



INFORMACIJSKI POOBLAŠČENEC  
REPUBLIKE SLOVENIJE

'14

**Letno poročilo**

Informacijskega pooblaščenca

za leto 2014





'14

**Letno poročilo**

**Informacijskega pooblaščenca**

**za leto 2014**



# 0 UVOD



*Spoštovani,*

*pred vami je poročilo Informacijskega pooblaščenca za leto 2014. Informacijski pooblaščenec je v tem letu na področju dostopa do informacij javnega značaja izdal rekordno število odločb. Poleg vedno novih pravnih vprašanj, s katerimi se s sodelavci soočamo, pa se v praksi žal srečujemo tudi s primeri, ki bi morali biti davno preseženi in že dolgo ne bi smeli več predstavljati problema.*

*Na področju dostopa do informacij javnega značaja sicer ni dvoma, da je raven transparentnosti višja, da se javni sektor zaradi nadzora javnosti posledično bolj zaveda svojih odgovornosti ter da je državljanom s tem omogočeno učinkovitejše sodelovanje pri odločanju o skupnih zadevah. Pa vendar kljub temu ugotavljamo, da se nekateri javni organi še vedno premalo zavedajo, da bi morali delovati transparentno in da jim bodo zaupali le državljani, ki bodo o njihovem delovanju primerno informirani. To zgovorno ilustrira podatek, da je Informacijski pooblaščenec v minulem letu izdal več kot 280 odločb v pritožbenih zadevah s področja dostopa do informacij javnega značaja, največ v zadnjih desetih letih.*

*Informacijski pooblaščenec je leta 2014 na področju dostopa do informacij javnega značaja v reševanje prejel 578 pritožbenih zadev, od tega 320 pritožb zoper zavrnilne odločbe in 258 pritožb zaradi molka organa. Prosilci in zavezanci so se na nas v 297 primerih obrnili s prošnjo za mnenje oz. pojasnilo; skupaj je bilo tako obravnavanih 875 zadev. Število pritožb zoper zavrnilne odločbe prvostopenjskih organov se je leta 2014 povečalo; leto poprej je bilo namreč teh pritožb (le) 271.*

*Iz Skupnega letnega poročila o izvajanju Zakona o dostopu do informacij javnega značaja za leto 2014, ki ga je sprejela Vlada RS, sicer izhaja, da naj bi število pritožbenih postopkov upadalo, vendar pa velja opozoriti, da se poročilo Vlade RS nanaša le na ožji državni sektor (državne organe in organe samoupravnih lokalnih skupnosti) ter zajema le okoli 500 zavezancev, Informacijski pooblaščenec pa je kot pritožbeni organ pristojen za več tisoč zavezancev. Glede na to, da je število pritožbenih postopkov zoper državne organe in organe samoupravnih lokalnih skupnosti leta 2014 padlo, gre torej zaključiti, da je naraslo število pritožbenih postopkov zoper zavezance iz širšega javnega sektorja.*

*Leta 2014 je naše delo na tem področju zaznamovala tudi novela Zakona o dostopu do informacij javnega značaja (ZDIJZ-C), ki je razširila krog zavezancev tudi na poslovne subjekte pod prevladujočim vplivom oseb javnega prava. Zlasti ti, t. i. novi zavezanci niso dovolj seznanjeni z obveznostmi, ki jim jih nalaga zakon in praviloma zavračajo tudi posredovanje tistih podatkov, za katere zakon določa absolutno javnost. Ker gre za povsem novo področje, kjer se praksa šele vzpostavlja, je Informacijski pooblaščenec od aprila 2014 dejansko zaznal porast zadev na tem področju.*

