvajanjem ZInfP, ZDIJZ v okviru pritožbenega postopka ter določbe 45. člena ZMed in ZVOP-1.

Informacijski pooblaščenec lahko po 2. členu ZInfP na Ustavnem sodišču RS vloži zahtevo po presoji ustavnosti zakonov, drugih predpisov ter splošnih aktov, izdanih za izvrševanje javnih pooblastil, če se pojavi vprašanje ustavnosti in zakonitosti v zvezi s postopkom, ki ga vodi, tako na področju dostopa do informacij javnega značaja kot na področju varstva osebnih podatkov.

Z vstopom Republike Slovenije v schengensko območje je Informacijski pooblaščenec prevzel 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[5], Zakonu o potnih listinah[6] in Zakonu o osebni izkaznici[7].

Pristojnosti Informacijskega pooblaščenca na podlagi ZPacP so:
- odločanje o pritožbah pacientov in drugih upravičenih oseb ob kršitvi določbe, ki ureja način seznanitve z zdravstveno dokumentacijo (10. 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 (5. 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 (7. odstavek 45. člena ZPacP).

Pristojnosti Informacijskega pooblaščenca po ZPLD-1 in ZOIzk-1 so omejene na določbe, ki urejajo, v katerih primerih in na kakšen način lahko upravljavci osebnih podatkov kopirajo potne listine oz. osebne izkaznice ter določajo način hrambe kopij (3.a člen ZOIzk-1 in 4.a člen ZPLD-1). Informacijski pooblaščenec v zvezi z navedenimi določbami opravlja naloge inšpekcijskega in prekrškovnega organa (odloča o prekršku v skladu z 19.a členom ZOIzk-1 in 34.a členom ZPLD-1).

Leta 2009 je Informacijski pooblaščenec pridobil pristojnosti po Zakonu o bančništvu[8]:
- podaja soglasja upravljavcem sistema SISBON pred začetkom uporabe pravil sistema iz 1. točke 13. 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 (14. 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) ter skladno s 397. členom ZBan-1 vodi postopke o prekršku zaradi kršitve določb 309.a člena ZBan-1 (10.–15. odstavek 397. člena ZBan-1).

Pristojnosti, ki jih je imel Informacijski pooblaščenec na podlagi Zakona o elektronskih komunikacijah[9], 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 na leto 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;

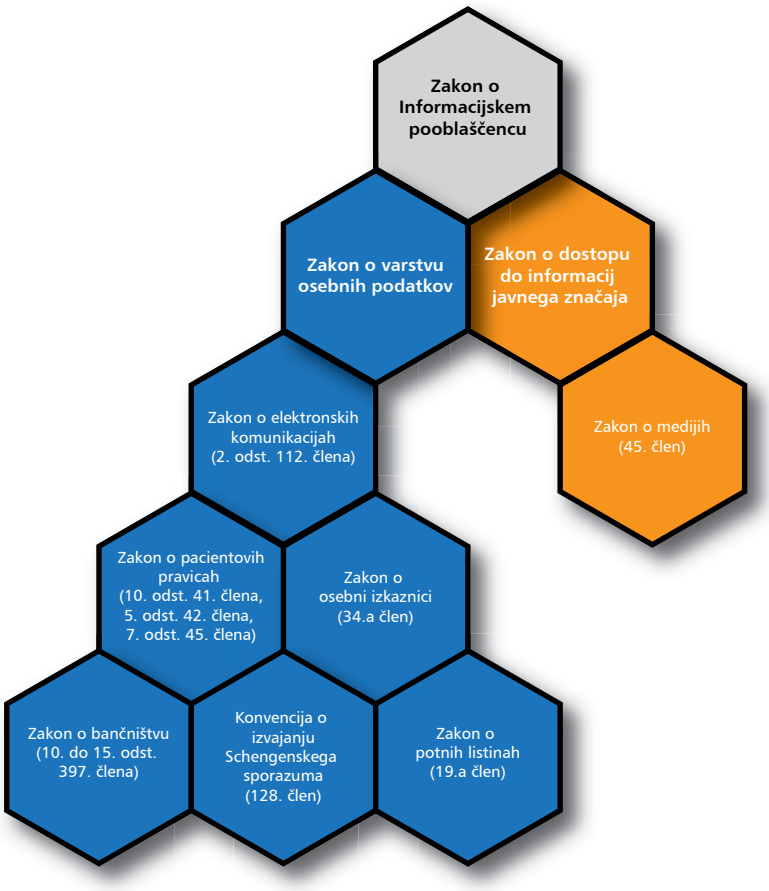
5 Uradni list RS, št. 15/2008; v nadaljevanju ZPacP.
6 Uradni list RS, št. 29/2011–UPB4; v nadaljevanju ZPLD-1.
7 Uradni list RS, št. 35/2011; v nadaljevanju ZOIzk-1.
8 Uradni list RS, št. 99/2010 –UPB5, s spremembami; v nadaljevanju ZBan-1.
9 Uradni list RS, št. 109/2012; v nadaljevanju ZEKom-1.

- 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.–168. člen ZEKom-1, razen določb iz 4. 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.–236. člen ZEKom-1).

Leta 2013 je Informacijski pooblaščenec s spremembo Zakona o potrošniških kreditih[10] pridobil novo pristojnost. 36. člen ZPotK-1 določa, da Informacijski pooblaščenec opravlja nadzor nad dajalci kreditov glede izvajanja:

- 2. odstavka 8. člena ZPotK-1, ki določa, da mora dajalec kredita pred sklenitvijo kreditne pogodbe oceniti kreditno sposobnost potrošnika, pri čemer informacije o njegovih prejemkih oziroma njegovem premoženjskem stanju pridobi od potrošnika, informacijo o zadolženosti potrošnika pa pridobi iz zbirk osebnih podatkov, ki se vodijo na podlagi zakona, ki ureja bančništvo;
- 1., 2. in 4. odstavka 9. člena ZPotK-1, ki določa vrste podatkov, ki jih lahko za pridobitev informacije o zadolženosti potrošnika obdelujejo dajalci kreditov, ki niso vključeni v sistem izmenjave informacij o boniteti strank po zakonu, ki ureja bančništvo, ter dajalcu kredita v primeru zavrnitve vloge nalaga obveznost, da mora potrošnika nemudoma in brezplačno na papirju ali drugem trajnem nosilcu podatkov obvestiti o pridobljenih informacijah iz zbirk osebnih podatkov, razen če poseben zakon določa drugače.

Slika 1: Pristojnosti Informacijskega pooblaščenca.



[10] Uradni list RS, št. 59/2010 in 30/2013-ZpotK-1B; v nadaljevanju ZPotK-1.

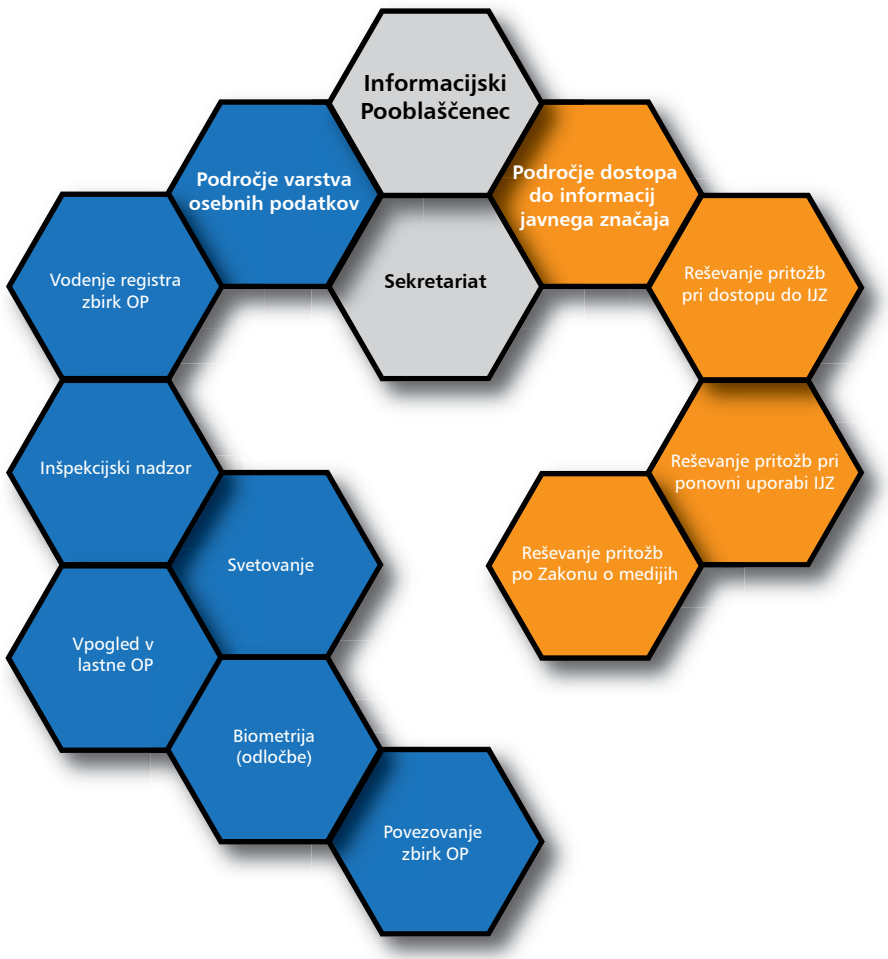
2.2. Organiziranost Informacijskega pooblaščenca

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

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 2013 je imel Informacijski pooblaščenec 32 zaposlenih:

- informacijsko pooblaščenko,
- namestnico za področje varstva osebnih podatkov,
- namestnico za področje dostopa do informacij javnega značaja,
- namestnika za področje informacijskih tehnologij,
- namestnika – vodjo državnih nadzornikov za varstvo osebnih podatkov,
- generalno sekretarko,
- devet svetovalcev,
- asistenta svetovalca,
- deset državnih nadzornikov za varstvo osebnih podatkov,
- dva raziskovalca,
- informatika (programerja aplikacij),
- tri administrativno-tehnične sodelavke (finančno referentko, poslovno sekretarko, dokumentaristko).

Preglednica 1: Izobrazbena struktura zaposlenih pri Informacijskem pooblaščencu 31. 12. 2013.

	Srednja izobrazba	Višja strokovna šola	Univerzitetna izobrazba	Magisterij	Doktorat	**Skupaj**
Informacijska pooblaščenka			1			1
Namestniki			2	2		4
Generalna sekretarka			1			1
Svetovalci			9			9
Asistenti svetovalca			1			1
Raziskovalci			2			2
Državni nadzorniki za varstvo osebnih podatkov			5	4	1	10
Informatik	1					1
Administrativno-tehnični sodelavci	1	2				3
Skupaj	2	2	21	6	1	**32**

Kljub povečanemu obsegu potreb po opravljanju inšpekcijskega nadzora nad izvajanjem določb ZVOP-1 in vnovičnem povečanju števila pritožbenih zadev na področju dostopa do informacij javnega značaja se je leta 2013 število zaposlenih zmanjšalo. Na dan 1. 1. 2013 je bilo pri Informacijskem pooblaščencu zaposlenih 33 oseb, od tega dve za določen čas za delo na Twinning projektu – Srbija ter ena za določen čas zaradi nadomeščanj, na dan 31. 12. 2013 pa je bilo zaposlenih 32 oseb, od tega tri za določen čas zaradi nadomeščanj.

2.3. Finančna sredstva Informacijskega pooblaščenca

Sredstva za delo Informacijskega pooblaščenca se zagotavljajo iz državnega proračuna in jih določi Državni zbor RS na predlog Informacijskega pooblaščenca (5. člen ZInfP).

Državni zbor RS je za delo Informacijskega pooblaščenca za leto 2013 v državnem proračunu določil integralna sredstva v višini 1.291.210,00 EUR (plače 1.052.017,10 EUR, materialni stroški 210.652,18 EUR, investicije 28.540,72 EUR).

S sklepom o prerazporeditvi pravic porabe je bilo oktobra s strani Ministrstva za notranje zadeve prerazporejenih 3.800,00 EUR za pokrivanje stroškov službenih poti informacijske

pooblaščenke, ki je bila imenovana v skupino petih strokovnjakov ad hoc skupino EU–ZDA. Na koncu leta 2013 je bilo tako na postavki materialni stroški 214.452,18 EUR in skupaj integralnih sredstev 1.295.010,00 EUR.

Leta 2013 je Informacijski pooblaščenec razpolagal z namenskimi sredstvi ter donacijami za sodelovanje v projektih, ki so bili financirani s strani Evropske unije, v skupni višini 104.527,88 EUR (prenesenih sredstev iz leta 2012 53.211,36 EUR in prejetih sredstev v letu 2013 51.316,52 EUR).

Zaradi proračunskih omejitev in varčevalnih ukrepov, ki jih je sprejela slovenska vlada leta 2013, je Informacijski pooblaščenec omejil izobraževanje zaposlenih, povsem skrčil obseg udeležbe na mednarodnih sestankih ter skrbno in zelo restriktivno porabljal finančna sredstva na postavki materialnih stroškov, investicij in plač. Informacijski pooblaščenec je leta 2013 bistveno znižal strošek najemnin, saj se je marca 2013 zaradi varčevanja preselil v poslovne prostore na Zaloški 59 v Ljubljani, ki so v lasti Republike Slovenije in jih je Vlada RS februarja s sklepom prenesla v upravljanje Informacijskemu pooblaščencu. Informacijski pooblaščenec je močno znižal tudi stroške izdaje publikacij, študentskega dela in drugih storitev.

Informacijski pooblaščenec je imel konec leta 2013 na voljo skupaj 1.399.537,88 EUR. Zaradi zgoraj navedenega in zaradi dodatne omejitve na postavki integralna sredstva (poraba 93 %) je bila ob koncu leta 2013 poraba proračunskih sredstev 1.380.117,83 EUR.

Informacijski pooblaščenec je v proračun za leto 2014 prenesel 7.063,62 EUR namenskih sredstev in sredstev donacij (6.717,20 EUR donacij in 346,42 EUR založenih sredstev).

Preglednica 2: Proračun Informacijskega pooblaščenca 2013 (v EUR).

	Veljavni proračun v EUR	Privzete obveznosti v EUR	Razpoložljiv proračun v EUR konec leta
Informacijski pooblaščenec	**1.399.537,88**	**1.380.117,83**	**19.420,05**
Podprogrami			
OPRAVLJANJE DEJAVNOSTI IP	**1.295.010,00**	**1.282.653,57**	**12.356,43**
PP 1271 Materialni stroški	214.452,18	206.304,91	8147,27
PP 1273 Investicije	28.540,72	28.522,65	18,07
PP 1267 Plače	1.052.017,10	1.047.826,01	4.191,09
NAMENSKA SREDSTVA	**2.700,00**	**2.700,00**	**0,00**
PP 7459 Namenska sredstva kupnine	2.700,00	2700,00	0,00
DONACIJE	**101.034,46**	**94.317,26**	**6.717,20**
PP 9378 EU Open Privacy Space	3,41	0,00	3,41
PP 9586 LAPSI 1.0	2.387,24	2.037,84	349,4
PP 9596 Twining Črna gora	342,88	0,00	342,88
PP 9950 Twining Srbija	85.974,07	85.899,26	74,81
PP 9958 Mednarodna spletna stran	1.226,86	648,59	578,27
PP 130130 LAPSI 2.0	9.600,00	5.673,57	3926,43
PP130134 Taiex projekt	1.500,00	58,00	1.442,00
ZALOŽENA SREDSTVA	**793,42**	**447,00**	**346,42**
PP 344 Založena sredstva	793,42	447,00	346,42

Leta 2012 je bilo za plače porabljenih manj sredstev (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.).

Preglednica 3: Namenska sredstva in donacije.

	Prenesena sredstva iz leta 2012	Prejeti prilivi	SKUPAJ sredstva v letu 2013
Informacijski pooblaščenec	**53.211,36**	**51.316,52**	**104.527,88**
NAMENSKA SREDSTVA	**2.700,00**	**0,00**	**2.700,00**
PP 7459 Namenska sredstva kupnine	2.700,00	0,00	2.700,00
DONACIJE	**49.717,94**	**51.316,52**	**101.034,46**
PP 9378 EU Open Privacy Space	3,41	0,00	3,41
PP 9586 LAPSI 1.0	87,24	2.300,00	2.387,24
PP 9596 Twining Črna gora	342,88	0,00	342,88
PP 9950 Twining Srbija	48.817,55	37.156,52	85.974,07
9958 Mednarodna spletna stran	466,86	760,00	1.226,86
PP 130130 LAPSI 2.0	0,00	9.600,00	9.600,00
PP130134 Taiex projekt	0,00	1.500,00	1.500,00
ZALOŽENA SREDSTVA	**793,42**		**793,42**
PP 344 Založena sredstva	793,42	0,00	793,42

Za plače zaposlenih (plače in dodatki, regres za letni dopust, povračila in nadomestila, prispevki delodajalcev za socialno varnost, prispevki za zdravstveno zavarovanje) je bilo leta 2013 porabljenih 1.047.826,01 EUR, kar je manj kot leta 2012 (1.138.678,08 EUR) in leta 2011 (1.139.495,82 EUR). Tudi za materialne stroške (pisarniški material in storitve, prevozni stroški, čiščenje poslovnih prostorov, električna energija, voda, komunalne storitve in komunikacije, službena potovanja, poslovne najemnine – Informacijski pooblaščenec je bil v najetih poslovnih prostorih do konca marca 2013) je bilo porabljenih manj sredstev (tj. 206.304,91 EUR) kot leta 2012, ko je bilo porabljenih 252.887,49 EUR, in leta 2011, ko je bilo porabljenih 302.103,22 EUR. Največji delež materialnih stroškov je predstavljala selitev Informacijskega pooblaščenca na novo lokacijo. Informacijski pooblaščenec je moral na novo lokacijo preseliti vse pohištvo in vso dokumentacijo, v novih poslovnih prostorih pa je moral pred vselitvijo izvesti najnujnejša popravila, preureditev in obnovo. Iz navedenega je razvidno, da se poraba sredstev za plače zaposlenih in materialne stroške že nekaj let stalno zmanjšuje.

Finančna sredstva iz postavke investicije so bila porabljena za gradbena dela, predelavo in zasteklitev prostora ter namestitev protivlomnega sistema na novi lokaciji na Zaloški 59, za nakup računalniške in ostale opreme in licenc ter za odkup vozila, ki ga je imel Informacijski pooblaščenec v najemu od leta 2010, za kar se je odločil zaradi racionalizacije stroškov (razlika je bila poravnana iz namenskih sredstev).

Sredstva v okviru Taiex projekta so bila porabljena za delovni obisk predstavnikov makedonskega pooblaščenca za dostop do informacij javnega značaja ter predstavnikov makedonskega ministrstva za notranje zadeve, namenska sredstva kupnine so bila v celoti porabljena za nakup oziroma odkup službenega vozila, sredstva za mednarodno spletno stran info-commissioners.org pa so bila porabljena za njeno urejanje in plačilo uporabe domene.

Projekt EU Open Privacy Space se bo dokončno zaprl v letu 2014, preostanek sredstev s pripadajočimi obrestmi se vrne v proračun Republike Slovenije. Leta 2014 se bo zaključil tudi projekt LAPSI 1.0 (Legal Aspects of Public Sector Information), preostanek sredstev se bo prav tako vrnil v državni proračun. Leta 2013 so bila v okviru omenjenega projekta sredstva porabljena za tisk. Projekt Twining Črna gora se je končal leta 2012, porabe v letu 2013 ni bilo. Projekt se bo dokončno zaprl januarja 2014, preostanek sredstev s pripadajočimi obrestmi pa bo vrnjen v proračun.

Projekt Twining Srbija je bil v celoti financiran s strani Evropske komisije in se je končal leta 2013. Za sodelovanje v projektu je Informacijski pooblaščenec v letih 2012 in 2013 prejel namenska sredstva v skupni višini 236.547,72 EUR, od tega je bilo iz leta 2012 v 2013 prenesenih 48.817,55 EUR, leta 2013 pa je bilo prejetih 37.156,52 EUR. Leta 2013 je bilo

85.899,26 EUR porabljenih za plače zaposlenih, ki so sodelovali pri projektu, pisarniški material, stroške notranje revizije, komunikacijo, izdatke za službena potovanja, stroške v zvezi z izvajanjem projekta in napotitvijo zaposlenih na misije v Srbijo, plačilo avtorskih honorarjev in nakup prenosnih računalnikov za potrebe projekta. Projekt je bil leta 2013 zaključen, ostanek sredstev s pripadajočimi obrestmi se v letu 2014 vrne v državni proračun.

Informacijski pooblaščenec sodeluje tudi v evropskem projektu LAPSI 2.0, ki se je začel leta 2013 in ga financira EU na podlagi pogodbe Evropske komisije z nosilcem projekta Katholieke Universiteit Leuven. Za sodelovanje v projektu bo Informacijski pooblaščenec s strani EU v letih 2013 in 2014 skupaj prejel namenska sredstva, in sicer 16.000,00 EUR, prejel pa jih bo v treh delih. Leta 2013 je prejel 9.600,00 EUR, od tega je bilo leta 2013 porabljenih 5.673,57 EUR za stroške službenih poti, povezanih z udeležbo na sestankih in konferencah v okviru projekta, izplačilo povečanega obsega dela zaposlenih, ki sodelujejo pri projektu, ter organizacijo osrednjega dogodka v Ljubljani: mednarodne konference Spremembe evropske direktive o ponovni uporabi informacij javnega značaja in odprtih podatkih. Preostanek sredstev se prenese v leto 2014.

Informacijski pooblaščenec je imel na računu tudi sredstva za kratkoročne obveznosti za prejete varščine v znesku 793,42 EUR. Založena sredstva predstavljajo predujem stranke za postavitev izvedenca po Zakonu o splošnem upravnem postopku[11]. Leta 2013 je bil iz sredstev poravnan račun za izvedenca za informatiko v znesku 447,00 EUR. Preostanek sredstev se prenese v leto 2014.

[11] Uradni list RS, št. 24/2006-UPB2, s spremembami in dopolnitvami; v nadaljevanju ZUP.

3 DELO NA PODROČJU DOSTOPA DO INFORMACIJ JAVNEGA ZNAČAJA

3.1. 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[12]. Ta v 2. odstavku 39. člena določa, da ima vsakdo pravico dobiti informacijo javnega značaja, za katero ima v zakonu utemeljen pravni interes, razen v primerih, ki jih določa zakon. Čeprav je pravica dostopa do informacij javnega značaja ena od temeljnih človekovih pravic in kot taka tudi zaščitena na ustavni ravni, se je začela uveljavljati šele 11 let po sprejetju Ustave RS, in sicer s sprejetjem Zakona o dostopu do informacij javnega značaja[13]. Dotlej so se posamezne določbe o javnosti informacij pojavljale le v nekaterih zakonih, celostno pa jih je uredil šele ZDIJZ. Tega je Državni zbor RS 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 Direktiva 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.

3.2. Število vloženih pritožb in število rešenih zadev

ZDIJZ zagotavlja dostop do informacij, ki so že ustvarjene, in sicer v kakršni koli obliki. S tem zakon zagotavlja preglednost porabe javnega denarja in odločitev javne uprave, saj ta dela v imenu ljudi in za ljudi. Zavezanci za dostop do informacij javnega značaja so vsi državni organi, organi lokalnih skupnosti, javne agencije, javni skladi in druge osebe javnega prava, nosilci javnih pooblastil in izvajalci javnih služb – zakon jih imenuje s skupno besedo organi. Informacija javnega značaja je informacija, ki izvira z delovnega področja organa, obstaja pa v obliki dokumenta, zadeve, dosjeja, registra, evidence ali drugega dokumentarnega gradiva, ki ga je organ izdelal sam, v sodelovanju z drugim organom ali ga je pridobil od drugih oseb. Informacije javnega značaja so prosto dostopne vsem, zato pravnega interesa za pridobitev informacije ni treba izkazovati, dovolj sta radovednost ter želja po znanju in obveščenosti. Vsak prosilec ima na svojo zahtevo od organa pravico pridobiti informacijo javnega značaja, in sicer tako, da jo dobi na vpogled ali da 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 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

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

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 1. 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 1. odstavka 6. člena ZDIJZ se dostop do zahtevane informacije dovoli tudi, če gre za podatke o porabi javnih sredstev ali za 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[14] 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 sodijo 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 2013 je Informacijski pooblaščenec prejel 610 pritožb, od tega 271 zoper zavrnilne odločbe in 339 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 258 odločb (od tega 53 v zadevah, ki jih je Informacijski pooblaščenec prejel v reševanje pred letom 2013, v enem primeru pa je po prejeti sodbi Upravnega sodišča v zadevi ponovno odločal), štirje prosilci so pritožbo umaknili, v dveh primerih je Informacijski pooblaščenec pritožbo s sklepom zavrgel, v enem primeru pa je zadeve združil.

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 mu zahtevane informacije javnega značaja tudi 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 27 primerih je Informacijski pooblaščenec pritožbo zaradi preuranjenosti ali pomanjkljive vloge s sklepom zavrgel, osem posameznikov je pritožbe umaknilo, ker so zahtevano dokumentacijo prejeli, v 11 primerih pa je Informacijski pooblaščenec prosilcem pojasnil, da za reševanje njihovih vlog ni pristojen in jih je odstopil v reševanje pristojnim organom.

Informacijski pooblaščenec je leta 2013 prejel tudi 206 zahtev za dostop do informacij javnega značaja, ki bi jih prosilci morali nasloviti na organe prve stopnje, ki z informacijami razpolagajo in morajo najprej odločiti o zahtevi prosilca. Informacijski pooblaščenec je v postopku dostopa do informacij javnega značaja pritožbeni organ, kar pomeni, da o zadevi odloča šele, ko dobi pritožbo prosilca, ki mu je organ prve stopnje vlogo za dostop do informacij javnega značaja z odločbo zavrnil. Zato je Informacijski pooblaščenec vse takšne vloge poslal oziroma odstopil v reševanje organom prve stopnje.

[14] 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 2013 je bilo opravljenih 54 takšnih ogledov.

Leta 2013 je Informacijski pooblaščenec prejel 622 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.

3.3. 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 2013 je bilo zoper odločbe Informacijskega pooblaščenca na Upravnem sodišču RS vloženih 23 tožb (zoper 8,9 % izdanih odločb). Ker sta dva tožnika tožbi umaknila, je delež odločb, zoper katere so bile vložene tožbe, še nekoliko manjši, in sicer 8,1 %. Delež vloženih tožb že nekaj let upada: leta 2011 so bile tožbe vložene zoper 13,1 % odločb, ki jih je izdal Informacijski pooblaščenec, leta 2012 pa zoper 10,5 %. 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 RS je leta 2013 odločilo o 33 tožbah, ki so bile vložene zoper odločbe Informacijskega pooblaščenca, in:

- tožbo zavrnilo (17),
- tožbi ugodilo, izpodbijano odločbo oziroma del odločbe odpravilo ali razveljavilo in zadevo vrnilo Informacijskemu pooblaščencu v ponovno odločanje (10),
- postopek zaradi umika tožbe ustavilo (2),
- tožbo zavrglo (2),
- tožbi delno ugodilo oziroma izpodbijano odločbo v enem delu odpravilo in vrnilo Informacijskemu pooblaščencu v ponovno odločanje, v preostalem delu pa zavrnilo ali zavrglo (1),
- tožbo v enem delu zavrnilo, v drugem pa zavrglo (1).

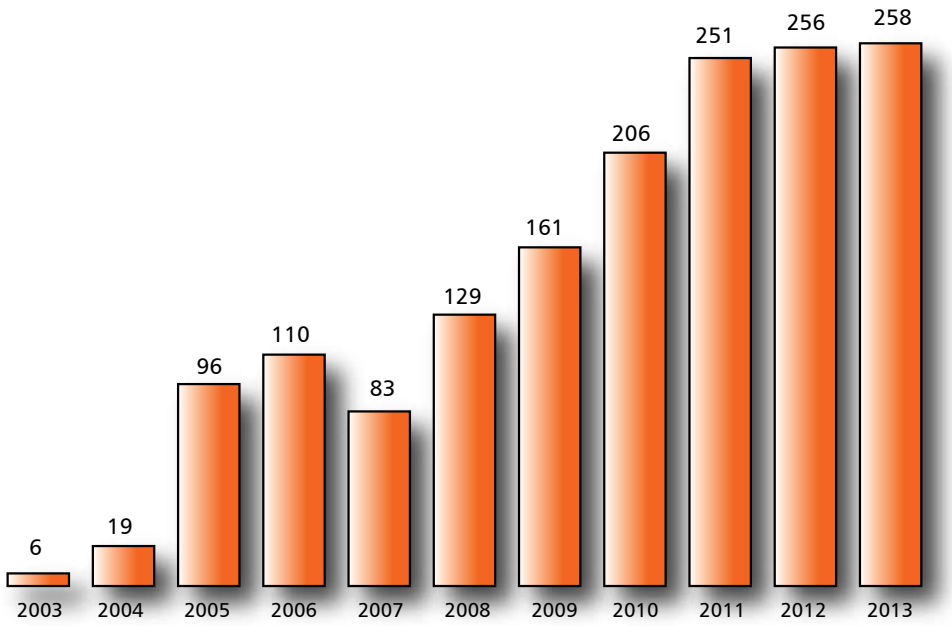
Leta 2013 ni bila zoper sodbe Upravnega sodišča RS na Vrhovno sodišče RS vložena nobena revizija.

Leta 2013 je Vrhovno sodišče RS odločilo o reviziji in pritožbi, ko sta bili vloženi zoper sodbo in sklep Upravnega sodišča RS. Sodišče je zahtevo za revizijo zavrglo, pritožbo zoper sklep pa zavrnilo.

3.4. Statistika po posameznih področjih ZDIJZ

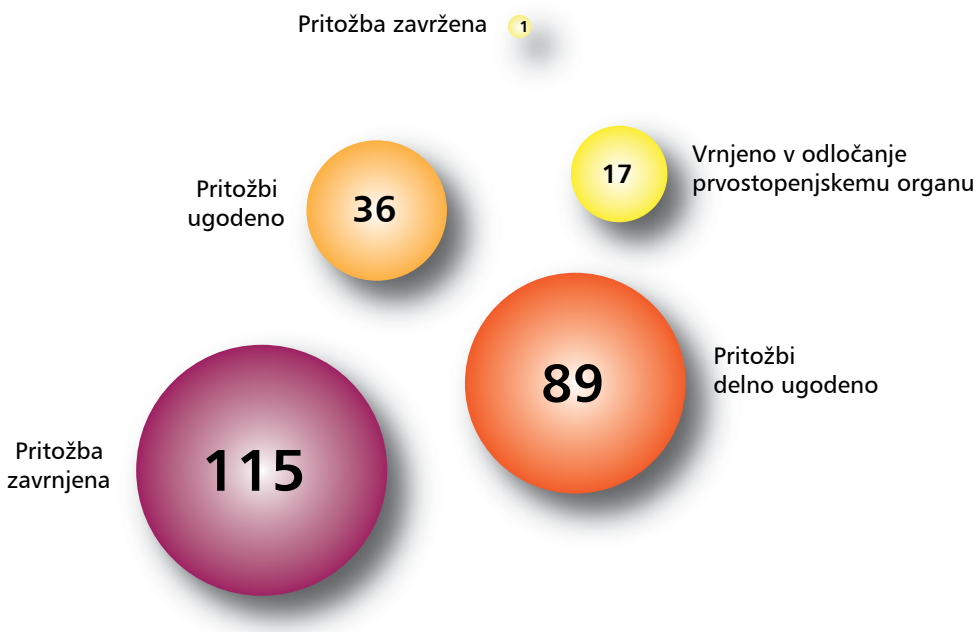
Število izdanih odločb na področju dostopa do informacij javnega značaja se je v primerjavi s preteklimi leti malenkost povečalo. Leta 2011 je bilo izdanih 251 odločb, leta 2012 256, leta 2013 pa 258.

Slika 3: Število izdanih odločb na področju dostopa do informacij javnega značaja med letoma 2003 in 2013.



Informacijski pooblaščenec je v izdanih odločbah:
- v 115 primerih pritožbo zavrnil,
- v 89 primerih dostop do informacije delno odobril,
- v 36 primerih pritožbi ugodil in zadevo rešil v korist prosilca,
- v 17 primerih zadevo vrnil v ponovno odločanje prvostopenjskemu organu,
- v enem primeru pritožbo zavrgel.

Slika 4: Odločitve Informacijskega pooblaščenca glede prejetih pritožb.



Informacijski pooblaščenec je v odločbah vsebinsko odločal oziroma presojal:

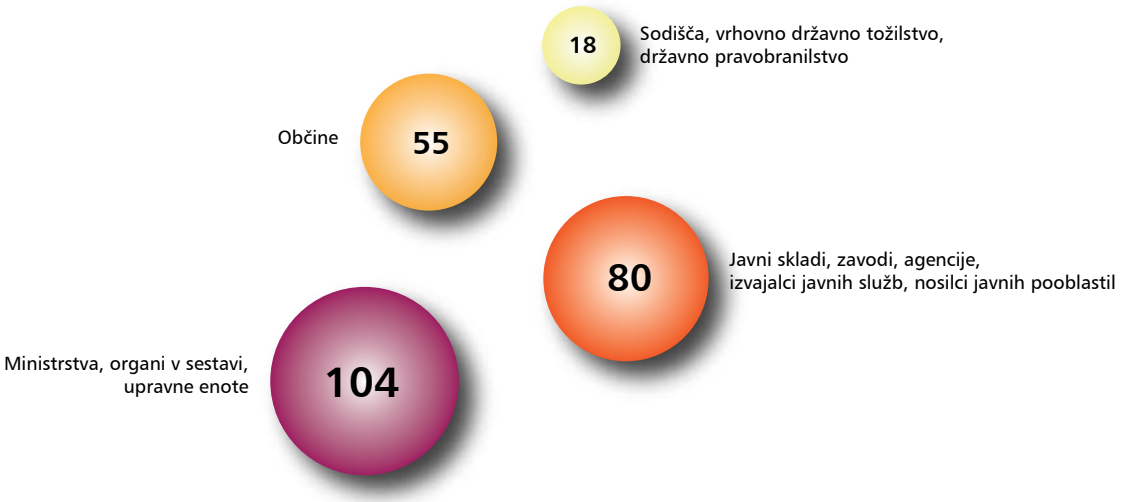
- ali zavezanec sploh ima dokument oziroma informacijo javnega značaja, ki jo je prosilec zahteval (104);
- ali zahtevani dokumenti vsebujejo osebne podatke, katerih razkritje bi pomenilo kršitev varstva osebnih podatkov v skladu z ZVOP-1 (91);
- ali prosilci zahtevajo informacije oziroma podatke, ki so v skladu z zakonom, ki ureja gospodarske družbe, opredeljeni kot poslovna skrivnost (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 (33);
- ali gre za kršitev pravil postopka (26);
- ali se zahtevane informacije nanašajo na delo in osebne podatke javnih uslužbencev in funkcionarjev (19);
- ali je organ pravilno zaračunal stroške posredovanja informacij javnega značaja (18);
- izdaja odločbe v postopku, ko je prosilec zahteval dokument iz postopka javnega naročanja (16);
- ali je interes javnosti glede razkritja močnejši od javnega interesa ali interesa drugih oseb za omejitev dostopa do zahtevane informacije (16);
- ali gre za delovno področje organa (13);
- 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 (11);
- 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 (10);
- izdaja odločbe v postopku, ko organ prosilcu ni izdal odločbe v zvezi z zahtevanimi dokumenti, ampak mu je dal informacije javnega značaja, ki jih prosilec sploh ni zahteval (10);
- ali je organ, na katerega je bila zahteva po dostopu do informacije javnega značaja naslovljena, sploh zavezanec v skladu s 1. odstavkom 1. člena ZDIJZ (9);
- 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 (9);
- ali je zahtevana informacija zavarovana skladno z zakonom, ki ureja avtorsko pravico– v takih primerih se prosilcu omogoči seznanitev z informacijo tako, da se mu jo da na vpogled (7);
- ali so zahtevane informacije podatki, ki so bili pridobljeni ali sestavljeni zaradi upravnega postopka, in bi njihovo razkritje škodovalo njegovi izvedbi (6);
- ali gre za ponovno uporabo informacije javnega značaja (6);
- ali so zahtevane informacije podatki, katerih razkritje bi pomenilo kršitev zaupnosti davčnega postopka ali davčne tajnosti skladno z zakonom, ki ureja davčni postopek (5);
- ali so zahtevane informacije podatki, ki so na podlagi zakona, ki ureja tajne podatke, opredeljeni kot tajni (2);
- ali gre za arhivsko gradivo (2);
- ali zahtevani dokument izpolnjuje pogoje za obstoj informacije javnega značaja v skladu s 1. odstavkom 4. člena ZDIJZ (1);
- pravo EU (1);
- ali gre za zlorabo pravice po ZDIJZ (1);
- ali gre za okoljske podatke (1);
- proaktivna objava 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).

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

- državne organe 122, od tega ministrstva in organe v sestavi ter upravne enote 104, sodišča, vrhovno državno tožilstvo, državno pravobranilstvo pa 18,
- javne sklade, zavode, agencije, izvajalce javnih služb in nosilce javnih pooblastil 80,
- občine 55.

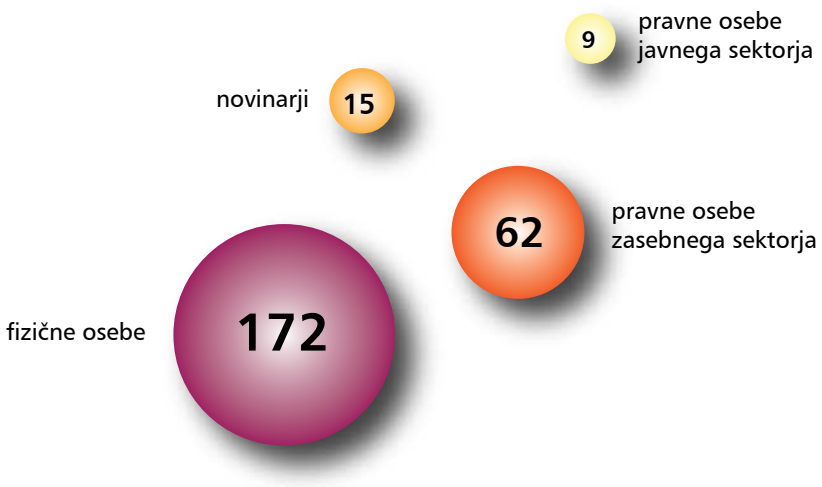
Ena pritožba se je nanašala na pravno osebo zasebnega sektorja, za katero pa je bilo ugotovljeno, da ni zavezanec po ZDIJZ.

Slika 5: Pritožbe prosilcev glede na zavezanca.



V 172 primerih so bili prosilci fizične osebe, v 62 primerih so se pritožile pravne osebe zasebnega sektorja, novinarji so se pritožili 15-krat, pravne osebe javnega sektorja pa 9-krat.

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



3.5. Storjeni prekrški po ZDIJZ, ZInfP in ZMed

Leta 2013 sta bila uvedena dva postopka o prekršku, in sicer:
- zaradi storitve prekrška po 3. odstavku 39. člena ZDIJZ, ker organ kljub pozivom Informacijskega pooblaščenca prosilcu ni posredoval zahtevanih informacij javnega značaja ali odločil o njegovi zahtevi z odločbo,
- zaradi storitve prekrška po 1. odstavku 15. člena ZInfP, ker organ Informacijskemu pooblaščencu ni posredoval zahtevanih dokumentov, ki so bili potrebni za odločitev v pritožbenem postopku.

En postopek je bil zaključen z izrekom sankcije (globe) kršitelju, drug postopek pa je bil ustavljen, ker je organ posredoval zahtevane dokumente.

Leta 2013 je Informacijski ooblaščenec prejel sodbo okrajnega sodišča v zvezi z zahtevo za sodno varstvo, ki je bila vložena zoper odločbo o prekršku Informacijskega pooblaščenca, s katero je kršitelju izrekel globo zaradi prekrška po 3. odstavku 39. člena ZDIJZ. Sodišče je zahtevi za sodno varstvo delno ugodilo in odločbo o prekršku spremenilo tako, da je storilcu znižalo izrečeno globo. V ostalem delu je zahtevo za sodno varstvo zavrnilo kot neutemeljeno.

3.6. Predstavitev najodmevnejših in precedenčnih primerov po področjih

V nadaljevanju je predstavljenih nekaj najzahtevnejših in najzanimivejših odločb iz leta 2013, ki so razvrščene po področjih.

3.6.1. Notranje delovanje organa

Informacijski pooblaščenec je delno odpravil odločbo št. 090-40/2013/4 z dne 13. 3. 2013 in Ministrstvu za notranje zadeve naložil posredovanje dela vloge, ki jo je organ na podlagi Uredbe o obrambnih in zaupnih naročilih[15] posredoval medresorski komisiji in ki vsebuje informacije o namembnosti naročila in informativne podatke o predmetu naročila.

V delu odločbe, ki ga je izpodbijal prosilec, se je organ skliceval na 11. točko 1. odstavka 6. člena ZDIJZ. Na ta način so varovani dokumenti ali deli dokumentov, ki so namenjeni komuniciranju znotraj organa ali med organi, kamor po mnenju organa sodijo taktika in metodika dela policije, tehnična opremljenost, uporaba specialnih tehničnih sredstev, notranja splošna navodila za izvajanje preiskav, navodila za identifikacijo postopkov, pa tudi občutljiva notranja navodila, načrti, ki določajo način, taktiko in metodiko zbiranja in izvajanja raznih vrst nadzora in preiskav. Če bi vsi tovrstni dokumenti postali javni, bi to lahko resno ogrozilo kritično, inovativno in učinkovito delo organa oz. učinkovito preiskovanje kaznivih dejanj ter ogrozilo varnost izvajalcev. Razkritje informacij o namembnosti naročila in informativnih podatkov o predmetu naročila, bi po mnenju organa škodovalo učinkovitemu delovanju in izvajanju nalog policije.