Glede na številne novosti, ki jih prinaša ZDIJZ-C, ocenjujemo, da je treba (še) več n-pora vložiti v promocijo pravice dostopa do informacij javnega značaja in v usposabljanje zavezancev za uporabo zakona v praksi. Tudi leta 2014 je Informacijski pooblaščenec zato izvajal različne pedagoške dejavnosti in upošteva svoje pristojnosti svetoval tako organom kot prosilcem. Prav s širjenjem znanja se namreč lahko učinkovito izognemo tistim pritožbenim postopkom, ki izvirajo zgolj iz nezadostne komunikacije med proslcem in organom zavezancem ali iz pomanjkljivega poznavanja prava dostopa do informacij javnega značaja. Kot drugostopenjski organ ugotavljamo, da so prosilci z ustavno pravico dostopa do informacij dobro seznanjeni in jo zato v praksi pogosto uresničujejo, obenem pa je pri zavezancih (tudi zaradi pomanjkanja kadrovskih in finančnih virov) še vedno zaznati nepoznavanje obveznosti, ki jim jih nalaga Zakon o dostopu do informacij javnega značaja. Prav zato je Informacijski pooblaščenec v minulem letu izvedel predstavitve za nove zavezance po ZDIJZ-C, v sodelovanju z Ministrstvom za javno upravo pa je bila zanje izdana tudi posebna brošura s pojasnili o pomenu novele ZDIJZ-C.

Četudi si v zadnjih letih organi javnega sektorja vse bolj prizadevajo za večjo transparentnost, je Informacijski pooblaščenec leta 2014 odločal v nekaj odmevnih primerih. Tako je na primer Banki Slovenije naložil razkritje podatkov iz pogodb, ki jih je sklenila za izvedbo stresnih testov v bankah, Ministrstvu za finance razkritje podatkov o kupcu zaprte izdaje državnih obveznic, Mestni občini Maribor pa razkritje sporazuma o poravnavi med Mednarodno univerzitetno športno zvezo, Slovensko univerzitetno športno zvezo in Mestno občino Maribor, ki se nanaša na odškodnino zaradi odpovedi zimske univerzijade. Presojal je javnost odločb Banke Slovenije o izrednih ukrepih zoper pet poslovnih bank, ki so bile dokapitalizirane iz javnih sredstev, in odločil, da so to prosto dostopne informacije. Državnemu izpitnemu centru je naložil, da mora javnosti posredovati podatke o povprečnih dosežkih učencev in učenk na nacionalnem preizkusu znanja iz določenih predmetov po šolah, DUTB je izdal odločbo, da morajo biti določene informacije iz zapisnikov sej upravnega odbora, ki se nanašajo na izbiro zunanjih svetovalcev, javno dostopne. Informacijski pooblaščenec je odločil tudi, da mora NKBM, kot poslovni subjekt pod prevladujočim vplivom, javnosti posredovati podatke o avtorskih, sve-tovalnih in intelektualnih storitvah, ki so po zakonu absolutno javni.

Ugodeno je bilo tudi pritožbi novinarja, ki je zahteval dostop do magnetograma 69. seje Vlade RS, na kateri se je ta seznanila s predlogom za imenovanje kandidatov za člana Evropske komisije. Pri zavrnitvi zahteve se je Vlada RS sklicevala na izjemi varstva tajnih podatkov in varstva notranjega delovanja, vendar po oceni Informacijskega pooblaščenca ni izkazala obstoja teh izjem od prostega dostopa, zato je bilo treba te informacije javnosti razkriti.

Informacijski pooblaščenec že od leta 2009 opozarja tudi na problematiko zaračunavanja stroškov dela v postopku dostopa do informacij javnega značaja, saj meni, da mora višina stroškov izvrševanja te pravice ostati v najmanjšem možnem obsegu ter ne sme pretirano ovirati dostopa do informacij javnega značaja. Nesprejemljivo je, da se stroški dela javnih uslužbencev obračunavajo po urnih postavkah in se tako »prevalijo« na novinarje in druge prosilce, četudi dostop do informacij javnega značaja ni v celoti brezplačen. Iz veljavne ureditve namreč izhaja, da se za posredovanje lahko zaračunajo le materialni stroški, med katere pa stroški dela javnih uslužbencev, ki za svoje delo že prejemajo plačo iz proračuna, brez dvoma ne sodijo.

Posebno mesto v pravu informacij javnega značaja bi moral imeti institut ponovne uporabe informacij javnega značaja (angl. re-use), ki v slovenskem prostoru še ni zaživel. Leta 2014 je Informacijski pooblaščenec obravnaval osem pritožbenih zadev, kar je sicer več kot leto prej (šest pritožb), vendar pa relativno majhno število pritožb kaže tudi na to, da so prosilci slabo seznanjeni s pravnimi možnostmi, ki jih imajo v primeru, kadar jim zavezanci vlogo za ponovno uporabo zavrnejo. Področje ponovne uporabe javnih informacij ima pomemben gospodarski potencial, ki je v praksi žal še vedno premalo izkoriščen.

Poleg pravnega področja dostopa do informacij javnega značaja pa pogled na področje varstva osebnih podatkov kaže na veliko vlogo Informacijskega pooblaščenca pri preprečevanju nezakonitosti ter neupravičenih posegov v zasebnost in dostojanstvo posameznika pri obdelavi osebnih podatkov. Nove tehnologije, zlasti informacijske, so že davno prerasle »tradicionalne« oblike zbiranja, obdelave in objave osebnih podatkov, zato se je bistveno povečala ogroženost naše zasebnosti. Nastajajo najrazličnejše velike in zelo povedne baze osebnih podatkov, upravljavci pa si prizadevajo, da bi osebne podatke čim učinkoviteje izkoristili za različne namene. Pravica do zasebnosti je danes ena najbolj cenjenih človekovih pravic, a

obenem zaradi razvoja sodobnih tehnologij tudi ena najbolj ranljivih, saj pravo zaradi svojega reakcijskega časa neizogibno zaostaja za razvojem sodobnih tehnologij. Prav zato so prijave, ki jih dobivamo, vse pogostejše povezane prav z uporabo teh tehnologij: neupravičen video-nadzor in zvočno snemanje, sledenje z GPS, nadzor uporabe spleta in elektronske pošte s strani delodajalcev, uporaba biometrije, nedopustna razkrivanja elektronskih naslovov, neposredno trženje, piškotki na spletu ...

Informacijski pooblaščenec je leta 2014 na področju varstva osebnih podatkov vodil 628 postopkov inšpekcijskega nadzora, 95 prekrškovnih postopkov, štiri postopke ugotavljanja upravičenosti izvajanja biometrijskih ukrepov, 11 postopkov izdajanja dovoljenj za iznos osebnih podatkov iz države, 14 postopkov izdajanja dovoljenj za povezovanje zbirk osebnih podatkov, 67 postopkov odločanja o pritožbah v zvezi s pravico posameznika do seznanitve z lastnimi osebnimi podatki. V okviru preventivnega delovanja pa je Informacijski pooblaščenec na področju varstva osebnih podatkov sodeloval z upravljavci osebnih podatkov, odgovarjal na pisna in ustna vprašanja posameznikov in upravljavcev osebnih podatkov, sproti obveščal javnost o vseh pomembnejših ugotovitvah in dogodkih s tega področja ter izdelal več kot 2.000 pisnih mnenj.

Leto 2014 je zaznamovalo nekaj odmevnih inšpekcijskih primerov; nekaj jih v poročilu posebej osvetljujemo. Beležili smo izrazit porast nezakonitega izvajanja videonadzora in zvočnega snemanja. Oboje se odraža v številnih vprašanjih in prijavah. Velikokrat smo se srečali z vprašanjem dopustnosti snemanja pogovorov in razprav na sejah in sestankih, na katerih je ob odsotnosti zakonskega temelja za tak poseg potrebna vnaprejšnja privolitev udeleženih posameznikov. Velja namreč splošno pravilo, po katerem je za vsak poseg v varstvo osebnih podatkov potreben pravni temelj. Pravica do varstva osebnih podatkov temelji na možnosti posameznika, da sam odloča, komu in za katere namene bo zaupal svoje osebne podatke. V primeru snemanja različnih razgovorov, sestankov, sej občinskih svetov in drugih organov morajo biti posamezniki predhodno seznanjeni, kdo bo upravljavec takšnih posnetkov, za katere namene se bodo posnetki uporabljali, koliko časa se bodo shranjevali, kdo bo eventualni uporabnik teh posnetkov ipd. Napredek tehnike in posledično dejstvo, da so tehnične naprave, ki omogočajo zvočno snemanje, poceni in dostopne komur koli, ne smeta postati izgovor za posege v zasebnost in varstvo osebnih podatkov posameznikov, še manj za njihovo toleriranje. Prav nasprotno – potreben je tehten premislek o njihovi uporabi, ki mora biti ne le skladna z zakonom, temveč tudi z občimi človeškimi standardi na področju zasebnosti in varstva osebnih podatkov.