Informacijski pooblaščenec je najprej ugotovil, da zahtevane informacije niso nastale v zvezi z notranjim delovanjem organa. Nastale so namreč v okviru postopka po Uredbi o obrambnih in zaupnih naročilih, na podlagi katere je moral naročnik, ki je želel pridobiti soglasje medresorske komisije iz 5. člena omenjene uredbe za izvedbo posameznega naročila, v pisni vlogi navesti predmet in namen naročila ter utemeljiti dejstva in razloge, iz katerih je nedvomno razvidna namembnost naročila, katere bistvene interese varnosti Republike Slovenije se mora pri izvedbi naročila varovati oz. kateri posebni varnostni ukrepi so zato pot-

[15] Uradni list RS, št. 80/2007, konec veljavnosti 30. 12. 2012, z Zakonom o javnem naročanju na področju obrambe in varnosti (Uradni list RS, št. 90/2012), v nadaljevanju Uredba o obrambnih in zaupnih naročilih.

rebni. Takšna vloga ni namenjena notranjemu delovanju organa, temveč predstavlja zunanjo komunikacijo, ki jo je predvidevala že sama Uredba o obrambnih in zaupnih naročilih. O notranjem delovanju organa bi govorili takrat, ko bi se znotraj organa npr. še usklajevali o vsebini predmeta in namenu naročila, ki bi izkazoval pristop k reševanju strokovnih vprašanj, izpostavljanju določenih problemov in proces oblikovanja odločitev organa. V fazi, ko je organ izpolnil vlogo in jo posredoval medresorski komisiji, pa gre za informacije, ki jih organ ne vodi na neformalen način za notranje potrebe, temveč tako, kot mu to nalaga Uredba o obrambnih in zaupnih naročilih. Obravnavana vloga je sicer povezana z zaupnim naročilom, vendar dokument ne nosi oznake tajnosti po Zakonu o tajnih podatkih[16]. Obrazec za izpolnitev vloge ima v opombah navodilo, da naročnik v vlogi praviloma ne navaja tajnih podatkov, če pa jih navede, se vloga označi skladno z določbami ZTP. Takšna narava dokumenta zelo očitno nakazuje na prepričanje, da ne gre za dokument oz. informacijo v zvezi z notranjim delovanjem organa, saj ne razkriva notranjega razmišljanja organa, temveč predstavlja tipičen primer »zunanjega delovanja«, s katerim organ izvršuje svoje pristojnosti, ki so v zvezi z nakupi sredstev, ki jih potrebuje pri svojem delu.

Zahtevane informacije ne bi prestale niti škodnega testa iz 11. točke 1. odstavka 6. člena ZDIJZ, saj organ, ki nosi dokazno breme, ni izkazal, da bi razkritje zahtevanih informacij povzročilo motnje pri delovanju oz. dejavnostih organa. Po stališču Upravnega sodišča RS je dokazno breme glede razlogov za nastanek motenj v delovanju organa na strani organa in dokazni standard »bi razkritje povzročilo motnje« je dokazni standard »onkraj dvoma«, ne pa zgolj »verjetnost« (sodba št. I U 1176/2010-12). Informacijski pooblaščenec se strinja z organom, da bi razkritje konkretnih podatkov o opremljenosti s tehničnimi sredstvi lahko ogrozilo učinkovito delo organa, vendar v konkretnem primeru zahtevane informacije tovrstnih podatkov ne razkrivajo. Gre za informacije, ki na splošno opredeljujejo potrebo organa po določenem tehničnem sredstvu, na podlagi katerih pa ni mogoče ugotoviti konkretno, katero sredstvo je predmet naročila, saj bi bila sicer vloga označena s stopnjo tajnosti. Na podlagi informacij, ki so predmet presoje, ni mogoče ugotoviti tehničnih zmogljivosti naročila, prav tako ni mogoče ugotoviti, v kakšnih primerih, s kakšno metodo, taktiko dela bi organ sredstvo uporabil. Vselej se lahko špekulira, a to ne more biti razlog za zakritje informacij. Organ je v medijih že večkrat tudi sam pojasnil razpolaganje in uporabo določenih sredstev, saj je po vsej verjetnosti ocenil, da s tovrstnimi podatki ne more ogroziti svojega dela. Zato ni konkretnega razloga, da bi splošne informacije o predmetu naročila, ki so zahtevane v tem primeru, obravnavali drugače. Kljub zaupnosti določenih naročil gre namreč tudi v takih primerih za porabo javnih sredstev, zato je javnost upravičeno zainteresirana, da vsaj okvirno razpolaga s podatki, za kaj se troši denar davkoplačevalcev in ali država razpolaga z javnimi sredstvi gospodarno in v skladu z zakonom. Informacijski pooblaščenec je zato zaključil, da glede zahtevanih informacij zatrjevana izjema ni podana.

3.6.2. Ali dokument obstaja

Z odločbo št. 090-15/2013/6 z dne 11. 3. 2013 je Informacijski pooblaščenec zavrnil pritožbo prosilca zoper odločbo Kabineta predsednika Vlade RS, s katero je organ zavrnil zahtevo za dostop do elektronskih sporočil, ki so bila na določeno temo v določenem obdobju izmenjana med kabinetom predsednika vlade in kabinetoma določenih ministrov.

Organ je zahtevo prosilca zavrnil s pojasnilom, da z zahtevano elektronsko korespondenco ne razpolaga oz. da do nje nima dostopa, tudi če obstaja.

Informacijski pooblaščenec je ugotovil, da organ z zahtevano informacijo res ne razpolaga. Četudi je med predsednikom vlade in zadevnima ministroma bila izmenjana korespondenca o temi, ki zanima prosilca, ti dokumenti niso v posesti organa, torej organ z njimi ne razpolaga, poleg tega pa nima pravne podlage, da bi jih lahko pridobil. Iz določb Uredbe o upravnem poslovanju[17] izhaja, da se elektronska pošta primarno uporablja v službene namene, javni uslužbenci pa so dolžni tudi elektronska sporočila, ki prispejo na njihov elektronski naslov (in ne na uraden elektronski naslov organa) ustrezno evidentirati v evidenco dokumentarnega gradiva. Niti zakon niti Uredba ne predvidevata sankcije za uslužbenca, ki tovrstno ravnanje opusti, poleg tega se ne šteje, da je vsa elektronska pošta, ki prispe

[16] Uradni list RS, št. 50/2006-UPB2 s spremembami; v nadaljevanju ZTP.
[17] Uradni list RS, št. 20/2005 s spremembami; v nadaljevanju Uredba.

v elektronske predale javnih uslužbencev ali je iz njih odposlana, avtomatično službene narave in v posesti organa. Uredba namreč, sicer v manjši meri, dopušča tudi možnost uporabe elektronske pošte v zasebne namene.

Organ nima pristojnosti, da bi pregledoval elektronski predal posameznega javnega uslužbenca ali funkcionarja (npr. ime.priimek@gov.si). Javni uslužbenci in javni funkcionarji se s sklenitvijo delovnega razmerja v javnem sektorju namreč ne odpovedo v celoti zasebnosti na delovnem mestu. V okviru veljavne zakonodaje niti organ sam niti Informacijski pooblaščenec nimata pristojnosti, da bi pregledala elektronski predal posameznega javnega uslužbenca (ali javnega funkcionarja) in ugotovila, ali bi določena elektronska pošta, ki je službene narave, morala biti evidentirana v sistem dokumentarnega gradiva, pa temu ni tako. Na ta način bi namreč posegli v ustavno zavarovano pravico do komunikacijske zasebnosti javnega uslužbenca oz. javnega funkcionarja. Ustava RS v 37. členu zagotavlja tajnost pisem in drugih občil. Samo zakon lahko predpiše, da se na podlagi odločbe sodišča za določen čas ne upošteva varstva tajnosti pisem in drugih občil ter nedotakljivost človekove zasebnosti, če je to nujno za uvedbo ali potek kazenskega postopka ali za varnost države. Iz navedene določbe izhaja več pogojev, ki morajo biti izpolnjeni za dopustnost posega v tajnost pisem in drugih občil, kadar gre pri tem tudi za poseg v zasebnost, vendar v konkretnem primeru ti pogoji niso izpolnjeni. Opozoriti je treba še na odločitev Evropskega sodišča za človekove pravice v primeru Copland proti Združenemu kraljestvu. V tem primeru je sodišče delavki priznalo širok krog pravice do zasebnosti in presodilo, da je delodajalec neupravičeno posegal v njeno zasebnost. Ključni element sodbe je, da delavka ni bila vnaprej opozorjena, kdaj in v kakšnih primerih lahko delodajalec nadzira njeno elektronsko pošto.

Informacijski pooblaščenec verjame, da mu je organ posredoval vse razpoložljive dokumente, s katerimi razpolaga v zvezi z vsebino, ki zanima prosilca (izpis iz sistema Lotus Notes za določeno zadevo in pojasnila glede določenih zadev). Toda med to dokumentacijo ni dokumentov, ki so predmet zahteve prosilca. V obravnavanem primeru tako ni izpolnjen prvi pogoj iz 1. odstavka 4. člena ZDIJZ, po katerem je informacija javnega značaja le tista informacija, s katero organ že razpolaga oz. jo ima v posesti. Informacijski pooblaščenec je zato zaključil, da pritožbi prosilca ni mogoče ugoditi.

3.6.3. Test javnega interesa, javni uslužbenci, notranje delovanje

Informacijski pooblaščenec je delno odpravil odločbo št. 090-49/2013/5 z dne 6. 5. 2013 in Komisiji za preprečevaje korupcije naložil posredovanje tonskega posnetka razgovora s predsednikom ene izmed parlamentarnih strank, ki je nastal v postopku priprave Zaključnega poročila o nadzoru nad premoženjskim stanjem predsednikov parlamentarnih strank (v na-daljevanju zaključno poročilo).

Pri zavrnitvi zahteve se je organ skliceval na izjemo varstva sodnega postopka. V času odločanja organa o zahtevi za dostop do predmetnega dokumenta Upravno sodišče RS namreč še ni odločilo o tožbi zoper zaključno poročilo.

Informacijski pooblaščenec ni sledil argumentom organa. Ta v izpodbijani odločbi namreč ni pojasnil, v čem naj bi bila vsebina zahtevanega posnetka drugačna od že javno objavljene vsebine, ki izhaja iz dela zaključnega poročila, ki se nanaša na konkretnega predsednika ene izmed parlamentarnih strank, in kakšne škodljive posledice bi imelo razkritje tega dela posnetka za izvedbo postopka pred Upravnim sodiščem RS. Pri tem je pomembno vedeti, da je sodišče zavrnilo predlog za začasno odredbo za odstranitev zaključnega poročila s spletnih strani organa. To pomeni, da zaključno poročilo ostaja javno dostopno, ker sodišče ni štelo, da je z njegovo javno objavo povzročena kakršna koli škoda, torej tudi ne nevarnost za izvedbo konkretnega sodnega postopka. Informacijski pooblaščenec je zaključil, da zatrjevana izjema ni podana.

Informacijski pooblaščenec je v nadaljevanju ugotovil, da gre za interni dokument, ki lahko predstavlja izjemo od javno dostopnih informacij zaradi varstva notranjega delovanja organa. Dejstvo je namreč, da seje senata organa niso javne in da potekajo v zaupnem duhu in (upoštevaje veljavne zakonske podlage) ob pričakovanju, da bo njihova vsebina ostala zaupna. Razkrivanje tovrstnih dokumentov torej lahko povzroči motnje pri delu organa,

saj se je treba zavedati, da udeleženci tovrstnih zaslišanj organa ne bi posredovali vseh odgovorov oz. navedli vseh dejstev, če bi vedeli, da bo njihovo zaslišanje v celoti prosto dostopno javnosti. Kljub temu pa je zahtevani posnetek treba razkriti javnosti, ker za to obstaja prevladujoč javni interes. V konkretnem primeru je imelo zaključno poročilo o nadzoru nad premoženjskim stanjem predsednikov parlamentarnih strank pomembne in daljnosežne politične posledice za celotno Republiko Slovenijo. Objava zaključnega poročila je privedla do zamenjave vlade, o tem so v javnosti tekle številne razprave, med drugim tudi široka javna razprava o integriteti obravnavanih javnih funkcionarjev ter njihovem odnosu do organa in njegovih ugotovitev. Zaključno poročilo kot tako predstavlja nekatere dejanske ugotovitve, iz zahtevanega zvočnega posnetka pa poleg tega izhaja tudi informacija o tem, kako je pred senatom organa tekel postopek, ali so bile določene ugotovitve organa obravnavanemu javnemu funkcionarju predstavljene, kakšen je bil njegov subjektivni odnos do teh ugotovitev in ne nazadnje, kakšen je bil njegov subjektivni odnos do organa kot do neodvisnega državnega organa. V javnosti se je v zvezi z zaključnim poročilom razvila širša javna razprava glede vprašanja politične odgovornosti nosilcev javnih funkcij in tudi glede konkretnega javnega funkcionarja, ki je župan največjega slovenskega mesta. Ne nazadnje se je ta javni funkcionar tudi sam večkrat javno izrekel tako glede same vsebine zaključnega poročila, kot tudi glede poteka postopka pred organom, v javnosti pa je bilo mogoče v zvezi s tem zaslediti očitke, da obravnavanim zavezancem ni bila dana možnost sodelovanja v postopku oz. možnost predložitve vseh dokazov. Konkretno zaključno poročilo odpira pomembno vprašanje politične odgovornosti javnih funkcionarjev, odprta razprava o tem vprašanju pa prispeva k dvigu politične kulture v Sloveniji, k razvijanju politične odgovornosti, h krepitvi integritete javnih funkcionarjev in javnih uslužbencev ter k spodbujanju odgovornega vodenja postopkov pred državnimi organi in transparentnega odločanja. Za celovito razumevanje zaključnega poročila, za odprto javno razpravo o integriteti javnih funkcionarjev v konkretnem primeru in na splošno ter za razpravo o transparentnosti vodenja postopkov in odločanja pred tako pomembnim državnim organom, kot je organ v konkretnem primeru, so pomembne tudi informacije, ki jih vsebuje zahtevani posnetek.

Upoštevaje vse navedeno je Informacijski pooblaščenec ugodil pritožbi prosilcev in v konkretnem primeru odločil, da zahtevani tonski posnetek sicer predstavlja izjemo od prosto dostopnih informacij javnega značaja, vendar gre za informacijo, katere razkritje je v javnem interesu.

3.6.4. Tajni podatki, umik stopnje tajnosti

Odločba Informacijskega pooblaščenca št. 090-157/2010/55 z dne 26. 4. 2013 je bila zadnja v nizu delnih odločb, s katerimi je odločal o pritožbi zoper dve odločbi, s katerima je Državni zbor RS odločil o zahtevi prosilca za dostop do dokumentacije, ki se nanaša na dogodke glede t. i. trgovine z orožjem oz. so v povezavi z dogodki izpred dvajsetih let, s katerimi razpolaga organ v okviru preiskovalnih komisij, ki so te dogodke obravnavale.

Predmet odločanja v tej dopolnilni odločbi je dokumentacija, ki se nahaja pri organu, vendar pa so originatorji teh dokumentov drugi organi (npr. SOVA, Urad predsednika RS, Vlada RS …). Del te dokumentacije ne nosi stopnje tajnosti oz. ji je bila stopnja tajnosti preklicana, vsebuje pa določene varovane osebne podatke, ki jih mora organ pred posredovanjem dokumentov prosilcu prekriti. Glede dokumentov, ki nosijo oznako stopnje tajnosti, je Informacijski pooblaščenec presojal, ali so ustrezno klasificirani kot tajni na podlagi ZTP in tako predstavljajo izjemo od prostega dostopa. Po ZTP je tajen tisti podatek, ki kumulativno izpolnjuje tako materialni kot formalni kriterij. Materialni kriterij vključuje dva vidika. Prvi je, da bi z razkritjem podatka nastala oz. očitno lahko nastala določena škoda, drugi pa je v povezavi škode s taksativno naštetimi interesnimi področji države (javna varnost, obramba, zunanje zadeve, obveščevalna in varnostna dejavnost državnih organov oz. se nanaša na sisteme, naprave, projekte in načrte ali znanstvene, raziskovalne, tehnološke, gospodarske in finančne zadeve, ki so pomembni za omenjene cilje). Oba materialna elementa se zrcalita v formalnem kriteriju tajnega podatka. Podatek je upravičeno lahko označen kot tajen le, če so izpolnjeni naslednji trije pogoji: podatek za tajnega določi za to pooblaščena oseba, izdelana mora biti vnaprejšnja pisna ocena o možnih škodljivih posledicah, ki bi nastale z razkritjem podatka (hrani se kot priloga dokumenta pri organu, ki je podatku določil stopnjo tajnosti, in vsebuje določitev objekta varstva, oceno teže in intenzivnosti možnih škodljivih posledic), in dokument, ki vsebuje tajni podatek, mora biti ustrezno označen kot tajen.

Zakonodajalec je stopnjo tajnosti TAJNO vezal na škodne posledice, razkritje informacije bi v tem primeru lahko hudo škodovalo varnosti ali interesu Republike Slovenije, označitev dokumentov INTERNO pa je vezal na škodo, kadar bi razkritje informacije lahko škodovalo delovanju ali izvajanju nalog organa. Pojem »hudo škodovalo varnosti ali interesu« je pravno nedoločen, zato je naloga organa, ki je takšno pravno normo uporabil za to, da je informacije odtegnil javnosti, da ji določi vsebino, tj. da konkretno navede, kako bi bila z razkritjem informacije varnost ali interes države hudo oškodovana. Informacijski pooblaščenec je ocenil, da pisne ocene možnih škodljivih posledic v konkretnem primeru tega pogoja ne izpolnjujejo. Originatorji dokumentov so v ocenah možnih škodljivih posledic uporabljali le besedne zveze iz zakona, niso pa dodali konkretnih pojasnil oz. obrazložitev, na kakšen način bi lahko razkritje zahtevanih dokumentov z oznako TAJNO hudo škodovalo varnosti ali interesu Republike Slovenije, pri dokumentih z oznako INTERNO pa škodovalo delovanju ali izvajanju nalog organa. Iz pisnih ocen škodljivih posledic ne izhaja niti, na katero varovano področje se zahtevana dokumentacija nanaša. Še več, pri dokumentih SOVE, ki nosijo oznako INTERNO, je navedeno, da bi razkritje škodovalo ugledu agencije v javnosti, kar je nedvomno v nasprotju z namenom in cilji ZTP, na podlagi katerega se lahko za tajnega določi le podatek, ki je tako pomemben, da bi z njegovim razkritjem nepoklicani osebi nastale, ali bi očitno lahko nastale, škodljive posledice za varnost države ali za njene politične ali gospodarske koristi, na izrecno določenih področjih, kamor pa ugled agencije zagotovo ne sodi. Tako ni jasno, katera zakonsko opredeljena področja bi razkritje ogrozilo. Pavšalna ocena, oprta zgolj na zakonsko normo, pomeni nezakonito uporabo instituta tajnosti, saj ni mogoče ugotoviti razlogov, ki so narekovali odločitev originatorjev dokumentov, da so jih označili z oznakama TAJNO in INTERNO, kar zakon, prav s pisno oceno možnih škodljivih posledic, v demokratični družbi zahteva. Originatorji dokumentov so tako zgolj na abstraktni ravni zatrjevali nastanek škode, ne da bi jo konkretizirali, zato ni mogoče ugotoviti, ali bi zatrjevana škodljiva posledica sploh nastala. Ob dejstvu, da sta od dogodkov, ki so zabeleženi v zahtevanih dokumentih, pretekli že dve desetletji, da se je o tem že zelo veliko govorilo v medijih, da so bile o tem objavljene knjige in da je bila velika količina dokumentov že razkrita javnosti, je škoda, ki jo zgolj pavšalno predvidevajo originatorji, povsem neizkazana oz. bi lahko že nastala z objavo že dostopnih dokumentov, ki se vsebinsko nanašajo na identična področja, kot so zavedena v dokumentih s stopnjo tajnosti, vendar je ni zaslediti, prav tako pa se nanjo niso sklicevali originatorji dokumentov. Gre za neke vrste dokumente z »zgodovinsko vrednostjo«, ki razen tega, da bi z razkritjem podali celostno sliko na takratno (že končano) dogajanje, ne morejo več škodovati varnosti ali interesu Republike Slovenije, čemur je sicer institut tajnosti namenjen. Iz navedenega izhaja, da ni prav nobenega razloga, da bi zahtevani dokumenti morali nositi kakršno koli stopnjo tajnosti, saj ni izpolnjen materialni pogoj za obstoj tajnega podatka, z vidika ocene teže in intenzivnosti možnih škodljivih posledic pa ni izpolnjen niti formalni kriterij. Izjema iz 1. točke 1. odstavka 6. člena ZDIJZ torej ni podana.

Glede na ugotovitev, da so podatki v nasprotju z zakonom, ki ureja tajne podatke, označeni s stopnjo tajnosti in glede na to, da je prosilec izrecno zahteval tudi umik stopnje tajnosti, je Informacijski pooblaščenec odločil, da morajo originatorji umakniti stopnjo tajnosti z obravnavanih dokumentov ter jih posredovati organu, ta pa jih mora posredovati prosilcu, pri čemer je dolžan prekriti varovane osebne podatke.

3.6.5. Notranje delovanje organa

Z odločbo št. 090-22/2013/6 z dne 19. 4. 2013 je Informacijski pooblaščenec odpravil odločbo Državnega izpitnega centra in mu naložil posredovanje seznama šol, ki so navedene v letnem poročilu splošne mature, v poglavju Analiza kakovosti splošne mature po šolah.

Organ je zahtevo prosilke zavrnil, pri čemer se je skliceval na 18. a člen Zakona o maturi[18], ki določa, da se podatki iz letne analize o kakovosti mature ne smejo uporabljati za razvrščanje šol. Navedeni člen je bil sprejet z namenom, da se prepove kakršno koli upravljanje s podatki, ki bi lahko pripeljalo do razvrščanja šol. Zaradi te določbe organ pripravi in objavi analizo s šifrantom, s katerim se zakrije identiteta šol.

[18] Uradni list RS, št. 1/2007-UPB1; v nadaljevanju ZMat.

Informacijski pooblaščenec je ugotovil, da gre pri zahtevanih podatkih za prosto dostopne informacije javnega značaja, ki ne vsebujejo izjem od prostega dostopa. Zahtevani podatki namreč niso takšne narave, da bi lahko varovali proces notranjega razmišljanja organa, podatki pa tudi ne izvirajo iz dokumentov, ki bi nastali ob oblikovanju politike organa in zato ne varujejo procesa oblikovanja odločitev organa ter z razkritjem ne bi ogrožali prostega pretoka idej pri oblikovanju odločitev ali ukrepov. Organ niti ni pristojen za oblikovanje politike na področju šolstva. Zahtevani dokumenti predstavljajo dejstva, zbirne podatke o rezultatih splošne mature. Tudi če bi bili zahtevani podatki v zvezi z notranjim delovanjem, njihovo razkritje organu ne bi moglo povzročiti takšne škode, ki bi resno in konkretno ogrozila njegovo delovanje oz. dejavnost. Organ bi namreč še naprej lahko opravljal vse svoje naloge, navedene v ZMat, vključno z zbiranjem in analiziranjem podatkov o maturi.

Neprepričljiv je argument organa, da so zahtevane informacije zgolj zato, ker bi lahko bile predmet napačnih interpretacij in zaključkov, netočne oz. nepravilne. Nezanesljivost zahtevanih podatkov namreč ni razlog za zavrnitev dostopa do teh informacij. Skrb organa, da bodo javnosti posredovane nezanesljive, neobdelane informacije, je sicer razumljiva, vendar ne more prerasti v izjemo notranjega delovanja organa. Organ ima namreč vedno možnost, da poda pojasnilo, s katerim se izogne napačnim interpretacijam podatkov. Tudi noveliran 18.a člen ZMat, na katerega se v konkretnem primeru sklicuje organ in ki določa, da se podatki o uspešnosti dijakov posameznih šol na maturi (ki izhajajo iz letne analize, ki jo pripravi organ) ne smejo uporabiti za razvrščanje šol, ne more biti razlog, da organ zavrne že sam dostop do teh podatkov. Navedeni člen ZMat dejansko prepoveduje le razvrščanje šol, ne prepoveduje pa samega dostopa do podatkov. Z vidika izjem, ki so navedene v 6. členu ZDIJZ, torej (novi) 18.a člen v ničemer ne spreminja dejanskega stanja glede zahtevanih informacij. Pomembno je tudi dejstvo, da bi posamični podatki, ki jih prosilka zahteva, sami po sebi predstavljali prosto dostopne informacije javnega značaja (pri čemer očitno ne bi nastala škoda, če bi jih prosilka pridobivala od vsake šole posebej), zato ne more biti sprejemljivo, da bi ti isti podatki, zgolj zaradi dejstva, ker so združeni v seznam, predstavljali izjemo od prostega dostopa. Poudariti je treba, da se v postopku po ZDIJZ vedno presoja posamičen dokument kot tak in ne dejstva, kaj bi prosilec, npr. s pomočjo uparjanja podatkov z zahtevanega dokumenta z drugimi, že prosto dostopnimi podatki, lahko izvedel, do kakšnih zaključkov bi prišel in ali bi bili takšni zaključki prosilca. Zahtevani dokument torej vsebuje le poimenski seznam šol, ki pa ne predstavlja nobene izmed izjem od prostega dostopa do informacij javnega značaja, zato ga mora organ prosilki posredovati.

3.6.6. Okoljski podatki

Z odločbo št. 090-66/2013/9 z dne 29. 5. 2013 je Informacijski pooblaščenec delno odpravil odločbo Agencije za radioaktivne odpadke in ji naložil posredovanje Priročnika vodenja projekta nizko in srednje radioaktivnih odpadkov, pri čemer je dolžna prekriti varovane osebne podatke.

Organ je z zavrnil zahtevo prosilca in navedel, da je zahtevani priročnik gradivo internega značaja in opredeljuje notranje postopke pri organu. Gre za vsebine, ki so del t. i. "know-howa" organa in se kot take štejejo za poslovno skrivnost. Priročnik ne vsebuje okoljskih vsebin, temveč zgolj procese in postopke, ki jih je treba izvesti v zvezi z vodenjem projekta odlagališča.

Informacijski pooblaščenec je v pritožbeni postopek kot stranskega udeleženca pozval gospodarsko družbo, ki je zahtevani priročnik izdelala, ta pa na poziv ni odgovorila. Nato je Informacijski pooblaščenec presojal, ali zahtevani dokument predstavlja izjemo po 2. točki 1. odstavka 6. člena ZDIJZ, in ugotovil, da ni izkazan obstoj poslovne skrivnosti po subjektivnem kriteriju (1. odstavek 39. člena Zakona o gospodarskih družbah[19]), saj za zahtevani dokument ne obstaja odredba o tem, kateri podatki se štejejo za poslovno skrivnost. Zahtevani priročnik prav tako ne prestane škodnega testa poslovne skrivnosti, kot ga določa 2. odstavek 39. člena ZGD-1 (po objektivnem kriteriju). Poudariti je treba, da so predmet poslovne skrivnosti lahko samo podatki, ki pomenijo konkurenčno prednost podjetja, organ pa pri izdelavi zahtevanega priročnika sploh ne nastopa na trgu, ampak

[19] Uradni list RS, št. 42/2006 s spremembami; v nadaljevanju ZGD-1.

izvaja javno službo ravnanja z radioaktivnimi odpadki, ki je urejena z Zakonom o varstvu pred ionizirajočimi sevanji in jedrski varnosti[20], zaradi česar na tem področju niti nima konkurentov niti ni mogoče govoriti o morebitni škodi za konkurenčni položaj organa. Poleg tega se delo organa na tem področju financira iz javnih sredstev (iz sredstev Sklada NEK), zato podatki, ki pri izvajanju te naloge nastanejo, ne morejo biti poslovna skrivnost, saj bi bilo to v nasprotju s 3. odstavkom 39. člena ZGD-1 v povezavi s 3. odstavkom 6. člena ZDIJZ. Da ne gre za podatke, katerih razkritje bi povzročilo občutno škodo za tržni položaj kakega drugega subjekta, pa potrjuje dejstvo, da gospodarska družba, ki je dokument izdelala, sploh ni prijavila stranske udeležbe v pritožbenem postopku.

V konkretnem primeru tudi ni moč govoriti o obstoju izjeme iz 9. točke 1. odstavka 6. člena ZDIJZ, saj zahtevani priročnik ni več v postopku izdelave pri organu ter ni več predmet posvetovanja znotraj organa. Gre za celovit in tehnično dokončno izdelan dokument, ki sicer lahko predstavlja le različico tiste verzije priročnika, ki bo v posameznih fazah projekta odlagališča tudi dejansko uporabljena, vendar to ne spremeni dejstva, da gre za dokončan dokument. Glede obstoja škode zaradi napačnega razumevanja vsebine dokumenta s strani javnosti je dokazno breme na organu, ki je ta element obravnavane izjeme zatrjeval zgolj na abstraktni ravni. Zaskrbljenost zaradi morebitnega napačnega razumevanja pa je mogoče odpraviti na druge načine, ki ne ovirajo dostopa do zahtevanih informacij, npr. s pojasnili. Seznanitev javnosti z zahtevanim dokumentom bi tako celo pripomogla, da bi javnost pravilno razumela zahtevani dokument ter laže sodelovala pri ustrezni ureditvi odlagališča.

Četudi bi bilo zahtevani priročnik mogoče opredeliti kot katero izmed izjem od prostega dostopa do informacij, bi bilo javnosti treba omogočiti dostop na podlagi 3. odstavka 6. člena ZDIJZ, ker gre za podatke o porabi javnih sredstev in za okoljske podatke. Tako izdelava zahtevanega priročnika kot tudi projekt odlagališča, ki je vsebina tega priročnika, sta financirana z javnimi sredstvi. Hkrati so podatki v zahtevanem priročniku podatki o nizko in srednje radioaktivnih odpadkih (v nadaljevanju NSRAO) ter podatki, ki so neposredno in neločljivo povezani s to vrsto podatkov (npr. pravne podlage za ravnanje s temi odpadki, namen in cilj projekta odlagališča teh odpadkov, finančni okvir in izdelki druge faze projekta, organiziranost projekta in ključni procesi njegove izvedbe), saj temeljijo na realnih in predvidenih podatkih o NSRAO v zvezi z odlagališčem in jih ni mogoče ločiti od te vrste podatkov, saj oboji skupaj tvorijo neločljivo celoto. Gre torej za priročnik, ki opisuje procese, ki se bodo izvajali v projektu odlagališča NSRAO, ki pa jih ni bilo mogoče oblikovati brez podatkov glede emisij v okolje, odpadkov, nevarnih snovi v obratu. Brez teh podatkov tudi ni bilo mogoče določiti faz, organizacije, namenov in ciljev projekta ter posledično tudi finančnih okvirov. Zahtevani dokument vsebuje procese in postopke, ki jih je treba izvesti v zvezi z vodenjem projekta odlagališča NSRAO, iz česar izhaja, da ta dokument vsebuje podatke glede NSRAO.

Upoštevaje definicije pojmov iz 3. člena Zakona o varstvu okolja[21], ki med temeljnimi načeli določa načelo sodelovanja in načelo javnosti, je Informacijski pooblaščenec ugotovil, da so podatki o NSRAO okoljski podatki, ki se nanašajo na odpadke, ker gre za določene snovi oz. predmete, ki jih bo njegov povzročitelj ali druga oseba, ki bo imela snov oz. predmet v posesti, zavrgel. V konkretnem primeru je te odpadke mogoče opredeliti še bolj natančno, in sicer gre za radioaktivne odpadke, ki so v ZVO-1 opredeljeni kot odpadki, ki so zaradi določenih radioaktivnih lastnosti po predpisih o varstvu pred ionizirajočimi sevanji uvrščeni med radioaktivne odpadke. Gre tudi za snovi, ki oddajajo ionizirajoče sevanje, zato njihov učinek na okolje označujemo tudi kot emisije. Hkrati je treba NSRAO opredeliti tudi kot t. i. nevarno snov.

Vsebino zahtevanega priročnika torej predstavljajo podatki glede nevarnih snovi, odpadkov in emisij. Dostop do takšnih podatkov se na podlagi druge alineje 3. odstavka 6. člena ZDIJZ dovoli ne glede na določbe 1. odstavka 6. člena ZDIJZ, ki opredeljujejo izjeme od prostega dostopa do informacij javnega značaja. ZDIJZ je z omenjeno določbo postavil zakonsko predpostavko, da je prevladujoč interes javnosti za razkritje podatkov podan vselej, kadar gre za podatke glede emisij v okolje, odpadkov, nevarnih snovi v obratu ali podatke iz varnostnega poročila in druge podatke, za katere tako določa zakon, ki ureja varstvo okolja. Na ta način je zakonodajalec razširil pravice, ki jih zagotavlja 2. odstavek 6. člena ZDIJZ, saj izkazovanje in dokazovanje prevladujočega interesa javnosti v takih primerih ni potrebno.

[20] Uradni list RS, št. 67/2002 s spremembami; v nadaljevanju ZVISJV.
[21] Uradni list RS, št. 41/2004 s spremembami; v nadaljevanju ZVO-1.

Informacijski pooblaščenec je zaključil, da vsebina zahtevanega priročnika, na podlagi druge alineje 3. odstavka 6. člena ZDIJZ, ne sme biti izvzeta iz prostega dostopa, kar pomeni, da je zahtevani priročnik tudi iz tega vidika prosto dostopna informacija javnega značaja. Organ je zato prosilcu dolžan posredovati zahtevani priročnik, pri čemer pa mora prekriti varovane osebne podatke.

3.6.7. Avtorsko delo

Z odločbo št. 090-83/2013/7 z dne 26. 6. 2013 je Informacijski pooblaščenec delno odpravil odločbo Občine Kanal ob Soči in ji naložil posredovanje fotokopije recepta za marijaceljski kolač in pogodbe za odkup tega recepta, pri čemer mora prekriti varovane osebne podatke.

Organ je zahtevo prosilca po posredovanju fotokopije recepta za kolač zaradi obstoja avtorskih pravic zavrnil, omogočil pa mu je vpogled. Za pogodbo o odkupu recepta je organ navedel, da ne obstaja.

Informacijski pooblaščenec je ugotovil, da organ razpolaga s pogodbo z naslovom Pogodba o stvaritvi avtorskega dela, na podlagi katere je bil v okviru projekta LAS odkupljen zahtevani recept. Ta pogodba vsebuje nekatere osebne podatke posameznice, s katero je bila pogodba sklenjena, ki so varovani osebni podatki, z izjemo imena in priimka. Podatek o tem, komu je organ izplačal sredstva iz proračuna, predstavlja podatek o porabi javnih sredstev in zato, na podlagi 3. odstavka 6. člena ZDIJZ, ne more predstavljati izjeme od prostega dostopa do informacij. Ob posredovanju fotokopije pogodbe prosilcu mora organ prekriti varovane osebne podatke.

Prosilec ima, na podlagi 17. člena ZDIJZ, pravico določiti, na kakšen način se želi seznaniti z zahtevano informacijo. Edino omejitev, ki vpliva na obliko posredovanja informacije, predstavlja določba 2. odstavka 25. člena ZDIJZ, po kateri lahko prosilec dobi samo vpogled v informacijo, ki je zavarovana skladno z zakonom, ki ureja avtorsko pravico. Ker je prosilec želel pridobiti fotokopijo recepta za kolač, je bilo treba ugotoviti, ali je ta dokument zavarovan z zakonom, ki ureja avtorsko pravico, in posledično, ali je iz tega razloga mogoče omejiti način seznanitve z zahtevano informacijo. V skladu s 5. členom Zakona o avtorski in sorodnih pravicah[22] je avtorsko delo individualna intelektualna stvaritev s področja književnosti, znanosti in umetnosti, ki je izražena na kakršen koli način, če ni v ZASP drugače določeno. Iz navedene definicije in obstoječe sodne prakse ter pravne teorije izhaja pet predpostavk, ki morajo biti kumulativno izpolnjene, da se posamezno delo šteje za avtorsko delo po ZASP, in sicer so to individualnost, intelektualnost oz. duhovnost, stvaritev, področje ustvarjalnosti in izraženost. Informacijski pooblaščenec je ugotovil, da v konkretnem primeru ni izpolnjen kriterij individualnosti dela. Individualnost dela predstavlja značilnost, ki avtorsko delo ločuje od drugih avtorsko varovanih del od avtorsko nevarovanih del ter hkrati od umetniške in kulturne dediščine, ki je last širše javnosti. Gre za zahtevo po tem, da ima delo vsaj toliko izvirnih potez, da se ga še lahko uvršča med avtorska dela. Če torej avtor neodvisno od nekega drugega dela ustvari svoje delo z individualnimi potezami, torej brez posnemanja oz. neposrednega prevzemanja iz drugega dela, je izpolnjena predpostavka individualnosti dela. Pri stvaritvi, ki vsebuje le nabor podatkov in dejstev, pogoj individualnosti ni izpolnjen in ta ni varovana kot avtorsko delo. V konkretnem primeru gre za recept, ki vsebuje seznam sestavin, potrebnih za pripravo kolača, in kratka navodila o tem, kako sestavine zmešati in pripraviti, da bo nastal želeni produkt. Ta recept se glede na individualnost oz. ustvarjalnost drugih, podobnih receptov na spletu ne razlikuje toliko, da bi ga bilo mogoče šteti za avtorsko delo. Recept ni napisan na poseben, izviren način, ne vsebuje kakih grafičnih elementov, po katerih bi se razlikoval od drugih receptov, objavljenih na spletu. Prav tako sama raba besed in stavčnih struktur ni drugačna od običajne rabe teh elementov v receptih, dostopnih javnosti. Avtorskopravno se varuje izraženost ideje in ne ideja sama. Dejstvo, da se je avtorica recepta morda domislila neke nove sestavine za pripravo kolača, še ne pomeni, da recept kot izraz te ideje izpolnjuje kriterij individualnosti. Za dosego tega kriterija bi recept moral biti izražen na izviren način (npr. v obliki pravljice, pesmi, slikovno itd.), torej bi moral biti podan drugače od ostalih receptov. V konkretnem primeru gre za standardno naštevanje sestavin in običajna navodila za pripravo kolača, kriterij individualnosti glede zahtevanega recepta ni izpolnjen in posledično ne predstavlja avtorskega dela, zaradi česar

[22] Uradni list RS, št. 94/2004 s spremembami; v nadaljevanju ZASP.

ni ovir, da bi ga organ prosilcu posredoval v obliki fotokopije.

Četudi bi recept predstavljal avtorsko delo, so materialne avtorske pravice na zahtevanem dokumentu s pogodbo za odkup tega recepta prenesene na organ in ima ta pravico do reproduciranja in distribucije reprodukcije zahtevanega dokumenta. Navedbe organa o nedopustnosti posredovanja fotokopije zahtevanega dokumenta prosilcu so zato povsem neutemeljene.

3.6.8. Poslovna skrivnost, test javnega interesa

Z odločbo št. 090-91/2013/9 z dne 15. 7. 2013 je Informacijski pooblaščenec zavrnil pritožbo prosilke zoper odločbo Ministrstva za finance, s katero je organ delno zavrnil zahtevo za dostop do predloga prestrukturiranja Nove Ljubljanske banke, d. d. (v nadaljevanju stranska udeleženka).

Organ je zahtevo prosilke delno zavrnil zaradi varstva poslovne skrivnosti stranske udeleženke. Organ je ugotovil, da zahtevani dokument predstavlja poslovno skrivnost po subjektivnem kriteriju ter da javni interes glede razkritja ni močnejši od interesa stranske udeleženke za omejitev dostopa do zahtevanega dokumenta. Ker pa gre pri delih zahtevanega dokumenta za podatke, ki se nanašajo na porabo javnih sredstev, je organ v tem delu zahtevi prosilke ugodil, v preostalem delu pa je njeno zahtevo zavrnil.

Informacijski pooblaščenec je ugotovil, da zahtevani dokument vsebinsko ustreza opredelitvi poslovne skrivnosti po 1. odstavku 39. člena ZGD-1, saj je v dokumentu izrecno opredeljeno, da vsebina tega dokumenta predstavlja poslovno skrivnost. Stranska udeleženka je storila vse potrebno, da bi zavarovala podatke, ki jih je označila kot poslovno skrivnost, vendar pa obravnavani dokument vsebuje nekatere podatke, ki so javni že na podlagi zakona in zato po 3. odstavku 39. člena ZGD-1 ne morejo predstavljati poslovne skrivnosti. To so informacije, ki izkazujejo porabo javnih sredstev, ki so, ne glede na označitev poslovne skrivnosti, vselej javne. Informacijski pooblaščenec je ugotovil, da, razen podatkov, ki jih je kot prosto dostopne označil organ, ni drugih konkretnih informacij, ki bi izkazovale porabo javnih sredstev. Samo morebitna možnost pridobivanja dodatnih državnih sredstev v prihodnosti še ne pomeni porabe javnih sredstev v smislu 3. odstavka 6. člena ZDIJZ.

Informacijski pooblaščenec je izvedel tudi test interesa javnosti (2. odstavek 6. člena ZDIJZ). Pojem »javni interes« je pravno nedoločen pojem, zato se v vsakem konkretnem primeru ugotavlja, ali so podane okoliščine, ki so v interesu širše skupnosti in ne zgolj posameznika. Res je, da smo ljudje po naravi najbolj občutljivi, kadar gre za naše zdravje, življenje in varnost, vendar v določenih okoliščinah občutljivost ni nič manjša, ko gre na primer za informacije, ki so povezane z delovanjem države na finančnem področju, saj se posledice tega delovanja velikokrat kažejo oz. vplivajo na omenjene vrednote. Država je kot večinski lastnik stranske udeleženke v preteklosti večkrat finančno posredovala bodisi z dokapitalizacijami ali drugimi načini financiranja, da bi banka ustrezala zakonskim obveznostim z vidika kapitalske ustreznosti. V javnosti se omenja, da banka potrebuje dodatna državna sredstva. V konkretnem primeru je predmet presoje program prestrukturiranja, ki razen v že omenjenem delu, ne govori o porabi javnih sredstev, temveč o načrtu, kako nastalo situacijo rešiti. Gre torej za podatke, ki so še v fazi usklajevanja z Evropsko komisijo, ki zahteva izpolnjevanje določenih pogojev, da bi se izvedla uspešna sanacija banke, kar je zagotovo v javnem interesu. Po navedbah organa je večji kot interes javnosti za razkritje zahtevanega dokumenta interes javnosti, da so v tej fazi ti podatki javnosti nedostopni, saj bi v nasprotnem primeru konkurenca lahko ugotovila, kje ima stranska udeleženka slabosti; na ta način se ščiti davkoplačevalski denar, ki je že bil vložen v stransko udeleženko. Glede na dejstvo, da dokončna odločitev o prestrukturiranju še ni sprejeta, je Informacijski pooblaščenec sledil navedbam organa in navedbam stranske udeleženke, da bi razkritje zahtevanih informacij, ki še ne predstavljajo dokončne odločitve, vplivalo na stabilnost bančnega sistema na globalnem trgu kot tudi na samo stransko udeleženko. Razkritje informacij, ki niso dokončne in so šele del strategije prestrukturiranja, bi nedvomno vplivalo na konkurenčno sposobnost banke na trgu, z vidika izgubljanja strank – komitentov, zmanjšanja sredstev (depozitov), prav tako bi se lahko poslabšale možnosti prodaje nestrateških naložb. Z razkritjem informacij v tej fazi sanacije banke bi dosegli ravno nasprotno od njenega namena. Povsem razumljivo je, da komitente in splošno javnost zanima, ali banka, ki je v večinski lasti države,

ravna gospodarno in ali je še vredna zaupanja, zlasti ob informacijah, ki se pojavljajo v medijih (sporni krediti, kadrovanje, nakupi vozil ...), vendar je treba poudariti, da test interesa javnosti ni namenjen temu, da se razkrije nekaj, kar je ''interesantno za javnost'', temveč da se razkrije tisto, kar je ''v interesu javnosti''. Podatki, ki jih zahteva prosilka, so morebiti za javnost interesantni, nikakor pa v tej fazi niso v interesu javnosti, saj mora vsaka država, ki želi biti demokratična, sicer zagotavljati pravico do prostega dostopa do informacij javnega značaja, vendar mora hkrati državljane varovati pred zlorabo te pravice v njihovo škodo, kar vsekakor velja tudi za konkretni primer, v katerem bi bila z razkritjem informacije lahko ogrožena poslovna skrivnost, ki bi vplivala tudi na samo izvedbo postopka sanacije bančnega sistema, ki ga je Republika Slovenija dolžna izvesti.

V obravnavani zadevi interes javnosti za razkritje zahtevanih informacij ni močnejši od interesa stranske udeleženke in javnega interesa, da se te informacije varuje kot poslovno skrivnost. Takšen rezultat testa je vezan na časovno točko in na dejstvo, da je postopek sanacije banke še v teku. Nobenega dvoma ni, da je ureditev bančnega sistema, ki bo zadostil vsem zahtevam tako Banke Slovenije kot tudi Evropske komisije, v javnem interesu, saj je od tega odvisna stabilnost gospodarstva v Republiki Sloveniji, to pa vpliva na splošno blaginjo in na nivo življenjskega standarda vseh prebivalcev Slovenije. Ko bo postopek zaključen in bo sprejeta dokončna odločitev, na kakšen način se bo stranska udeleženka sanirala oz. prestrukturirala, pa bodo nedvomno podani pogoji za večjo transparentnost zahtevanih informacij.

3.6.9. Davčna tajnost, notranje delovanje, javni uslužbenci

Z odločbo št. 090-60/2013/17 z dne 5. 7. 2013 je Informacijski pooblaščenec delno odpravil odločbo Davčne uprave RS in ji naložil posredovanje določenih delov zahtevanega poročila o opravljenem izrednem notranjem nadzoru glede dela konkretne javne uslužbenke v zvezi s postopkom odmere davka za določenega davčnega zavezanca.

Organ je zahtevo prosilke zavrnil s sklicevanjem na davčno tajnost, notranje delovanje organa in varstvo osebnih podatkov. Po prekritju podatkov, ki so davčna tajnost, zahtevano poročilo ne predstavlja več informacije, ki jo zahteva prosilka. Organ je zatrjeval, da bi razkritje zahtevanega poročila povzročilo motnje v delovanju organa, predvsem v smislu učinkovitosti delovanja notranjega nadzora, saj bi bila njegova funkcija pomembno oslabljena zaradi zavedanja, da se pisna komunikacija ali dokumentacija lahko javno razkrijeta, četudi vsebujeta zgolj verjetne informacije in sume, ki so namenjeni seznanitvi vodstva zaradi izboljšanja delovnega procesa ali odprave drugih pomanjkljivosti.

Informacijski pooblaščenec je ugotovil, da četudi je treba del zahtevanega poročila prekriti, ta še vedno predstavlja informacijo, ki jo prosilka zahteva. Glede podatkov, ki so označeni kot davčna tajnost, je Informacijski pooblaščenec sledil navedbam organa in pritožbo prosilke v tem delu zavrnil, ker gre za absolutno izjemo od prosto dostopnih informacij. Preostali del zahtevanega poročila pa ne vsebuje izjem od prostega dostopa in jih je organ dolžan posredovati prosilki. Zahtevano poročilo je nedvomno nastalo v zvezi z notranjim delovanjem, vendar razkritje dokumenta ne bi povzročilo motenj pri delovanju oz. dejavnostih organa. Iz dela zahtevanega poročila, ki se nanaša na ugotovitve o delu konkretne javne uslužbenke, ni mogoče razbrati »občutljivih« internih informacij. Iz tega dela poročila tudi ne izhajajo način dela in metodologija dela notranjega nadzora oz. ugotovitve, ki bi bile povezane z internim delovanjem organa in bi lahko vplivale na delo oz. dejavnost organa v prihodnje. Glede na to, da je zahtevano poročilo nastalo že leta 2011, je organ morebitne nepravilnosti že moral odpraviti, zato je povsem neutemeljeno sklicevanje, da bi z razkritjem lahko nastala škoda, ker bi tak dokument davčnim zavezancem dal možnost, da bi izkoristili organizacijske in zakonske pomanjkljivosti, ki so ugotovljene v poročilu. Glede na to, da so podatki o davčnih tajnostih prekriti, razkritje preostalih zahtevanih podatkov ne more vplivati na konkretne postopke davčnega nadzora. Razkritje podatkov o tem, kakšne so bile ugotovitve notranjega nadzora v zvezi s postopanjem konkretnega javnega uslužbenca, ne more resno ogroziti procesa delovanja organa oz. povzročiti motenj v njegovem delovanju. Za obstoj izjeme notranjega delovanja v skladu s sodno prakso ne zadostuje dokazni standard »da je zelo verjetno«, da bi razkritje lahko pripeljalo do motenj, temveč dokazni standard »onkraj dvoma«. Nadalje je Informacijski pooblaščenec ugotovil, da v besedilu zahtevanega poročila ni drugih osebnih podatkov posameznice kot tisti, ki so

v zvezi z njenim delom pri organu (ugotovitve posebnega internega nadzora glede odgovornosti javne uslužbenke pri izvajanju delovnih nalog, za katere je sklenila delovno razmerje v javnem sektorju, v povezavi z obravnavanjem posameznega davčnega zavezanca). Na podlagi 3. odstavka 6. člena ZDIJZ ti podatki niso varovani osebni podatki in kot taki ne predstavljajo izjeme po tretji točki 1. odstavka 6. člena ZDIJZ. Namen 3. odstavka 6. člena ZDIJZ je tudi v povečanju zavedanja javnih uslužbencev, da je njihovo delo javno in da ima javnost možnost nadzora nad njihovim delom v posameznih, konkretnih postopkih. Le tako se povečujeta odgovornost in transparentnost delovanja posameznih javnih uslužbencev, s tem pa tudi odgovornost in transparentnost delovanja organov javnega sektorja kot celote. Ob tem velja poudariti, da je namen izjem po ZDIJZ (tudi izjeme varstva osebnih podatkov in izjeme davčne tajnosti) varstvo legitimnih interesov, ne pa prikrivanje morebitnih nepravilnosti pri delu posameznih javnih uslužbencev oz. pomanjkljivosti delovnih postopkov pri organu kot celoti.

3.6.10. Poslovna skrivnost

Z odločbo št. 090-249/2013 z dne 20. 12. 2013 je Informacijski pooblaščenec zavrnil pritožbo stranskega udeleženca zoper odločbo Inšpektorata za javni sektor, s katero je bilo delno ugodeno zahtevi prosilke za dostop do fotokopije pogodbe, ki jo je organ sklenil s stranskim udeležencem.

Zahtevi prosilke za dostop do pogodbe je organ delno ugodil (v pogodbi je prekril ime in priimek skrbnika pogodbe na strani izvajalca – stranskega udeleženca). Organ je v postopek pozval stranskega udeleženca, ki je v zahtevani pogodbi pogodbena stranka, in ta je razkritju nasprotoval iz razloga varstva poslovne skrivnosti. Organ je pri odločitvi upošteval določbo 3. odstavka 6. člena ZDIJZ in zavrnil dostop do zahtevane pogodbe le v delu, ki se nanaša na varovane osebne podatke.

Informacijski pooblaščenec je ugotovil, da so glede zahtevane pogodbe izpolnjeni vsi kriteriji, ki jih ZGD-1 določa za opredelitev poslovne skrivnosti po subjektivnem kriteriju. Vendar pa je treba določene določbe iz zahtevane pogodbe razkriti, ker so javne že po zakonu in zato po 3. odstavku 39. člena ZGD-1 ne morejo predstavljati poslovne skrivnosti. Takšni so podatki o porabi javnih sredstev, ki so javni na podlagi 3. odstavka 6. člena ZDIJZ. V konkretnem primeru so to podatki iz pogodbe, ki imajo finančni učinek in za organ ustvarjajo finančne obveznosti, posredne ali neposredne, pa tudi podatki, ki kažejo, katere storitve je organ prejel za dogovorjeno plačilo in kako (na kakšen način) bo izpolnjeval svoje finančne obveznosti. Javen je tudi podatek o časovnem okviru, za katerega se sklepa pogodba – zgolj pogodbeni znesek, brez podatka o času trajanja izvajanja storitve, namreč ne daje celovitega podatka o višini obveznosti in višini porabe javnih sredstev, ki bo nastala na podlagi sklenjene pogodbe. Kot poslovne skrivnosti stranskega udeleženca tudi ni mogoče šteti pogodbenih določil o dogovarjanju morebitnih sprememb, sporazumnem reševanju sporov in določbe, da pogodba začne veljati s podpisom vseh pogodbenih strank. Če bi dopustili možnost, da stranski udeleženec tovrstne podatke enostransko označi za poslovno skrivnost, bi onemogočili nadzor javnosti nad zakonitostjo splošnega postopka sklepanja pogodb pri organu. Obravnavana pogodba vsebuje t. i. standardna pogodbena določila (ki jih vsebuje vsaka sklenjena pogodba), ki dokazujejo, da je organ pri sklepanju predmetne pogodbe upošteval splošna načela obligacijskega prava oz. da pogodba od slednjih v ničemer ne odstopa. Te določbe zato ne morejo predstavljati poslovne skrivnosti stranskega udeleženca.

Nadalje je Informacijski pooblaščenec ugotovil, da so podatki o tem, kdo je v imenu in za račun organa sklenil predmetno pogodbo ter kdo je kontaktna oseba s strani organa, podatki javnih uslužbencev oz. javnega funkcionarja (ministra), ki so prav tako prosto dostopni na podlagi 3. odstavka 6. člena ZDIJZ. Iz istega razloga ne more predstavljati poslovne skrivnosti podatek o tem, kdo so pri organu upravičeni uporabniki storitev, za katere se sklepa pogodba, ter kdo je skrbnik pogodbe na strani naročnika – organa. Gre namreč za osebe, zaposlene pri organu, ki so javni uslužbenci, uporaba portala, ki je predmet obravnavane pogodbe, pa je nedvomno v zvezi z opravljanjem njihovega dela. Ni pa prosto dostopna informacija o tem, kdo je skrbnik pogodbe na strani izvajalca (stranskega udeleženca), zato se ti podatki prekrijejo. Podatki o tem, kdo sklepa pogodbo v imenu gospodarske družbe, niso varovani, kajti podpisnik pogodbe je direktor, ki je zakoniti zastopnik družbe. Javnost

tega podatka določajo ZGD-1, Zakon o poslovnem registru[23] in Zakon o sodnem registru[24]. Podatek, ki je po zakonu javen in ga zato ni mogoče določiti kot poslovno skrivnost, je tudi podatek o dogovorjenem plačilnem roku, ki je predpisan z zakonom oz. določen s 25. členom Zakona o izvrševanju proračuna Republike Slovenije za leti 2013 in 2014[25]. Enako velja za protikorupcijsko klavzulo, ki je bila v pogodbo vnesena na podlagi 14. člena Zakona o integriteti in preprečevanju korupcije[26].

Informacijski pooblaščenec je zaključil, da je organ pravilno ugotovil, da obravnavana pogodba vsebuje le varovane osebne podatke kot izjemo od prostega dostopa, zato je pritožbo stranskega udeleženca zavrnil.

3.6.11. Ponovna uporaba informacij javnega značaja

Z odločbo št. 090-249/2013 z dne 20. 12. 2013 je Informacijski pooblaščenec odpravil odločbo Vrhovnega sodišča RS in mu zadevo vrnil v ponovno odločanje.

Prosilec je na organ naslovil zahtevo za ponovno uporabo javno objavljenih podatkov o objavah sklepov in pisanj, izdanih v postopkih zaradi insolventnosti. Namen prosilca je pravočasno obveščanje uporabnikov o rokih, ki tečejo od datumov sklepov oz. dejanj. Za ta namen bi prosilec podatke uvažal prek spletnega servisa in tako z novimi podatki ciklično dopolnjeval svojo obstoječo zbirko, ki bi jo ponudil uporabnikom. Prosilec bi zahtevane podatke uporabil za pridobitni namen.

Organ je zahtevo zavrnil, ker prosilec zahteva podatke, za katere drug zakon določa, da so dostopni samo upravičenim osebam (četrta alineja 6. odstavka 6. člena ZDIJZ). V skladu z določbami 2. in 5. odstavka 122.a člena Zakona o finančnem poslovanju, postopkih zaradi insolventnosti in prisilnem prenehanju[27] organ podatke, ki jih zahteva prosilec, posreduje v informatizirani obliki le taksativno navedenim upravičencem. V 6. odstavku 122.a člena ZFPPIPP so omejeni tudi nameni, za katere se podatki o postopkih zaradi insolventnosti, ki se upravičenim subjektom posredujejo v informatizirani obliki, sploh lahko uporabijo. Iz trenutne ureditve ne izhaja, da bi bila ponovna uporaba informacij eden izmed zakonsko dovoljenih namenov uporabe podatkov o postopkih zaradi insolventnosti. Organ je zaključil, da prosilec v zahtevi ne zatrjuje, da bi bil oseba ali institucija iz 2. ali 5. odstavka 122.a člena ZFPPIPP, prav tako ne navaja, da bi podatke uporabljal za enega izmed namenov, določenih v 6. odstavku 122.a člena ZFPPIPP.

Informacijski pooblaščenec je v pritožbenem postopku ugotovil, da 122.a člena ZFPPIPP nikakor ni mogoče razumeti na način, da gre za izključne upravičence. O izključnih upravičencih bi lahko govorili takrat, ko podatki, do katerih bi bili slednji upravičeni, ne bi bili prosto dostopni, v danem primeru pa je takšna razlaga nelogična in v nasprotju z namenom zakona. Posledično tudi niso izpolnjeni pogoji iz četrte točke 6. odstavka 6. člena ZDIJZ, ki je omejen na podatke, ki so dostopni samo upravičenim osebam, medtem ko v danem primeru izrecno govorimo o podatkih, ki morajo biti in na podlagi zakona tudi so dostopni vsem. Namen določbe ZFPPIPP, ki določa spletne strani za objavo v postopkih zaradi insolventnosti, je povsem jasen – širok dostop javnosti, kar je identično tudi namenu prosilca. Cilj ponovne uporabe informacij javnega značaja je, da ima vsak prosilec pravico, da pod enakimi pogoji kot druge osebe pridobi pravico do ponovne uporabe informacij v pridobitne ali nepridobitne namene (4. odstavek 5. člena ZDIJZ). Organ ne sme povzročiti diskriminacije med prosilci znotraj iste ali primerljivih kategorij ponovne uporabe informacij. Slednje izhaja tudi iz Direktive 2003/98/ES Evropskega parlamenta in Sveta z dne 17. 11. 2003 o ponovni uporabi informacij javnega sektorja, ki jo je slovenski zakonodajalec implementiral z ZDIJZ. Direktiva 2003/98/ES v 10. členu ureja načelo prepovedi razlikovanja, ki pravi, da pogoji za ponovno uporabo dokumentov ne smejo biti diskriminatorni za primerjalne kategorije ponovne uporabe, kot je v obravnavanem primeru. Tako Direktiva 2003/98/ES in posledično tudi ZDIJZ sicer predvidevata možnost, da lahko

[23] Uradni list RS, št. 49/2006, s spremembami; v nadaljevanju ZPRS-1.
[24] Uradni list RS, 54/2007, s spremembami.
[25] Uradni list RS, št. 104/2012, s spremembami.
[26] Uradni list RS, št. 45/2010, s spremembami.
[27] Uradni list RS, št. 63/2013-UBP7; v nadaljevanju ZFPPIPP.

organ pod določenimi pogoji podeli izključno pravico ponovne uporabe informacij, kar bi po oceni Informacijskega pooblaščenca lahko predstavljalo razlog za zavrnitev pravice do ponovne uporabe. Vendar po podatkih Pooblaščenca, ki je pristojen za vodenje evidence vseh podeljenih izključnih pravic, v obravnavanem primeru izključna pravica ni podeljena. Informacijski pooblaščenec je opozoril, da se organ v primeru, če ugotovi, da so vsi podatki, ki so predmet zahteve za ponovno uporabo, prosto dostopni in objavljeni na svetovnem spletu, nikakor ne more sklicevati na četrto alinejo 6. odstavka 6. člena ZDIJZ. Organ mora v takem primeru določiti pogoje za ponovno uporabo informacij javnega značaja, ki ne bodo povzročili diskriminacije med prosilci. Organ mora vse navedeno upoštevati v ponovnem postopku odločanja o zahtevi prosilca.

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

Informacijski pooblaščenec lahko leto 2013 na področju dostopa do informacij javnega značaja oceni kot pozitivno. Tako prosilci kot zavezanci so z institutom dostopa do informacij javnega značaja bolje seznanjeni. Število prejetih pritožb zoper zavrnitev dostopa do informacij leta 2013 je primerljivo z letom 2012, spet pa je zaznati naraščanje števila pritožb zoper molk prvostopenjskih organov (leta 2012 je bilo takih pritožb 242, leta 2013 pa 339). Ob tem je Informacijski pooblaščenec prejel precej vprašanj, pobud in prošenj za pojasnila v zvezi z uporabo ZDIJZ v praksi (622).

Na podlagi navedenih podatkov in izvedenih pritožbenih postopkov Informacijski pooblaščenec ocenjuje, da se je osveščenost javnosti o pravici dostopa do informacij javnega značaja povečala, večina zavezancev pa je na prvi stopnji delovala bolje kot leto dni prej. Na to kaže tudi odstotek izdanih zavrnilnih odločb s strani Informacijskega pooblaščenca, ki je višji kot preteklo leto (44,6 %), kar pomeni, da so organi prve stopnje večkrat odločili pravilno in da so bile pritožbe prosilcev neutemeljene. Kljub temu Informacijski pooblaščenec na tem področju v praksi opaža razliko v delovanju med državnimi organi in ostalimi zavezanci (širši javni sektor, nosilci javnih pooblastil in izvajalci javnih služb). Slednji so predvsem s postopkom obravnave prejete zahteve (posredovanje zahtevane informacije v roku 20 delovnih dni oz. izdaja zavrnilne odločbe) še vedno slabo seznanjeni, kar se odraža v številu pritožb zoper molk prvostopenjskih organov. Ob tem velja poudariti, da je v večini teh primerov po pozivu Informacijskega pooblaščenca na podlagi 3. odstavka 255. člena ZUP zadeva rešena v korist prosilca ter zavezanci zahtevane informacije posredujejo. Navedeno kaže na to, da razlog za »molk« ni želja po zavrnitvi dostopa do zahtevane informacije, ampak nepoznavanje zakona in posledično nepravilna procesna obravnava prejete zahteve.

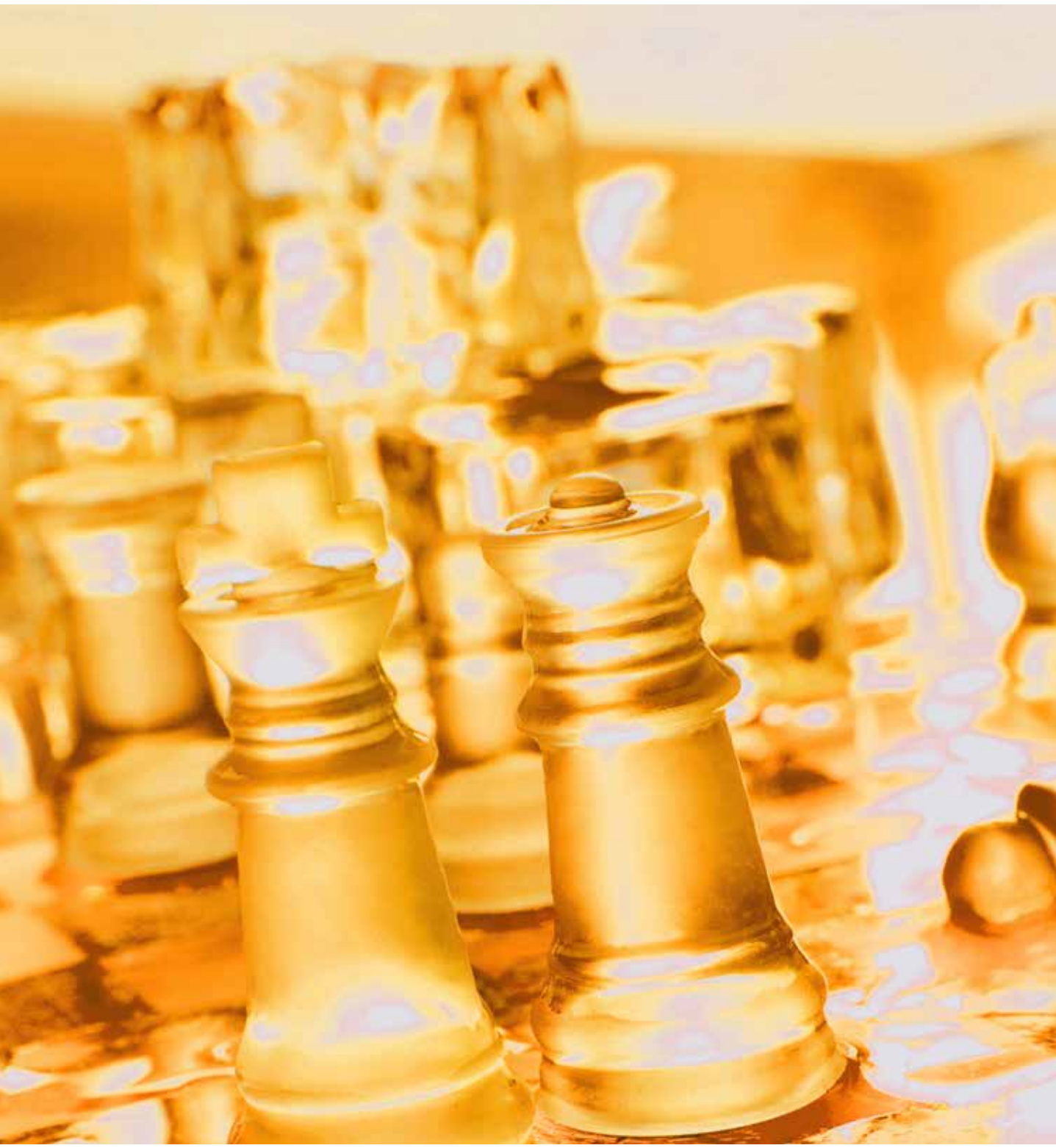
Zanimivo je, da je bilo največ odločb Informacijskega pooblaščenca izdanih v zvezi z vprašanjem, ali zahtevani dokument obstaja (v preteklih letih je bila najpogostejša izjema varstva osebnih podatkov), kar kaže, da prosilci tudi v primeru domnevnega neobstoja dokumenta želijo, da Informacijski pooblaščenec preveri dejansko stanje in ugotovi, ali informacija res ne obstaja. Ob navedenem velja opozoriti, da se organi zavezanci na prvi stopnji ter Informacijski pooblaščenec kot pritožbeni organ na tem področju srečujemo z vse bolj zahtevnimi primeri. Tudi leta 2013 so bile najzahtevnejše zadeve v zvezi z dostopom 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, osebni podatki). Ob tem Informacijski pooblaščenec ocenjuje, da do pritožbenih postopkov pogosto pride tudi 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 za uradne osebe za dostop do informacij javnega značaja pri organih zavezancih. Leta 2013 je bilo znova zaznati povečanje števila pritožb zoper stroške dostopa do informacij. Pri tem Informacijski pooblaščenec, kot že nekaj let zapored, opozarja, da je nesprejemljiva praksa nekaterih zavezancev, da stroške zaračunavajo tudi za vpogled (ta je po zakonu brezplačen) oz. da želijo vse stroške svojega delovanja na tem področju »prevaliti« na prosilce.

Leto 2013 je zaznamovala tudi priprava novele ZDIJZ, s katero se krog zavezanih organov

širi, in sicer na vse pravne osebe, v katerih ima prevladujoč vpliv država, lokalna skupnost ali druga pravna oseba javnega prava. Navedeno spremembo Informacijski pooblaščenec toplo pozdravlja, saj je v preteklih letih večkrat opozoril, 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.

Na področju ponovne uporabe informacij javnega značaja je leto 2013 zaznamovala sprememba Direktive Evropskega parlamenta in Sveta z dne 17. 2. 2003 o ponovni uporabi informacij javnega sektorja. Namen predloga sprememb te 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.

Leta 2013 je Informacijski pooblaščenec prejel šest pritožb s področja ponovne uporabe informacij javnega značaja, kar je več kot leto dni pred tem (leta 2012 je namreč prejel dve pritožbi). Tudi v tem letu je Informacijski pooblaščenec 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. V tem okviru je bil tudi soorganizator uspešne mednarodne konference, ki je potekala 24. 10. 2013 v Ljubljani (http://www.lapsi-project.eu/lapsi-20-conferences).



4 DELO NA PODROČJU VARSTVA OSEBNIH PODATKOV

4.1. Koncept varstva osebnih podatkov v Republiki Sloveniji

Koncept varstva osebnih podatkov v Republiki Sloveniji temelji na določbi 38. člena Ustave RS, po kateri je varstvo osebnih podatkov 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 v primeru njihove zlorabe.

Za normativno urejanje varstva osebnih podatkov je zlasti pomemben 2. odstavek 38. člena Ustave RS, 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[28], ki ga je Državni zbor RS 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[29].

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 RS, ZVOP-1, ZInfP in zakonov, ki podrobneje predpisujejo obdelavo osebnih podatkov na posameznem področju, se v Republiki Sloveniji pri obdelavi neposredno uporabljajo tudi določbe Konvencije o varstvu posameznikov glede na avtomatsko obdelavo osebnih podatkov, ki je bila ratificirana in objavljena leta 1994[30]. 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

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

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[31]. 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[32] 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).

4.2. Dejavnost državnih nadzornikov za varstvo osebnih podatkov

4.2.1. 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[33], specifične pristojnosti državnega nadzornika pa so določene v 53. členu ZVOP-1.

4.2.2. 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 2013 zaradi suma kršitev določb ZVOP-1 vodil 712 inšpekcijskih zadev, 253 v javnem in 459 v zasebnem sektorju. Zoper pravne osebe javnega sektorja je na podlagi prijav uvedel 231 inšpekcijskih zadev, 22 postopkov pa je uvedel po uradni dolžnosti, če je npr. na podlagi objav v medijih zaznal sum kršitve varstva osebnih podatkov ali v okviru načrtovanih ogledov. Zoper zavezance v zasebnem sektorju je na podlagi prijav odprl 435 inšpekcijskih zadev, 24 postopkov je začel po uradni dolžnosti. Število prijav in pritožb zaradi suma kršitev določb ZVOP-1 se je v primerjavi s statističnimi podatki za leto 2012 povečalo (leta 2012 jih je bilo 747, leta 2013 pa 852), čeprav je bilo skupno število inšpekcijskih zadev nekoliko manjše kot leta 2012 (takrat jih je bilo 725). Število prijav, ki jih je prejel Informacijski pooblaščenec, je večje od števila odprtih inšpekcijskih zadev oziroma uvedenih inšpekcijskih postopkov, ker je zoper določene zavezance prejel

[31] Uradni list RS, št. 67/2007; v nadaljevanju ZVOP-1A.
[32] Uradni list RS, št. 29/2011–UPB8, s spremembami; v nadaljevanju ZP-1.
[33] Uradni list RS, št. 43/2007–UPB1; v nadaljevanju ZIN.

več prijav. Tako je Informacijski pooblaščenec leta 2013 zoper zavezance v javnem sektorju prejel 241 prijav (leta 2012 je prejel 237 prijav), zoper zavezance v zasebnem sektorju pa 611 prijav (leta 2012 jih je bilo 510). 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.

Informacijski pooblaščenec je zaradi suma kršitev določb ZVOP-1 zoper pravne osebe javnega sektorja na podlagi prijav odprl 231 inšpekcijskih zadev. V 89 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. V osmih primerih prijavitelji niso odgovorili na poziv za dopolitev prijave, ki jim ga je poslal nadzornik, ker za uvedbo postopka ni bilo dovolj podatkov, zato inšpekcijski postopek ni bil uveden. Leta 2013 je bilo izdanih še devet obvestil o neuvedbi inšpekcijskega postopka za prijave, prejete konec leta 2012. Informacijski pooblaščenec je eno prijavo odstopil v reševanje pristojni instituciji. Po preučitvi prejetih prijav je bilo leta 2013 začetih 133 inšpekcijskih postopkov, 22 pa še po uradni dolžnosti, skupaj torej 155. V okviru inšpekcijskih postopkov v javnem sektorju je bilo opravljenih 50 inšpekcijskih pregledov. Za odpravo ugotovljenih nepravilnosti je bilo izrečenih pet opozoril na zapisnik in izdanih 12 odločb.

Leta 2013 je bilo zaključenih 139 inšpekcijskih postopkov. S sklepom o ustavitvi postopka jih je bilo zaključenih 126, od tega 64 iz preteklih let. Z odločbo se je zaključilo 12 zadev iz leta 2012, z zaznamkom v zapisniku o inšpekcijskem nadzoru pa je bil ustavljen en postopek. V 60 inšpekcijskih postopkih (od tega je bilo 30 postopkov iz leta 2012) Informacijski pooblaščenec ni zaznal kršitev določb ZVOP-1.

Leta 2013 je Upravno sodišče RS odločilo v petih upravnih sporih, ki so jih sprožili zavezanci zoper odločbe, s katerimi je Informacijski pooblaščenec odredil odpravo ugotovljenih nepravilnosti. Sodišče je v štirih primerih tožbam ugodilo, odločbo Informacijskega pooblaščenca odpravilo in mu zadevo vrnilo v ponoven postopek, v enem primeru pa je sodišče tožbo zavrglo. Zoper sklep o zavrženju je zavezanec vložil pritožbo na Vrhovno sodišče RS, ki pa še ni odločilo.

Informacijski pooblaščenec je 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 – 68,
- nezakonito zbiranje osebnih podatkov – 43;
- piškotki – 28;
- neustrezno zavarovanje osebnih podatkov – 26,
- nezakonito izvajanje videonadzora in sporna uporaba videoposnetkov – 15,
- neposredno trženje – 7,
- razno: npr. pogodbena obdelava osebnih podatkov, nezakonito uničenje osebnih podatkov, obdelava netočnih in neažurnih osebnih podatkov, obdelava osebnih podatkov v nasprotju z namenom zbiranja, zavrnitev posredovanja osebnih podatkov, v okviru inšpekcijskih postopkov po uradni dolžnosti je Informacijski pooblaščenec preverjal izvajanje določb ZVOP-1 v celoti – 66.

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 – 118, od tega 42 zoper vzgojno-izobraževalne ustanove in 20 zoper zdravstvene ustanove,
- državne organe – 108, od tega sodišča, tožilstva, pravobranilstvo – 19 ,
- občine – 27.

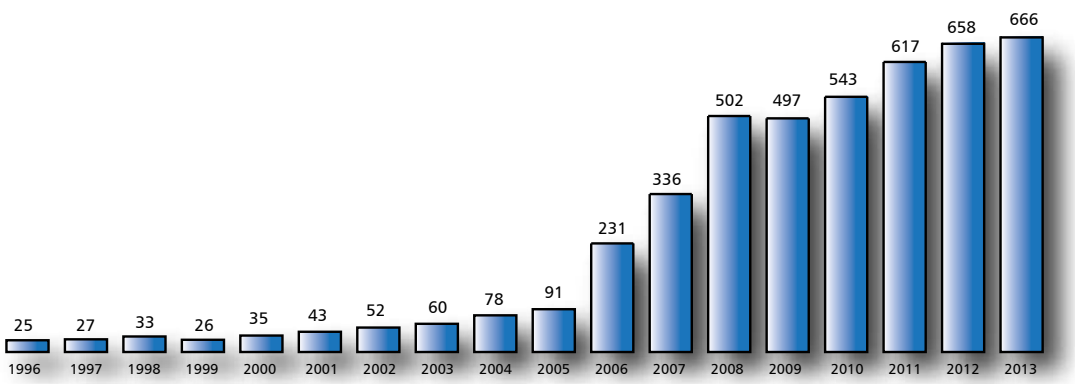
Informacijski pooblaščenec je leta 2013 zoper zavezance v zasebnem sektorju vodil 459 zadev, od tega 435 na podlagi prijav in 24 po uradni dolžnosti. Kar v 116 primerih so bili prijavitelji obveščeni, da Informacijski pooblaščenec postopka inšpekcijskega nadzora ne bo uvedel, ker iz njihove prijave ni izhajal sum kršitev določb ZVOP-1 ali ker tudi po pozivu Informacijskega pooblaščenca niso posredovali dovolj podatkov za uvedbo inšpekcijskega postopka. Informacijski pooblaščenec je osem 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. Na podlagi sedmih prijav je Informacijski pooblaščenec takoj uvedel postopek o prekršku, ker je po preučitvi prijave zaključil, da uvedba inšpekcijskega postopka ne bi bila smiselna, saj je šlo za enkratno dejanje v preteklosti, ki ga z inšpekcijskimi postopki za nazaj ni možno več preprečiti ali odpraviti, in ker je bilo prijavi priloženih dovolj dokazov o storitvi prekrška. 16 prijav je posredoval v reševanje pristojnim institucijam, v petih primerih pa je pristojnim organom naznanil sum storitve kaznivega dejanja in o tem obvestil prijavitelja. Izdal je še 16 obvestil o neuvedbi inšpekcijskega postopka in napotitev na pravice po ZVOP-1, ki so se nanašale na prijave, prejete konec leta 2012. Tako je bilo leta 2013 na podlagi prejetih prijav začetih 283 postopkov inšpekcijskega nadzora, 24 jih je bilo uvedenih po uradni dolžnosti, skupaj torej 307. Državni nadzorniki za varstvo osebnih podatkov so v zasebnem sektorju opravili 88 inšpekcijskih pregledov. Zaradi ugotovljenih nepravilnosti so izrekli 16 opozoril v zapisniku o inšpekcijskem nadzoru in izdali 14 ureditvenih odločb, od tega devet v postopkih, začetih pred letom 2013. En zavezanec je zoper prejeto odločbo sprožil upravni spor. Leta 2013 je bilo izdanih 244 sklepov o ustavitvi postopka, od tega 138 v postopkih, ki so bili začeti pred letom 2013. Sedem postopkov je bilo ustavljenih z zaznamkom v zapisniku o inšpekcijskem nadzoru. V 102 inšpekcijskih postopkih (48 iz leta 2013) Informacijski pooblaščenec ni zaznal kršitev določb ZVOP-1.

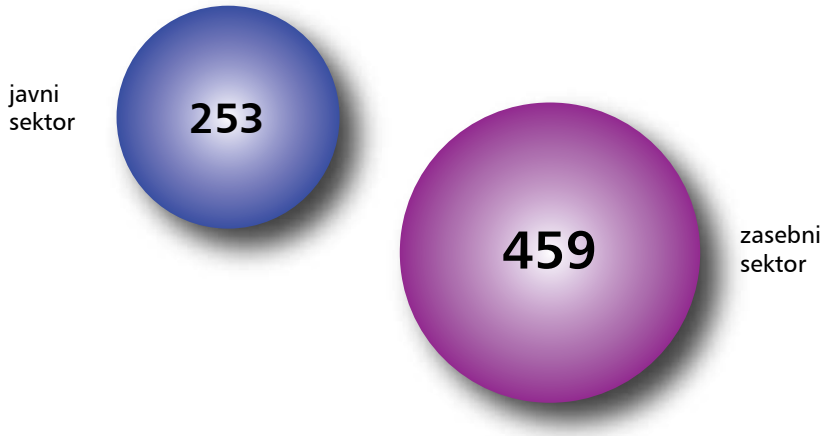
Sumi kršitve določb ZVOP-1 so se nanašali na:

- 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 – 105 ,
- zlorabe osebnih podatkov za namene neposrednega trženja – 87,
- piškotki – 62,
- nezakonito zbiranje osebnih podatkov – 58,
- nezakonito izvajanje videonadzora – 41,
- neustrezno zavarovanje osebnih podatkov – 23,
- razno: npr. predčasno uničenje osebnih podatkov, zavrnitev posredovanja osebnih podatkov, obdelava netočnih in neažurnih osebnih podatkov, obdelava osebnih podatkov v nasprotju z namenom zbiranja, pogodbena obdelava, izvajanje biometrijskih ukrepov, iznos osebnih podatkov v tretje države – 83.

Slika 7: Število inšpekcijskih zadev na podlagi prejetih prijav zaradi suma kršitev določb ZVOP-1 med letoma 2006 in 2013.



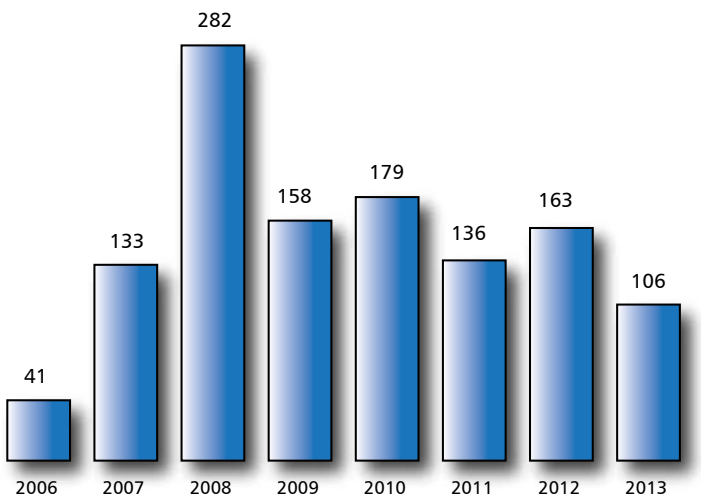
Slika 8: Sumi nezakonite obdelave osebnih podatkov leta 2013, primerjava med javnim in zasebnim sektorjem.



4.2.3. Storjeni prekrški

Zaradi kršitev določb ZVOP-1 je bilo leta 2013 uvedenih 106 postopkov o prekršku, 18 postopkov zoper pravne osebe javnega sektorja in njihove odgovorne osebe, 62 postopkov zoper pravne osebe zasebnega sektorja in njihove odgovorne osebe ter 26 postopkov zoper posameznike (v to številko so vključene tudi odgovorne osebe državnih organov in samoupravnih lokalnih skupnosti, saj v skladu z ZP-1 Republika Slovenija in samoupravne lokalne skupnosti za prekrške ne odgovarjajo, odgovarjajo le njihove odgovorne osebe). Za ugotovljeni prekršek lahko prekrškovni organ v skladu s 53. členom ZP-1 izreče opozorilo, če je storjeni prekršek neznaten in če pooblaščena uradna oseba oceni, da je glede na pomen dejanja opozorilo zadosten ukrep. Če je storjen hujši prekršek, prekrškovni organ izda odločbo o prekršku, s katero kršitelju izreče sankcijo. V skladu s 4. členom ZP-1 sta sankciji za prekršek globa in opomin, glede na 57. člen ZP-1 pa se lahko globa izreče tudi v obliki plačilnega naloga.

Slika 9: Število uvedenih postopkov o prekršku med letoma 2006 in 2013.



V prekrškovnih postopkih, vključno z odprtimi postopki iz preteklih let, je Informacijski pooblaščenec leta 2013 izdal:
- 26 opozoril,
- 72 odločb o prekršku (36 opominov in 36 glob).

Število izdanih odločb o prekršku se je v primerjavi z letom 2012 zmanjšalo (takrat jih je bilo 119), več je bilo izrečenih opozoril (leta 2011 jih je bilo izrečenih 17).

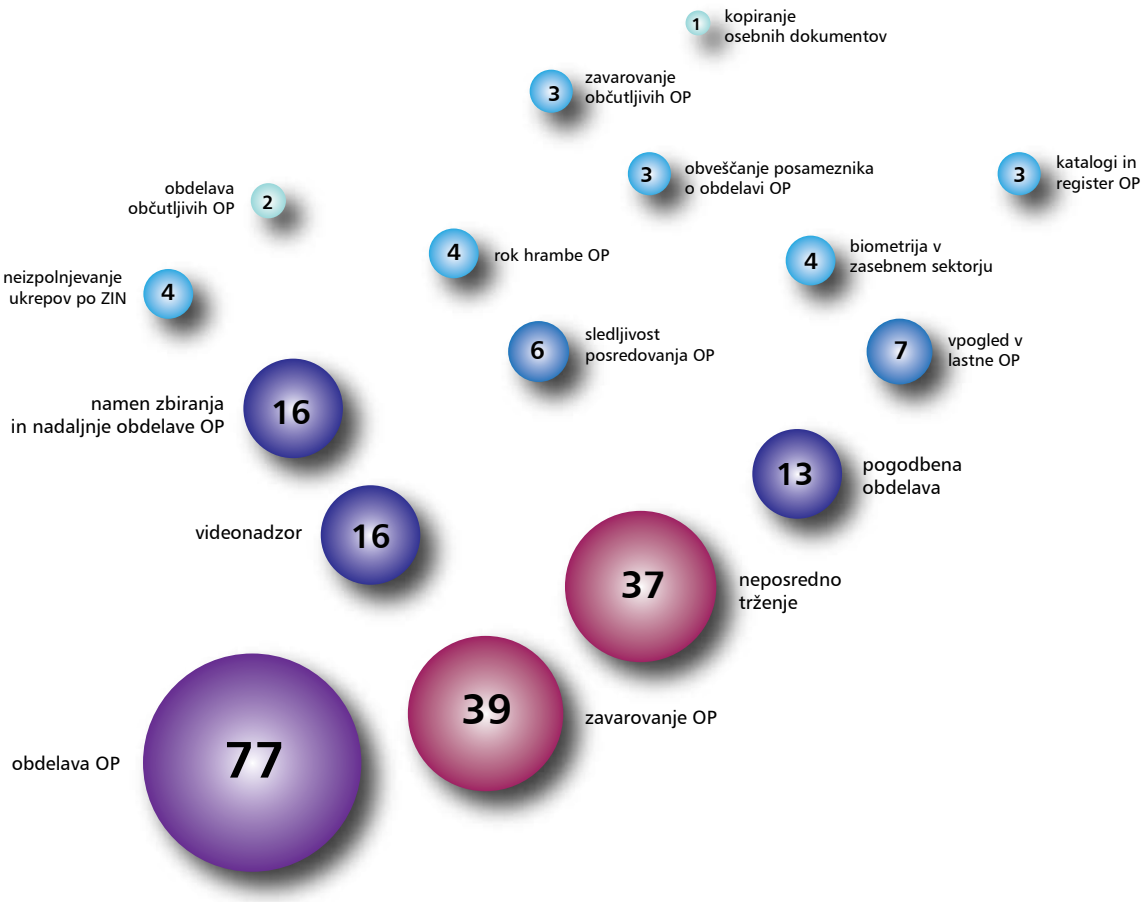
Informacijski pooblaščenec je v skladu z načelom ekonomičnosti v okviru postopkov inšpekcijskega nadzora izrekel tudi 90 opozoril po 53. členu ZP-1 za manjše kršitve (leta 2012 87, leta 2011 75), 25 (leta 2012 24) v javnem in 65 (leta 2012 63) v zasebnem sektorju.