V javnosti odmevni dogodki pa vedno razkrivajo, kako hudi posegi v zasebnost se nam v resnici dogajajo in kako nemočni smo kot posamezniki. Ob takih dogodkih je pričakovanje javnosti tako veliko, da Informacijski pooblaščenec le težko pojasni svojo nepristojnost. Iskrena želja vseh, ki delamo pri Informacijskem pooblaščenecu, da bi v posameznih primerih vendarle lahko pomagali, pa ni dovolj. Informacijski pooblaščenec namreč mora enako kot vsi organi javnega sektorja spoštovati načelo zakonitosti in sme ukrepati le v okviru z zakonom zaupanih mu pristojnosti. Eden takih dogodkov, ko je javnost pričakovala tudi ukrepanje Informacijskega pooblaščenca, je bila objava posnetka dogajanja na eni od mariborskih srednjih šol. V konkretnem primeru je bil podan sum storitve kaznivega dejanja, ni pa šlo za kršitev zakona o varstvu osebnih podatkov. Ker Informacijski pooblaščenec v zvezi s tem dogodkom ni imel nobenih pristojnosti in zato nobenih možnosti za ukrepanje, se tudi ni odzval na zahteve po podajanju sodb. S sodelavci smo trdno zavzeli stališče, da se moramo organi javnega sektorja izogibati vrednostnim ocenam, saj namen našega delovanja ni medijska prepoznavnost. Mejo smo dolžni začrtati tako, da lahko svoje delo opravljamo strokovno in profesionalno ter ne glede na to, ali je naše ravnanje od javnosti pričakovano in medijsko odmevno ali celo všečno.

Leto 2014 pa je bilo tudi prelomno. Predvsem zaradi sodbe Sodišča EU, ki je spletne iskalnike – konkretno Google –, prvič prepoznalo kot upravljavce osebnih podatkov. To pomeni, da tudi zanje velja obveznost izbrisa netočnih, neažurnih, nepopolnih podatkov o posameznikih, ki jih spletni iskalnik prikaže med rezultati iskanja po posameznikovem osebnem imenu. Za zagotovitev posameznikove pravice mora biti umik rezultatov, seveda ob izpolnjenih pogojih, izveden na vseh relevantnih domenah tako, da so njegove pravice učinkovito in polno varovane.

Lani so v javnosti postajale vedno bolj aktualne razprave in pomisleki o civilni uporabi brez-pilotnih letalnikov, opremljenih z najrazličnejšimi senzorji, ki omogočajo posege v našo za-



sebnost. Informacijski pooblaščenec ocenjuje, da to nedvomno kaže na nujnost regulacije tega področja, tako na nacionalni kot na evropski ravni, saj se le z ustrežno normativno ureditvijo lahko zagotovi njihovo varno uporabo in obenem spoštuje temeljne človekove pravice. Prepričani smo, da identifikacija brezpilotnih letalnikov in nadzor nad njimi v zračnem prostoru ne bosta mogoča brez sistema upravnih dovoljenj. Področje komercialne uporabe brezpilotnih letalnikov terja nove in učinkovite pristope za varstvo osebnih podatkov, kot so predhodne presoje vplivov, nove metode obveščanja posameznikov ter okrepljene aktivnosti za dvig ozaveščenosti pri operaterjih brezpilotnih letalnikov, ki se lahko vključijo v postopke izdaje ustreznih dovoljenj.

Velike izzive na področju varstva osebnih podatkov in zasebnosti prinaša tudi t. i. koncept big data, pri katerem gre za obdelavo velikih količin kompleksnih in praviloma nestrukturiranih podatkov iz medsebojno neodvisnih podatkovnih virov z namenom identifikacije in napovedovanja trendov in korelacij. Velike množice podatkov omogočajo veliko – lahko se napove širjenje epidemij, odkriva povezave med učinki različnih zdravil, možno pa je tudi profiliranje posameznikov, napovedovanje njihovega vedenja in sprejemanja odločitev, ki imajo lahko občutne posledice za posameznika. Zato je v dobi izobilja podatkov še toliko pomembnejše, celo nujno opozarjati, da ostajajo temeljna načela varstva osebnih podatkov, kot so minimizacija in sorazmernost obdelave, usklajenost z namenom obdelave, transparentnost in pravice posameznika glede lastnih osebnih podatkov. Opuščanje teh temeljnih načel bi lahko vodilo v povečano profiliranje in avtomatizirano odločanje, npr. o tem, ali smo kot posamezniki primerni za pridobitev kredita ali službe, kakšno zdravstveno zavarovanje bomo imeli in kakšni paketi energetskih ali telekomunikacijskih storitev nam bodo ponujeni.

Med izredno pomembne naloge Informacijskega pooblaščenca sodi tudi zagotavljanje systemskega uresničevanja varstva osebnih podatkov in sodelovanje z resornimi ministrstvi pri pripravi predpisov, ki posegajo na področje varstva osebnih podatkov. Cilj je seveda zagotavljanje zakonite obdelave osebnih podatkov v okviru novih oblik in načinov obdelave osebnih podatkov ter vzpostavljanja novih zbirk. Informacijski pooblaščenec pa je žal tudi v lanskem letu zaznal nadaljevanje trenda priprave predlogov zakonov, ki pomenijo resne posege v zasebnost zaradi obdelave osebnih podatkov, a se sprejemajo brez ustrežnih analiz in ocen posledic, ki jih bodo imeli za ustavno zagotovljeno varstvo zasebnosti. Številna ministrstva namreč ob pripravi zakonov teh niso pošiljala v usklajevanje Informacijskemu pooblaščenca, kar seveda pozneje povzroča težave v praksi in nujne zahteve za ocene ustavnosti.

Tak primer je bila tudi pooblaščenčeva zahteva za oceno ustavnosti tistih členov Zakona o elektronskih komunikacijah, ki so določali obvezno hrambo podatkov o prometu elektronskih komunikacij. Ustavno sodišče RS je posledično julija 2014 razveljavilo člene zakona, ki so pomenili nesorazmerne posege v zasebnost prav vsakega od nas povsem brez povoda, zakon pa je predvideval tudi predolgo hrambo teh podatkov. Informacijski pooblaščenec je odločitev Ustavnega sodišča sprejel z velikim zadovoljstvom, saj gre za zelo pomemben korak v varstvu pravic posameznikov do zasebnosti. Ustavno sodišče je prepoznalo pomen varstva osebnih podatkov v odnosu do modernih komunikacijskih tehnologij, še posebej kadar so te uporabljene s strani državnih represivnih organov oz. je namen izvajanje njihovih pristojnosti. Odločitev Ustavnega sodišča predstavlja pomemben prispevek k razpravi o nujnosti in sorazmernosti uporabe nadzorovalnih tehnologij v kontekstu kazenskih postopkov in delovanja obveščevalnih služb. Informacijski pooblaščenec na problem pretiranih posegov državnih organov v zasebnost posameznikov redno opozarja. Veliko skrb vzbujajoči so namreč primeri, ko se z namenom lažje identifikacije storilca kaznivega dejanja ali prekrška izvaja splošen nadzor, ki prizadene zasebnost vseh – torej pretežno tistih, ki pravila prostovoljno spoštujejo in državi niso dali nobenega povoda za ukrepanje. Običajno je prav vse lažja dostopnost novih tehnologij vodila k težnjam po uvajanju novih pooblastil organov pregona. V praksi to pomeni zlasti brezpilotne letalnike in IMSI-lovilce.

Čeprav je mednarodno sodelovanje za zagotavljanje kakovostnega dela Informacijskega pooblaščenca zelo pomembno, je leto 2014 zaznamovalo varčevanje. Zato smo se zaposleni udeležili le nekaterih najnujnejših mednarodnih seminarjev in konferenc, na katerih smo sodelovali tudi s svojimi prispevki. Informacijski pooblaščenec je redno sodeloval v Delovni skupini 29, ki združuje vse varuhe zasebnosti v Evropski uniji (EU) in daje Evropski komisiji strokovna mnenja s področja varstva osebnih podatkov in številnih drugih organih Evropske skupnosti ter Sveta Evrope. Zaradi zmanjšanja proračunskih sredstev smo se udeležili le plenarnih sestankov ter sestankov štirih izmed sicer številnih podskupin Delovne skupine 29. Poleg tega se je Informacijski pooblaščenec kot nacionalni nadzorni organ za posamezna področja obdelave



osebnih podatkov na ravni EU udeleževal le najnujnejših plenarnih sestankov nadzornih organov za Schengenski informacijski sistem, Europol, Carinski informacijski sistem in Eurodac. Udeležili smo se tudi zasedanj Mednarodne delovne skupine za telekomunikacije (IWGDPT) ter odbora TP-D pri Svetu Evrope.