Kršitelji so zoper izdane odločbe o prekršku vložili 12 zahtev za sodno varstvo (zoper 16,7 % izdanih odločb, leta 2012 pa zoper 25,2 %), od tega 11 zoper globe in torej le eno zoper opomin. Skoraj vse zahteve za sodno varstvo so bile vložene zoper izrečene globe, kar je posledica dejstva, da so globe po ZVOP-1 visoke, zlasti če gre za stek prekrškov. Informacijski pooblaščenec namreč nima možnosti odločati o višini izrečene globe (v hitrem postopku o prekršku lahko storilcu izreče globo v znesku, v katerem je predpisana, če je predpisana v razponu, pa izreče najnižjo predpisano globo). Le sodišče sme storilcu odmeriti sankcijo pod mejo, ki je predpisana, če tako določa zakon ali če ugotovi, da so podane posebne olajševalne okoliščine, ki utemeljujejo izrek milejše sankcije. Informacijski pooblaščenec izreka globe, kadar gre za prekrške, s katerimi je bilo občutno poseženo v pravico do varstva osebnih podatkov posameznika, ali v primerih, ko so pooblaščene osebe znotraj določenega upravljavca zlorabile pravico dostopa do osebnih podatkov v določeni zbirki, pridobljeno za potrebe opravljanja svojega dela.

Leta 2013 je Informacijski pooblaščenec ustavil devet postopkov o prekršku, ker za izrek ukrepa po ZP-1 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 – 77,
- zavarovanje osebnih podatkov: 24. in 25. člen ZVOP-1 – 39,
- neposredno trženje: 72. in 73. člen ZVOP-1 – 37,
- videonadzor: 74., 75., 76. in 77. člen ZVOP-1 – 16,
- namen zbiranja in nadaljnje obdelave osebnih podatkov: 16. člen ZVOP-1 – 16,
- pogodbeno obdelavo: 11. člen ZVOP-1 – 13,
- vpogled v lastne osebne podatke: 30. in 31. člen ZVOP-1 – 7,
- sledljivost posredovanja osebnih podatkov: 3. odstavek 22. člena ZVOP-1 – 6,
- neizpolnjevanje ukrepov, izrečenih v postopkih inšpekcijskega nadzora, kršitve določb ZIN – 4,
- rok hrambe osebnih podatkov: 21. člen ZVOP-1 – 4,
- izvajanje biometrijskih ukrepov v zasebnem sektorju: 80. člen ZVOP-1 – 4,
- vzpostavitev katalogov zbirk osebnih podatkov in posredovanje podatkov v register zbirk osebnih podatkov: 26. in 27. člen ZVOP-1 – 3,
- obveščanje posameznika o obdelavi osebnih podatkov: 19. člen – 3,
- zavarovanje občutljivih osebnih podatkov: 14. člen ZVOP-1 – 3,
- obdelava občutljivih osebnih podatkov: 13. člen ZVOP-1 – 2,
- kopiranje osebnih dokumentov: 3.a člen ZOIzk in 4.a člen ZPLD – 1.

Slika 10: Najpogostejše kršitve določb ZVOP-1 leta 2013.



Leta 2013 je Informacijski pooblaščenec prejel 24 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:

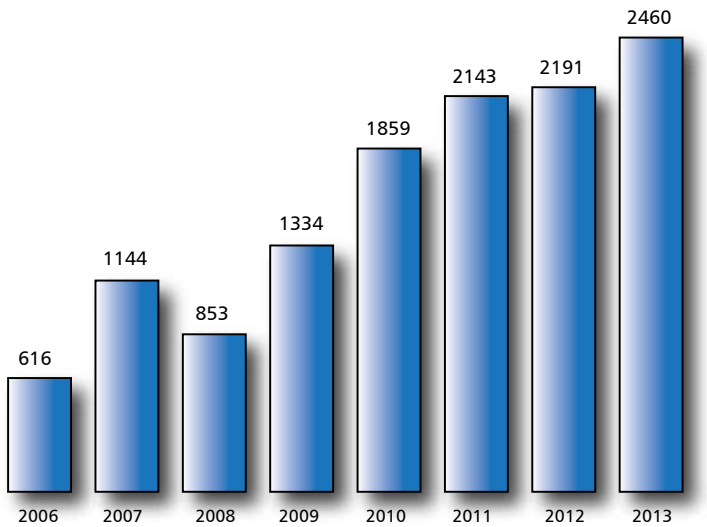
- zahteva za sodno varstvo je bila zavrnjena kot neutemeljena, odločba Informacijskega pooblaščenca pa potrjena – 10,
- zahtevi za sodno varstvo je bilo ugodeno, odločba Informacijskega pooblaščenca odpravljena, postopek o prekršku pa ustavljen – 7,
- zahtevi za sodno varstvo je bilo ugodeno v delu, 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 – 6,
- zahtevi za sodno varstvo je bilo ugodeno na način, da je bila izpodbijana odločba spremenjena v pravni klasifikaciji prekrška – 1.

Informacijski pooblaščenec je v treh primerih, ko je okrajno sodišče postopek o prekršku ustavilo, zoper odločitev sodišča vložil pritožbo na višje sodišče. Višje sodišče je leta 2013 odločilo o eni zadevi, in sicer je protožbi Informacijskega pooblaščenca ugodilo, sodbo okrajnega sodišča razveljavilo in mu zadevo vrnilo v ponovno odločanje.

4.3. 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 2013 prejel 2.460 prošenj za podajo pisnega pojasnila ali mnenja v zvezi s konkretnimi vprašanji. Število prošenj se že več let zapored rahlo povečuje: leta 2012 jih je bilo 2.191, leta 2011 pa 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 71 mnenj in pojasnil, medtem ko je posameznikom, ki so zastavili vprašanja, na katera je v preteklosti že odgovarjal, posredoval le kratek odgovor oziroma jih je le napotil na že izdelano mnenje. Takšnih kratkih odgovorov in napotitev je bilo 2.389. 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 11: Število zaprosil za mnenja med letoma 2006 in 2012.



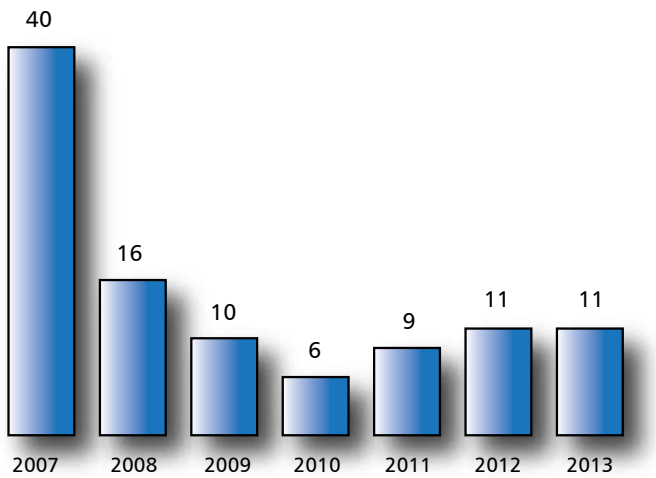
Zaprosila za mnenja in pojasnila so zadevala različna področja. Informacijski pooblaščenec izdana mnenja razvršča v 46 področij (npr. bančništvo, biometrija, davčni postopki, delovna razmerja, društva, elektronska pošta, enotna matična številka občana in davčna številka, iznos osebnih podatkov v tretje države, knjižničarstvo, mediji, moderne tehnologije, neposredno trženje in nagradne igre, občine, pogodbena obdelava, policijski postopki, postopki na 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, upravni 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 https://www.ip-rs.si/varstvo-osebnih-podatkov/iskalnik-po-odlocbah-in-mnenjih/odlocbe-in-mnenja-varstvo-osebnih-podatkov/.

4.4. 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 3. odstavka 80. člena ZVOP-1 mora Informacijski pooblaščenec pri odločanju o tem, ali je nameravana uvedba biometrijskih ukrepov v zasebnem sektorju v skladu z določbami ZVOP-1, upoštevati 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).

Slika 12: Število vlog za izdajo odločbe o dopustnosti izvajanja biometrijskih ukrepov med letoma 2007 in 2013.



Informacijski pooblaščenec je leta 2013 prejel 11 vlog za izdajo dovoljenja za uvedbo biometrijskih ukrepov. Izdal je 11 odločb, v katerih je odločil o dopustnosti izvajanja biometrijskih ukrepov, od tega jih je bilo pet izdanih v postopkih, začetih leta 2012. V štirih primerih je Informacijski pooblaščenec vlogam za izvajanje biometrijskih ukrepov v celoti ugodil, v štirih primerih je ugodil delno, tri vloge pa je zavrnil.

Informacijski pooblaščenec je v celoti ugodil štirim zahtevam za izvajanje biometrijskih ukrepov.

1) Zahtevi vlagatelja, da za namen varovanja ljudi in premoženja vstopanje pooblaščenih zaposlenih v območje posebne reaktorske hale vlagatelja poteka z uporabo treh čitalcev prstnih odtisov. Informacijski pooblaščenec je ugotovil, da želi vlagatelj z izvajanjem biometrijskih ukrepov nadzorovati dostop do ožjega območja svoje reaktorske hale, ki predstavlja posebno varnostno občutljivo območje ter zato zahteva še posebej skrbno in

učinkovito varovanje. Ugotovljeno je bilo, da je tako varovanje potrebno zaradi nevarnosti radioaktivnega sevanja, kateremu bi lahko bili izpostavljeni posamezniki, ki bi nepooblaščeno dostopali do tega območja. Poleg tega bi nepooblaščene osebe pri dostopu do takega območja lahko povzročile nesrečo ali sabotažo, zaradi katere bi lahko bila ogrožena življenja in zdravje večjega števila ljudi. Informacijski pooblaščenec je ob tem upošteval tudi premoženjsko škodo, ki bi lahko nastala kot posledica dostopanja nepooblaščenih posameznikov do varovanih prostorov, tako na premoženju vlagatelja kot na premoženju širšega kroga subjektov. Obseg takih posledic je organ upošteval pri tehtanju, na podlagi katerega je ugotovil, da je izvajanje biometrijskih ukrepov v tem primeru nujno potrebno za varnost ljudi in za varnost premoženja. Vlagatelj bo lahko z biometričnim varovanjem območja reaktorske hale dostop do teh prostorov omogočil samo pooblaščenim zaposlenim in tako zagotovil najstrožji režim varovanja. Pri tem je bilo upoštevano, da namerava vlagatelj biometrijske ukrepe izvajati zgolj nad ožjim krogom zaposlenih, ki so posebej pooblaščeni za dostopanje do varovanega območja reaktorske hale ter so tudi posebej usposobljeni za dela in naloge, ki se odvijajo v teh prostorih.

2) Zahtevi vlagatelja, da za namen varovanja poslovnih skrivnosti dovoli izvajanje biometrijskih ukrepov, ki temeljijo na biometrijski prepoznavi obraza, za vstopanje pooblaščenih zaposlenih v varno sistemsko sobo vlagatelja. Ugotovljeno je bilo, da vlagatelj z izvajanjem teh ukrepov zasleduje cilj nadzora dostopa do svoje varne sistemske sobe, v kateri so strežniki oziroma strežniška diskovna polja, na katerih hrani dokumente in podatke svojih strank. V zvezi s tem je bilo poudarjeno, da subjekti razpolagajo s različno dokumentacijo, ki – glede na podatke, ki jih vsebuje – zahteva različne stopnje varovanja, da pa je v skladu z določbo 80. člena ZVOP-1 z biometrijskimi ukrepi dopustno varovati zgolj tisto dokumentacijo, ki vsebuje poslovne skrivnosti in/ali tajne podatke, zato je moral vlagatelj izkazati, da hranjena dokumentacija vsebuje tudi takšne podatke. V postopku je vlagatelj izkazal, da se na varovanih strežnikih nahaja dokumentacija, ki vsebuje poslovne skrivnosti, ni pa uspel izkazati, da bi dokumentacija vsebovala tudi tajne podatke. Pri vlagatelju so za dostop do varne sistemske sobe pooblaščeni le trije zaposleni, ki bodo lahko, v skladu z odločbo, v te prostore vstopali s pomočjo izvajanja biometrijskih ukrepov. Vlagatelj lahko biometrijske ukrepe izvaja zgolj za nadzor dostopa do svojih varovanih prostorov, ne pa tudi za evidentiranje prisotnosti zaposlenih na delovnem mestu.

3) Zahtevi vlagatelja, da za namen varovanja poslovnih skrivnosti dovoli izvajanje biometrijskih ukrepov, ki temeljijo na biometrijski prepoznavi prstnega odtisa, in sicer za vstopanje v dve pisarni predsednika uprave vlagatelja, v dve pisarni člana uprave vlagatelja in v pisarno vodje tajništva vlagatelja. Vlagatelj je želel z biometrijskimi ukrepi nadzirati dostop do nekaterih pisarn vodstva podjetja, v katerih je dokumentacija, ki vsebuje tudi poslovne skrivnosti. Vlagatelj je v vlogi poleg poslovnih skrivnosti kot varovane dobrine navajal tudi opravljanje njegove dejavnosti, varstvo premoženja in varovanje zaupnih podatkov po Zakonu o bančništvu (ZBan-1). V zvezi z opravljanjem dejavnosti in varstvom premoženja je Informacijski pooblaščenec ugotovil, da gre za pravni dobrini, za varovanje katerih je dopustno izvajati biometrijske ukrepe, vendar pa v konkretnem primeru obstoj teh dobrin in nujnost izvajanja ukrepov za njihovo zavarovanje niso bili izkazani. Glede varovanja zaupnih podatkov po ZBan-1 pa je Informacijski pooblaščenec opozoril, da ZVOP-1 pri taksativnem naštevanju pravnih dobrin, ki jih je dopustno varovati z biometrijskimi ukrepi, ne uporablja termina »zaupni podatki« in da zato ti podatki sami po sebi ne predstavljajo pravne dobrine, za varovanje katere bi bilo te ukrepe dopustno izvajati, zato se v postopku tudi ni posebej ugotavljalo, ali vlagatelj z zaupnimi podatki po ZBan-1 dejansko razpolaga ali ne. Vlagatelj bo biometrijske ukrepe izvajal za vstopanje v pet svojih službenih prostorov na dveh različnih lokacijah, v te prostore pa bo s pomočjo biometrijskih ukrepov vstopalo osem zaposlenih pri vlagatelju.

4) Zahtevi vlagatelja, da za namen varstva premoženja in varovanja poslovnih skrivnosti dovoli izvajanje biometrijskih ukrepov, ki temeljijo na prepoznavi prstnega odtisa, nad tistimi zaposlenimi vlagatelja, ki pri vlagatelju vstopajo v prostor za prevzem in predajo plemenitih kovin in v trezor. Vlagatelj je v postopku izkazal, da je strogo nadzorovanje vstopa v prostore, kjer se hranijo in drugače obdelujejo plemenite kovine, nujno potrebno z vidika varovanja premoženja. Vlagatelj je, podobno kot banke, izpostavljen visokemu varnostnemu tveganju – dostop nepooblaščene osebe do velike količine plemenitih kovin in potencialna odtujitev le-teh bi pomenila veliko škodo za premoženje vlagatelja. Biometrijska kontrola dostopa je glede preprečevanja dostopa nepooblaščenim najzanesljivejša od trenutno dostopnih tehnologij varovanja. Vlagatelj z milejšimi ukrepi ne bi mogel doseči takega standarda

varovanja, kot ga zahteva varovanje premoženja tako visoke vrednosti. Plemenite kovine, ki jih obdeluje in hrani, so zelo visoke vrednosti. Vlagatelj je poleg tega izkazal tudi, da razpolaga s poslovnimi skrivnostmi v smislu določb Zakona o gospodarskih družbah, saj v prostorih, ki jih želi varovati z biometrijskimi ukrepi, hrani vso dokumentacijo, povezano s svojim poslovanjem, trgovanjem s plemenitimi kovinami, dokumentacijo z oznako davčne tajnosti in zahteve Urada za preprečevanje pranja denarja. Biometrijske ukrepe je vlagatelj nameraval izvajati le nad tistimi zaposlenimi, ki bodo imeli dostop do navedenih prostorov, kar je v skladu z načelom sorazmernosti. Informacijski pooblaščenec je ugotovil, da je namen varovanja premoženja in poslovnih skrivnosti, ki ga zasleduje vlagatelj, dovolj tehten, resen in utemeljen ter da tehnične rešitve, ki jih nameravani biometrični ukrepi predvidevajo, s stališča načela sorazmernosti upravičujejo uvedbo biometrijskih ukrepov za vstop v prostor za prevzem in predajo plemenitih kovin in trezor.

Informacijski pooblaščenec je delno ugodil štirim zahtevam za izvajanje biometrijskih ukrepov.

1) Informacijski pooblaščenec je v treh postopkih delno ugodil zahtevam za izvajanje biometrijskih ukrepov treh povezanih podjetij, ki imajo poslovne prostore v skupnem poslovnem objektu, in vloge katerih so se nanašale na izvajanje smiselno enakih biometrijskih ukrepov. Informacijski pooblaščenec je v zvezi s povezanostjo treh vlagateljev poudaril, da gre kljub taki povezanosti pri vsakemu od njih za samostojnega upravljavca osebnih podatkov, ki se bodo obdelovali pri izvajanju biometrijskih ukrepov, in da mora zato vsak od njih vzpostaviti samostojno, od drugih dveh ločeno zbirko osebnih podatkov, tako da bo vsak upravljavec tiste zbirke osebnih podatkov, ki bo nastala pri izvajanju biometrijskih ukrepov nad njegovimi zaposlenimi, medtem ko do osebnih podatkov iz zbirk drugih dveh povezanih podjetij ne sme dostopati ali jih drugače obdelovati.

Informacijski pooblaščenec je posameznim vlagateljem dovolil izvajanje biometrijskih ukrepov z uporabo čitalnikov prstnih odtisov:

- Za namen varstva ljudi in premoženja, za vstopanje v skladiščne prostore vlagatelja, v katerih se hrani medicinska oprema in materiali, in sicer nad zaposlenimi, ki imajo pooblastilo za vstopanje v te prostore. Navedeni skladiščni prostori vlagatelja se nahajajo v njegovih poslovnih prostorih, do njih pa bodo s pomočjo biometrijskih ukrepov dostopali tisti zaposleni, ki so pooblaščeni za dostop do medicinske opreme in materialov, ki se v teh prostorih hranijo. Ugotovljeno je bilo, da sta zasledovana namena varstvo življenja in zdravja ljudi ter premoženja v konkretnem primeru dovolj tehtna, resna in utemeljena, ker bi bila posledica dostopa tretjih, nepooblaščenih oseb do varovane medicinske opreme in materialov lahko ogrožanje življenja in/ali zdravja posameznikov, ki jim je ta oprema namenjena, poleg tega pa gre tudi za opremo in materiale večje vrednosti, katerih odtujitev ali poškodovanje bi lahko predstavljala precejšen poseg v premoženje vlagatelja. Vlagatelj bo biometrijske ukrepe za dostopanje do teh prostorov lahko izvajal nad tistimi zaposlenimi, ki bodo pooblaščeni za dostopanje do skladišč z varovano medicinsko opremo in materiali.
- Za namen varovanja poslovnih skrivnosti, za vstopanje v pisarno direktorja, ki se nahaja v poslovnih prostorih vlagatelja, in sicer nad direktorjem in zaposlenimi v tajništvu direktorja. Pisarna direktorja vlagatelja se nahaja v njegovih poslovnih prostorih, do nje pa bodo z izvajanjem biometrijskih ukrepov dostopali direktor in zaposleni v njegovem tajništvu. Ugotovljeno je bilo, da je v pisarni direktorja med drugim tudi dokumentacija, ki vsebuje poslovne skrivnosti. Vlagatelj je krog zaposlenih, nad katerimi je želel izvajati biometrijske ukrepe za vstopanje v ta prostor, omejil na nekaj posameznikov, ki so pooblaščeni za dostopanje do direktorjeve pisarne in s tem tudi do poslovnih skrivnosti, ki so predmet varstva. Biometrijske ukrepe za vstopanje v ta prostor bo vlagatelj izvajal s tremi čitalci prstnih odtisov.
- Za namen varovanja poslovnih skrivnosti za vstopanje v dva prostora, v katerih se hrani dokumentacija iz postopkov javnih naročil, in sicer nad zaposlenimi, ki so pooblaščeni za vstopanje v ta prostora. V omenjenih dveh prostorih, ki se nahajata znotraj poslovnih prostorov vlagatelja, se hrani dokumentacija, ki jo vlagatelj obdeluje v zvezi s postopki javnih naročil, vanju pa bi z izvajanjem biometrijskih ukrepov vstopali tisti posamezniki, ki so pri vlagatelju zaposleni na javnih naročilih. Dokumentacija, ki se obdeluje v postopkih javnega naročanja in ki se hrani v omenjenih dveh prostorih, vsebuje večjo količino poslovnih skrivnosti vlagatelja in/ali njegovih poslovnih partnerjev, zaradi česar zahteva strožje varstvo. Ugotovljeno je bilo, da je namen varstva poslovnih skrivnosti, ki ga pri uvajanju biometrijskih ukrepov za vstopanje v ta dva prostora zasleduje vlagatelj,

dovolj tehten, resen in utemeljen ter da tehnične rešitve, ki jih nameravani biometrični ukrepi predvidevajo, s stališča načela sorazmernosti upravičujejo uvedbo biometrijskih ukrepov za vstop v prostora vlagatelja, v katerih se hrani dokumentacija iz postopkov javnih naročil.

- Za namen varstva premoženja in varovanja poslovnih skrivnosti, za vstopanje v strežniško sobo, in sicer nad zaposlenim sistemskim administratorjem vlagatelja, ki je pooblaščen za dostop do strežniške sobe. V strežniškem oziroma telekomunikacijskem prostoru vlagatelja je strežnik, na katerem se hranijo za poslovanje vlagatelja pomembni podatki, tudi podatki, ki predstavljajo poslovne skrivnosti. Vlagatelj želi z biometrijskimi ukrepi varovati poslovne skrivnosti, ki se nahajajo na strežniku, pa tudi sam strežnik, ki predstavlja premoženje večje vrednosti. Premoženje, ki ga bo vlagatelj varoval z izvajanjem biometrijskih ukrepov, je zanj (poleg poslovnih skrivnosti, ki se na njem nahajajo) tako pomembno, da je bilo treba ugotoviti, da njegovo varovanje odtehta tudi poseg v informacijsko zasebnost zaposlenih, ki ga predstavlja izvajanje biometrijskih ukrepov, zlasti, ker se bodo ti ukrepi izvajali le nad enim zaposlenim. Informacijski pooblaščenec je ugotovil še, da je v skladu z načelom sorazmernosti tudi vlagateljeva odločitev, da bo premoženje (najpomembnejšo strojno opremo) in poslovne skrivnosti (vsaj tiste v elektronski obliki) hranil centralizirano, tj. v enem prostoru, ki ga namerava zavarovati z biometrijskimi ukrepi.

Informacijski pooblaščenec je posameznemu vlagatelju zavrnil izvajanje biometrijskih ukrepov:

- Za vstopanje v službene prostore vlagatelja skozi glavni vhod v poslovni objekt in za vstopanje skozi vhod, ki vodi neposredno v službene prostore vlagatelja. Vlagatelj je želel biometrijske ukrepe izvajati nad vsemi zaposlenimi. Vlagatelj je navedel, da želi z izvajanjem biometrijskih ukrepov zavarovati premoženje, poslovne skrivnosti in tajne podatke, ki naj bi bili v njegovih poslovnih prostorih oziroma pisarnah (poslovne skrivnosti in tajni podatki naj bi se hranili na večini računalnikov in na strežniku). Informacijski pooblaščenec je v odločbi poudaril, da bi bilo izvajanje biometrijskih ukrepov na navedenih dveh vhodih in nad vsemi zaposlenimi v skladu z 80. členom ZVOP-1 samo, če varovanih pravnih dobrin ne bi bilo mogoče ustrezno zavarovati z omejenim izvajanjem biometrijskih ukrepov, tj. z njihovim izvajanjem zgolj za vstopanje v posamezne prostore oziroma območja znotraj poslovnih prostorov vlagatelja. Sestavni del presoje, ali biometrijski ukrepi ustrezajo kriteriju »nujne potrebnosti« je tako tudi ugotavljanje sorazmernosti teh ukrepov, tj. ali želi vlagatelj te ukrepe izvajati tako, da bo z njimi v najmanjši možni meri posegel v informacijsko zasebnost zaposlenih in hkrati dosegel namen, zaradi katerega jih želi izvajati. V konkretnem postopku je bilo ugotovljeno, da pri vlagatelju znotraj poslovnih prostorov obstajajo posamezni prostori, za vstopanje v katere je, zaradi zavarovanja premoženja in/ali poslovnih skrivnosti, izvajanje biometrijskih ukrepov nujno potrebno, da pa izvajanje teh ukrepov na način iz te točke ni nujno potrebno, ker je enako stopnjo varstva premoženja in poslovnih skrivnosti mogoče zagotoviti z izvajanjem teh ukrepov v manjšem obsegu, tj. tako, da se jih ne izvaja na glavnih vhodih v objekt oziroma v poslovne prostore in nad vsemi zaposlenimi, ampak omejeno in zgolj nad tistimi zaposlenimi, ki so pooblaščeni za vstopanje v varovane prostore znotraj poslovnih prostorov. Glede poslovnih skrivnosti, ki naj bi jih vlagatelj s temi ukrepi želel varovati, je Informacijski pooblaščenec ugotovil, da je za poslovno skrivnost že po definiciji nujno, da je znana določenemu, omejenemu krogu ljudi, kar v obravnavanem primeru pomeni, da se navedbe vlagatelja, da se poslovne skrivnosti nahajajo na vseh računalnikih, kar naj bi pomenilo, da imajo dostop do njih vsi pri njem zaposleni, ne ujemajo s samim pojmom poslovne skrivnosti. Poudarjeno je bilo tudi, da je treba pri presoji upravičenosti izvajanja biometrijskih ukrepov upoštevati celosten sistem varovanja v 80. členu ZVOP-1 naštetih pravnih dobrin ter presojati, ali je izvajanje teh ukrepov tako nujni sestavni del postopkov in ukrepov tega sistema, da odtehta tudi poseg v informacijsko zasebnost, ki ga taki ukrepi predstavljajo. V tem okviru je treba naprej ugotoviti, da je vlagatelj že sprejel oziroma izvedel vse druge postopke in ukrepe, potrebne za zavarovanje teh dobrin, da pa je za stopnjo varnosti, ki jo varovanje teh dobrin zahteva, potrebno tudi izvajanje biometrijskih ukrepov, saj te dobrine v nasprotnem primeru ne bi bile ustrezno zavarovane. V opisanem primeru slednje ni bilo izkazano.
- Za vstopanje v dve sejni sobi, ki se nahajata znotraj poslovnih prostorov vlagatelja, ki je želel biometrijske ukrepe izvajati nad direktorjem in zaposlenimi v tajništvu. Vlagatelj je navedel, da želi z izvajanjem teh ukrepov varovati multimedijsko opremo, ki je v teh dveh prostorih, in da bi se ukrepi izvajali le nad pooblaščenimi zaposlenimi,

druge osebe pa bi v prostora vstopale s pomočjo brezkontaktne kartice. Informacijski pooblaščenec je ugotovil, da teh ukrepov ni mogoče opredeliti kot nujno potrebne za varovanje premoženja, saj vlagatelj ni izkazal, da gre pri multimedijski opremi za premoženje večje vrednosti ali za drugače posebno pomembno premoženje, ki ga je treba varovati na ta način. Poleg tega je bila upoštevana tudi narava samih sejnih sob; gre za prostora, v katera bo imelo zaradi predavanj in izobraževanj dostop večje število posameznikov in za vstopanje v katera je vlagatelj poleg izvajanja biometrijskih ukrepov želel vzpostaviti tudi sistem vstopanja z brezkontaktnimi karticami. V zvezi s tem je bilo poudarjeno, da je izvajanje biometrijskih ukrepov lahko učinkovito za dostopanje do prostorov, v katerih se hrani neko vrednejše in/ali pomembnejše premoženje, in v primeru, da gre za prostore, v katere lahko vstopajo le pooblaščene osebe, tj. omejen krog posameznikov, kar je tudi namen izvajanja teh ukrepov. V obravnavanem primeru pa je vlagatelj želel biometrijske ukrepe izvajati za vstopanje v prostora, ki sta že v osnovi namenjena širšemu krogu ljudi, kot alternativni način vstopanja pa je nameraval uporabljati brezkontakne kartice, zato ni bilo mogoče trditi, da je izvajanje teh ukrepov za vstopanje v prostora nujno potrebno, ker za varovanje premoženja ne obstaja noben milejši ukrep, hkrati pa omogočiti vstopanje tudi s takšnim, milejšim ukrepom. Biometrijski ukrepi so lahko učinkoviti samo, če predstavljajo edini način vstopanja v zavarovane prostore, zato bi omogočanje vstopanja tudi z brezkontaktnimi karticami izničilo vse prednosti biometrijskih ukrepov pred drugimi načini vstopanja. Poseg v informacijsko zasebnost zaposlenih, do katerega bi prišlo z izvajanjem teh ukrepov, ob dvojnem sistemu vstopanja ne bi prispeval k varnosti premoženja, ki je v obeh sejnih sobah, saj bi bila stopnja varnosti praktično enaka, kot če bi se v prostora vstopalo samo z brezkontaktnimi karticami.

2) Informacijski pooblaščenec je vlagatelju za namen varstva ljudi in premoženja dovolil izvajanje biometrijskih ukrepov z uporabo čitalnikov prstnih odtisov, in sicer je izvajanje biometrijskih ukrepov dovolil nad tistimi zaposlenimi, ki opravljajo delovne naloge v navedenih prostorih in so za dostop do teh prostorov pooblaščeni:

- za vstopanje v prostore znotraj dializnega centra, v katerih vlagatelj meša in hrani dializno raztopino,
- za vstopanje v prostore znotraj dializnega centra, v katerih vlagatelj hrani zdravila,
- za vstopanje v prostore znotraj dializnega centra, v katerih vlagatelj hrani zdravstveno dokumentacijo svojih pacientov.

Informacijski pooblaščenec je ugotovil, da je izvajanje biometrijskih ukrepov za vstopanje v te prostore v konkretnem primeru mogoče opredeliti kot nujno potrebno za varnost ljudi in premoženja, saj je ocenil, da sta namena, glede na vse ugotovljene okoliščine, dovolj tehtna, resna in utemeljena ter da tehnične rešitve, ki jih nameravani biometrični ukrepi predvidevajo, s stališča načela sorazmernosti upravičujejo uvedbo biometrijskih ukrepov za vstopanje v te prostore. V postopku je bilo ugotovljeno, da se v vseh treh obravnavanih prostorih nahaja bodisi občutljiva oprema bodisi občutljive, nevarne in drage substance ali pa dokumentacija, ki vsebuje občutljive osebne podatke. Izvajanje biometrijskih ukrepov za vstopanje v prostore, v katerih se meša in hrani dializna raztopina, je bilo prepoznano kot nujno potrebno za varnost ljudi in premoženja. Ugotovljeno je bilo, da je v prostoru naprava, ki predstavljata premoženje večje vrednosti, predvsem pa bi zaradi nepravilnega delovanja take naprave ali kontaminacije tekočine lahko prišlo do resnega ogrožanja zdravja ali celo življenja pacientov, zaradi česar je vlagatelj dolžan storiti vse, da za zagotavljanje varnosti sprejme ustrezne ukrepe, med katere sodijo tudi ukrepi za preprečevanje dostopa nepooblaščenim osebam v take prostore. Ker bi vstopanje in delovanje nepooblaščenih oseb v teh prostorih lahko imelo hude posledice za premoženje ter zlasti za življenje in zdravje pacientov, je organ ocenil, da varovanje slednjih pravnih vrednot v konkretnem primeru odtehta poseg, ki ga predstavlja izvajanje biometrijskih ukrepov nad zaposlenimi. Do smiselno enakega zaključka je Informacijski pooblaščenec prišel tudi pri presoji izvajanja biometrijskih ukrepov za vstopanje v prostore, v katerih se hranijo zdravila, in v prostore, v katerem je zdravstvena dokumentacija vlagateljevih pacientov. V prostorih, v katerih vlagatelj hrani zdravila, je velika koncentracija različnih zdravil, saj ima vlagatelj v dializnem centru samo en tak prostor, kjer hrani zlasti vsa občutljivejša in nevarnejša zdravila ter zdravila velike vrednosti. V primeru neustreznega zavarovanja takih zdravil bi lahko prišlo do njihove nepooblaščene in nepravilne uporabe ter posledično do ogrožanja zdravja in življenja ljudi, zato je Informacijski pooblaščenec ocenil, da varovanje ljudi in premoženja tudi v tem primeru odtehta poseg, ki ga predstavlja izvajanje biometrijskih ukrepov. S smiselno enako argumentacijo je bilo dovoljeno tudi izvajanje teh ukrepov za vstopanje v

prostore, v katerih je zdravstvena dokumentacija pacientov vlagatelja. Izguba ali uničenje zdravstvene dokumentacije kot posledica vstopanja nepooblaščenih oseb v ta prostor bi lahko v znatni meri ogrozila zdravje pacientov, saj dokumentacija vsebuje podatke o njihovem večletnem zdravljenju, o poteku in načinih oskrbe ter druge zdravstvene podatke; izguba ali uničenje dokumentacije bi posredno povzročila tudi premoženjsko škodo, tako pacientom kakor vlagatelju. Posledice vstopanja nepooblaščenih oseb v varovani prostor bi bile torej tudi v tem primeru lahko zelo resne, zato je varstvo ljudi in premoženja odtehtalo poseg, ki ga predstavlja izvajanje obravnavanih ukrepov. Informacijski pooblaščenec je v zvezi z določanjem zaposlenih, nad katerimi bo vlagatelj izvajal biometrijske ukrepe, v odločbi opozoril, da zgolj podelitev pooblastila določenim zaposlenim, katerih delovne naloge ne vključujejo oziroma ne zahtevajo vstopanja v zadevne prostore, ne more biti zadosten pogoj za izvajanje biometrijskih ukrepov nad njimi, temveč morajo biti narava njihovega dela in njihove delovne naloge dejansko takšne, da neizogibno vključujejo tudi vstopanje v zadevne prostore.

Informacijski pooblaščenec je vlagatelju zavrnil izvajanje biometrijskih ukrepov na glavnem vhodu v njegov dializni center za vstopanje zaposlenih v prostore tega centra in za registracijo njihovega delovnega časa. V zvezi z izvajanjem teh ukrepov za registracijo delovnega časa zaposlenih je Informacijski pooblaščenec ugotovil, da vlagatelj v postopku ni z ničemer utemeljil, da bi bila registracija delovnega časa z biometrijskimi ukrepi nujno potrebna za varovanje katere od pravnih dobrin iz 80. člena ZVOP-1. Vlagatelj v postopku niti ni konkretno navedel, katero od teh dobrin želi varovati z registracijo na tak način in tudi ni izkazal, zakaj bi bilo to dobrino treba zavarovati prav z biometrijskimi ukrepi, pa tudi ne, da ne obstajajo nobeni milejši ukrepi (ukrepi, ki bi v manjši meri posegali v informacijsko zasebnost zaposlenih) za njeno zavarovanje. Informacijski pooblaščenec je na podlagi navedenega ugotovil, da registracije delovnega časa zaposlenih z biometrijskimi ukrepi ni mogoče opredeliti kot nujno potrebne za zavarovanje katere od v 80. členu ZVOP-1 naštetih pravnih dobrin. V zvezi z izvajanjem biometrijskih ukrepov nad zaposlenimi za nadzor dostopov v dializni center je bilo ugotovljeno, da jih je želel vlagatelj izvajati na glavnem vhodu, ki je namenjen tako vstopanju zaposlenih kot tudi pacientov in drugih posameznikov, z izvajanjem teh ukrepov pa je želel preprečiti dostopanje nepooblaščenih oseb v dializne centre. Informacijski pooblaščenec je ocenil, da izvajanje takih ukrepov na glavnem vhodu v dializni center ni nujno potrebno že zato, ker je enako stopnjo varstva ljudi in premoženja mogoče zagotoviti z izvajanjem teh ukrepov v manjšem obsegu, tj. tako, da se teh ukrepov ne izvaja nad vsemi zaposlenimi, ampak zgolj na tistimi, ki so pooblaščeni za vstopanje v varovane prostore znotraj dializnega centra. Poleg tega je Informacijski pooblaščenec opozoril na navedbo vlagatelja, da v dializnem centru velja poseben urnik ter da je glavni vhod v dializni center določen čas odprt oziroma prosto dostopen. Vrata naj bi bila odprta v času, ko pacienti v dializni center prihajajo in iz njega odhajajo. V odločbi je bilo poudarjeno, da ni mogoče trditi, da je izvajanje biometrijskih ukrepov na glavnem vhodu v objekt nujno potrebno, hkrati pa je prav ta glavni vhod določen del dneva odprt in prosto dostopen. V zvezi z navedbami vlagatelja, da bi mu vstopanje v dializni center s pomočjo biometrijskih ukrepov omogočalo nesporen pregled nad tem, kdo od zaposlenih je v določenem času dneva sodeloval s pacienti, je bilo ugotovljeno, da za ugotavljanje tega dejstva obstaja vrsta sredstev, ki so milejša od izvajanja biometrijskih ukrepov na predlagani način. Vstopanje z brezkontaktnimi karticami in/ali PIN-kodami, organizacija dela in urniki dela, podpisovanje ob prihodu na delo, nadzor nadrejenih in pričanja pacientaov so samo nekatera od njih.

Informacijski pooblaščenec je v celoti zavrnil tri zahteve za izvajanje biometrijskih ukrepov.

1) Zahtevo vlagatelja, ki je želel biometrijske ukrepe izvajati nad vsemi svojimi zaposlenimi, za vstopanje v njegove poslovne prostore skozi glavni vhod. Vlagatelj je v vlogi kot namen uvedbe navajal varstvo ljudi in premoženja ter varovanje poslovnih skrivnosti in tajnih podatkov, vendar je v postopku uspel izkazati le namena varstva premoženja in varovanja poslovnih skrivnosti. Informacijski pooblaščenec je moral v postopku presoditi, ali je vlagatelj izkazal, da varovanih dobrin ni mogoče primerljivo učinkovito varovati z drugimi ukrepi, ki ne vključujejo izvajanja biometrijskih ukrepov, pa tudi, da želenega cilja ni mogoče doseči z izvajanjem biometrijskih ukrepov v manjšem obsegu, predvsem z njihovim izvajanjem nad ožjim krogom zaposlenih. Način izvajanja biometrijskih ukrepov, kot ga je želel vlagatelj, v primerjavi s sistemom, v katerem gre za izvajanje teh ukrepov nad omejenim delom zaposlenih in zgolj za vstopanje v posamezne prostore, predstavlja poseg v informacijsko

zasebnost precej večjega števila posameznikov, hkrati pa predlagani sistem varovanja, v katerem imajo vsi zaposleni dostop do poslovnih skrivnosti in varovanega premoženja, znatno zmanjšuje učinkovitost samih ukrepov. Sistem varovanja teh dobrin bi namreč moral predstavljati premišljen, dodelan, dopolnjujoč se in vsestransko uravnotežen sistem postopkov in ukrepov za njihovo zavarovanje, pri čemer bi bilo izvajanje biometrijskih ukrepov v tak sistem, kot njegov integralni del, vključeno samo takrat, ko bi šlo za varovanje pravnih dobrin, ki jih našteva 80. člen ZVOP-1, in varnosti z drugimi ukrepi varovanja ne bi bilo mogoče zagotoviti, ter tako, da bi se ti ukrepi izvajali v najmanjšem možnem obsegu. Ugotovljeno je bilo, da je predlagani sistem vlagatelja s tega vidika izrazito neuravnotežen in posledično tudi nesorazmeren, saj za vstopanje v njegove poslovne prostore predvideva izvajanje ukrepa, ki predstavlja občuten poseg v zasebnost vseh zaposlenih, znotraj poslovnih prostorov pa bi imeli vsi zaposleni dostop do vseh varovanih dobrin. Na podlagi navedenega je bilo ugotovljeno, da izvajanja biometrijskih ukrepov ni mogoče opredeliti kot nujno potrebnega za varstvo premoženja in poslovnih skrivnosti, ker bi lahko vlagatelj primerljivo (ali celo višjo) stopnjo varovanja navedenih dobrin dosegel z izvajanjem drugih ukrepov za njihovo zavarovanje, ki sploh ne bi ali pa bi le v manjši meri posegali v informacijsko zasebnost zaposlenih. Informacijski pooblaščenec je v zvezi z vlagateljevo navedbo, da bodo delavci pogodbenega čistilnega servisa v njegove prostore vstopali s ključem, poudaril, da ni mogoče trditi, da je izvajanje biometrijskih ukrepov na glavnem vhodu v poslovne prostore nujno potrebno, ker za varovanje ne obstaja noben milejši ukrep, hkrati pa določenim subjektom omogočati vstop z drugačnimi ukrepi, tj. s ključem. Vstopanje v poslovne prostore vlagatelja naj bi bilo torej možno (najmanj) na dva načina, tj. s pomočjo biometrijskih ukrepov in s pomočjo ključev, kar pa pomeni, da bodo zlorabe, ki naj bi jih vlagatelj z biometrijskimi ukrepi preprečil, še vedno možne, saj bi nepooblaščena oseba, ki bi našla, ukradla ali drugače nepooblaščeno prišla do ključa varovanih prostorov, v te prostore, tudi po nameravani uvedbi biometrijskih ukrepov, še vedno lahko vstopila s tem ključem, kar pomeni, da uvedba biometrijskih ukrepov možnosti zlorab, ki jih je navajal vlagatelj, ne bi odpravila.

2) Zahtevo vlagatelja, ki je želel biometrijske ukrepe izvajati za beleženje delovnega časa svojih zaposlenih. Vlagatelj v svoji zahtevi ni navedel oziroma konkretiziral premoženja, ki ga želi varovati z biometrijskimi ukrepi, ter ni navedel ali izkazal, na kakšen način bi lahko bili njegova dejavnost in/ali premoženje ogroženi, če za registracijo delovnega časa ne bi izvajal biometrijskih ukrepov. Vlagatelj bi namreč v postopku moral izkazati, da je evidentiranje delovnega časa njegovih zaposlenih z biometrijskimi ukrepi nujno potrebno za opravljanje njegove dejavnosti in/ali za varstvo njegovega premoženja. Ker gre pri izvajanju biometrijskih ukrepov za relativno resen poseg v informacijsko zasebnost zaposlenih, bi morala za odobritev takega posega na drugi strani obstajati resna potreba po zavarovanju opravljanja konkretne dejavnosti oziroma konkretnega premoženja. Vlagatelj v predmetnem postopku ni navedel, zakaj in kako bi bila lahko ogrožena njegova dejavnost in/ali njegovo premoženje, če delovnega časa ne bi beležil z izvajanjem biometrijskih ukrepov, ampak na kak drug način. Prav tako ni konkretiziral nujne potrebnosti evidentiranja delovnega časa z biometrijskimi ukrepi za varstvo navedenih dobrin, ampak je njegova argumentacija ostajala na povsem splošni ravni (učinkovitost upravljanja, produktivnost v proizvodnji), poleg tega pa ni določno opredelil, zakaj evidentiranja delovnega časa ni mogoče izvajati na druge, milejše načine. Vlagatelj bi moral glede na povedano v konkretnem primeru izkazati, da bi bila bodisi njegova dejavnost bodisi premoženje, če za registracijo delovnega časa zaposlenih ne bi uporabil prav biometrijskih ukrepov, ogrožena v obsegu, ki odtehta tudi poseg v informacijsko zasebnost posameznika, ki ga predstavljajo taki ukrepi, kar pa, po ugotovitvah Informacijskega pooblaščenca, v obravnavanem primeru nikakor ni bilo izkazano.

3) Zahtevo vlagatelja, ki je želel biometrijske ukrepe izvajati nad vsemi svojimi zaposlenimi in nad študenti za vstopanje v njegove poslovne prostore skozi glavni vhod. Vlagatelj je kot namen uvedbe teh ukrepov navedel varnost premoženja, varovanje tajnih podatkov in varovanje poslovnih skrivnosti, pri čemer pa v postopku ni predložil nobenega dokaza in ni na noben drug način izkazal, da dejansko razpolaga s tajnimi podatki in poslovnimi skrivnostmi, ter ni opredelil premoženja, ki bi ga želel na tak način varovati. Prav tako vlagatelj ni navedel, zakaj je to premoženje treba varovati z biometrijskimi ukrepi, in kje znotraj njegovih poslovnih prostorov se tako premoženje nahaja (ali v vseh prostorih ali samo v nekaterih). V postopku ni bilo mogoče ugotoviti, na kakšen način in s čigave strani so varovane dobrine ogrožene, kakšna je stopnja ogroženosti ter zakaj v zahtevi navedenih dobrin ne bi bilo mogoče varovati z drugimi ukrepi, ki v manjši

meri posegajo v informacijsko zasebnost zaposlenih. Glede na navedeno v predmetnem postopku Informacijski pooblaščenec sploh ni mogel opraviti presoje, ali bi varovanje zakonsko določenih vrednot odtehtalo poseg, ki ga predstavljajo obravnavani ukrepi, saj vlagatelj, kljub večkratnim pozivom, svoje vloge ni dopolnil s pravno relevantnimi dejstvi in okoliščinami, ki bi utemeljevale njegovo zahtevo za izvajanje biometrijskih ukrepov. Informacijski pooblaščenec je glede navedbe vlagatelja, da bi želel biometrijske ukrepe izvajati tudi nad posamezniki, ki pri njem opravljajo študentsko delo, v postopku izrecno poudaril, da ZVOP-1 dopušča zgolj izvajanje biometrijskih ukrepov nad zaposlenimi in da torej izvajanje teh ukrepov nad osebami, ki pri upravljavcu niso zaposlene (npr. študenti), ni dovoljeno. Na podlagi navedenega je Informacijski pooblaščenec zaključil, da nameravana uvedba biometrijskih ukrepov ni nujno potrebna za namene varstva premoženja, varovanja poslovnih skrivnosti in varovanja tajnih podatkov, saj vlagatelj sploh ni izkazal, da razpolaga s pravnimi dobrinami, za varovanje katerih je izvajanje teh ukrepov dopusten, še manj pa nujen ukrep.

Informacijski pooblaščenec je leta 2013 prejel dve odločitvi Upravnega sodišča RS v zvezi s tožbami, ki sta ju zoper zavrnilni odločbi Informacijskega pooblaščenca vložila vlagatelja. Sodišče je obe tožbi zavrnilo.

4.5. Ugotavljanje ustrezne ravni varstva osebnih podatkov v tretjih državah

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

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

Informacijski pooblaščenec mora kot pristojni nadzorni organ za varstvo osebnih podatkov glede na določbe sedme točke 1. 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 posebne odločbe glede iznosa osebnih podatkov v tretje države opraviti tudi vsebinski preizkus, 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 2013 prejel 14 vlog za iznos osebnih podatkov, en vlagatelj je svojo vlogo pozneje umaknil. Izdal je 16 odločb, od tega pet v zadevah, ki jih je v reševanje prejel leta 2012. Vsem vlagateljem je iznos osebnih podatkov dovolil:

- Družbi, ki se ukvarja s trženjem zdravil (izvoznik podatkov), je dovolil, da po prejemu odločb (družbi so bile izdane tri odločbe) svojim pogodbenim obdelovalcem osebnih podatkov v Združenih državah Amerike, Indiji in na Novi Zelandiji (uvozniki podatkov) iznaša in posreduje osebne podatke zaposlenih, občasnih delavcev in svetovalcev. Uvozniki podatkov bodo izvozniku podatkov zagotavljali opravila v zvezi z zagotavljanjem storitve elektronske pošte in sporočanja v aplikaciji MS Exchange, kar vključuje omogočanje pošiljanja sporočil, upravljanje in usmerjanje sporočil, podporo

osebja, dnevne varnostne kopije in arhiviranje sporočil. Osebni podatki, ki bodo pri tem preneseni, so: ime, številka službenega telefona in službenega mobilnega telefona, službeni elektronski naslov in osebni podatki, ki se prenašajo prek elektronske pošte.

- Družbi za trgovino in investicije (izvoznik podatkov) je dovolil, da po prejemu odločbe svojim pogodbenim obdelovalcem osebnih podatkov v tretjih državah (Indija, Filipini, Združene države Amerike, Kitajska in Kostarika) (uvoznikom podatkov) iznaša in posreduje osebne podatke, ki se nanašajo na zaposlene pri izvozniku podatkov, pogodbene sodelavce in svetovalce (ime, naslov, telefonska številka in številka telefaksa, e-naslov, kraj opravljanja dela, plačila, ugodnosti, naziv, raven izobrazbe, opis delovnega mesta, ocena delovne uspešnosti usposabljanja, datum rojstva, davčna številka, zakonski stan, družinski člani, bančni račun, številka kreditne kartice), obstoječe in potencialne stranke (ime, naslov, telefonska številka in številka telefaksa, e-naslov, kraj opravljanja dela, naziv delovnega mesta, podjetje, opis delovnega mesta, bančni račun, številka kreditne kartice) ter prodajalce (ime, naslov, telefonska številka in številka telefaksa, e-naslov, kraj opravljanja dela, naziv delovnega mesta, podjetje, funkcija, bančni račun, števila kreditne kartice). Namen iznosa podatkov je podpora naročanju, podpora pri obdelavi obveznosti do dobaviteljev, podpora zbiranju zaradi računovodskega poročanja, knjiženje izterjanih zneskov, izterjave, vodenje sporov, uskladitve in periodično obdelovanje, obračunavanje uporabniških storitev, zajem in obdelava dokumentov, podpora procesom »Purchase to Pay« ter »Supply Chain Management«, obdelava zahtevkov za povračilo stroškov, tehnična podpora in upravljanje določenih orodij ter drugih povezanih finančnih, računovodskih obdelav podatkov.

- Slovenskima podružnicama tujih trgovskih podjetij (izvoznika podatkov) je dovolil, da po prejemu odločb (vsaki družbi je izdal tri odločbe) osebne podatke:
  - nekdanjih, sedanjih in bodočih zaposlenih, prostovoljcev, sodelavcev in partnerjev,
  - nekdanjih, sedanjih in bodočih strank,
  - nekdanjih, sedanjih in potencialnih svetovalcev, strokovnjakov, dobaviteljev, izvajalcev, podizvajalcev, zastopnikov in posrednikov,
  - tožnikov, dopisnikov, obiskovalcev in povpraševalcev,
  - koristnikov, odvisnih oseb, staršev, skrbnikov in kontaktnih oseb v nujnih primerih iznašata v Združene države Amerike, Panamo, Malezijo in Indijo ter jih tam posredujeta svojim pogodbenim obdelovalcem (uvoznikom podatkov) za namen zagotavljanja določenih proizvodov in storitev informacijske tehnologije. Osebni podatki, ki bodo pri tem preneseni, so: naziv in ime; domači naslov; številke domačega telefona, faksa in prenosnega telefona; domači e-naslov; družinski stan; premoženjsko stanje (najemnik, lastnik); odgovori na varnostna vprašanja (npr. kraj rojstva, materino dekliško ime); članstvo v klubih in društvih; osebni finančni podatki (npr. bančni račun, podatki o kreditnih karticah); podatki v zvezi z dohodki in zaposlitvijo; nepremičninsko in drugo premoženje; hipoteke in druga posojila; kreditno stanje in podatki v zvezi s krediti; podatki v zvezi s stroški in izdatki; podatki o zaposlitvi in številka zaposlenega; identifikacijski podatki o IT-sistemu ali premoženjskem stanju; omrežne prijave; podatki o uporabi programske opreme; tonski, video- in podatkovni zapisi ustvarjeni prek IT-orodij za izobraževanje, namene kakovosti ipd.; »online« interaktivna in tonska komunikacija (npr. blogi, klepeti, spletna kamera in spletna komunikacija); status »export« skladnosti; službeni naslov, oddelek in lokacija delovnega mesta; službeni naziv, e-naslov, podatki o uporabniških imenih, podatki o spletnih prijavah in gesla; številke službenih telefonov, faksov in mobilnih telefonov; fotografija ali videonadzor, številka potnega lista; številka vozniškega dovoljenja; številka socialnega zavarovanja; delovne ocene; disciplinski postopki; spol; nivo delovnega mesta; vzroki za prekinitev; datum rojstva in starost; digitalni elektronski podpis; EMŠO; davčna številka; geolokacijski podatki. Poleg navedenih bodo preneseni tudi nekateri občutljivi osebni podatki: zdravstveni podatki (poklicno zdravje); članstvo v zvezah; podatki o postopkih internih preiskav.

- Družbi za merjenje in upravljanje energije (izvoznik podatkov) je dovolil, da po prejemu odločbe svojemu pogodbenemu obdelovalcu osebnih podatkov v Združenih državah Amerike (uvozniku podatkov) iznaša in posreduje osebne podatke, ki se nanašajo na zastopnike in končne uporabnike, vključno z delavci, sodelavci in kupci izvoznika podatkov, ter posameznike, ki osebne podatke skušajo sporočiti ali prenesti

uporabnikom storitev, ki jih zagotavlja uvoznik podatkov. Podatki vključujejo elektronsko pošto, dokumente in druge podatke v elektronski obliki v okviru spletnih storitev Microsoft, npr. kontaktne podatke, rojstne datume, podatke o zaposlitvi, podatke o plači delavca ipd. Pri tem ni mogoče zagotoviti, da uvozniku ne bi bili preneseni tudi občutljivi osebni podatki, saj je uporaba poštnih predalov povsem odvisna od presoje posameznikov. Uvoznik podatkov bo za izvoznika podatkov namreč izvajal opravila v zvezi z zagotavljanjem spletnih storitev Microsoft (storitve računalništva v oblaku).

- Naftni družbi (izvoznik podatkov) je dovolil, da po prejemu odločbe osebne podatke fizičnih oseb, vključenih v program zvestobe, iznaša v Vietnam in jih tam posreduje svojemu pogodbenemu obdelovalcu (uvozniku podatkov) za namen zajemanja podatkov iz papirnatih form in njihovega prenosa v digitalno obliko. Osebni podatki, ki bodo pri tem preneseni, so: ime in priimek, dan rojstva, naslov in kraj bivanja, e-naslov, številka telefona, številka mobilnega telefona, vozne navade, življenjski stil (hobiji), način bivanja (enočlansko gospodinjstvo, veččlansko gospodinjstvo, družina z otroki …).

- Banki (izvoznik podatkov) je dovolil, da po prejemu odločbe osebne podatke komitentov banke, zaposlenih v banki in pogodbenih partnerjev iznaša v Rusko federacijo in jih tam posreduje svojemu pogodbenemu obdelovalcu (uvozniku podatkov). Uvoznik podatkov bo za izvoznika podatkov opravljal dejavnosti v zvezi z izvajanjem določene IT-podpore, povezane predvsem z oskrbovanjem in popravili opreme za zagotavljanje uporabnosti kompleksa strojne opreme. Osebni podatki, ki bodo pri tem preneseni, so:
  - matični podatki o komitentu/zaposlenemu: davčna številka/EMŠO, šifra komitenta, ime in priimek, datum in kraj rojstva, podatki iz kadrovske evidence zaposlenih (izobrazba, delovno mesto, čas in kraj usposabljanja s preizkusi znanja, preventivni pregledi, poškodbe pri delu, evidenca prihodov in odhodov z evidenco ur za plačilo …), naslov stalnega prebivališča (ulica, hišna številka, poštna številka, kraj pošte, država), telefonska številka, e-naslov, naslov začasnega prebivališča (ulica, hišna številka, poštna številka, kraj, država), vrsta, številka, izdajatelj, datum in kraj izdaje osebnega dokumenta, namen odprtja računa, podatki o karticah (Mastercard, Maestro), zaposlitev;
  - matični podatki o poslih: vrsta posla (TRR, izredni limit, osebni kredit, stanovanjski kredit, poroštvo, druge terjatve), limit (višina, trajanje, prekoračitve), številka pogodbe in datum sklenitve posla, oznaka valute, znesek ob odobritvi, znesek anuitete oz. obroka, vrsta anuitete oz. obroka, odplačilna doba v mesecih, datum zapadlosti posla, podatki o moratoriju, datum vnosa posla v SISBON;
  - poslovni dogodki, ki vplivajo na potek posla: odplačilo dolga, predčasno poplačilo, sprememba odplačilne dobe, sprememba obroka;
  - poslovni dogodki, ki niso v skladu s pogodbo: odpoved posla zaradi neplačila dolga, neplačan zapadli dolg, blokacija, deblokacija.

Informacijski pooblaščenec je pri presoji pravne podlage za nameravano posredovanje osebnih podatkov ugotovil, da gre v vseh 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). Kot pravna podlaga za posredovanje osebnih podatkov se tako štejejo določbe 11. člena 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 ter zagotavlja ustrezne postopke in ukrepe iz 24. člena tega zakona. Pogodbeni obdelovalec sme 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 ter mora vsebovati tudi dogovor o postopkih in ukrepih iz 24. člena ZVOP-1. Informacijski pooblaščenec je po pregledu pogodb, 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. 2. 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 2. odstavek 26. člena Direktive 95/46/ES Evropskega parlamenta in Sveta z dne 24. 10. 1995 o zaščiti posameznikov pri

obdelavi osebnih podatkov in o prostem gibanju takih podatkov. Sprejete standardne pogodbene klavzule z obema dodatkoma 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 ter dogovor o postopkih in ukrepih za zavarovanje osebnih podatkov.

V naslednjih treh primerih se bodo podatki posredovali na podlagi zavezujočih poslovnih pravil (ang. binding corporate rules). Informacijski pooblaščenec je po pregledu dokumentacije, ki so jo predložili izvozniki podatkov, ugotovil, da so zavezani k spoštovanju zavezujočih poslovnih pravil, ki jih je sprejela mednarodna skupina, katere člani so. Zavezujoča poslovna pravila, sprejeta po ustreznem postopku, podrobneje predpisanim z dokumenti Delovne skupine iz 29. člena, ki zavezujejo vse članice mednarodne skupine, štejejo za taka, da zagotavljajo, da skupina na področju prenosov podatkov v tretje države zagotavlja ustrezne ukrepe zavarovanja osebnih podatkov ter temeljnih pravic in svoboščin posameznikov, in navedejo možnosti njihovega uresničevanja ali varstva, skladno sedmo točko 1. odstavka 70. člena ZVOP-1. Postopek sprejema zavezujočih poslovnih pravil zajema postopek pred vodilnim organom za varstvo osebnih podatkov glede na sedež določene članice v EU (v konkretnih primerih sta to Danska in Francija), ki zavezujoča pravila potrdi in s tem zagotavlja, da ustrezajo zahtevam zakonodaje s področja varstva osebnih podatkov v EU, ter postopek vzajemnega priznavanja pravil, v katerega so vključeni tudi ostali organi iz relevantnih držav članic EU. Informacijski pooblaščenec je sodeloval tudi v postopku vzajemnega priznavanja zavezujočih poslovnih pravil.

Na podlagi zavezujočih poslovnih pravil je Informacijski pooblaščenec dovolil iznos osebnih podatkov:

- Farmacevtski družbi (izvoznik podatkov) je dovolil, da po prejemu odločbe svojim pogodbenim obdelovalcem in drugim upravljavcem oziroma drugim članicam skupine, pri čemer se del članic nahaja v tretjih državah, iznaša in posreduje osebne podatke zaposlenih in sodelavcev, dobaviteljev in poslovnih partnerjev, udeležencev kliničnih študij in raziskovalcev, uporabnikov in kupcev ter zdravstvenih delavcev. Izvoznik podatkov bo osebne podatke posredoval za naslednje namene: administracija, poročanje, organizacijski in utemeljeni poslovni nameni, upravljanje zaposlenih, komuniciranje, vzdrževanje poslovnih operacij, zagotavljanje skladnosti, izvajanje ocen o vplivih na zdravje, podpora pacientom, prodaja in marketing, izvajanje finančnih in drugih transakcij, izvajanje farmakovigilančnih aktivnosti. Posredovali se bodo naslednji podatki:
    - splošni in identifikacijski podatki o zaposlenih, začasno zaposlenih, pripravnikih, kandidatih, svetovalcih itd. (ime, priimek, naslov, telefonska številka, faks, e-naslov in drugi kontaktni podatki, narodnost, datum rojstva, številka osebne izkaznice in potnega lista, status, podatki o družinskih članih, fotografija …), informacije za upravljanje s talenti;
    - podatki o socialni varnosti (davčna številka, podatki o zdravstvenem zavarovanju, bolniške odsotnosti, delovne omejitve itd.);
    - administrativni in finančni podatki (delovno mesto, izobrazba, podatki o zaposlitvi, številka bančnega računa, kreditne kartice, podatki o prejemkih in nagradah itd.);
    - podatki za pomoč pacientom (zdravstveni podatki, povpraševanje po proizvodih in storitvah, uporabniških transakcijah, gesla za pridobivanje internetnih informacij);
    - podatki o zdravstvenem stanju (fizične lastnosti, genski podatki, biološki vzorci, informacije o predpisanih zdravilih, življenjskem slogu ipd.);
    - podatki udeležencev v kliničnih raziskavah (koda udeleženca, začetnice, datum rojstva, spol, ime in kontaktni podatki, če gre za poročanje o neželenih učinkih, podatki o zdravstvenem stanju udeležencev, o meritvah in doziranjih itd.);
    - podatki o strankah, dobaviteljih in poslovnih partnerjih, zdravstvenih delavcih (ime, naslov, kontaktni podatki, poslovni in raziskovalni podatki, finančni podatki, podatki o usposobljenosti itd.).

- Podjetju za revizijo in druge finančno računovodske storitve (izvoznik podatkov) je dovolil, da po prejemu odločbe svojim pogodbenim obdelovalcem osebnih podatkov in upravljavcem osebnih podatkov v tretjih državah (uvoznikom podatkov), to je drugim družbam v poslovni skupini, iznaša in posreduje:
    - podatke v zvezi z zaposlenimi (partnerji, zaposleni pogodbeniki, sorodniki in bližnje

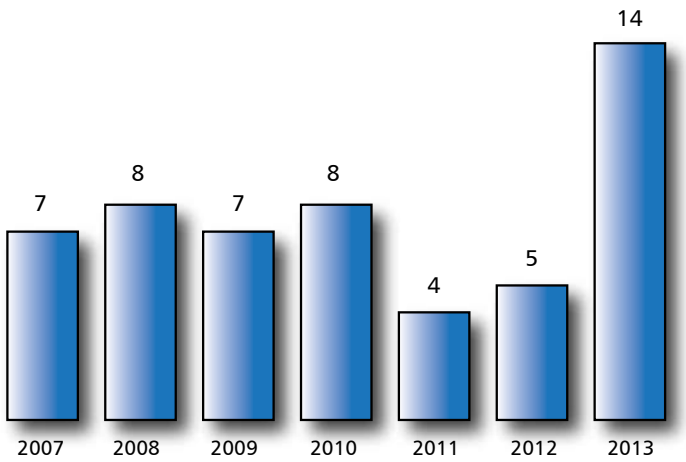
osebe, vlagatelji zahtevkov, upravičenci in prejemniki plačil). Namen prenosa je upravljanje z osebjem, oglaševanje, izdajanje licence, upravljanje s podatki, spoštovanje standardov in internih politik idr. Podatki, ki se bodo obdelovali, so: osebni podatki, podatki o družini, izobrazbi, zaposlitvi in partnerstvu, podatki o ugodnostih in finančne podrobnosti, zvočne in/ali vizualne podobe. V državah, kjer je to dovoljeno, se lahko zbirajo tudi občutljivi osebni podatki o rasi, političnem prepričanju, verskem prepričanju, zdravju, kaznovanosti, članstvu v sindikatu;

- podatke o stranki (osebje družb, sedanje in bodoče stranke, poslovni partnerji, avtorji, novinarji idr.). Namen prenosa je opravljanje strokovnih storitev, vodenje računov in evidenc, oglaševanje, upravljanje s podatki idr. Podatki, ki se bodo obdelovali, so: osebni podatki, podatki o družini, izobrazbi, zaposlitvi, ugodnostih, dobavljenem blagu in storitvah in zvočne/vizualne podobe;
- ostale poslovne podatke (nanašajo se na svetovalce, izvajalce in ostale strokovnjake, zaposlene pri dobaviteljih, poslovne partnerje, avtorje, založnike, urednike, umetnike itd.). Namen prenosa je dobava in nabava blaga ter storitev družbam, vodenje računov in evidenc, oglaševanje, upravljanje s podatki idr. Podatki, ki se bodo obdelovali, so: osebni podatki, podatki o izobrazbi, zaposlitvi, ugodnostih, dobavljenem blagu in storitvah.

- Družbi, ki se ukvarja s trženjem farmacevtskih izdelkov (izvoznik podatkov), je dovolil, da po prejemu odločbe svojim pogodbenim obdelovalcem in drugim upravljavcem osebnih podatkov v tretjih državah (uvozniki podatkov) v okviru skupine, katere članica je, iznaša in posreduje osebne podatke zaposlenih, strank, dobaviteljev in tretjih oseb, s katerimi sodeluje. Podatki se bodo posredovali za namen rednega poslovanja članic skupine.

Informacijski pooblaščenec je torej zaključil, da so v vseh navedenih primerih izpolnjeni pogoji za iznos osebnih podatkov v tretje države in njihovo posredovanje uvoznikom podatkov, ter poudaril, da pri izvozniku podatkov ni preverjal obstoja pravne podlage z vidika določb 8., 10., 13. in 16. člena ZVOP-1 oz. zakonitosti obdelave posameznih vrst osebnih podatkov. Zakonitost obdelave posameznih vrst osebnih podatkov pri izvozniku podatkov namreč ni predmet tega postopka in jo lahko Informacijski pooblaščenec preverja le v postopku inšpekcijskega nadzora.

Slika 13: Število vlog za izdajo odločbe glede iznosa osebnih podatkov med letoma 2006 in 2013.



4.6. Izdajanje dovoljenj za povezovanje javnih evidenc

Povezovanje zbirk osebnih podatkov urejajo 84., 85. in 86. člen 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 slednji 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, 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. Povezovanje zbirk osebnih podatkov predstavlja avtomatsko in elektronsko povezovanje zbirk osebnih podatkov, ki jih vodijo upravljavci za različne namene, in sicer tako, da se določeni podatki samodejno ali na zahtevo prenesejo ali vključijo v drugo povezano zbirko ali v več povezanih zbirk. Zbirki osebnih podatkov sta povezani, če se določeni podatki iz ene zbirke neposredno vključijo v drugo zbirko, s čimer se druga zbirka spremeni (poveča, ažurira ipd.).

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

Informacijski pooblaščenec je leta 2013 prejel šest vlog za pridobitev dovoljenja za povezovanje zbirk osebnih podatkov. Izdal je pet odločb, s katerimi je trem upravljavcem (Vrhovnemu sodišču RS sta bili izdani dve odločbi) dovolil povezovanje zbirk osebnih podatkov, v enem primeru pa povezovanja zbirk ni dovolil.

Informacijski pooblaščenec je dovolil povezovanje naslednjih zbirk osebnih podatkov:

1. Ministrstvu za notranje zadeve in javno upravo je dovolil, da Evidenco licenc in Evidenco imetnikov službenih izkaznic, ki ju vodi na podlagi Zakona o zasebnem varovanju[34], poveže med seboj ter s:
   - Centralnim registrom prebivalstva, katerega upravljavec je Ministrstvo za notranje zadeve in javno upravo,
   - Poslovnim registrom Slovenije, katerega upravljavec je Agencija RS za javnopravne evidence in storitve ter
   - Evidenco o zavarovanih osebah obveznega zdravstvenega zavarovanja, katere upravljavec je Zavod za zdravstveno zavarovanje Slovenije.

Povezava med zbirkami se lahko izvede na način, da se kot povezovalni znak uporabi EMŠO ali matična številka poslovnega subjekta.

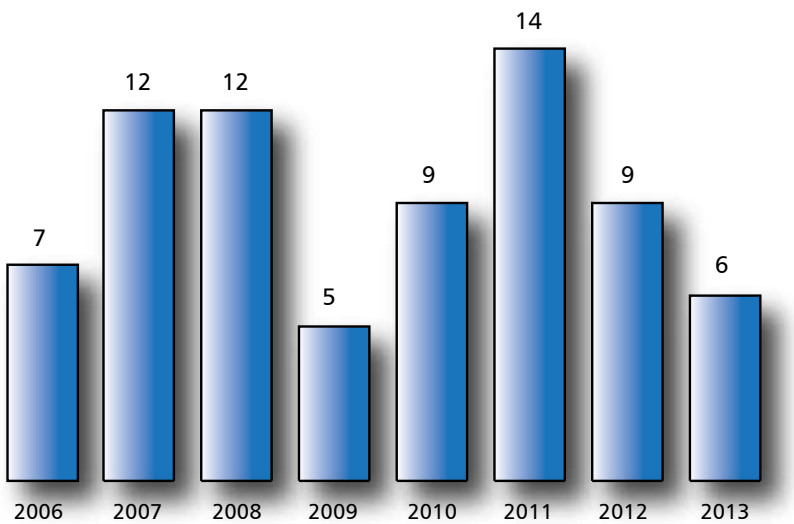
2. Ministrstvu za kmetijstvo in okolje ter Ministrstvu za notranje zadeve je dovolil neposredno računalniško povezavo Evidence subjektov in Centralnega registra prebivalstva.
   Kot povezovalni znak se uporabi EMŠO ali matična številka poslovnega subjekta ali davčna številka.

3. Vrhovnemu sodišču RS je dovolil, da Informacijski sistem izvršba poveže s:
   - Centralnim registrom prebivalstva, katerega upravljavec je Ministrstvo za notranje zadeve in javno upravo,
   - Centralnim registrom nematerializiranih vrednostnih papirjev, katerega upravljavec je KDD – Centralna klirinško depotna družba, d. d.,
   - Evidenco o zavarovanih osebah obveznega zdravstvenega zavarovanja, katere upravljavec je Zavod za zdravstveno zavarovanje Slovenije,
   - Registrom transakcijskih računov, katerega upravljavec je Agencija RS za javnopravne evidence in storitve,
   - Informacijskim sistemom eINS (insolvenčni vpisnik), katerega upravljavec je Vrhovno sodišče RS.

[34] Uradni list RS, št. 17/2011.

Povezava med zbirkami se lahko izvede z uporabo EMŠO ali davčne številke.
Informacijski pooblaščenec je zavrnil vlogo Ministrstva za izobraževanje znanost in šport, s katero je vlagatelj zaprosil za izdajo odločbe oziroma predhodnega dovoljenja za povezavo dveh svojih zbirk osebnih podatkov, in sicer Centralne evidence udeležencev vzgoje in izobraževanja (CEUVIZ) z Evidenco upravičencev do sofinanciranja plačil staršev za vrtec iz državnega proračuna (SPS). Vlagatelj je želel zbirki povezati zaradi odprave administrativnih ovir in nepotrebnega podvajanja dela ter zaradi načela ekonomičnosti postopkov, kot povezovalni znak pa bi uporabil EMŠO. S povezovanjem zbirk bi se opravil avtomatičen prenos podatka o višini znižanega plačila staršev za vrtec iz CEUVIZ v SPS. Informacijski pooblaščenec je proučil določbe Zakona o vrtcih[35], Zakona o organizaciji in financiranju vzgoje in izobraževanja[36] ter ZUP, na katere se je skliceval vlagatelj, in ugotovil, da nameravana povezava ni določena v nobenem zakonu, kar pa kot pogoj za povzovanje zbirk osebnih podatkov iz uradnih evidenc in javnih knjig zahteva 1. odstavek 84. člena ZVOP-1. Tako na odločitev Informacijskega pooblaščenca ni vplivalo niti dejstvo, da se CEUVIZ in SPS vodita za iste oziroma podobne namene, to je za namene izpolnjevanja nalog, povezanih s pravico do sofinanciranja plačil staršev za vrtec iz državnega proračuna.

Slika 14: Število vlog za izdajo odločbe glede povezljivosti zbirk osebnih podatkov med letoma 2006 in 2013.



4.7. Seznanitev z lastnimi osebnimi podatki

V skladu s 3. 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.

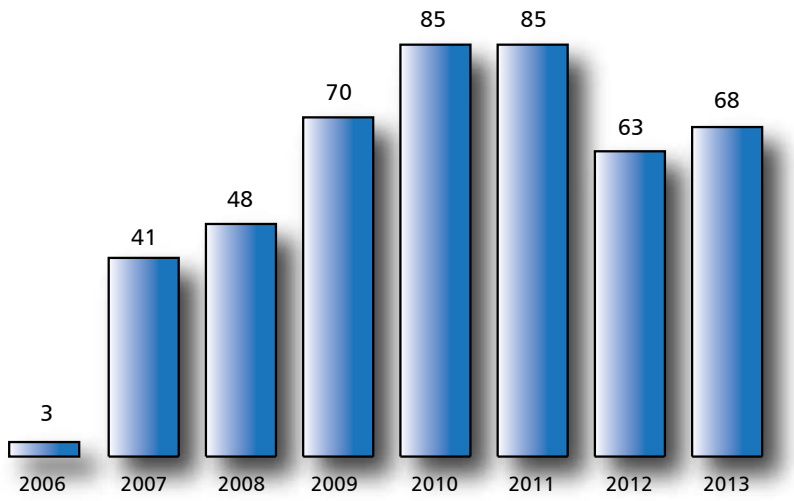
Informacijski pooblaščenec je leta 2013 uvedel 68 pritožbenih postopkov v zvezi s pravico do seznanitve z lastnimi osebnimi podatki (leta 2012 je uvedel 63 postopkov, leta 2011 in 2010 pa 85). V okviru pritožbenih postopkov je Informacijski pooblaščenec reševal tudi pritožbe, ko posamezniki niso pridobili zdravstvene dokumentacije po ZPacP. Teh je bilo 11 (leta 2010 so bile štiri, leta 2011 jih je bilo 18, leta 2012 pa deset).

Informacijski pooblaščenec je po preučitvi pritožb ugotovil, da je v primerjavi s preteklimi leti delež molka upravljavcev osebnih podatkov, torej primerov, da upravljavci na zahtevo

[35] Uradni list RS, št. 100/2005-UPB2, s spremembami.
[36] Uradni list RS, št. 16/2007-UPB, s spremembami.

posameznika v zvezi s seznanitvijo z lastnimi osebnimi podatki sploh niso odgovorili, ostal na isti ravni (52 %). Posameznik lahko v primeru molka upravljavca in tudi v primeru zavrnitve seznanitve vloži pritožbo Informacijskemu pooblaščencu.

Slika 15: Število pritožb v zvezi s pravico do seznanitve z lastnimi osebnimi podatki med letoma 2006 in 2013.

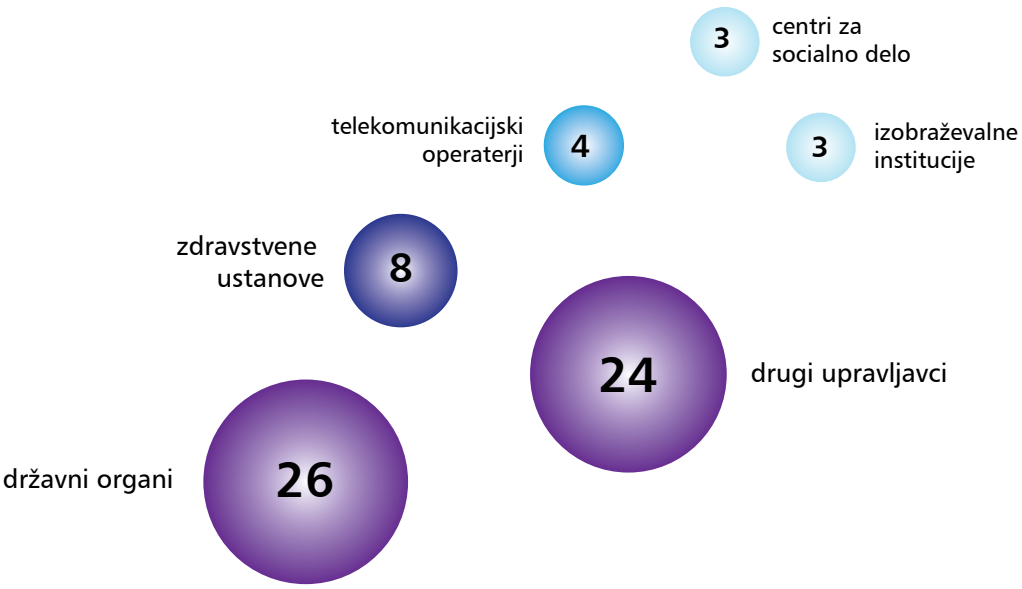


Vložene pritožbe zaradi zavrnitve seznanitve z lastnimi osebnimi podatki so zadevale naslednje vrste upravljavcev osebnih podatkov:

- državni organi (večinoma ministrstva in organi v njihovi sestavi) – 26,
- zdravstvene ustanove – 8,
- telekomunikacijski operaterji – 4,
- izobraževalne institucije – 3,
- centri za socialno delo – 3
- drugi upravljavci (npr. zavarovalnica, škofija, zavetišče za živali, odvetnik, zdravilišče, dom starejših občanov, lovska družina) – 24.

V šestih izmed zgoraj navedenih primerov so posamezniki vložili pritožbe, ker jim seznanitve z lastnimi osebnimi podatki niso omogočili njihovi delodajalci.

Slika 16: Pritožbe v zvezi s pravico do seznanitve z lastnimi osebnimi podatki glede na skupine upravljavcev osebnih podatkov leta 2013.



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 lastnimi osebnimi podatki. V 24 primerih so upravljavci takoj po pozivu Informacijskega pooblaščenca posameznikom omogočili vpogled in pridobitev zahtevanih podatkov ali pa so jim posredovali pojasnilo, zakaj jim seznanitve ne bodo omogočili. 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 zahtevi posameznika odločil z odločbo. Tako je izdal pet odločb, s katerimi je upravljavcem naložil, da morajo posameznikom omogočiti seznanitev z njihovimi osebnimi podatki, od tega je v treh odločbah zahtevi posameznika ugodil delno. Zaradi potrebe po popolni ugotovitvi dejanskega stanja (ogled razpoložljivega dokumentarnega gradiva) je Informacijski pooblaščenec v prostorih upravljavcev osebnih podatkov opravil tri oglede, na katere so bili vabljeni tudi posamezniki, ki so vložili pritožbe. Informacijski pooblaščenec je z odločbo zavrnil 14 pritožb (od tega pet vlog, prejetih leta 2012), sedem pritožb 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 zaradi nepristojnosti ali ker pritožnik svoje vloge po pozivu ni dopolnil ali ker je bila vloga preuranjena. Informacijski pooblaščenec je petim posameznikom svetoval, kako naj postopajo, pet pritožb je odstopil v reševanje pristojnim organom, trije posamezniki pa so pritožbe umaknili.

Leta 2013 je bila zoper eno odločbo Informacijskega pooblaščenca vložena tožba na Upravno sodišče RS. Navedeno sodišče je odločilo v dveh upravnih sporih, v obeh primerih je tožbo kot neutemeljeno zavrnilo.

4.8. 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[37], 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 RS, ampak se mora zahteva nanašati na konkreten postopek.

Leta 2013 je Informacijski pooblaščenec vložil dve zahtevi za oceno ustavnosti.

4.8.1. Zahteva za presojo ustavnosti 1., 7. in 8. odstavka 20. člena Zakona o davčnem postopku[38] (javna objava osebnih podatkov davčnih neplačnikov)

Informacijski pooblaščenec je vložil zahtevo za oceno ustavnosti 1., 7. in 8. odstavka 20. člena ZDavP-2, ker je v postopku inšpekcijskega nadzora ugotovil, da je z uporabo izpodbijanih zakonskih določb kršena pravica posameznikov do varstva osebnih podatkov, ki jo zagotavlja 38. člen Ustave RS. V postopku inšpekcijskega nadzora je namreč ugotovil, da so na spletnih straneh Davčne uprave RS (DURS) in Carinske uprave RS (CURS) objavljeni osebni podatki posameznikov (osebno ime, datum rojstva in »razred« višine zapadlih neplačanih davčnih obveznosti) in da so ti podatki objavljeni v skladu z zakonom. Zaradi tega Informacijski pooblaščenec kot upravni organ zavezancema (DURS in CURS) ni mogel naložiti umika zakonito objavljenih osebnih podatkov, ne glede na to, da je prepričan o protiustavnosti zakonskih določb, ki vsakemu od zavezancev nalagajo javno objavo.

Izpodbijane določbe ne prestanejo t. i. strogega testa sorazmernosti, po katerem mora biti ukrep, ki omejuje človekove pravice, primeren in nujen, da se dosežejo zasledovani legitimni cilji, škoda, ki bi posameznikom utegnila nastati zaradi ukrepa, pa mora odtehtati

[37] Uradni list RS, št. 64/2007-UPB1, s spremembami.
[38] Uradni list RS, št. 13/2011-UPB4, 32/2012-ZDavP-2E in 94/2012-ZDavP-2F; v nadaljevanju ZDavP-2.

pozitivne učinke tega ukrepa. Javna objava osebnih podatkov davčnih neplačnikov ne more doseči sicer legitimnih ciljev krepitve davčne kulture in izboljšanja plačilne discipline, česar predlagatelj in zakonodajalec že v postopku sprejema izpodbijanega predpisa nista uspela izkazati. Svojo trditev, da je učinek javne objave ravno nasproten od želenega, je Informacijski pooblaščenec dokazoval z odzivi medijev, javnosti in davčnih zavezancev na sprejem izpodbijanih določb, na napoved objave in dejansko objavo davčnih dolžnikov ter z učinki, ki jih je imela javna objava na Hrvaškem.

Ne glede na to, da zakonodajalec in predlagatelj izpodbijanih določb resnih ocen o nujnosti tega ukrepa sploh nista napravila, sta celo sama priznala, da je ukrep uporabljiv zgolj kot komplementaren drugi ukrep, pri čemer drugih ukrepov niti nista predlagala, kaj šele, da bi jih sprejela. Več davčnih strokovnjakov in DURS sama pa so celo prepričani, da je večji del dolga s seznama neplačnikov neizterljivega ali »pogojno« izterljivega ter da so problemi in rešitve za stanje davčnega dolga drugje.

Poseg v pravice posameznikov do varstva osebnih podatkov z javno objavo je v ožjem smislu nesorazmeren tudi zaradi načina objave (seznam se objavi na svetovnem spletu) in zaradi kriterijev, ki definirajo neplačnike (dolg, ki je na 25. dan pred mesecem objave star več kot 90 dni od zapadlosti, če presega 5.000 evrov). Iz zakonodajnega gradiva namreč ni mogoče ugotoviti, zakaj se je predlagatelju prav 90 dni od zapadlosti zdela primerno dolga doba, da dolg postane tako dolgotrajen, da je »vreden« javne objave, še manj pa je jasno, zakaj je prav 5.000 evrov dolga tista meja, ki si »zasluži« javno objavo. Treba se je zavedati, da svetovni splet praktično ne pozna pozabe in da je umik neupravičeno ali nezakonito (ali celo po pomoti) objavljenih osebnih podatkov Sizifovo delo. Posamezniku tako lahko ostanejo dolgotrajne posledice (vedno bo dostopen podatek, da je bil nekoč davčni dolžnik – neplačnik), prav tako je samo vprašanje sredstva in časa, kdaj bodo podatki prečrpani in zelo verjetno uporabljeni tudi za druge namene.

Pri neplačevanju davkov se z vidika interesa javnosti postavlja predvsem vprašanje, kaj je država (oziroma njeni pristojni organi) storila za to, da bi te davke izterjala. Veliko bolj učinkovito, kot javno objaviti, kdo so posamezniki, od katerih davčni organi ne zmorejo (ali nočejo) izterjati davčnega dolga, bi bilo javno objaviti, kaj je davčni organ storil za izterjavo dolga in zakaj pri tem ni bil uspešen. Ker imamo v demokratični državi uveljavljen postopek izvršbe, (domnevno pravilno) dejstvo, da posameznik v 90 dneh od zapadlosti ni plačal (domnevnega) davčnega dolga, pravzaprav sploh ni relevanten podatek – relevanten podatek bi bil razlog za neplačilo, torej razlog za neuspešno izvršbo s strani davčnega organa oziroma pojasnilo, ali je davčni organ izvršbo sploh poskusil opraviti v primernem roku. Takšen legitimen nadzor javnosti nad državo (ali državni organi izpolnjujejo naložene jim dolžnosti oziroma zakaj ne izterjajo davčnih dolgov) pa je mogoče doseči tudi brez javne objave imen, priimkov in rojstnih datumov posameznikov, ki davkov bodisi namerno ne plačajo bodisi jih iz objektivnih razlogov ne morejo plačati – pomemben je predvsem podatek o višini davčnega dolga, kaj je davčni organ storil, da bi bil dolg poplačan, in zakaj do poplačila tudi po poteku 90 dni od zapadlosti še ni prišlo.

Informacijski pooblaščenec meni, da je pobiranje davkov javna naloga oblasti in zato zadostuje, da so z osebnimi podatki posameznikov, ki niso plačali davkov, seznanjeni organi, pristojni za pobiranje davkov, javnost pa naj se seznani s tem, kaj je država storila za to, da bi davke izterjala.

Poleg vsega je ukrep javne objave seznama neplačnikov nesorazmeren tudi zaradi dejstva, da ni predviden postopek izpodbijanja nepravilno ali neupravičeno objavljenih podatkov na seznamu in umik teh podatkov s spleta. Zato so izpodbijane določbe ZDavP-2 neskladne tudi z 22. členom Ustave RS, saj posamezniku pred upravnimi ali sodnimi organi ni zagotovljen pošten (predvsem predvidljiv) dokazni postopek, ki bi v celoti (oziroma sploh) spoštoval načelo kontradiktornosti.

4.8.2. Zahteva za presojo ustavnosti in zakonitosti XIII. poglavja (hramba podatkov), 162.–169. člena Zakona o elektronskih komunikacijah[39]

Informacijski pooblaščenec je v postopku inšpekcijskega nadzora, v katerem je pri enem izmed telekomunikacijskih operaterjev ugotavljal zakonitost izvajanja določb ZEKom-1 o obvezni hrambi podatkov o prometu elektronskih komunikacij, ugotovil, da se v zbirko podatkov, ki se obvezno hranijo, pri zavezancu vsak dan vključi več milijonov novih podatkov. Podatki, ki jih morajo hraniti operaterji po izpodbijanih določbah ZEKom-1, so podatki o prometu in lokaciji ter z njimi povezani podatki, ki določajo naročnika ali uporabnika javne komunikacijske storitve. Ti podatki se shranijo o slehernem telefonskem klicu, vključno z govornimi klici, govorno pošto, konferenčnimi ali podatkovnimi klici, dopolnilnimi storitvami, vključno s preusmeritvijo in predajo klica, pošiljanjem sporočil in multimedijskimi storitvami, vključno s storitvijo kratkih sporočil, nadgrajenimi medijskimi storitvami in multimedijskimi storitvami. Prav tako se ti podatki shranijo o dostopu do interneta, elektronske pošte in uporabi telefonije prek internetnega protokola. Po sporni ureditvi obvezne hrambe podatkov se hranijo tudi podatki o lokaciji uporabnikov javnih komunikacijskih storitev. Država torej zahteva, da ponudniki komunikacijskih storitev shranijo tudi podatek o tem, od kod (s katere lokacije) je posameznik komuniciral, in na ta način nadzirajo tudi njegovo gibanje.

Razlog za regulacijo obvezne hrambe podatkov o prometu in lokaciji uporabnikov javnih komunikacijskih storitev naj bi bila boljša raziskanost (hujših) kaznivih dejanj. Sorazmernost med pričakovanim učinkom in posegi v pravice posameznika bi bila podana, če bi se raziskanost (hujših) kaznivih dejanj po uvedbi obvezne hrambe podatkov resnično (bistveno) povečala. Pomembno višja stopnja raziskanosti (hujših) kaznivih dejanj bi lahko opravičila prevlado javnega interesa, ki je v učinkih generalne in specialne prevencije, nad interesi slehernega posameznika, da uživa zasebnost, se svobodno (nenadzorovano) giblje, komunicira, izraža mnenja ipd. Vendar je na podlagi relativno skopih empiričnih podatkov po štirih oziroma šestih letih obvezne hrambe podatkov mogoče zaključiti, da je Slovenija primer države, kjer obvezna hramba ne pripomore k večji raziskanosti kaznivih dejanj. Podobno so ugotovili še v nekaterih drugih državeh EU.

Informacijski pooblaščenec je opozoril na raziskavo Delovne skupine za hrambo podatkov, ki ugotavlja, da ima splošna hramba podatkov lahko celo negativen učinek na raziskanost kaznivih dejanj. Da bi se izognili hrambi osebnih podatkov, kot jo določa zakon, se posamezniki zatekajo h komunikaciji v internetnih kavarnah, prek brezžičnih internetnih dostopnih točk, anonimnih storitev, javnih telefonov, predplačniških – neregistriranih SIM-kartic, pa tudi (znova) k uporabi neelektronske komunikacije. Takšno vedenje pa ne le, da hrambo podatkov po ZEKom-1 dela nesmiselno, ampak ima širše neželene učinke – otežuje oziroma celo onemogoča uspešno izvajanje tudi klasičnih zakonitih usmerjenih preiskovalnih tehnik (npr. prisluškovanja kot prikritega ukrepa). Tako lahko zavedanje posameznikov o obstoju in obsegu obvezne hrambe podatkov prav zaradi intenzivnosti njegovega posega v vrsto človekovih pravic na koncu pripelje do zmanjšanja možnosti za uspešno preiskavo kaznivih dejanj.

Po prepričanju Informacijskega pooblaščenca ta ukrep ni primeren za doseganje cilja: boljšo raziskanost (hujših) kaznivih dejanj, varnost in obrambo države, tudi zato, ker je relativno preprosto mogoče ponarediti klicno identiteto. Možnost vpliva na podatke, ki se obvezno hranijo, bistveno relativizira njihovo dokazno vrednost. Če navedeno povežemo s pričakovanimi koristmi države od obvezne hrambe podatkov, lahko zaključimo, da država, kot kaže, pričakuje, da bodo (hujša) kazniva dejanja izvrševali nevedni in nespretni storilci, ki bodo naivno mislili, da jih represivni organi ne bodo prepoznali kot naročnike telefonskih številk. Ker je takšno pričakovanje v realnem življenju povsem neutemeljeno, saj so storilci kaznivih dejanj od preprostega varovala, od predplačniških telefonov, prešli na ponarejanje klicne identitete, lahko ugotovimo, da bodo slej ali prej v zbirki podatkov, ki se obvezno hranijo, zgolj in samo nedolžni sleherniki, ki bodo povlečeni v preiskave kaznivih dejanj, ker bo na njihovo udeležbo kazala ponarejena klicna identiteta. Storilcev (hujših) kaznivih dejanj v tej zbirki ne bo mogoče najti. Tako se namreč izkaže, da podatki niso zaupanja vredni sami po sebi, ampak bi jih morali razumeti zgolj kot indic – informacijo, ki je izhodišče za ugotavljanje dejanskega stanja, ne pa dejansko stanje samo.

[39] Uradni list RS, št. 109/2012; v nadaljevanju ZEKom-1.

Informacijski pooblaščenec je opozoril zlasti na nesorazmernost ukrepa obvezne hrambe podatkov. Pomisleki o nesorazmernosti izhajajo iz dejstva, da ukrep zadeva in prizadene slehernega uporabnika elektronskih komunikacijskih sredstev, tudi tiste, ki se v celoti ravnajo po pravu in ne kršijo nobenega prepisa. Informacijski pooblaščenec tako zatrjuje, da je pri izpodbijani zakonski ureditvi podatkov, ki se obvezno hranijo, sicer spoštovano legalitetno načelo, povsem spregledano pa je načelo sorazmernosti. Zakonodajalec je torej urejal obdelavo osebnih podatkov na način, ki ni skladen s pravno državo, saj ni spoštoval lastnih omejitev pri urejanju posegov v človekove pravice. Z absolutističnim pristopom k regulaciji podatkov, ki se hranijo, pa je posegel v več človekovih pravic. Obvezna hramba podatkov o prometu in lokaciji ter z njimi povezanih podatkov, ki določajo naročnika, tako vpliva na posameznikovo dojemanje svobode/represivnosti oblasti, posega v njegovo pravico do svobode gibanja, zasebnosti, tajnosti pisanj, varstva osebnih podatkov in svobodo izražanja.

Na očitno nesorazmernost zakonske ureditve kaže tudi izjemen razkorak med količino shranjenih in dejansko zahtevanih (potrebnih) osebnih podatkov. V postopku inšpekcijskega nadzora je bilo namreč ugotovljeno, da zavezanec letno prejme (le) od 400 do 700 sodnih odredb za posredovanje shranjenih prometnih podatkov, iz česar je mogoče zaključiti, da so velikanske količine osebnih podatkov večine uporabnikov elektronskih komunikacij obdelovane zgolj »za vsak slučaj« ter ne zavezancu ne državi niso resnično potrebni. Podatki o prometu in lokaciji ter z njimi povezani podatki o naročniku ali uporabniku javne komunikacijske storitve se namreč ne obdelujejo zgolj zaradi posameznikovega naročila operaterju, da opravi določeno storitev, in v obsegu, ki je potreben za opravo storitve. Podatki se štirinajst mesecev[40] hranijo predvsem za državo – za njen represivni aparat, za policijo, Slovensko obveščevalno-varnostno agencijo in obveščevalno varnostno službo Ministrstva za obrambo. Shranjujejo se zgolj zaradi peščice primerov, v katerih je izdana sodna odredba in v katerih naj bi ti podatki olajšali iskanje osumljencev storitve kaznivih dejanj ter tistih, ki ogrožajo nacionalno varnost, ustavno ureditev, varnostne, politične in gospodarske interese države ter obrambo države, vendar gre pri tem argumentu pretežno za politično privlačno hipotetično izhodišče (izgovor), pri čemer pa je poseg v človekove pravice velike večine konformnih posameznikov realno dejstvo. Ta poseg se ponavlja s hrambo vsakega novega podatka in je po prepričanju Informacijskega pooblaščenca v očitnem nesorazmerju z doseženimi cilji obvezne hrambe.

Obvezna hramba podatkov po ZEKom-1 je izrecno v nasprotju s 37. členom Ustave RS, ki vsakomur zagotovlja tajnost pisem in drugih občil in po katerem lahko samo zakon predpiše, da se na podlagi odločbe sodišča za določen čas ne upošteva varstvo tajnosti pisem in drugih občil in nedotakljivost človekove zasebnosti, če je to nujno za uvedbo ali potek kazenskega postopka ali za varnost države. S strani države v ZEKom-1 zapovedana obvezna hramba prometnih podatkov glede na Ustavo RS ne izpolnjuje vsaj dveh pogojev za njeno dopustnost: ni nujna v demokratični družbi in ni odrejena z odločbo sodišča. Poleg tega obvezna hramba podatkov izničuje tudi v 38. členu Ustave RS definirano pravico posameznikov do varstva osebnih podatkov, saj t. i. prometni podatki kot sestavni del komunikacije uživajo enako stopnjo varstva kot vsebina sama. O tem se je že večkrat izreklo tudi Evropsko sodišče za človekove pravice in Ustavno sodišče RS.

V zvezi z navedenim Informacijski pooblaščenec pripominja, da so, zatrjujoč kršitve določenih pravic in svoboščin posameznikov, predvsem pa očitno nesorazmernost ukrepa obvezne hrambe podatkov, ustavna sodišča Nemčije, Romunije in Češke ter Višje sodišče Irske ta ukrep že prepoznala kot sporen. Sodišče EU je na podlagi pobude Avstrije in Irske za presojo skladnosti Direktive 2006/24/ES z Evropsko konvencijo o temeljnih pravicah in svoboščinah Direktivo razveljavilo.

Informacijski pooblaščenec je izpostavil tudi, da je zakonodajalec hrambo podatkov v izpodbijanih členih prenesel v nasprotju z nameni Direktive 2006/24/ES. Kot vsaka direktiva je tudi ta namenjena usklajevanju pravnih ureditev držav članic, tokrat na področju obvezne hrambe podatkov, pridobljenih ali obdelanih v zvezi z zagotavljanjem javno dostopnih elektronskih komunikacijskih storitev ali javnih komunikacijskih omrežij. Cilj takšne usklajenosti je zagotavljanje enakih pravic in obveznosti vsem pravnim in fizičnim osebam na območju EU. Direktiva mora biti kot sekundarni pravni vir prenesena neposredno in popolnoma. V primeru prenosa Direktive 2006/24/ES ni bilo tako, zato so izpodbijane določbe

[40] Oziroma osem mesecev, če gre za podatke o dostopu do interneta, e-pošte in uporabi telefonije prek internetnega protokola.

ZEKom-1 po mnenju Informacijskega pooblaščenca tudi v nasprotju s 3.a členom Ustave RS. Direktiva je bila namreč v ZEKom-1 prenesena tako, da je bistveno razširila »uporabnost« (namen) obvezno shranjenih osebnih podatkov uporabnikov javnega komunikacijskega omrežja. Namen Direktive je bil vzpostavitev obveznosti hrambe določenih podatkov, ki jih obdelujejo operaterji, vendar naj bi se posegi države v tako shranjene podatke omejili le na namen preprečevanja, preiskovanja, odkrivanja in pregona hudih kaznivih dejanj, kakor jih opredeljuje nacionalna zakonodaja vsake od držav članic. Nameni hrambe podatkov po ZEKom-1 pa močno odstopajo od zamišljene enotne ureditve v EU, saj se ti podatki hranijo za potrebe kazenskih postopkov brez omejitev na huda kazniva dejanja, za namen obrambe države in za namene zagotavljanja nacionalne varnosti in ustavne ureditve ter varnostnih, političnih in gospodarskih interesov države, kot jih določata zakona, ki urejata obrambo države in Slovensko obveščevalno-varnostno agencijo.

4.8.3. Mnenje Informacijskega pooblaščenca v zvezi z zahtevo za presojo ustavnosti Zakona o policiji[41]

Vrhovno sodišče RS je na Ustavno sodišče RS vložilo zahtevo za oceno ustavnosti prve alineje 1. odstavka 63. člena in 64. člena ZPol, ker je ocenilo, da ti določbi prekomerno posegata v pravico do varstva osebnih podatkov iz 38. člena Ustave RS ter v pravico do spoštovanja zasebnega in družinskega življenja iz 8. člena Evropske konvencije o človekovih pravicah. Osebni podatki posameznikov, ki so bili enkrat vpisani v evidenco DNK, so se namreč hranili trajno. Poleg tega ureditev ni ločevala med obsojenimi posamezniki in med vsemi ostalimi, ki so bili v kazenskem postopku oproščeni oziroma je ovadbo zavrgel že tožilec. Za vse je torej veljal enak režim, za obsojene in za tiste, ki so jim DNK vzeli zaradi krive ovadbe.

Ker se je zahteva Vrhovnega sodišča RS v bistvenih točkah ujemala z razmišljanjem Informacijskega pooblaščenca, slednji ni vložil nove zahteve za oceno ustavnosti določb Zakon o nalogah in pooblastilih policije[42], ampak je glede na novo ureditev Ustavnemu sodišču RS posredoval svoje mnenje z dodatnimi argumenti na strani Vrhovnega sodišča RS (amicus curiae), računajoč na to, da bo Ustavno sodišče ocenilo, da so njegova pojasnila lahko v pomoč pri sprejemanju odločitve o ustavnosti spornih določb o hrambi vzorcev DNK v policijskih evidencah.

V času odločanja o zahtevi je bil namreč sprejet ZNPPol, ki je obdelavo osebnih podatkov v evidencah preiskav DNK uredil nekoliko drugače kot ZPol. Informacijski pooblaščenec je po pregledu nove ureditve (128. in 129. člen ZNPPol) ugotovil, da tudi ta še vedno krši načelo varstva osebnih podatkov v povezavi s prepovedjo pretiranih ukrepov države (načelo sorazmernosti), saj ne razlikuje med obsojenimi in nedolžnimi posamezniki in za obe skupini velja enak rok hrambe. Če je bil posameznik ovaden in mu je bil odvzet bris ustne sluznice ter ugotovljen profil DNK, pozneje pa je tožilec ovadbo zavrgel, to še ne pomeni izbrisa posameznika iz te zbirke. Edini razlog izbrisa iz zbirke DNK je tudi po novi ureditvi potek zelo dolgih rokov, ki velja tako za obsojene kot za oproščene osebe.

Informacijski pooblaščenec je v mnenju izpostavil primer S. in Marper v. Združeno Kraljestvo, v katerem je Evropsko sodišče za človekove pravice (ESČP) sklepno ugotovilo, da iz ureditve, po kateri se lahko prstni odtisi, biološki vzorci in DNK profili oseb, ki so bile osumljene, ne pa tudi obsojene, hranijo neomejeno in nediskriminatorno, ne izhaja pravično ravnotežje med javnim in zasebnim interesom. Takšna ureditev po mnenju ESČP nesorazmerno posega v posameznikovo pravico do zasebnega življenja in kot takšna v demokratični družbi ne more biti nujna.

Informacijski pooblaščenec se je skliceval tudi na dva dokumenta, ki ju je Evropska komisija pripravila leta 2011 v okviru celovite reforme varstva osebnih podatkov v Evropski uniji, in sicer predlog splošne Uredbe o varstvu osebnih podatkov in predlog Direktive o varstvu osebnih podatkov za policijsko področje, ki nakazujeta, kakšna bo prihodnja ureditev varstva osebnih podatkov in kaj velja upoštevati pri pripravi zakonodaje. Slednja nalaga jasno razlikovanje med različnimi kategorijami posameznikov (obsojeni posamezniki; tisti,

41 Uradni list RS, št. 49/1998 s spremembami; v nadaljevanju ZPol.
42 Uradni list RS, št. 15/2013; v nadaljevanju ZNPPol.

za katere obstaja resna podlaga, da so ali da bodo storili kaznivo dejanje; žrtve kaznivih dejanj; priče in ostale osebe).

ZNPPol za razliko od ZPol določa, da se po preteku dveh rokov (hramba in nato blokiranje) podatki iz evidence preiskav DNK brišejo. Odsotnost zapovedi brisanja profilov DNK v ZPol je namreč eden glavnih očitkov Vrhovega sodišča RS pri zahtevi za oceno ustavnosti tega zakona. Vendar pa pregled rokov, ki urejajo celotno hrambo podatkov, če se upoštevajo najdaljši možni roki, pokaže, da lahko presežejo življenjsko dobo posameznika. Po določbah ZNPPol bi se osebni podatki teoretično lahko hranili tudi 100 let, kar pa ne predstavlja bistvene razlike z ZPol, ki določa neomejen rok hrambe.

Informacijski pooblaščenec se strinja z Vrhovnim sodiščem RS, da je pod določenimi pogoji (npr. za osebe, obsojene za težka kazniva dejanja) hramba DNK-profilov dopustna tudi po dosegu namena njihovega zbiranja. Nikakor pa ni jasno, zakaj naj bi se hranil DNK-profil posameznika, zoper katerega je državno tožilstvo (policijsko) ovadbo zavrglo ali je preiskavo ustavil senat na predobravnavnem naroku ali je sodišče obtožbo zavrnilo ali obtoženca obtožbe oprostilo. V demokratični družbi je namreč z vidika domneve nedolžnosti nesprejemljivo, da se posameznike, za katere kazenska odgovornost ni bila ugotovljena, obravnava na enak način kot obsojene osebe.

4.8.4. Odločitev Ustavnega sodišča v zvezi z zahtevo za presojo ustavnosti 29. člena Zakona o preprečevanju omejevanja konkurence[43]

Informacijski pooblaščenec je leta 2012 na Ustavno sodišče RS vložil zahtevo za oceno ustavnosti določb 29. člena ZPOmK-1. Zahteva je izpostavila vprašanje dopustnosti ravnanja nadzornih organov, ki svoje pristojnosti izvršujejo v okviru upravnih – inšpekcijskih in/ali prekrškovnih postopkov, da sicer na podlagi zakonske določbe, vendar brez odredbe sodišča in izven namenov, ki jih določa 37. člen Ustave RS, posežejo v (elektronsko) komunikacijo.

Ustavno sodišče RS je na seji 10. 10. 2013 zahtevo Informacijskega pooblaščenca zaradi odsotnosti procesne predpostavke zavrglo (sklep št. U-I-92/12-13). Informacijski pooblaščenec lahko vloži zahtevo za oceno ustavnosti le, če nastane vprašanje ustavnosti ali zakonitosti v zvezi s postopkom, ki ga vodi. Ključen za ugotovitev obstoja procesne predpostavke je bil odgovor na vprašanje, ali lahko Informacijski pooblaščenec svoj inšpekcijski postopek vodi tako, da vstopa v drug (upravni) postopek in preverja zakonitost obdelave osebnih podatkov s strani pristojnega organa – v konkretnem primeru je šlo za Agencijo za varstvo konkurence, ki je v svojem postopku posegala v elektronske poštne predale posameznikov. Ustavno sodišče je odločilo, da Informacijski pooblaščenec inšpekcijskega nadzora nad izvajanjem ZVOP-1 ne sme izvajati tako, da pri izvrševanju svojih zakonsko določenih pooblastil poseže v posamične pravne postopke, ki jih vodijo za to pristojni državni organi. To bi bilo v nasprotju z načelom samostojnosti, ki ga za upravne organe določa 120. člen, za sodišča pa 125. člen Ustave RS. Takšno ravnanje bi bilo tudi v nasprotju z rednim sistemom pravnih sredstev oziroma vzpostavljeno hierarhično strukturiranostjo državne oblasti (načelo večstopenjskega odločanja) in s tem v nasprotju z načeli pravne države (2. člen Ustave RS). Ta načela zahtevajo, da o pravicah in obveznostih fizičnih in pravnih oseb odločajo pristojni organi v postopkih, ki so določeni v zakonih, prav tako se odločitve organov lahko preverjajo le v vnaprej določenih postopkih s pravnimi sredstvi pred pristojnimi organi. To pomeni, da bi posameznik, katerega osebne podatke bi določeni organ za namen vodenja določenega pravnega postopka obdeloval v nasprotju z zakonom, lahko svoje pravice uveljavljal oziroma varoval pred pristojnimi instančnimi organi na način, določen s predpisi, ki urejajo posamezno področje, in ne prek Informacijskega pooblaščenca.

Ker je po prepričanju Ustavnega sodišča RS Informacijski pooblaščenec posegel v postopek Agencije za varstvo konkurence izven svojih pooblastil, je štelo, da procesna predpostavka za vložitev zahteve za oceno ustavnosti ni izpolnjena.

Informacijski pooblaščenec odločitev Ustavnega sodišča RS glede pristojnosti sprejema, obžaluje pa, da se sodišče ni odločilo za vsebinsko presojo (na omejitve pristojnosti bi lahko

[43] Uradni list RS, št. 36/2008, s spremembami; v nadaljevanju ZPOmK-1.

opozorilo tudi v tem primeru), saj meni, da so v zahtevi izpostavljeni problemi pereči in bi opredelitev najvišjega sodišča do njih potrebovali vsi nadzorni organi.

4.9. Izbrani primeri kršitev varstva osebnih podatkov

V nadaljevanju je predstavljenih sedem zanimivejših odločitev Informacijskega pooblaščenca v inšpekcijskih postopkih, ki jih je vodil leta 2013.

4.9.1. Snemanje telefonskih pogovorov s strani javnega zavoda

Informacijski pooblaščenec je zoper javni zavod uvedel postopek inšpekcijskega nadzora, saj je ugotovil, da zavezanec klicateljem na javno objavljeno telefonsko številko svojega kontaktnega centra, preden jim omogoči pogovor, predvaja avtomatski odzivnik, ki klicatelja seznani s snemanjem pogovora z namenom zagotavljanja kakovosti storitev.

V postopku inšpekcijskega nadzora je bilo ugotovljeno, da je zavezanec snemanje telefonskih klicev uvedel z namenom izboljšanja in zagotavljanja kakovosti storitev. Na podlagi poslušanja zvočnih posnetkov telefonskih razgovorov je namreč pripravljal predloge programa za usposabljanje operaterjev klicnega centra (trening retorike, ravnanje s strankami v težavnih situacijah ipd.). Na podlagi najpogosteje zastavljenih vprašanj v telefonskih pogovorih je pridobil tudi usmeritve o tem, katere informacije je treba dodatno javno objaviti, da bodo v čim večjem obsegu dostopne posameznikom. Zavezanec je v svojem pojasnilu navedel, da izrecne zakonske podlage za snemanje telefonskih razgovorov sicer nima, vendar meni, da lahko razgovore z ustreznim obvestilom klicateljem snema na podlagi določb ZEKom-1.

Informacijski pooblaščenec je v postopku inšpekcijskega nadzora najprej ugotovil, da skladno z definicijo osebnega podatka iz 1. točke 6. člena ZVOP-1 tudi glas oz. govor predstavlja osebni podatek, ki se nanaša na posameznika, ter da z zvočnim snemanjem posameznikovega glasu oz. govora skupaj z drugimi podatki, ki posameznika delajo določljivega, nedvomno nastane zbirka osebnih podatkov. Tako kot za druge osebne podatke velja tudi za zvočne posnetke posameznikovega glasu oz. govora, ki posameznika dela določljivega, da je za njihovo obdelavo treba imeti ustrezno pravno podlago. Zavezanec kot pravna oseba javnega sektorja lahko osebne podatke v konkretnem primeru obdeluje le na podlagi zakona (1. odstavek 9. člena ZVOP-1), izjemoma pa tudi, če je to nujno za izvrševanje zakonitih pristojnosti, nalog ali obveznosti javnega sektorja, če se s to obdelavo ne poseže v upravičen interes posameznika, na katerega se osebni podatki nanašajo (4. odstavek 9. člena ZVOP-1).

Pravno podlago za snemanje telefonskih pogovorov s strani zavezanca iz javnega sektorja bi tako lahko predstavljal področni zakon, ki ureja zaupnost komunikacij (ZEKom-1), ali pa izjema iz 4. odstavka 9. člena ZVOP-1. Na podlagi določbe 5. odstavka 147. člena ZEKom-1 je vsakršna oblika nadzora oziroma prestrezanja komunikacij (npr. poslušanje, snemanje, shranjevanje komunikacij), ki jih izvajajo tretje osebe brez soglasja zadevnih uporabnikov prepovedana, razen v taksativno navedenih primerih. Skladno z določbo 7. odstavka 147. člena ZEKom-1 je dovoljeno snemati v okviru zakonite poslovne prakse zato, da se zagotovi dokaz o tržni transakciji ali kateri koli drugi poslovni komunikaciji, pod pogojem, da so stranke v komunikaciji predhodno obveščene o snemanju, njegovem namenu in trajanju hrambe posnetka. Posneto sporočilo je treba nemudoma izbrisati, najpozneje do poteka dobe, v kateri se posel lahko zakonito izpodbija.

Informacijski pooblaščenec je postopek zaključil z ugotovitvijo, da zavezanec za konkretno snemanje telefonskih pogovorov, kljub predhodnem obvestilu o snemanju, nima pravne podlage. Določba 7. odstavka 147. člena ZEKom-1 namreč snemanje komunikacij dovoljuje le, če gre za namen, »da se zagotovi dokaz o tržni transakciji ali kateri koli drugi poslovni komunikaciji«. Pri tem je treba termin »poslovna komunikacija« razlagati restriktivno. Upoštevati je namreč treba, da 7. odstavek 147. člena ZEKom-1 določa zgolj izjemo od

splošne prepovedi snemanja iz 5. odstavka istega člena, kar pomeni, da je snemanje na tej podlagi dopustno le v izjemnih, posebej utemeljenih primerih. Poleg tega iz roka hrambe posnetega sporočila, ki je v 7. odstavku 147. člena ZEKom-1 določen kot »najpozneje do izteka dobe, v kateri se posel lahko zakonito izpodbija«, jasno razvidno, da se lahko snemajo le tiste »poslovne komunikacije«, ki pripeljejo do sklenitve, spremembe oziroma prenehanja določenega poslovnega razmerja. Zaradi navedenega bi lahko pod pogojem, da so kličoči predhodno obveščeni o snemanju, njegovem namenu in trajanju hrambe posnetka, zavezanec snemal le tiste telefonske pogovore, ki jih potrebuje z namenom zagotovitve tržne transakcije, ali katere koli druge pogovore, ki lahko pripeljejo do sklenitve/spremembe/prenehanja določenega poslovnega razmerja. Namena »zagotavljanje kakovosti storitev« po mnenju Informacijskega pooblaščenca ni moč šteti med zakonite namene, zaradi katerih ZEKom-1 v izjemnih primerih dovoljuje snemanje pogovorov.

Zavezanec tudi ni izkazal, da telefonske pogovore snema na podlagi določbe 4. odstavka 9. člena ZVOP-1, ki predstavlja izjemo od splošne zahteve po zakonski podlagi za obdelavo osebnih podatkov v javnem sektorju.

Zato je Informacijski pooblaščenec zavezancu odredil prenehanje izvajanja snemanja telefonskih pogovorov na klicni številki klicnega centra in uničenje hranjenih posnetkov, poleg tega pa tudi prenehanje predvajanja obvestila »Zaradi zagotavljanja kakovosti storitev se vaš klic snema.« na avtomatskem odzivniku klicne številke klicnega centra.

4.9.2. Pomanjkljivo zavarovanje občutljivih osebnih podatkov s strani zdravstvene ustanove

Informacijski pooblaščenec je pri zdravstveni ustanovi opravil inšpekcijski ogled, katerega namen je bil preveriti ustreznost postopkov in ukrepov za zavarovanje osebnih podatkov ter preveriti, kako zavezanec spoštuje odločbo, ki mu jo je Informacijski pooblaščenec izdal leta 2007 v zvezi z zagotavljanjem zavarovanja osebnih podatkov pri njihovi obdelavi.

V okviru inšpekcijskega ogleda je bilo ugotovljeno, da zavezanec uporablja programsko opremo, ki omogoča sledljivost obdelave osebnih podatkov, in sicer kdo in kdaj do osebnih podatkov dostopa in kakšen je bil namen spremembe oziroma dostopa do le-teh. Do samega ogleda zavezanec notranjih nadzorov zakonitosti dostopov do podatkov ni izvajal. Informacijski pooblaščenec je pri ogledu pridobil interne akte, ki urejajo zavarovanje osebnih podatkov, glede katerih pa je bilo ugotovljeno, da ne predpisujejo postopka pridobitve ali uporabe revizijskih sledi dostopov do osebnih podatkov. Ugotovljeno je bilo tudi, da uporabniška gesla ne potečejo ter da imajo vsi zdravniki in medicinske sestre enake pravice dostopa. Vsak zdravnik lahko vidi podatke o vseh pacientih, ki so se ali se še zdravijo pri zavezancu. Zavezanec je glede tega zastopal stališče, da je bistveno, da so lečečemu zdravniku takoj na voljo vsi podatki o pacientu, ki jih potrebuje za svoje strokovno delo.

24. člen ZVOP-1, ki ureja zavarovanje osebnih podatkov, med drugim določa tudi, da morajo biti postopki in ukrepi za zavarovanje osebnih podatkov ustrezni glede na tveganje, ki ga predstavlja obdelava in narava osebnih podatkov, ki se obdelujejo. Varnostne mehanizme in ukrepe je namreč treba prilagoditi glede na tveganje, ki ga obdelava podatkov prinaša. Najprej je zato treba ustrezno oceniti tveganja. Informacijski pooblaščenec je ugotovil, da zavezanec v svojih zbirkah osebnih podatkov obdeluje veliko količino osebnih podatkov, velik delež teh podatkov pa glede na področje delovanja zavezanca predstavljajo občutljivi osebni podatki, katerih zloraba bi lahko imela za posameznika težke, dolgotrajne in v določenih primerih tudi nepovratne posledice. Glede na občutljivost podatkov, ki jih zavezanec obdeluje, bi morala vsaka analiza tveganj pokazati, da gre za podatke z visoko oziroma celo najvišjo ravnjo tveganja, zaradi česar morajo biti ukrepi in postopki za zavarovanje teh osebnih podatkov na najvišji ravni, da se z njimi minimizirajo, če že ne izničijo tveganja, ki jim pretijo.

Notranji nadzor, katerega namen je zaznava nezakonite obdelave osebnih podatkov in sprejem postopkov in ukrepov za preprečitev takšnih obdelav, predstavlja ukrep, ki je namenjen varovanju posebej občutljivih osebnih podatkov. Izvajati bi ga morali upravljavci osebnih podatkov, ki obdelujejo večje količine osebnih podatkov, ki obdelujejo občutljive osebne podatke in vsi drugi upravljavci osebnih podatkov, pri katerih analiza tveganja

pokaže, da je tovrsten ukrep nujen in ustrezen glede na visoka tveganja. Brez tovrstnega nadzora je pri večjih upravljavcih in velikih količinah podatkov nezakonite dostope do osebnih podatkov praktično nemogoče zaznati. Ker gre pri izvajanju notranjega nadzora nad zakonitostjo obdelave osebnih podatkov za ukrep, ki lahko povzroči tudi prekomerno obdelavo osebnih podatkov, nesorazmerne zahteve do zaposlenih in druge posledice, je primerno, da se ga kot ukrep natančno opredeli in da se v ustreznem internem aktu opredeli obseg, pogostost, izvajalce, cilje, način izvajanja, poročanje, ukrepanje in druge elemente, s katerimi se protokolira izvajanje notranjega nadzora ter se zagotovi njegovo sorazmernost in učinkovitost.

Informacijski pooblaščenec je zato zavezancu odredil, da v internem aktu protokolira izvajanje notranjega nadzora, in sicer tako, da opredeli obseg, pogostost, izvajalce, cilje, način izvajanja, poročanje in ukrepanje v primeru zaznanih nezakonitih obdelav osebnih podatkov.

Informacijski pooblaščenec je v okviru inšpekcijskega ogleda ugotovil tudi, da zavezanec za namen dostopa do informacijskega sistema, ki sicer omogoča sledljivost obdelave osebnih podatkov, uporablja sistem uporabniških imen in gesel, ki ne potečejo, poleg tega pa ne obstajajo nobene zahteve glede kompleksnosti izbranega gesla, kar odstopa od ustaljenih dobrih praks na področju informacijske varnosti. Glede na naravo osebnih podatkov, ki jih zavezanec obdeluje v informacijskem sistemu, so takšne prakse, upoštevaje tveganja, nedopustne. Zaradi tega je Informacijski pooblaščenec zavezancu odredil tudi, da mora v internem aktu določiti in začeti izvajati politiko upravljanja gesel za ta informacijski sistem.

4.9.3. Policijska pooblastila pri dostopih do podatkov uporabnikov spleta

Informacijski pooblaščenec je prejel prijavo, ki se je nanašala na uporabo pooblastil policije v zvezi s pridobivanjem podatkov o uporabnikih spletnih strani z vsebino, ki jo posredujejo prejemniki storitve (gre za spletne strani, kot so spletni forumi, spletne strani medijev ipd.). Ker je iz prijave izhajal sum, da so bili osebni podatki uporabnikov spletnih forumov v neznanem številu primerov pridobljeni brez ustrezne pravne podlage, je Informacijski pooblaščenec od policije zahteval pojasnila v zvezi s tem, kolikokrat in od katerih upravljavcev spletnih forumov so leta 2012 zahtevali osebne podatke o uporabnikih in na kateri pravni podlagi, poleg tega pa tudi pojasnilo, zakaj za pridobitev osebnih podatkov s strani upravljavcev spletnih forumov kot ponudnikov storitev informacijske družbe (in ne s strani operaterjev elektronskega komunikacijskega omrežja) uporabljajo določbe Zakona o kazenskem postopku[44] in ne določb Zakona o elektronskem poslovanju na trgu[45].

Informacijski pooblaščenec je na podlagi analize s strani policije prejetih podatkov ugotovil naslednje:

- Leta 2012 je policija od ponudnikov storitev informacijske družbe 35-krat zahtevala podatke o uporabnikih spletnih forumov.
- Policija bi morala kot vsak drug uporabnik osebnih podatkov v zahtevku za posredovanje podatkov navesti toliko podatkov, da se lahko upravljavec prepriča o obstoju pravnega temelja in potrebnosti zahtevanih informacij, torej bi morala navesti vsaj pravno kvalifikacijo obravnavanega kaznivega dejanja, ki se preganja po uradni dolžnosti, česar pa policija v kar 30 % pisnih zahtevkov ni navedla.
- Najpogosteje je bila kot pravna podlaga za zahtevanje osebnih podatkov naveden 148. člen ZKP, 55. člen ZPol oziroma 3. odstavek 149.b člena ZKP.
- Policija se v prvi zahtevi do ponudnika storitev niti v enem zahtevku ni sklicevala na določbe 8. člena ZEPT, ki določa: Ponudniki storitev morajo vsem pristojnim organom na njihovo zahtevo najkasneje v roku treh dni od njenega prejema sporočiti podatke, na podlagi katerih je mogoče identificirati prejemnike njihove storitve (ime in priimek, naslov, firma, elektronski naslov). Navedene podatke morajo ponudniki storitev sporočiti zaradi odkrivanja in preprečevanja kaznivih dejanj na podlagi odredbe sodišča, brez odredbe sodišča pa, če tako določa področni zakon.
- V štirih primerih je bila glede na pridobljene podatke ponudnikom storitev informacijske družbe na predlog policije izdana odredba sodišča.

[44] Uradni list RS, št. 32/2012-UPB8 in 47/2013; v nadaljevanju ZKP.
[45] Uradni list RS, št. 96/2009; v nadaljevanju ZEPT.

- Ponudniki storitev informacijske družbe so v 23 primerih (66 %) podatke o uporabnikih posredovali brez sodne odredbe na pisno zahtevo policije, v dveh primerih (6 %) po odredbi sodišča, v sedmih primerih podatkov niso dostavili (oziroma iz pridobljene dokumentacije ni razvidno, da bi bili podatki dostavljeni).
- Policija je v večini primerov zahtevala podatke o uporabniku IP naslova, torej prometne podatke.
- Iz ugotovitev izhaja tudi, da je v enem primeru policija od ponudnika storitve informacijske družbe zahtevala umik fotografije; v enem primeru je policija zahtevala podatke o vseh uporabnikih določene domene za obdobje skoraj treh mesecev, v enem primeru pa je policija zahtevala vsebino SMS-sporočil, telefonske številke prejemnikov, število poslanih SMS-sporočil in druge podatke.
- Odgovora na vprašanje, zakaj za pridobitev osebnih podatkov s strani upravljavcev spletnih forumov kot ponudnikov storitev informacijske družbe uporabljajo določbe ZKP in ne določb ZEPT, Informacijski pooblaščenec ni prejel.

Na podlagi izvedene analize je Informacijski pooblaščenec ugotovil, da policija očitno ne pozna določbe ZEPT ali jo ignorira, saj se leta 2012 niti v eni zahtevi ni sklicevala na omenjene določbe ZEPT, temveč se je sklicevala na neustrezne določbe ZKP, ZPol ali celo ZVOP-1, v nekaterih primerih pa celo ni navedla nobene pravne podlage. Očitno je tudi, da gre za nepoznavanje razlike med operaterji (ponudniki javno dostopnih komunikacijskih omrežij in storitev), katerih delovanje primarno ureja ZEKom, in upravljavci spletnih strani (ponudniki storitev informacijske družbe), katerih delovanje primarno ureja ZEPT. Določb ZEPT očitno ne poznajo niti ponudniki storitev informacijske družbe, saj v veliki večini primerov podatke dostavijo policiji tudi brez odredbe sodišča. Ob vsem navedenem ne gre samo za vprašanje zakonitosti obdelave osebnih podatkov (tako posredovanja kot nadaljnje uporabe osebnih podatkov), ki jo nadzira Informacijski pooblaščenec, temveč se zastavlja tudi vprašanje uporabljivosti tako zbranih dokazov v matičnem – kazenskem postopku. Če so namreč dokazi pridobljeni s kršitvijo ustavno varovanih človekovih pravic oziroma s kršitvijo določb ZKP, sodišče sodne odločbe na take dokaze ne bo moglo opreti.

Informacijski pooblaščenec je z ugotovitvami inšpekcijskega nadzora seznanil Ministrstvo za notranje zadeve in Vrhovno državno tožilstvo RS in jima predlagal izdelavo odzivnega poročila s seznamom ukrepov za odpravo ugotovljenih nepravilnosti. Do konca leta 2013 je Informacijski pooblaščenec prejel vmesno poročilo ministrstva. Zadeva se naprej rešuje v letu 2014.

4.9.4. Izguba podpisov volivcev za razpis zakonodajnega referenduma

Po medijskem poročanju o izginulih listih seznama podpisnikov pobude Sindikata kemične, nekovinske in gumarske industrije (Sindikat KNG) volivcem za vložitev zahteve za razpis zakonodajnega referenduma o Zakonu o ukrepih Republike Slovenije za krepitev stabilnosti bank[46] je Informacijski pooblaščenec pri Državnem zboru RS (DZ) in Ministrstvu za notranje zadeve (MNZ) po uradni dolžnosti uvedel postopek inšpekcijskega nadzora nad izvajanjem določb ZVOP-1.

V postopku inšpekcijskega nadzora je bilo ugotovljeno, da ob prejemu seznama z osebnimi podatki pobudnikov referenduma o ZUKSB, ki so ga v DZ osebno predali predstavniki Sindikata KNG, število podpisnikov ni bilo znano, niti ni tega števila ob prevzemu seznama ustrezno preveril oziroma dokumentiral DZ. Število listov seznama pobudnikov ni bilo preverjeno oziroma dokumentirano niti ob njegovem fotokopiranju niti ob predaji seznama MNZ v preverjanje verodostojnosti podpisnikov. Prav tako ni ustreznega dokumentiranja in preverjanja dejanskega obsega seznama z osebnimi podatki ob prejemu fotokopij s strani DZ zagotovilo ministrstvo. Ko je bil seznam s strani zaposlenega na MNZ razdeljen med 28 uslužbencev v preverjanje, sama razdelitev seznama med posamezne zaposlene ni bila ustrezno evidentirana, prav tako s strani odgovorne osebe na MNZ ni bilo evidentirano število znova zbranih listov seznama. Takšna naj bila po navedbah obeh zavezancev njuna dolgoletna praksa ob prejemu referendumskih pobud. Šele po intervenciji pobudnika glede nezadostnega števila preverjenih podpisnikov je bilo v internem preverjanju v DZ prešteto in ugotovljeno, da je bilo v originalnem prejetem seznamu podpisnikov 307 listov; z MNZ

[46] Uradni list RS, št. 105/2012, 63/2013 - ZS-K in 23/2014 - ZDIJZ-C; v nadaljevanju ZUKSB.

je bilo vrnjenih 271 fotokopiranih pregledanih listov in tako je bil ugotovljen manko 36 fotokopiranih listov z osebnimi podatki 361 podpisnikov pobude.

Zaradi odsotnosti ustreznega evidentiranja števila listov seznama podpisnikov tako v DZ (ob neposrednem prevzemu, ob fotokopiranju, ob ponovnem prevzemu s strani MNZ) kot tudi na MNZ (ob prevzemu s strani DZ, ob razdelitvi v preverjanje uslužbencem ministrstva), Informacijski pooblaščenec naknadno ni mogel ugotoviti, kateri listi seznama z osebnimi podatki so bili obdelani na določeni točki, ugotovljeno pa je bilo, da sta oba zavezanca ravnala v nasprotju z zahtevami ZVOP-1 glede varovanja osebnih podatkov, saj z opustitvijo potrebnega preverjanja in evidentiranja obsega in vsebine seznama podpisnikov pobude volivcev za razpis zakonodajnega referenduma, ki predstavlja zbirko zaupnih osebnih podatkov, nista zagotovila postopkov in ukrepov za zavarovanje osebnih podatkov, predpisanih v 24. členu ZVOP-1, s katerimi se varujejo osebni podatki in s katerimi se prepreči slučajno ali namerno nepooblaščeno uničevanje, sprememba ali izguba osebnih podatkov (t. i. notranja sledljivost). Kot upravljavca osebnih podatkov sta bila namreč oba zavezanca dolžna zagotoviti ustrezno zavarovanje in integriteto celotnega seznama podpisnikov, in sicer v celotnem postopku njegove obdelave.

Poleg tega je bilo s strani obeh zavezancev ugotovljeno ravnanje v nasprotju s 3. odstavkom 22. člena ZVOP-1, saj zavezanca nista zagotovila t. i. zunanje sledljivosti. DZ ob posredovanju seznama v preverjanje MNZ, to pa ob posredovanju preverjenega seznama nazaj v DZ nista zagotovila, da bi bilo mogoče pozneje ugotoviti, kateri osebni podatki podpisnikov pobude so sploh bili oziroma niso bili posredovani drugemu zavezancu.

Zaradi ugotovljenih nepravilnosti je Informacijski pooblaščenec odgovornima osebama DZ in MNZ izrekel ukrep v skladu z ZP-1.

4.9.5. Predčasno uničenje zdravstvene dokumentacije

Informacijski pooblaščenec je na podlagi prijave uvedel postopek inšpekcijskega nadzora zoper zdravilišče, ker naj bi nezakonito, to je že po treh letih od končanega zdravljenja, uničilo zdravstveno dokumentacijo določenega posameznika.

V postopku inšpekcijskega nadzora je bilo ugotovljeno, da ima zavezanec v internih aktih določene različne roke hrambe osebnih podatkov uporabnikov zdravstvenih storitev (15 ali 5 let) in da dokumentacijo praviloma izloča in uničuje enkrat na leto. Kljub navedenim rokom hrambe pa je zavezanec zaradi prostorske stiske in omejenih tehničnih možnosti za hrambo zelo velikih količin zdravstvene dokumentacije v papirni obliki dokumentacijo hranil le tri leta po zaključenem zdraviliškem zdravljenju. Zavezanec je enkrat na leto pregledal zdravstvene kartone in jih pripravil za uničenje. Dokumentacijo, ki je bila namenjena uničenju, je le stehtal, poimenskega seznama bolnikov, katerih zdravstvene kartone je uničil, ni izdeloval zaradi zelo velikega števila primerov (cca. 2500–3000). V postopku je bilo ugotovljeno tudi, da zavezanec v elektronski obliki daljši čas hrani podatke, ki jih posreduje Zavodu za zdravstveno zavarovanje Slovenije zaradi plačila opravljenih storitev in odpustna pisma.

V skladu s 3. točko 6. člena ZVOP-1 predstavlja tudi hramba osebnih podatkov vrsto obdelave osebnih podatkov, za katero je treba imeti ustrezno pravno podlago. Pravila v zvezi z roki hrambe osebnih podatkov so določena v 21. členu ZVOP-1, ki v 1. odstavku določa, da se osebni podatki lahko shranjujejo le toliko časa, dokler je to potrebno za dosego namena, zaradi katerega so se zbirali ali nadalje obdelovali. Po izpolnitvi namena obdelave se osebni podatki zbrišejo, uničijo, blokirajo ali anonimizirajo, če niso na podlagi zakona, ki ureja arhivsko gradivo in arhive, opredeljeni kot arhivsko gradivo oziroma če zakon za posamezne vrste osebnih podatkov ne določa drugače.

Iz 13. člena Zakona o zdravstveni dejavnosti[47] izhaja, da zdravilišča opravljajo specialistično ambulantno dejavnost, ki predstavlja nadaljevanje oziroma dopolnitev osnovne zdravstvene dejavnosti, in obsega poglobljeno diagnostiko, zdravljenje bolezni ali bolezenskih stanj ter izvajanje ambulantne rehabilitacije. 19. člen ZZDej določa še, da zdraviliška zdravstvena dejavnost obsega preventivno varstvo ter specialistično ambulantno in bolnišnično

[47] Uradni list RS, št. 23/2005-UPB, s spremembami.

rehabilitacijo s souporabo naravnih zdravilnih sredstev. To dejavnost izvajajo naravna zdravilišča, če izpolnjujejo pogoje, ki jih določi minister, pristojen za zdravje. Ker se glede na navedeno zdravilišča štejejo kot izvajalci zdravstvene dejavnosti, morajo pri hrambi osebnih podatkov upoštevati določbe specialnega zakona, to je Zakon o zbirkah podatkov s področja zdravstvenega varstva. Ta v prilogi pod zbirko št. IVZ 1 določa, da se zdravstveni karton in popis bolezni hranita 10 let po smrti bolnika, ostala osnovna medicinska dokumentacija pa se hrani 15 let.

Zaradi nejasnosti v zvezi z roki hrambe dokumentacije, ki nastane med obravnavo v zdravilišču, je Informacijski pooblaščenec pred sprejemom odločitve Ministrstvo za zdravje zaprosil za pisno pojasnilo, ali se z vidika vrste izvajalca zdravstvenih storitev medicinska dokumentacija, ki jo obdelujejo naravna zdravilišča, šteje k zdravstvenemu kartonu in popisu bolezni ali k ostali osnovni medicinski dokumentaciji. Od opredelitve vrste medicinske dokumentacije je namreč odvisen rok njene hrambe. Ministrstvo za zdravje je po posvetovanju z Inštitutom za varovanje zdravja RS zavzelo stališče, da je treba medicinsko dokumentacijo, ki nastaja v zdraviliščih, šteti k zdravstvenim kartonom in popisom bolezni, ki se hrani 10 let po smrti bolnika.

Informacijski pooblaščenec je sledil mnenju resornega ministrstva in je zavezancu izdal odločbo, s katero mu je odredil, da mora zagotoviti, da se bodo osebni podatki uporabnikov zdravstvenih storitev hranili in uničevali v skladu z določbami ZZPPZ, to je 10 let po smrti uporabnika, ter da mora zagotoviti sledljivost uničenja osebnih podatkov uporabnikov zdravstvenih storitev na način, da bo za vsako uničenje razvidno, kdaj je bilo izvedeno in podatki katerih oseb so bili uničeni (ime in priimek pacienta, številka zdravstvenega kartona).

Informacijski pooblaščenec je zaključil, da pomanjkanje prostora oziroma velika količina dokumentov v fizični obliki ne sme biti razlog za kršenje zakona in predčasno uničenje oziroma nezakonito obdelavo osebnih podatkov. Osebni podatki se namreč lahko hranijo tudi v elektronski obliki, saj ZZPPZ ne predpisuje, v kakšni obliki morajo izvajalci zdravstvenih storitev hraniti dokumentacijo z osebnimi podatki. Hramba zdravstvene dokumentacije v elektronski obliki odpravi težave s pomanjkanjem prostora, poleg tega pa tak način hrambe omogoča lažje iskanje podatkov oziroma preverjanje, katere osebne podatke je treba uničiti. Tudi uničenje osebnih podatkov v elektronski obliki je lažje kot uničenje dokumentov v fizični obliki. Uničenje osebnih podatkov pred potekom roka, ki je določen v področnih predpisih, je kršitev področnega predpisa, poleg tega lahko pomeni tudi odškodninsko odgovornost upravljavca osebnih podatkov za vso škodo, ki izvira iz prehitrega uničenja.

Informacijski pooblaščenec je presodil tudi, da gre v primeru uničenja zdravstvene dokumentacije za obdelavo občutljivih osebnih podatkov, ki že zaradi svoje narave zahtevajo dosledno izvajanje predpisanih postopkov in ukrepov za njihovo zavarovanje. Zavarovanje osebnih podatkov v skladu s 24. členom ZVOP-1 obsega organizacijske, tehnične in logično-tehnične postopke in ukrepe, s katerimi se varujejo osebni podatki, preprečuje slučajno ali namerno nepooblaščeno uničevanje podatkov, njihova sprememba ali izguba ter nepooblaščena obdelava teh podatkov tako, da se med drugim (peta točka 1. odstavka) omogoča poznejše ugotavljanje, kdaj so bili posamezni osebni podatki vneseni v zbirko osebnih podatkov, kdaj so bili uporabljeni ali drugače obdelani in kdo je to storil, in sicer za obdobje, ko je mogoče zakonsko varstvo pravice posameznika zaradi nedopustnega posredovanja ali obdelave osebnih podatkov (notranja sledljivost). Zato tehtanje dokumentacije, ki je namenjena uničenju, nikakor ne zadošča; zavezanec mora zagotoviti, da je iz dokumentov, ki nastanejo ob uničenju, razvidno, kdaj je bila dokumentacija uničena in na katere uporabnike zdravstvenih storitev se je nanašala (ime in priimek uporabnika, številka zdravstvene kartoteke ali številka obravnave).

4.9.6. Objava osebnih podatkov strank servisa na »zaslonu dobrodošlice«

V postopku inšpekcijskega nadzora, ki ga je Informacijski pooblaščenec začel na podlagi prijave, je bilo ugotovljeno, da zavezanec na servisu uporablja elektronsko knjigo naročanja in da se na »zaslonu dobrodošlice« izpišejo naslednji osebni podatki naročenih strank: ime in priimek stranke, čas sprejema stranke, znamka vozila stranke, registrska številka vozila stranke ter ime in priimek servisnega svetovalca. Objava na zaslonu je časovno omejena in

odvisna od števila servisov določenega dne, v povprečju je to ena ura na dan. Ko je vozilo stranke na vrsti, se njeni podatki z zaslona samodejno izbrišejo. Če stranka ni kupec vozila v mreži prodajalcev in ni podpisala pogodbe s splošnimi pogoji, je računalniški program ne zazna in se njeno ime na zaslonu ne izpiše.

Omenjeni zasloni so po navedbah zavezanca namenjeni strankam, da se seznanijo s podatkom, kdaj bodo na servis sprejete ter na katerega servisnega svetovalca se morajo obrniti. Število zadovoljnih strank se je z uvedbo zaslona povečalo, zato uporaba »zaslona dobrodošlice« po mnenju zavezanca predstavlja nujni organizacijski ukrep, ki strankam prihrani čas in denar, serviserjem pa omogoča boljšo pripravo na delo in s tem izboljša storitve servisa. Poleg tega je uporaba zaslona na način, ki ga uporablja zavezanec, sprejeta tudi v ostalih državah EU s primerljivo zakonodajo na področju varstva osebnih podatkov. Omenjeni zaslon servisi v mreži v ostalih članicah EU uporabljajo od leta 2004, v Sloveniji pa od leta 2009.

Informacijski pooblaščenec je poudaril, da je treba uporabo določene tehnologije, ki vključuje obdelavo osebnih podatkov, obravnavati tudi z vidika namena njene uporabe. Če je namen upravljavca obdelovati osebne podatke posameznika (ime in priimek stranke ter registrsko številko vozila), potem gre po naravi stvari za obdelavo osebnih podatkov, za katero mora obdelovalec imeti ustrezno pravno podlago. Splošne pravne podlage za obdelavo osebnih podatkov določa 8. člen ZVOP-1, pravne podlage za obdelavo osebnih podatkov, kamor se šteje zavezanec, pa določa 10. člen ZVOP-1.

Objava osebnih podatkov na »zaslonu dobrodošlice« pomeni sporočanje, širjenje in dajanje osebnih podatkov na razpolago vsakomur, ki je v času objave podatkov v prostorih servisa. Takšna obdelava osebnih podatkov pa zagotovo ni potrebna in primerna zaradi izpolnjevanja pogodbenih ali kakih drugih obveznosti zavezanca in tudi ni nujna zaradi uresničevanja zakonitih interesov zasebnega sektorja, iz česar izhaja, da zavezanec za obdelavo (objavo) osebnih podatkov na omenjenem zaslonu nima pravne podlage v 2. in 3. odstavku 10. člena ZVOP-1. Prav tako za takšno obdelavo nima podlage v zakonu ali v osebni privolitvi posameznika. Po pregledu splošnih pogojev za nakup novega vozila in splošnih pogojev za popravilo vozila je bilo namreč ugotovljeno, da stranka ni seznanjena s tem, da se bodo njeni osebni podatki obdelovali za namene objave na »zaslonu dobrodošlice«, kar pomeni, da zavezanec z objavo osebnih podatkov strank na zaslonu ravna v nasprotju z določbami 8. in 10. člena ZVOP-1.

Zaradi navedenega je Informacijski pooblaščenec zavezancu odredil, da v vseh svojih servisih na »zaslonu dobrodošlice« neha objavljati osebne podatke svojih strank – pogodbenikov (ime in priimek stranke z registrsko številko vozila stranke) ali namesto tega pridobi izrecno osebno privolitev posamezne stranke za objavo njenih osebnih podatkov na »zaslonu dobrodošlice«.

4.9.7. Zahteva posameznika po prenehanju obdelave osebnih podatkov za namen opravljanja dimnikarskih storitev

Leta 2013 je bil zaključen postopek, uveden leta 2011 po prejemu pritožbe posameznika, ki je pri podjetju, ki opravlja dimnikarske storitve, vložil ugovor po 3. odstavku 32. člena ZVOP-1, ker mu je zavezanec poslal več dopisov, s katerimi je najavil storitev čiščenja kurilne naprave na trda in tekoča goriva na določenem naslovu. Posameznik je trdil, da opravljanja storitev dimnikarske službe zavezancu ni naročil, prav tako z njim nikoli ni imel nobenega stika ter mu ni posredoval podatka o lastništvu nepremičnine in svojem stalnem prebivališču. Zato je od zavezanca zahteval, da dokaže, da je pooblaščeni koncesionar za izvajanje storitev dimnikarske službe na naslovu, kjer ima nepremičnine, ter da z izpisom iz evidence kurilnih naprav dokaže, da se tam nahaja kurilna naprava. Posameznik je menil, da zavezanec kot izvajalec dimnikarske službe ni upravičen ali dolžan pregledovati stavb z namenom iskanja kurilnih naprav ter da lastništvo nepremičnine ni zadostna podlaga za nastanek upravičenj zavezanca iz naslova dimnikarske službe, saj bi moral izkazati obstoj malih kurilnih naprav na omenjenem naslovu, česar pa ni storil. Navedeno pomeni, da se osebni podatki posameznika ne uporabljajo zaradi uresničevanja zakonitega javnega interesa, temveč izključno zaradi interesa zavezanca, ki poskuša s splošnim preiskovanjem lastnikov nepremičnin povečati obseg svojega poslovanja. Posameznik je zato zahteval

prenehanje obdelave svojih osebnih podatkov.

Informacijski pooblaščenec je v okviru svojega postopka ugotovil, da je Vlada RS z odločbo št. 35404-31/2007/4 z dne 8. 11. 2007 (v nadaljevanju: Odločba) za koncesionarja za izvajanje obvezne državne gospodarske javne službe izvajanja meritev, pregledovanja in čiščenja kurilnih naprav, dimnih vodov ali zračnikov zaradi varstva okolja in učinkovite rabe energije, varstva človekovega zdravja in varstva pred požarom na dimnikarskem območju Mestne občine Kranj izbrala zavezanca za dobo osmih let. Odločbo je Upravno sodišče RS s sodbo št. U 2354/2007-13 z dne 5. 11. 2008 (v nadaljevanju: Sodba) odpravilo in zadevo vrnilo Vladi RS v ponoven postopek, ki pa v času uvedbe postopka nove odločbe še ni izdala. Zato je posameznik trdil, da zavezanec nima koncesije za opravljanje dimnikarske službe na območju, kjer se nahajata njegovi nepremičnini.

Izhajajoč iz navedb v prijavi je Informacijski pooblaščenec v postopku presojal, ali zavezanec osebne podatke posameznika (ime, priimek in naslov) obdeluje na podlagi 3. odstavka 10. člena ZVOP-1, in sicer ker bi bilo to nujno zaradi uresničevanja zakonitih interesov zasebnega sektorja (zavezanca) in bi ti interesi očitno prevladali nad interesi posameznika, na katerega se nanašajo osebni podatki. Posameznik, katerega osebni podatki se obdelujejo v skladu s 4. odstavkom 9. člena ali 3. odstavkom 10. člena ZVOP-1, ima pravico kadar koli z ugovorom zahtevati prenehanje njihove obdelave. Upravljavec ugovoru ugodi, če posameznik dokaže, da niso izpolnjeni pogoji za obdelavo po navedenih členih. V tem primeru se njegovih osebnih podatkov ne sme več obdelovati (3. odstavek 32. člena ZVOP-1). Če upravljavec ugovoru ne ugodi, lahko posameznik zahteva, da o obdelavi odloči Informacijski pooblaščenec.

Za Informacijskega pooblaščenca je bilo pri odločitvi ključno vprašanje, ali zavezanec obdeluje osebne podatke posameznika zakonito. Zato je Ministrstvo za okolje in prostor zaprosil za pojasnila, ali ima zavezanec kot nosilec koncesije pravni temelj za opravljanje obvezne gospodarske javne službe in ga je iz tega razloga mogoče šteti za upravljavca – torej subjekt, ki zakonito pridobiva in nadalje obdeluje osebne podatke posameznikov, ki vstopajo z njim v pogodbena razmerja po kontrahirni dolžnosti (obvezna javna gospodarska služba), in če da, kateri temelj je to. Ministrstvo je pojasnilo, da je Odločba res odpravljena, vendar je še vedno v veljavi koncesijska pogodba, ker glede na veljavno zakonodajo niso obstajale okoliščine za njeno razvezo. To pomeni, da zavezanec kljub Sodbi veljavno izvaja dimnikarsko službo.

Zakonodajalec je v 148. členu Zakona o varstvu okolja[48] namreč določil, da področje dimnikarske službe sodi med obvezne državne gospodarske javne službe varstva okolja. V skladu z navedenim členom je Vlada RS izdala Uredbo o načinu, predmetu in pogojih izvajanja obvezne državne gospodarske javne službe izvajanja meritev, pregledovanja in čiščenja kurilnih naprav, dimnih vodov in zračnikov zaradi varstva okolja in učinkovite rabe energije, varstva človekovega zdravja in varstva pred požarom[49], ki določa, da se dimnikarska služba opravlja s podelitvijo koncesije, in sicer se za njeno opravljanje na posameznem območju podeli ena koncesija, ki je izključna in jo torej opravlja le izbrani koncesionar. Slovenija je razdeljena na 194 dimnikarskih območij. ZVO-1 je določil, da se dimnikarska služba na malih kurilnih napravah izvaja v javnem interesu, tj. zaradi varstva okolja, učinkovite rabe energije, varstva človekovega zdravja in varstva pred požarom.

Po 5. členu Zakona o gospodarskih javnih službah[50] je uporaba javnih dobrin, ki se zagotavljajo z obveznimi gospodarskimi javnimi službami, obvezna, če zakon ali na njegovi podlagi izdani predpis za posamezne primere ne določa drugače. Po 1. in 2. odstavku 6. člena Uredbe je uporaba dimnikarskih storitev obvezna za vse uporabnike dimnikarskih storitev. Uporabniki dimnikarskih storitev pa so definirani kot osebe, ki nadzorujejo in uporabljajo malo kurilno napravo, pomožno napravo, dimni vod ali zračnik oziroma kot lastniki nepremičnin, če statusa uporabnika ne bi bilo mogoče določiti po prejšnjih kriterijih. Uporabnik dimnikarske storitve mora po 29. členu Uredbe omogočiti neovirano in varno opravljanje storitev dimnikarske službe, na najavljen termin koncesionarju pripraviti neoviran in prost dostop do kurilne naprave, dimnih vodov, pomožnih naprav ali zračnikov, dovoliti mora vpogled v načrte teh naprav in omogočiti vstop v prostore, v katerih so

[48] Uradni list RS, št. 13/2006-UPB1, s spremembami; v nadaljevanju ZVO-1.
[49] Uradni list RS, št. 129/2004, 57/2006, 105/2007 in 102/2008; v nadaljevanju Uredba.
[50] Uradni list RS, št. 32/1993 in 66/2000 – odl. US; v nadaljevanju ZGJS.

naprave ali skozi katere te potekajo oziroma v katerih se opravljajo storitve dimnikarske službe, ter omogočiti vpogled v načrte zgradbe, v katerih so nameščene te naprave ali skozi katere te potekajo. Če uporabnik ne izpolni svojih dolžnosti, koncesionar o tem obvesti inšpekcijo, pristojno za varstvo okolja. Inšpektor lahko uporabniku odredi, da zagotovi vse, kar je potrebno za izvedbo storitev dimnikarske službe.

Iz citiranih pravnih podlag izhaja, da je uporabnik dolžan uporabiti dimnikarsko storitev, tudi če nastopa le v svojstvu lastnika nepremičnine, ter da se dimnikarska služba na malih kurilnih napravah opravlja kot obvezna gospodarska javna služba v javnem interesu, katere izvajanje mora zagotavljati država.

Informacijski pooblaščenec je tako zaključil, da pravna podlaga za obdelavo osebnih podatkov posameznika s strani zavezanca ni v 3. odstavku 10. člena ZVOP-1, saj navedeno določilo pride v poštev le, kadar upravljavec izkazuje zgolj nujnost obdelave osebnih podatkov zaradi uresničevanja zakonitih interesov zasebnega sektorja in nima pravne podlage za obdelavo določenih osebnih podatkov v zakonu, osebni privolitvi ali pogodbenem razmerju. Temelj za obdelavo osebnih podatkov posameznika je v tem primeru 1. odstavek 10. člena ZVOP-1, in sicer v povezavi s 148. členom ZVO-1, saj gre za izvajanje javne službe v javnem interesu, kljub temu da ZVO-1 ne določa natančno ne obdelave osebnih podatkov in tudi ne nabora osebnih podatkov za namen opravljanja dimnikarske službe. V primeru izvajanja obvezne gospodarske javne službe na področju dimnikarskih storitev je uporabnik (posameznik kot lastnik nepremičnine) na podlagi ZVO-1 in Uredbe v prisilnem razmerju s koncesionarjem – izvajalcem dimnikarskih storitev (zavezancem). Obdelava določenih osebnih podatkov uporabnika (osebnega imena in naslova) je zgolj posledica tega zakonsko vzpostavljenega prisilnega razmerja za namen uresničevanja javnega interesa, kot ga je prepoznal in uzakonil ZVO-1. Za ta namen (najava storitev zaradi preverjanja, ali posameznik ima malo kurilno napravo ali ne, ter zaradi opravljanja dimnikarskih storitev) sme izvajalec javne službe na podlagi 1. odstavka 10. člena ZVOP-1 obdelovati določene osebne podatke uporabnikov, ki jih prav tako za ta namen pridobi iz javnih knjig in evidenc. V skladu z določbo 38. člena Uredbe mora koncesionar voditi tudi evidence svojih storitev na malih kurilnih napravah, dimnih vodih, zračnikih in pomožnih napravah ter evidence opravljenih meritev emisij snovi v zrak iz malih kurilnih naprav.

Informacijski pooblaščenec je zaradi navedenega pritožbo posameznika z odločbo zavrgel, saj v primeru obdelave osebnih podatkov na podlagi 1. odstavka 10. člena ZVOP-1 posameznik nima pravice zahtevati prenehanja obdelave svojih osebnih podatkov.

Posameznik je zoper prejeto odločbo Informacijskega pooblaščenca sprožil upravni spor oziroma vložil tožbo na Upravno sodišče RS, ki je tožbo zavrnilo, ker je ugotovilo, da je bil postopek pred izdajo izpodbijane odločbe pravilen, prav tako je bila pravilna odločitev Informacijskega pooblaščenca. Posameznik je zoper sodbo Upravnega sodišča RS vložil tudi revizijo na Vrhovno sodišče RS, ki pa jo je slednje kot neutemeljeno zavrnilo.

4.10. Splošna ocena stanja varstva osebnih podatkov in priporočila

Informacijski pooblaščenec je leta 2013 na področju varstva osebnih podatkov vodil 712 inšpekcijskih zadev, od tega 253 na področju javnega sektorja in 459 na področju zasebnega sektorja (leta 2012 jih je bilo 725, leta 2011 jih je bilo 682, leta 2010 pa 599), ter 106 prekrškovnih postopkov (leta 2012 jih je bilo 158, leta 2011 jih je bilo 136, leta 2010 pa 179).

Poleg inšpekcijskih in prekrškovnih postopkov je Informacijski pooblaščenec leta 2013 prejel še 2.460 zaprosil za mnenja in pojasnila s področja varstva osebnih podatkov (leta 2012 je bilo takih zaprosil 2.191, leta 2011 jih je bilo 2.143, leta 2010 pa 1.859), šest vlog za izdajo dovoljenja za povezovanje zbirk osebnih podatkov (leta 2012 jih je bilo devet, leta 2011 jih je bilo 14, leta 2010 pa devet), 11 vlog za izdajo dovoljenja za izvajanje biometričnih ukrepov (leta 2012 jih je bilo 11, leta 2011 jih je bilo devet, leta 2010 pa šest), 14 vlog za izdajo dovoljenja za iznos osebnih podatkov (leta 2012 jih je bilo pet, leta 2011 je Informacijski pooblaščenec prejel štiri, leta 2010 pa jih je dobil osem), 68 pritožb zaradi

zavrnitve zahteve za seznanitev z lastnimi osebnimi podatki (leta 2012 jih je bilo 63, leta 2011 in 2010 pa jih je bilo 85), od tega 11 pritožb zaradi zavrnitve zahteve za seznanitev po ZPacP (leta 2012 je bilo takih pritožb deset).

Sredi junija 2013 so stopile v veljavo določbe 157. člena ZEKom-1 o piškotkih, ki se nanašajo na shranjevanje podatkov ali pridobivanje dostopa do podatkov, shranjenih v terminalski opremi naročnika ali uporabnika javnih komunikacijskih storitev. Po uveljavitvi določb 157. člena ZEKom-1 je Informacijski pooblaščenec kot organ, pristojen za inšpekcijski nadzor nad izvajanjem navedenih določb, do konca leta 2013 v obravnavo prejel 35 prijav, ki so se nanašale na 141 zavezancev (upravljavcev spletnih strani). Prijave so se večinoma nanašale na pomanjkljiva ali neobstoječa obvestila ter neustrezne mehanizme za pridobivanje privolitve. Zavezanci, zoper katere je Informacijski pooblaščenec uvedel inšpekcijske postopke, so v veliki večini primerov ugotovljene nepravilnosti oziroma kršitve odpravili že na podlagi seznanitve z ugotovljenimi nepravilnostmi, zaradi česar Informacijskemu pooblaščencu ureditvenih odločb sploh ni bilo treba izdati.

Informacijski pooblaščenec ugotavlja, da se je število prijav, ki jih zaradi suma kršitve predpisov prejme vsako leto, počasi umirilo in ne narašča več tako, kot se je to dogajalo v preteklih letih, kar velja tudi za ostale vloge, ki jih na področju varstva osebnih podatkov prejme vsako leto. Zato je leta 2013 lahko več pozornosti namenil t. i. načrtovanemu ex offo inšpekcijskemu nadzoru, ki ga izvaja skladno s sprejetim letnim načrtom.

Poleg prijav, ki so bile v obravnavanem obdobju vložene v zvezi s piškotki, je Informacijski pooblaščenec podobno kot prejšnja leta tudi leta 2013 veliko prijav prejel zaradi izvajanja videonadzora ter zaradi uporabe osebnih podatkov za namene neposrednega trženja. Poleg navedenih prijav je treba še posebej izpostaviti prijave, ki so bile vložene zaradi preusmeritve in posledično branja elektronske pošte, ki prihaja na službeni elektronski naslov zaposlenih, prijave, ki so bile vložene zaradi objave osebnih podatkov na spletnih straneh upravljavcev osebnih podatkov, prijave, ki so bile vložene zaradi pošiljanja plačljivih SMS-sporočil, ter prijave, ki so bile vložene zaradi obdelave netočnih in neažurnih podatkov.

Informacijski pooblaščenec pri obravnavi prijav ugotavlja, da delodajalci po prekinitvi delovnega razmerja pogosto ne ukinejo oz. ne izbrišejo službenega elektronskega naslova, ki ga je uporabljal bivši zaposleni, pač pa namesto tega pošto, ki prihaja na službeni elektronski naslov bivšega zaposlenega, enostavno preusmerijo na elektronski naslov druge osebe. Pri takšnem ravnanju ne gre le za nezakonito uporabo osebnega podatka (elektronskega naslova zaposlenega), pač pa s takšno preusmeritvijo osebi, na katero preusmerijo prejeto elektronsko pošto, omogočijo, da se nezakonito seznani tudi z osebnimi podatki tretjih oseb, to je oseb, ki pošiljajo elektronsko pošto na elektronski naslov bivšega zaposlenega (seznanijo se z njihovimi e-naslovi, s prometnimi podatki ter z vsebino poslanih sporočil). Delodajalci takšno ravnanje upravičujejo s tem, da na tak način zagotavljajo kontinuiran poslovni proces in preprečujejo poslovno škodo ob eventuelni izgubi naročila. Tega opravičila ni mogoče resno upoštevati, saj lahko delodajalci kontinuiran poslovni proces zelo preprosto zagotovijo tudi brez nezakonite obdelave osebnih podatkov in posegov v t. i. komunikacijsko zasebnost posameznikov, ki lahko pomeni tudi storitev kaznivega dejanja kršitve tajnosti občil po 139. členu Kazenskega zakonika[51]. Ena od preprostih možnosti, kako se po prenehanju delovnega razmerja delavca izogniti nezakoniti obdelavi osebnih podatkov ter ob tem hkrati zagotoviti nemoteno nadaljevanje poslovnega procesa, je npr. ta, da se za ukinjen elektronski naslov za določen čas zagotovi avtomatsko povratno sporočilo, s katerim se pošiljatelja obvesti, da je elektronski naslov ukinjen in da naj zato poslovno pošto pošlje na drug elektronski naslov. Podobno velja tudi v primeru daljše odsotnosti delavca, saj tudi v tem primeru preusmeritev elektronske pošte na drug naslov ni dopustna niti na podlagi osebne privolitve posameznika, na katerega se elektronski naslov nanaša. Upoštevati je namreč treba, da se s preusmeritvijo elektronske pošte drugi osebi ne razkrivajo zgolj osebni podatki posameznika, na katerega se elektronski naslov nanaša, temveč tudi osebni podatki posameznikov, ki pošiljajo elektronsko pošto na preusmerjeni naslov.

Pri obravnavi prijav v zvezi z javno objavo osebnih podatkov na spletnih straneh upravljavca osebnih podatkov Informacijski pooblaščenec ugotavlja, da upravljavci osebnih podatkov na svojih spletnih straneh osebne podatke objavljajo predvsem zaradi malomarnosti, kar pa

[51] Kazenski zakonik, Uradni list RS, št. 50/2012-UPB2.

nikakor ne upravičuje njihovega ravnanja. Do takšne objave tako najpogosteje pride zato, ker upravljavci nimajo predpisanih postopkov in ukrepov, s katerimi bi zagotovili, da se pred objavo določenega gradiva na ustrezen način preveri, ali gradivo, ki ga nameravajo objaviti, vsebuje tudi osebne podatke, do katerih javnost ni upravičena. Informacijski pooblaščenec zato upravljavce spletnih strani v izogib bodočim takšnim kršitvam poziva, da predpišejo in zagotovijo ustrezne organizacijske in tehnične postopke in ukrepe, s katerimi bodo lahko uspešno prepričevali takšno nezakonito razkrivanje osebnih podatkov.

Informacijski pooblaščenec je v obravnavanem obdobju prejel tudi več prijav zaradi pošiljanja plačljivih SMS-sporočil s strani avstrijskega podjetja Dimoco. Pri obravnavi teh prijav Informacijski pooblaščenec ni našel elementov kršitve določb ZVOP-1, pač pa je lahko ugotovil zgolj nepošteno poslovno prakso omenjenega podjetja, na katero potrošnike prek svojih spletnih strani opozarja tudi Zveza potrošnikov Slovenije. Ugotovitve kažejo, da omenjeno podjetje na spletnih straneh ponuja različne vsebine (npr. test inteligenčnega kvocienta, različne igre). Ko posameznik želi priti do rezultata npr. testa inteligenčnega kvocienta, mora na spletu v posebno okence vpisati svojo številko mobilnega telefona, z naslednjim okencem na spletni strani, v katerega vpiše kodo, ki jo je prejel preko SMS-sporočila, pa se (običajno nevede) včlani v SMS-klub. To, da se je s takšnim ravnanjem včlanil v SMS-klub, posameznik opazi šele, ko prejme višji mesečni račun svojega mobilnega operaterja. Z včlanitvijo v SMS-klub se je namreč strinjal, da mu ponudnik pošilja SMS-sporočila po ceni 2,49 EUR/SMS, kar znesek na mesečnem računu za telefon opazno zviša. Informacijski pooblaščenec zato priporoča, da posamezniki pred posredovanjem oziroma vnosom svoje telefonske številke ob reševanju raznih testov ali igranju raznih iger pozorno preberejo pravila, ki so prepogosto navedena v drobnem tisku ali na posebni podstrani, ter da v primeru, ko prejmejo sumljivo SMS-sporočilo, le-tega pozorno preberejo ter se, glede na njegovo vsebino, nanj ne odzovejo ali pa se takoj odjavijo od prejemanja naročenih plačljivih sporočil.

Informacijski pooblaščenec zaradi napačnega razumevanja določb ZVOP-1 vsako leto prejme tudi številne prijave posameznikov, ki zatrjujejo, da določen upravljavec o njih vodi nepopolne, netočne oziroma neažurne osebne podatke. V zvezi s takšnimi prijavami je treba pojasniti, da Informacijski pooblaščenec ni pristojen presojati, ali upravljavec o določenem posamezniku vodi točene in ažurne podatke. Posamezniku, ki meni, da določen upravljavec o njem vodi netočne oziroma neažurne osebne podatke, zato svetujemo, naj od upravljavca osebnih podatkov na podlagi 30. in 31. člena ZVOP-1 najprej pisno (priporočeno oziroma s povratnico) zahteva vpogled, prepis oziroma izpis svojih osebnih podatkov ter informacije o virih, na katerih temeljijo zapisi. Na podlagi tako dobljenih podatkov in informacij bo lahko posameznik na podlagi 32. in 33. člena ZVOP-1 od upravljavca osebnih podatkov zahteval dopolnitev, popravo, blokiranje ali izbris svojih osebnih podatkov, pri čemer bo moral sam izkazati, da so osebni podatki, ki se nanašajo nanj, nepopolni, netočni, neažurni oziroma zbrani in obdelani v nasprotju z zakonom. Če upravljavec posameznikovo zahtevo po dopolnitvi, popravi, ažuriranju ali izbrisu osebnih podatkov zavrne, posameznik te svoje pravice ne more uveljavljati pri Informacijskem pooblaščencu, pač pa lahko na podlagi 34. in 35. člena ZVOP-1 zahteva sodno varstvo na Upravnem sodišču RS. Informacijski pooblaščenec lahko v zvezi z zavrnjeno zahtevo posameznika po dopolnitvi, popravi, blokiranju ali izbrisu njegovih osebnih podatkov ukrepa le v primeru, če upravljavec o njegovi zahtevi ne odloči v roku 15 dni in ga o tem ne obvesti, ter v primeru, če se osebni podatki posameznika obdelujejo nezakonito (brez podlage v zakonu ali osebni privolitvi posameznika). Upravljavce osebnih podatkov zato opozarjamo, da morajo v primeru zahteve posameznika do seznanitve z njegovimi osebnimi podatki iz 30. in 31. člena ZVOP-1 in v primeru zahteve posameznika do dopolnitve, poprave, blokiranja ali izbrisa osebnih podatkov iz 32. in 33. člena ZVOP-1 v zakonsko določenem roku zahtevi posameznika bodisi ugoditi in ga o tem pisno obvestiti, ali pa ga v istem roku pisno obvestiti o razlogih, zaradi katerih njegovi zahtevi ne bodo ugodili.

Pomemben del aktivnosti Informacijskega pooblaščenca se nanaša tudi na uvajanje novih pooblastil organov pregona, zlasti glede zelo pogostih sprememb na področju ureditve kazenskih postopkov. Informacijski pooblaščenec ugotavlja, da je še vedno veliko težav pri tolmačenju komunikacijske zasebnosti, in opozarja, da za pridobitev podatkov o identiteti komunicirajočih posameznikov ni dovolj ne pisna zahteva državnega organa in ne sodna odredba, saj gre za zahtevo iz 37. člena Ustave RS. Ta določa, da je zagotovljena tajnost pisem in drugih občil ter da se lahko samo na podlagi odločbe sodišča za določen čas ne upošteva varstva tajnosti pisem in drugih občil ter nedotakljivost človekove zasebnosti, če

je to nujno za uvedbo ali potek kazenskega postopka ali za varnost države. Ustava RS 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. Informacijski pooblaščenec je konec leta 2013 objavil poročilo, v katerem je ugotovil zaskrbljujočo prakso policije, ki je kljub jasnim določbam ZEPT ter ZKP leta 2012 od ponudnikov storitev informacijske družbe s pisnimi zahtevki 35-krat zahtevala podatke o uporabnikih spletnih strani z vsebino, ki jo posredujejo prejemniki storitve. V 31 primerih je to storila brez potrebne odredbe sodišča in v 30 % pisnih zahtevkov ni kvalificirala obravnavanega kaznivega dejanja. Prav tako je očitno, da gre za nepoznavanje razlike med operaterji (ponudniki javno dostopnih komunikacijskih omrežij in storitev), katerih delovanje primarno ureja ZEKom-1, in upravljavci spletnih strani (ponudniki storitev informacijske družbe), katerih delovanje primarno ureja ZEPT. Gre namreč za to, da policija od ponudnikov storitev informacijsko družbe zahteva prometne podatke (podatek o IP-naslovu), kar pomeni, da lahko te podatke od operaterjev zahteva le po 1. odstavku 149. b člena ZKP, torej s sodno odredbo, od ponudnikov storitev informacijske družbe, ki niso hkrati tudi operaterji, pa prav tako le s sodno odredbo, kot to določa 4. odstavek 8. člena ZEPT.

Na področju sodobnih informacijsko-komunikacijskih tehnologij se poleg trendov, ki smo jih obravnavali v predhodnem poročilu (računalništvo v oblaku, t. i. »big data«), nadaljujejo novi izzivi za varstvo osebnih podatkov. Gre predvsem za vse širšo uporabo brezpilotnih letalnikov (angl. Remotely Piloted Automated Systems), ki omogočajo prikrita, težko zaznavna in obsežna zbiranja osebnih podatkov in občutne posege v zasebnost. S tem, ko se brezpilotni letalniki lahko opremijo z zelo različnimi senzorji, ki omogočajo zajem videa, slike, zvoka ter podatkov o temperaturi, gibanju, lokaciji itd., bo njihova uporaba predstavljala velik izziv tako za regulatorje kot za varuhe zasebnosti.

Informacijski pooblaščenec ugotavlja, da so upravljavci zbirk osebnih podatkov že dodobra seznanjeni z zahtevami ZVOP-1 in da so aktivnosti Informacijskega pooblaščenca na področju ozaveščanja ter inšpekcijskega nadzora učinkovite. Ob sicer velikem številu obsežnih zlorab v tujini, ki vključujejo izgube velikanskih količin osebnih podatkov, tovrstnim obsežnim kršitvam v Sloveniji nismo priča, pri čemer je treba upoštevati, da tako velike kršitve le težko ostanejo neodkrite.

Pri uporabi informacijskih sistemov, v katerih se obdelujejo osebni podatki, ostaja velik poudarek na pravočasnem upoštevanju zahtev varstva osebnih podatkov s pomočjo predhodnih presoj vplivov na zasebnost, s katerimi je mogoče pravočasno identificirati in zmanjšati tveganja za zlorabe osebnih podatkov. Informacijski pooblaščenec opaža, da je njihova koristnost še vedno premalo prepoznana. Dodatne napore bi veljalo zlasti usmeriti k izboljšanemu ozaveščanju določenih strokovnih profilov, kot so razvijalci sistemov in aplikacij, informatiki in strokovnjaki s področja elektrotehnike, saj bi se z upoštevanjem načela vgrajene zasebnosti (angl. Privacy by Design) lahko izognili marsikateri zlorabi temeljnih načel varstva osebnih podatkov, predvsem pa težavam glede zakonitosti, sorazmernosti in informacijske varnosti.

Prijave, ki so bile v obravnavanem obdobju vložene v zvezi s piškotki, je Informacijski pooblaščenec zavoljo omejenih kadrovskih resursov razvrstil in obravnaval po lestvici prioritet, ki temelji na kriterijih pomembnosti/prepoznavnosti posamezne spletne strani ter na ocenjeni resnosti posega v zasebnost. Pri obravnavi prijav je Informacijski pooblaščenec ugotovil, da so kršitve določb 157. člena ZEKom-1 v praksi dokaj pogoste. Spletne strani so svoje uporabnike sicer dosledno obveščale o rabi piškotkov, niso pa vedno zagotovile ustreznih nadzornih mehanizmov, ki bi dejansko dovoljevali oziroma prepovedovali nameščanje piškotkov. Predvsem je bilo zabeleženih več primerov, ko je spletna stran piškotke, za katere je po začetku veljave omenjenega 157. člena potrebna izrecna privolitev uporabnika, nameščala že kar ob prvem obisku spletne strani, ter primerov, ko je upravitelj spletne strani preveč široko tolmačil določbe 2. odstavka 157. člena ZEKom-1 o izjemah (nujnih piškotkih), za katere privolitev ni potrebna. Informacijski pooblaščenec glede večine primerov sicer z veseljem ugotavlja, da so bili upravljavci omenjene pomanjkljivosti pripravljeni odpraviti takoj po prejemu poziva Informacijskega pooblaščenca, torej še pred izdajo dokončne odločbe. Kot problematične smo zaznali zlasti oglaševalske in analitične piškotke, pa tudi piškotke določenih vtičnikov, ki jih praviloma nastavljajo tretje strani in ki omogočajo beleženje uporabnikove vsakodnevne spletne aktivnosti čez več različnih spletnih strani (“sledilni piškotki”). Informacijski pooblaščenec je zato v dialogu z zavezanci oblikoval Smernice za rabo piškotkov ter odgovore na pogosta vprašanja v zvezi

s piškotki in jih objavil na svojih spletnih straneh. S strani upravljavcev spletnih strani je bilo Informacijskemu pooblaščencu posredovanih veliko vprašanj glede spletne analitike, in sicer konkretno, kako jo izvesti tako, da bo dovoljena na podlagi domnevne privolitve in že ob prvem obisku. Informacijski pooblaščenec je tako predvsem glede spletnih strani v javnem sektorju ter spletnih strani večjih slovenskih medijev dosegel opustitev uporabe nekaterih bolj invazivnih vtičnikov.

Informacijski pooblaščenec z zanimanjem aktivno spremlja razvoj dogodkov na področju reforme zakonodaje o varstvu osebnih podatkov v EU, in sicer je aktivno sodeloval v okviru podskupine Future of Privacy. Nekatere od predvidenih rešitev, kot so večji poudarek odgovornim osebam za varstvo osebnih podatkov, presoje vplivov na varstvo osebnih podatkov in certifikacija, po mnenju Informacijskega pooblaščenca predstavljajo bolj učinkovite ukrepe za varstvo osebnih podatkov. Posebnega pomena bo prav gotovo vprašanje zavezancev in teritorialni domet bodoče zakonodaje, saj nekatere zelo velike upravljavce osebnih podatkov, kot sta Google in Facebook, trenutno le v omejeni meri zavezujejo določbe evropske zakonodaje.

Področje, ki je tudi v svetovnem merilu dobilo večjo pozornost, je vprašanje delovanja varnostno-obveščevalnih služb. Zlasti Snowdnova odkritja glede ameriške preiskovalne agencije (National Security Agency, NSA) so sprožila val ogorčenja in vprašanj glede tega, kdo in v kolikšni meri posega v našo zasebnost. Razkritje Edwarda Snowdna o popolnem nadzoru nad podatki z interneta, telekomunikacijskimi operaterji v Združenih državah Amerike in podatki, ki jih v t. i. oblak Googla, Facebooka, Microsofta, Amazona, ipd. množično dajejo tudi Evropejci, je sprožilo ustanovitev posebne ad hoc skupine EU–ZDA, katere naloga je bila ugotoviti dejansko stanje aktivnosti NSA glede množičnega zbiranja informacij in osebnih podatkov o državljanih EU. V omenjeno skupino je bila s strani Evropske komisije kot ena od petih vrhunskih evropskih strokovnjakov s področja varstva osebnih podatkov imenovana tudi informacijska pooblaščenka Nataša Pirc Musar.

CH3
CH3

5 DRUGE DEJAVNOSTI INFORMACIJSKEGA POOBLAŠČENCA

5.1. 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 in ostalih predpisov z zakoni in drugimi predpisi, ki urejajo obdelavo osebnih podatkov.

Informacijski pooblaščenec je leta 2013 zaznal skrb vzbujajoče veliko število predlogov sprememb zakonov oziroma predlogov novih zakonov, ki prinašajo 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 2013 je Informacijski pooblaščenec prejel 106 vlog za podajo mnenja na predloge zakonov in drugih predpisov. Podal je naslednja mnenja:

- Predlog Zakona o spremembah in dopolnitvah Zakona o subvencioniranju študentske prehrane (mnenje z dne 19. 12. 2013),
- Predlog Državnopravobranilskega reda (mnenje z dne 19. 12. 2013),
- Predlog Zakona o spremembah in dopolnitvah Zakona o gozdovih (mnenje z dne 18. 12. 2013),
- Predlog sprememb in dopolnitev 26. člena Zakona o voznikih (mnenje z dne 17. 12. 2013),
- Pobuda za sklenitev sporazuma med Vlado Republike Slovenije in Svetom ministrov Bosne in Hercegovine o sodelovanju pri delu skupnih preiskovalnih skupin, čezmejnem tajnem opazovanju oziroma sledenju, pošiljanju in primerjavi profilov DNK in drugega identifikacijskega materiala ter uradnikih za zvezo (mnenje z dne 16. 12. 2013),
- Predlog sprememb in dopolnitev Zakona o kazenskem postopku (mnenje z dne 12. 12. 2013),
- Predlog Zakona o odvzemu in presaditvi delov človeškega telesa zaradi zdravljenja (mnenji z dne 16. 8. in 11. 12. 2013),
- Pobuda za sklenitev sporazuma med Vlado Republike Slovenije in Vlado Črne gore o sodelovanju pri delu skupnih preiskovalnih skupin, čezmejnem tajnem opazovanju oziroma sledenju, pošiljanju in primerjavi profilov DNK in drugega identifikacijskega materiala ter uradnikih za zvezo (mnenje z dne 10. 12. 2013),
- Predlog Zakona o spremembah in dopolnitvah Zakona o brezplačni pravni pomoči (mnenje z dne 5. 12. 2012),
- Predlog spremembe 15. člena Zakona o knjižničarstvu (mnenje z dne 2. 12. 2013),
- Predlog Uredbe o izvedbi ukrepov kmetijske politike (mnenje z dne 2. 12. 2013),
- Predlog za spremembo Zakona o elektronskem poslovanju na trgu (mnenje z dne 27. 11. 2013),
- Osnutek Zakona o spremembah in dopolnitvah Zakona o kmetijstvu (mnenje z dne 25. 11. 2013),
- Predlog Zakona o spremembah in dopolnitvah Zakona o tujcih (mnenje z dne 22. 11. 2013),
- Predlog Zakona o državnem geodetskem referenčnem sistemu (mnenje z dne 19. 11. 2013),
- Predlog Zakona o slovenskem državnem holdingu (mnenji z dne 19. 9. in 11. 11. 2013),
- Osnutek spremembe pravne podlage sistema informacij o boniteti strank in izmenjave osebnih podatkov o spornih okoliščinah (mnenje z dne 8. 11. 2013),
- Predlog sprememb in dopolnitev Zakona o sodiščih (mnenji z dne 6. 11. in 12. 12. 2013),
- Predlog Uredbe o zagotavljanju upravičenosti do založitve sredstev v nujnih konzularnih primerih (mnenje z dne 5. 11. 2013),
- Predlog Letnega programa statističnih raziskovanj 2014 (mnenje z dne 4. 11. 2013),
- Predlog Zakona o igrah na srečo (mnenje z dne 22. 10. 2013),
- Predlog Zakona o spremembah in dopolnitvah Zakona o kmetijsko-gozdarski zbornici (mnenji z dne 15. 2. in 22. 10. 2013),
- Predlog Zakona o spremembah in dopolnitvah Zakona o odvzemu premoženja nezakonitega izvora (mnenje z dne 22. 10. 2013),
- Predlog Zakona o preprečevanju dela in zaposlovanja na črno (mnenje z dne 14. 10. 2013),

- Predlog Zakona o spremembah in dopolnitvah Zakona o inšpekcijskem nadzoru (mnenje z dne 16. 10. 2013),
- Predlog Zakona o preprečevanju dela in zaposlovanja na črno (mnenje z dne 16. 10. 2013),
- Predlog Zakona o spremembah in dopolnitvah Zakona o zdravstvenem varstvu in zdravstvenem zavarovanju (mnenje z dne 17. 10. 2013),
- Predlog Zakona o spodbujanju razvoja turizma (mnenje z dne 10. 10. 2013),
- Predlog Zakona o prijavi prebivališča (mnenja z dne 5. 4., 18. 4., 14. 6 in 23. 9. 2013),
- Predlog Zakona o spremembah in dopolnitvah Zakona o bančništvu (mnenje z dne 23. 9. 2013),
- Predlog Zakona o inšpekciji dela (mnenje z dne 12. 9. 2013),
- Splošni akt o zavarovanju hranjenih podatkov na podlagi 4. odstavka 165. člena Zakona o elektronskih komunikacijah (mnenje z dne 3. 9. 2013),
- Pravilnik o kakovosti storitve za enotno evropsko telefonsko številko za klice v sili 112 (mnenje z dne 27. 8. 2013),
- Predlog Zakona o spremembah in dopolnitvah Zakona o odvzemu premoženja nezakonitega izvora (mnenje z dne 26. 8. 2013),
- Predlog Sporazuma med Vlado Republike Slovenije in Vlado Republike Kosovo o policijskem sodelovanju (mnenje z dne 26. 8. 2013),
- Predlog Dogovora med Vlado Republike Slovenije in Vlado Republike Makedonije o policijskem sodelovanju (mnenje z dne 21. 8. 2013),
- Predlog Pravilnika o izvajanju 153. člena Zakona o elektronskih komunikacijah (mnenji z dne 28. 6. in 21. 8. 2013),
- Predlog Pravilnika o obliki, vsebini in načinu hrambe prevoznice za prevoz gozdnih lesnih sortimentov (mnenje z dne 19. 8. 2013),
- Sprememba 3. odstavka 3.a člena Zakona o sistemu plač v javnem sektorju (mnenje z dne 14. 8. 2013),
- Predlog Zakona o spremembah in dopolnitvah Zakona o gospodarskih družbah (mnenje z dne 13. 8. 2013),
- Predlog Pravilnika o obdelavi podatkov o elektronskih komunikacijah policije in dostopu do policijskih zbirk podatkov (mnenje z dne 12. 8. 2013),
- Predlog Zakona o zdravstveni dejavnosti (mnenje z dne 9. 8. 2013),
- Predlog spremembe Energetskega zakona (mnenje z dne 9. 8. 2013),
- Predlog Zakona o spremembah in dopolnitvah Zakona o motornih vozilih (mnenje z dne 9. 8. 2013),
- Predlog Uredbe Evropskega parlamenta in Sveta o zahtevah za homologacijo za uvedbo avtomobilskega sistema eCall in sprememba Direktive 2007/46/ES (mnenje z dne 6. 8. 2013),
- Osnutek sprememb Zakona o spodbujanju razvoja turizma (mnenje z dne 30. 7. 2013),
- Predlog Splošnega akta o razčlenjenem računu (mnenje z dne 30. 7. 2013),
- Predlog Uredbe o poenostavitvi izmenjave informacij in podatkov med Policijo ali Carinsko upravo Republike Slovenije ter pristojnimi organi v drugih državah članicah Evropske unije (mnenje z dne 30. 7. 2013),
- Predlog Zakona o starševskem varstvu in družinskih prejemkih (mnenje z dne 18. 7. 2013),
- Predlog Zakona o povračilu škode osebam, ki so bile izbrisane iz registra stalnega prebivalstva (mnenje z dne 9. 7. 2013),
- Predlog Zakona o makrobonitetnem nadzoru finančnega sistema (mnenji z dne 20. 6. in 27. 9. 2013),
- Sprememba Uredbe o upravnem poslovanju (mnenje z dne 19. 6. 2013),
- Pobuda za sklenitev sporazuma med Ministrstvom za notranje zadeve Republike Slovenije in Zvezno službo Ruske federacije za nadzor nad trgovino s prepovedanimi drogami, o sodelovanju v boju proti nedovoljeni trgovini s prepovedanimi drogami, psihotropnimi snovmi in predhodnimi sestavinami (mnenje z dne 18. 6. 2013),
- Predlog Zakona o spremembah in dopolnitvah Zakona o prekrških (mnenje z dne 13. 6. 2013),
- Osnutek Pravilnika o enotnem informacijskem sistemu na področju javnega naročanja (mnenje z dne 5. 6. 2013),
- Pravilnik o prijavah na področju varnosti in zdravlja pri delu (mnenje z dne 3. 6. 2013),
- Predlog Splošnega akta o razčlenjenem računu (mnenje z dne 27. 5. 2013),
- Predlog Zakona o spremembah in dopolnitvah Zakona o finančnem poslovanju, postopkih zaradi insolventnosti in prisilnem prenehanju (mnenje z dne 17. 5. 2013),

- Predlog Zakona o spremembah in dopolnitvah Zakona o verski svobodi (mnenje z dne 13. 5. 2013),
- Pobuda za sklenitev Sporazuma med Vlado Republike Slovenije in Vlado Združenih držav Amerike o izboljšanju mednarodne davčne skladnosti in izvajanju FATCA (mnenje z dne 10. 5. 2013),
- Predlog Zakona o spremembah in dopolnitvah Zakona o delovnem času in obveznih počitkih mobilnih delavcev ter o zapisovalni opremi v cestnih prevozih (mnenji z dne 9. 5. in 20. 6. 2013),
- Predlog Zakona o spremembah in dopolnitvah Zakona o volilni in referendumski kampanji (mnenje z dne 8. 5. 2013),
- Predlog Zakona o evidenci volilne pravice (mnenje z dne 7. 5. 2013),
- Predlog Zakona o spremembah in dopolnitvah Zakona o političnih strankah (mnenje z dne 7. 5. 2013),
- Predlog Uredbe o Europolu (mnenje z dne 6. 5. 2013),
- Predlog Pravilnika o opremi in vmesnikih za zakonito prestrezanje informacij (mnenje z dne 29. 4. 2013),
- Predlog Pravilnika o načinu posredovanja hranjenih podatkov o prometu telefonskih in podatkovnih storitev v mobilnem in fiksnem elektronskem komunikacijskem omrežju (mnenje z dne 26. 4. 2013),
- Predlog Pravilnika o reševanju pritožb zoper delo policistov (mnenje z dne 26. 4. 2013),
- Predlog Zakona o spremembah in dopolnitvah Zakona o državni upravi – skrajšani postopek, ZDU-1G (mnenje z dne 24. 4. 2013),
- Osnutek predloga Zakona o spremembah in dopolnitvah Zakona o sodiščih in osnutek predloga Zakona o spremembah in dopolnitvah Zakona o sodniški službi (mnenje z dne 23. 4. 2013),
- Predlog spremembe 148. člena Zakona o varstvu okolja (mnenje z dne 17. 4. 2013),
- Pravilnik o katastru čebelje paše, čebelarskem pašnem redu in programu napovedi medenja (mnenji z dne 11. 4. in 29. 4. 2013),
- Osnutek Pravilnika o določitvi strokovnega spremstva pri udejstvovanju lovskih gostov na skupnih lovih (mnenje z dne 10. 4. 2013),
- Predlog Zakona o spremembah in dopolnitvah Zakona o opravljanju plačilnih storitev za proračunske uporabnike (mnenje z dne 10. 4. 2013),
- Sporazum med Kanado in Evropsko unijo o obdelavi in prenosu podatkov iz evidence imen letalskih potnikov (mnenje z dne 8. 4. 2013),
- Predlog Uredbe SVI, Uredbe PRP in sprememb Uredbe 526/2006/ES (mnenje z dne 8. 4. 2013),
- Predlog Zakona o lekarniški dejavnosti (mnenje z dne 26. 3. 2013),
- Predlog Zakona o finančni upravi; evidenca poročevalskih enot in deklarantov (mnenje z dne 25. 3. 2013),
- Predlog Uredbe EU o poročanju o dogodkih v civilnem letalstvu (mnenje z dne 25. 3. 2013),
- Zakon o spremembah in dopolnitvah Zakona o pacientovih pravicah (mnenje z dne 20. 3. 2013),
- Predlog Pravilnika o usmerjanju in nadzoru policije (mnenje z dne 20. 3. 2013),
- Predlog Zakona o štipendiranju (mnenje z dne 8. 3. 2013),
- Predlog Direktive o preprečevanju uporabe finančnega sistema za pranje denarja in financiranje terorizma (mnenje z dne 8. 3. 2013),
- Predlog Sprememb in dopolnitev Letnega programa statističnih raziskovanj 2013 (mnenji z dne 7. 3. in 14. 6. 2013),
- Stališče Informacijskega pooblaščenca glede uvajanja nove opredelitve psevdonimnih podatkov v predlagani reformi varstva osebnih podatkov v EU (mnenje z dne 5. 3. 2013),
- Pripombe na predlog uredbe Evropskega parlamenta in Sveta o podatkih o plačniku, ki spremljajo prenose denarnih sredstev (mnenje z dne 28. 2. 2013),
- Osnutek Pravilnika o nacionalnem preverjanju znanja v osnovni šoli (mnenje z dne 19. 2. 2013),
- Predlog Zakona o spremembah in dopolnitvah Zakona o javnih uslužbencih (mnenje z dne 18. 2. 2013),
- Zakon o davčnem postopku (mnenje z dne 14. 2. 2013),
- Predlog Zakona o spremembah in dopolnitvah Zakona o zavarovalništvu (mnenje z dne 11. 2. 2013),
- Predlog Pravilnika o zahtevah za računalniške programe in elektronske naprave, upravljanje in delovanje informacijskega sistema ter vsebino, obliko, način in roke

za predložitev dokumentov iz 11. odstavka 38. člena Zakona o davčnem postopku (mnenje z dne 11. 2. 2013),
- Predlog Zakona o finančni službi (mnenje z dne 21. 1. 2013),
- Pobuda za sklenitev Sporazuma med Republiko Slovenijo in Republiko Turčijo o socialnem zavarovanju (mnenje z dne 10. 1. 2013),
- Predlog Uredbe o postopkih v primeru insolventnosti (mnenje z dne 9. 1. 2013),
- Predlog Zakona o dedovanju (mnenje z dne 2. 1. 2013).

V dveh primerih je bilo namesto izdaje pisnega mnenja s prosilcem za mnenje dogovorjeno, da se zadeve preučijo na skupnem sestanku:
- Zakon o spremembah in dopolnitvah Zakona o izvršbi in zavarovanju (sestanek dne 10. 7. 2013),
- Mnenje o elektronskem obveščanju državljanov o obdelavi njihovih osebnih podatkov (sestanek dne 30. 8. 2013).

5.2. Sodelovanje z javnostmi

Informacijski pooblaščenec je leta 2013 vseskozi skrbel za javnost svojega dela ter osveščanje pravnih in fizičnih oseb prek rednih in doslednih odnosov z mediji (sporočila za javnost, izjave, komentarji, intervjuji pooblaščenke, novinarske konference) ter prek svoje spletne 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) in dostopa do informacij javnega značaja (dostop do informacij, dostop do informacij za medije, ponovna uporaba informacij javnega značaja, 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 EU in drugod po svetu),
- izdane publikacije (priročniki in smernice, aktualno letno poročilo),
- domače in tuje članke z obeh področij,
- vzorce oziroma obrazce, namenjene fizičnim osebam za uveljavljanje njihovih pravic (zahteva za dostop do informacij javnega značaja, pritožba zoper molk ali zavrnilno odločbo organa, zahteva za ponovno uporabo informacij javnega značaja, prijava zlorabe osebnih podatkov, pritožba zaradi kršitve pravice do seznanitve z lastnimi osebnimi podatki, zahteva za seznanitev s podatki v Nacionalnem schengenskem informacijskem sistemu v Sloveniji) in upravljavcem zbirk osebnih podatkov za lažje delo pri vlaganju različnih zahtev in zagotovitvi ustreznega varovanja osebnih podatkov (zahteva za izdajo odločbe glede povezljivosti evidenc, obvestilo o povezovanju evidenc, prijava biometrijskih ukrepov pred njihovo uvedbo, vloga za iznos osebnih podatkov v tretje države, katalogi zbirk osebnih podatkov, pravilnik o zavarovanju osebnih podatkov, pogodba za potrebe pogodbene obdelave osebnih podatkov po 11. členu ZVOP-1, opozorila in obvestila ob neposrednem trženju),
- ažurno objavo izdanih mnenj Informacijskega pooblaščenca s področja varstva osebnih podatkov,
- ažurno objavo vseh odločb, s katerimi je Informacijski pooblaščenec odločil o pritožbah v zvezi z informacijami javnega značaja,
- predstavitev zahtev za oceno ustavnosti, ki jih je na Ustavno sodišče RS vložil Informacijski pooblaščenec,
- objavo sodb Upravnega sodišča RS in Vrhovnega sodišča RS v zadevah, ki jih je vodil Informacijski pooblaščenec in zoper katere so bile vložene tožbe,
- pripombe Informacijskega pooblaščenca na predloge predpisov,
- katalog Informacijskega pooblaščenca ter Centralni 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 bil leta 2013 prisoten tudi na spletnem družabnem omrežju Facebook, kjer prek svojega profila skrbi za dvig ozaveščenosti glede pomena varstva osebnih podatkov.

Informacijski pooblaščenec prav tako aktivno sodeluje v Svetu projekta SAFE-SI in Spletno oko, ki delujeta na področju varne rabe interneta. V okviru te dejavnosti je izvedel številna predavanja o varstvu osebnih podatkov na internetu za šolarje, učitelje in starše.

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

Leta 2013 je Informacijski pooblaščenec ob evropskem dnevu varstva osebnih podatkov (28. januarja) pripravil dogodek, s katerim je želel opozoriti na varno rabo pametnih mobilnih naprav. Marsikdo si danes življenja brez pametnih mobilnih naprav ne more več predstavljati. Želimo biti povezani, vedno dosegljivi, vedno družabni. Pa je to varno? In kaj to pomeni za našo zasebnost? Osrednji del dogodka je bila okrogla miza in predstavitev vodiča ABC varnosti in zasebnosti na mobilnih napravah, ki je nastal kot plod sodelovanja Informacijskega pooblaščenca in programa ozaveščanja Varni na internetu, ki ga izvaja Slovenski center za posredovanje pri omrežnih incidentih SI-CERT, ki deluje pod okriljem Javnega zavoda Arnes. Navedeni vodič predstavlja težave oziroma zlorabe, ki se lahko pripetijo v mobilnem svetu, ter podaja priporočila za varno rabo mobilnih aplikacij in naprav. Mobilne naprave so pravi mali računalniki, z vsemi funkcionalnostmi, žal pa tudi z vsemi tegobami spletnega sveta. Virusi, zlorabe in posegi v zasebnost so realnost, zato so Informacijski pooblaščenec in strokovnjaki, ki so sodelovali na okrogli mizi, opozorili na temelje varne rabe pametnih naprav in poudarili, da so pametne naprave namreč pametne le toliko, kot smo pametni njihovi uporabniki.

Že tradicionalno je Informacijski pooblaščenec ob tej priložnosti podelil nagradi za dobro prakso na področju varstva osebnih podatkov. V zasebnem sektorju je nagrado prejela Zavarovalnica Maribor, d. d., v kateri je zavedanje o pomenu varstva osebnih podatkov vpeljano v sistem dela in se odraža tako v zavesti zaposlenih kakor tudi v tehničnih rešitvah, s katerimi preprečujejo morebitne zlorabe. V javnem sektorju je nagrado prejelo Vrhovno sodišče RS, ki je s svojo odzivnostjo in naklonjenostjo varstvu osebnih podatkov in zasebnosti posameznikov na primeru elektronske Zemljiške knjige (e-ZK) dokazalo, da je še tako toge in natančne zakonske določbe mogoče uporabljati z roko v roki z načelom sorazmernosti. Priznanja so dobila še podjetja, ki so leta 2012 pridobila certifikat po standardu za varovanje informacij ISO/IEC 27000 in s tem izkazala visoko raven zavarovanja osebnih podatkov (Inštitut za nutricionistiko, 3GEN, d. o. o., iPLUS, d. o. o., Elektro Slovenija, d. o. o., GENIS, d. o. o., MICROCOP, d. o. o., Agencija za trg vrednostnih papirjev, HSE Invest, d. o. o., Loterija Slovenije, d. d.).

Informacijski pooblaščenec je podelil tudi posebno priznanje za napore na področju t. i. vgrajene zasebnosti, naziv ambasador zasebnosti 2012, ki ga je prejel Direktorat za informatiko in e-storitve na Ministrstvu za pravosodje in javno upravo za upoštevanje vgrajene zasebnosti pri svojem uspešnem delu na evropskih projektih STORK, SPOCS, STORK 2.0 in drugih ter pri izdelavi Analize možnosti za uvedbo varnejših in uporabniku prijaznejših e-identitet. Nagrajenec si je močno prizadeval za varno priznavanje e-identitet za državljane ter je tudi druge evropske države prepričal v potenciale t. i. STORK-pristopa, pri katerem bi državljani lahko od državnih organov po elektronski poti pridobili svoje osebne podatke in jih prav tako po elektronski poti posredovali naprej različnim ponudnikom storitev. Državljan ima pri takšnem pristopu nadzor nad tokovi svojih podatkov, obdelujejo pa se samo tisti osebni podatki, ki so resnično potrebni. Koncept vgrajene zasebnosti poudarja, da morajo biti premisleki o zasebnosti opravljeni že v začetku razvoja določene storitve in vgrajeni v njeno arhitekturo. Enako velja za poslovne prakse in tudi pripravo zakonodaje. Koncept temelji na proaktivnem delovanju in izogibanju težavam, ne pa na poznejšem odpravljanju posledic. Potencialne težave z vidika varstva osebnih podatkov in zasebnosti naj bi torej pravočasno predvideli ter oblikovanje sistema ali rešitve vnaprej prilagodili tako, da se tveganja za zlorabe zmanjšajo, namesto da bi čakali, da se ta tveganja uresničijo.

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 delovanja javnega sektorja ter zagotavljanja pogojev za učinkovitejšo participacijo državljanov pri odločanju o skupnih zadevah. Ob svetovnem dnevu pravice vedeti je Informacijski pooblaščenec 30. 9. 2013 organiziral delovni posvet na temo izvajanja ZDIJZ. Nataša Pirc Musar, informacijska pooblaščenka, in mag. Goran Klemenčič, predsednik Komisije za preprečevanje korupcije, sta predstavila razvoj tega področja, načrtovane spremembe zakonodaje ter vlogo in pomen transparentnega delovanja za preprečevanje korupcije in izgradnjo integritete. Predstavniki organov zavezancev so udeležence seznanili s primeri dobrih praks pri izvajanju ZDIJZ, predstavniki prosilcev (novinarjev in nevladnih organizacij) pa so izpostavili težave, s katerimi se srečujejo v praksi.

Informacijski pooblaščenec je 24. 10. 2013 organiziral mednarodno konferenco na temo ponovne uporabe javnih informacij. Konferenca je bila organizirana v okviru evropskega projekta, ki ga financira Evropska komisija in pri katerem kot eden izmed partnerjev sodeluje tudi Informacijski pooblaščenec. Gre za projekt LAPSI (Legal Aspects of Public Sector Information; http://www.lapsi-project.eu/), ki je namenjen izgradnji tematske mreže na področju ponovne uporabe informacij javnega značaja. Projekt vodi Katoliška univerza v Luevnu, pri njem pa sodeluje 23 partnerjev, strokovnjakov s številnih pravnih področij, ki se dotikajo informacij javnega značaja in njihove ponovne uporabe. Ena od oblik sodelovanja v okviru tega projekta so tudi tematske konference. Namen konference v Ljubljani je bil predstaviti novosti in izzive, ki jih prinaša sprememba Direktive 2003/98/ES Evropskega parlamenta in Sveta z dne 17. 11. 2003 o ponovni uporabi informacij javnega sektorja. Dogodek je bilo mogoče spremljati tudi v živo prek spleta.

Informacijski pooblaščenec je tudi leta 2013 nadaljeval preventivno delo in je veliko pozornosti namenil nadaljnji širitvi orodij in pripomočkov za dvig ozaveščenosti. Leta 2013 je Informacijski pooblaščenec zaradi varčevalnih ukrepov zelo omejil tisk svojih publikacij in tiskovin, izdal je le Letno poročilo Informacijskega pooblaščenca za leto 2012 v slovenščini. Ostale publikacije in letno poročilo za leto 2012 v angleščini so bili objavljeni zgolj v elektronski obliki. Poleg tega je pripravil smernice za posamezna področja varstva osebnih podatkov, ki so dostopne na spletni strani in zaradi varčevalnih ukrepov niso bile natisnjene, in sicer Smernice o inteligentni video analitiki ter Smernice o uporabi piškotkov na spletnih straneh. 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 ter 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 ter jih objavlja na svoji spletni strani ali na drug primeren način ter pripravlja in daje neobvezna navodila in priporočila glede varstva osebnih podatkov na posameznem področju.

Center za raziskovanje javnega mnenja Politbarometer je tudi leta 2013 v okviru projekta Javnomnenjske raziskave o odnosu javnosti do aktualnih razmer in dogajanj v Sloveniji izvedel več raziskav. Raziskava iz januarja 2013 vključuje tudi oceno uspešnosti delovanja državnih nadzornih organov. V ocenjevanje so bili vključeni informacijska pooblaščenka, varuhinja človekovih pravic, predsednik Računskega sodišča, guverner Banke Slovenije ter predsednik Komisije za preprečevanje korupcije. V raziskavi je navedeno, da so respondenti njihovo delovanje ocenili izrazito in visoko pozitivno (za razliko od ocene delovanja osrednjih državnih organov (državni zbor, vlada, predsednik vlade)). Na vrh se je umestila informacijska pooblaščenka Nataša Pirc Musar. Ob tem ne gre prezreti, da se je Informacijski pooblaščenec uvrstil najvišje med osrednjimi državnimi in družbenimi ustanovami, ki jim Slovenci najbolj zaupajo, tudi v raziskavah leta 2010, 2011 in 2012, kar 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 2011 v Ottawi, Kanada, sprejela odločitev,

da ustvari in javnosti predstavi skupno spletno stran vseh pooblaščencev. To zahtevno nalogo so informacijski pooblaščenci zaupali slovenskemu Informacijskemu pooblaščencu, ki je tako prevzel iniciativo in ustvaril spletno stran info-commissioners.org. 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 zdaj le-te sprejele, letna poročila pooblaščencev, novice o njihovem delovanju, informacije o pomembnih dogodkih, sprejetih prelomnih odločitvah itd. Informacijski pooblaščenec je za delovanje te spletne strani skrbel tudi leta 2013.

5.3. Mednarodno sodelovanje

5.3.1. Sodelovanje v mednarodnih delovnih telesih

Informacijski pooblaščenec kot državni nadzorni organ za varstvo osebnih podatkov sodeluje s pristojnimi organi 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 leta 2013 na ravni EU udeležil le najnujnejših plenarnih sestankov ter občasno še sestankov štirih izmed številnih podskupin Delovne skupine po 29. členu. Skupaj je tako Informacijski pooblaščenec sodeloval v osmih 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, v Tehnološki podskupini, v podskupini BCR in v podskupini BTLE),
- v Skupnem nadzornem organu za Europol,
- v Skupnem nadzornem organu za Schengen,
- v Skupnem nadzornem organu za carino,
- na koordinacijskih sestankih Evropskega nadzornika za varstvo osebnih podatkov in nacionalnih organov za varstvo osebnih podatkov za nadzor nad SIS II,
- na 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 nacionalnih organov za varstvo osebnih podatkov za nadzor nad VIS,
- na koordinacijskih sestankih Evropskega nadzornika za varstvo osebnih podatkov in nacionalnih organov za varstvo osebnih podatkov za nadzor nad 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 nadaljevala obravnavo različnih delov predloga reforme varstva osebnih podatkov. Glede predloga Uredbe o varstvu osebnih podatkov se je delovna skupina lani osredotočala predvsem na tiste njene dele, ki se nanašajo na možnost Evropske komisije, da izdaja izvedbene akte, sprejela je tudi dodatno mnenje o predlogu Direktive o varstvu osebnih podatkov na področju policijskega sodelovanja in pravosodnega sodelovanja v kazenskih zadevah. Delovna skupina je sprejela naslednja pomembna mnenja: Mnenje o varstvu osebnih podatkov pri aplikacijah za pametne naprave, Mnenje o omejitvi namena, dve Mnenji o predlogih za oceno učinka na varstvo podatkov za pametno omrežje in pametne merilne sisteme, ki jo je pripravila strokovna skupina projektne skupine za pametno omrežje pri Komisiji, Mnenje o pametnem nadzoru na mejah, Mnenje o ponovni uporabi informacij javnega značaja ter Delovni dokument o pridobivanju soglasja za piškotke. Predstavniki Informacijskega pooblaščenca so imeli pomembno vlogo pri pripravi mnenja o omejitvi namena, o ponovni uporabi informacij javnega značaja in pri pripravi delovnega dokumenta o pridobivanju soglasja za piškotke, pri katerih so sodelovali kot (so)predlagatelji in poročevalci na plenarnem sestanku.

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 (za spremembo krovne uredbe za področje varovanja osebnih podatkov), (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 leta 2013 nadaljevala razprave in pripravo mnenj za Delovno skupino po 29. členu glede reformnih predlogov za varstvo osebnih podatkov. Predstavniki Informacijskega pooblaščenca so v okviru Tehnološke podskupine kot (so) poročevalci aktivno sodelovali predvsem v okviru tematike piškotkov in izdelave modela za oceno resnosti incidenta pri poročanju o kršitvah varstva osebnih podatkov. Podskupina se je sicer leta 2013 ukvarjala tudi s pametnimi merilnimi sistemi, z računalništvom v oblaku, z novimi politikami zasebnosti, ki sta jih objavila Google in Microsoft, z internetom stvari, z različnimi standardizacijami ter s tehnikami anonimizacije. V okviru podskupine BCR je Informacijski pooblaščenec aktivno sodeloval pri pripravi Obrazložitvenega dokumenta o zavezujočih poslovnih pravilih za obdelovalce, ki je bil pozneje sprejet s strani Delovne skupine po 29. členu. Informacijski pooblaščenec je sodeloval tudi v podskupini BTLE, ki se je od Snowdnovega razkritja o obsežnem nadzoru posameznikov, tudi evropskih državljanov, s strani ameriške varnostno-obveščevalne službe, leta 2013 najprej osredotočala predvsem na pripravo mnenja o programih PRISM in drugih obveščevalnih programih za zbiranje podatkov. BTLE je poleg tega pripravila mnenje o sorazmernosti pri obdelavi osebnih podatkov s strani organov pregona ter mnenje o »Pametnih mejah«. Podskupina se je tudi leta 2013 ukvarjala z evidencami podatkov o potnikih v letalskem prometu ter z iznosom podatkov API v tretje države, z novim sistemom Mednarodnega združenja za zračni transport IATA, imenovanim NDC, s sporazumom EU-US TFTP2 ter s predlogom 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.

Informacijska pooblaščenka je bila marca 2013 izvoljena za predsednico Skupnega nadzornega organa za Europol. Člani tega nadzornega organa so predstavniki nacionalnih nadzornih organov za varstvo osebnih podatkov vseh držav članic EU, njegovo poslanstvo pa je, da v skladu s Sklepom Sveta o ustanovitvi Europola opravlja neodvisen pregled njegovih dejavnosti in tako zagotavlja, da med shranjevanjem, obdelavo in uporabo podatkov, ki jih ima Europol, niso kršene pravice posameznikov. Skupni nadzorni organ poleg tega spremlja tudi dopustnost prenosa podatkov, ki izhajajo iz Europola.

Informacijski pooblaščenec je aktivno sodeloval tudi v Mednarodni delovni skupini za varstvo osebnih podatkov v telekomunikacijah (IWGDPT – International Working Group on Data Protection in Telecommunications), v okviru katere se srečujejo predstavniki Informacijskih pooblaščencev in organov za varstvo osebnih podatkov in zasebnosti s celega sveta. Delovna skupina je na zasedanjih v Pragi in Berlinu sprejela naslednje štiri dokumente: Working Paper on Privacy and Aerial Surveillance, Working Paper on the Human Right to Telecommunications Secrecy, Working Paper and Recommendations on the Publication of Personal Data on the Web, Website Contents Indexing and the Protection of Privacy ter Working Paper on Web Tracking and Privacy: Respect for Context, Transparency and Control Remains Essential.

V okviru Sveta Evrope je predstavnik Informacijskega pooblaščenca tudi leta 2013 sodeloval kot član Posvetovalnega odbora (T-PD) po Konvenciji Sveta Evrope o varstvu posameznikov glede na avtomatsko obdelavo osebnih podatkov (Konvencija št. 108). Odbor T-PD po opravljenem glavnem strokovnem delu, pripravi besedila predlaganih sprememb, še vedno sodeluje v procesu posodabljanja Konvencije 108, ki se nadaljuje tudi v okviru posebnega ad hoc Odbora za varstvo osebnih podatkov Sveta Evrope (CAHDATA), ki bo pripravil končno besedilo spreminjevalnega protokola Konvencije 108. Biro Odbora T-PD je leta 2013 pripravil osnutek obrazložitvenega poročila modernizirane konvencije, Odbor pa je tudi pretežni del 30. plenarnega zasedanja lani oktobra posvetil obravnavi sprememb Konvencije. Tega plenarnega zasedanja se je kot nacionalni strokovnjak in hkrati predstavnik v CAHDATA udeležil predstavnik Ministrstva za pravosodje. Sodelovanje Informacijskega pooblaščenca se bo v okviru T-PD nadaljevalo in bo v sodelovanju z Ministrstvom za pravosodje do sprejema sprememb pretežno usmerjeno v posodabljanje Konvencije in druge tekoče naloge v skladu z dvoletnim programom Odbora.

5.3.2. Ostale mednarodne dejavnosti

IInformacijska pooblaščenka Nataša Pirc Musar je bila 19. julija 2013 s strani Evropske komisije imenovana v posebno ad hoc skupino EU–ZDA, katere naloga je bila ugotoviti dejansko stanje aktivnosti ameriške preiskovalne agencije (National Security Agency, NSA) glede množičnega zbiranja informacij in osebnih podatkov o državljanih EU. Nataša Pirc Musar je v posebni skupini sodelovala kot ena od petih vrhunskih evropskih strokovnjakov s področja varstva osebnih podatkov. Skupina je ob koncu svojega mandata za Evropsko komisijo pripravila poročilo o ugotovitvah.

Na podlagi 60. člena Sklepa Sveta 2007/533/PNZ o vzpostavitvi, delovanju in uporabi druge generacije Schengenskega informacijskega sistema ter 44. člena Uredbe (ES) št. 1987/2006 Evropskega parlamenta in Sveta o vzpostavitvi, delovanju in uporabi druge generacije Schengenskega informacijskega sistema (SIS II) je Informacijski pooblaščenec pristojen za neodvisni nadzor nad zakonitostjo obdelave osebnih podatkov v SIS II na svojem ozemlju in pri prenosu s svojega ozemlja. Leta 2013 Informacijski pooblaščenec ni prejel nobene pritožbe glede izvajanja te pravice na prvi stopnji.

Leta 2013 je v Republiki Sloveniji potekala evalvacija izvajanja schengenskega pravnega reda z vidika varstva osebnih podatkov, pri izvedbi katere je aktivno sodeloval tudi Informacijski pooblaščenec.

Informacijski pooblaščenec je leta 2013 gostil predstavnike sorodnih institucij iz Hrvaške, Bosne in Hercegovine ter Makedonije. Predstavil jim je svoje delovanje ter dobre prakse s področij, za katere je pristojen.

Informacijski pooblaščenec je leta 2013 pripravil odgovore na 45 vprašanj in vprašalnikov tujih organov za varstvo osebnih podatkov, mednarodnih organizacij in tujih nevladnih organizacij.

Leta 2013 je Informacijski pooblaščenec kot vodilni partner uspešno zaključil Twinning Light Project SR/2009/IB/JH/01 – Improvement of Personal Data Protection v Srbiji. Projekt se je osredotočal na izboljšanje varstva osebnih podatkov v Srbiji in krepitev nacionalnega nadzornega organa za varstvo osebnih podatkov, izobraževanje kadrov nadzornega organa, analizo in predloge sprememb pravnega okvira za varstvo osebnih podatkov v državi, pripravo kampanj osveščanja o varstvu osebnih podatkov, izobraževanje izbranih skupin upravljavcev in obdelovalcev osebnih podatkov ter tesnejše sodelovanje Srbije z EU na tem področju.

V okviru mednarodnega sodelovanja na področju dostopa do informacij javnega značaja je Informacijski pooblaščenec leta 2013 začel dvoletno sodelovanje v mednarodnem konzorciju pri projektu LAPSI 2.0, ki je namenjen nadaljevanju projekta LAPSI 1.0 in izgradnji tematske mreže strokovnjakov na področju ponovne uporabe informacij javnega značaja s ciljem odprave ovir v praksi za njeno izvajanje. V okviru sodelovanja pri tem projektu je Informacijski pooblaščenec oktobra 2013 v Ljubljani organiziral mednarodno konferenco na temo ponovne uporabe javnih informacij, katere namen je bila predstavitev novosti in izzivov, ki jih prinaša sprememba Direktive 2003/98/ES Evropskega parlamenta in Sveta o ponovni uporabi informacij javnega sektorja. Leta 2013 so se zaposleni pri Informacijskem pooblaščencu v okviru tega projekta udeležili sestankov v Leuvenu (Belgija), Pragi (Češka) in na Samosu (Grčija).

5.3.3. Sodelovanje na mednarodnih srečanjih

Leta 2013 so se zaposleni pri Informacijskem pooblaščencu udeležili le najnujnejših mednarodnih seminarjev in konferenc. Na večini spodaj navedenih srečanj so sodelovali s svojimi prispevki, udeležili pa so se jih na povabilo organizatorjev, ki so tudi krili stroške udeležbe.

- 9.–10. april 2013, Dublin, Irska: Europen Data Forum 2013,
- 10.–12. april 2013, Beograd, Srbija: Annual Conference of Supervisory Body in the Area of Protection of Personal Data in Central and Eastern Europe,
- 24. in 25. april 2013, Dunaj, Avstrija: Diskusija z Informacijskim pooblaščencem,

- 14.–18. maj 2013, Lizbona, Portugalska: Conference of the European Data Protection Authorities,
- 14. in 15. maj 2013, Priština, Kosovo – seminar v organizaciji ženevskega Centra za demokratični nadzor nad oboroženimi silami (Democratic Control of Armed Forces),
- 27. maj 2013, Potsdam, Nemčija: Mednarodni simpozij Open Data – Complementary Concept or Restriction of Freedom of Information,
- 19.–22. junij 2013, Vis, Hrvaška: Seminar Capacity Building and Exchange,
- 18. in 19. julij 2013, Kijev, Ukrajina: Posvet pri ombudsmanu,
- 31. avgust–3. september 2013, Vis, Hrvaška: Seminar Monitoring Public Procurments in Security Sector,
- 3.–5. september 2013, Krakov, Poljska: 23rd Economic Forum,
- 17.–20. september 2013, Berlin, Nemčija: 8th International Conference of Information Commissioners,
- 23.–26. september, Varšava, Poljska: 35. International Data Protection and Privacy Commissioners Cenference,
- 23. september 2013, Zagreb, Hrvaška: Konferenca Građani imaju pravo znati,
- 29. september–2. oktober 2013, Tunis, Tunizija: Konferenca Freedom of Access to Information: Issues and Challenges of Implementation,
- 2. in 3. oktober 2013, Sarajevo, Bosna in Hercegovina: 25 th Case Handling Workshop,
- 10. in 11. december 2013, Bruselj, Belgija: Europe Data Protection Congress,
- 12. december 2013, Zagreb, Hrvaška: Okrogla miza 10 godina prava na pristup informacijama u Republiki Hrvatskoj.

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
Jasna Duralija, svetovalka
Alenka Jerše, generalna sekretarka
Eva Kalan, svetovalka
Kristina Kotnik Šumah, namestnica informacijske pooblaščenke
Tina Kraigher, asistentka svetovalca
Blaž Pavšič, državni nadzornik za varstvo osebnih podatkov
mag. Andrej Tomšič, namestnik informacijske pooblaščenke

Oblikovanje:

mag. Matjaž Drev in Bons, d. o. o.

Lektorirala:

Katja Klopčič Lavrenčič

Informacijski pooblaščenec Republike Slovenije
Zaloška cesta 59
1000 Ljubljana

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

Ljubljana, maj 2014

ISSN 1854-9500