Informacijski pooblaščenec že vrsto let sistematično spremlja prakso in zbira mnenja na posameznih življenjskih področjih ter nato izda smernice, ki so se v praksi pokazale za zelo uporabne, tako za upravljavce zbirk osebnih podatkov kot tudi za posameznike. Izdali smo jih tudi leta 2014 – dotaknili smo se (ne)dopustnosti uporabe GPS-sledilnih naprav, posebno pozornost pa namenili nujnosti izdelave predhodne presoje vplivov na zasebnost pri vsakokratnem uvajanju novih policijskih pooblastil.

Kljub številnim vprašanjem, na katera je že bilo odgovorjeno, Informacijskega pooblaščenca čakajo še mnogi izzivi, ki jih prinaša sodobni čas. Soočamo se s pomanjkanjem pravnih norm pri obdelovanju osebnih podatkov s sodobnimi tehnologijami. Te pa že dolgo niso več znanstvena fantastika – brezpilotni letalniki, pametni videonadzor, internet stvari, trojanski konji, big data, avtomatska prepoznavna registrskih tablic, nove oblike biometrije, vsak dan pametnejši telefoni in naprave, neskončna možnost profiliranja in avtomatiziranega odločanja. Obstoječa pravna podlaga ne ustreza več današnjemu načinu življenja, ki ga krojijo sodobne tehnologije; te nam dajejo veliko, a hkrati v zameno pričakujejo tudi veliko naših podatkov. V postopku sprejemanja v EU je zato Splošna uredba o varstvu osebnih podatkov. Novosti oz. dolžnosti za upravljavce zbirk osebnih podatkov bo veliko, posamezniki pa naj bi dobili več pravic, tudi t. i. pravico do pozabe oz. pravico do izbrisa podatkov, ki se obdelujejo brez zakonite podlage. Pravo mesto pa končno dobiva tudi načelo vgrajene zasebnosti, ki nas opozarja, da se je z varstvom osebnih podatkov treba ukvarjati vedno na začetku, torej pred vsakokratnim uvajanjem novih ukrepov in sistemov za obdelavo podatkov, ne šele po tem, ko posameznik že utrpi škodo.

Namesto zaključka: Pravica dostopa do informacij javnega značaja in pravica do varstva osebnih podatkov sta temeljni človekovi pravici, pri nas zapisani v Ustavi. Bodimo ponosni nanju in zahtevajmo, da se uresničujeta v največji možni meri. Obe imata pomembno vlogo v družbi in sta odločilen pokazatelj njene demokratičnosti. Predvsem pa sta civilizacijska pridobitev in neprecenljivi vrednoti.

Mojca Prelesnik,  
informacijska pooblaščenka



**1. INFORMACIJSKI POOBLAŠČENEC**

1.1.	Nastanek Informacijskega pooblaščenca	1
1.2.	Pristojnosti Informacijskega pooblaščenca	1
1.3.	Organiziranost Informacijskega pooblaščenca	5
1.4.	Finančna sredstva Informacijskega pooblaščenca	7

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

2.1.	Pravna ureditev na področju dostopa do informacij javnega značaja v Republiki Sloveniji	13
2.2.	Število vloženih pritožb in število rešenih zadev	15
2.3.	Število vloženih tožb na Upravnem sodišču Republike Slovenije, število sodb Upravnega in Vrhovnega sodišča Republike Slovenije	16
2.4.	Statistika po posameznih področjih ZDIJZ	17
2.5.	Storjeni prekrški po ZDIJZ, ZInFP in ZMed	20
2.6.	Predstavitev najodmevnejših in precedenčnih primerov po področjih	21
2.6.1.	Stresni testi, poslovna skrivnost	21
2.6.2.	Ponovna uporaba	22
2.6.3.	Osebni podatki	23
2.6.4.	Poslovna skrivnost	24
2.6.5.	Proaktivna objava	26
2.6.6.	Dokument v izdelavi	27
2.6.7.	Notranje delovanje organa	28
2.6.8.	Poslovni subjekt pod prevladujočim vplivom, poslovna skrivnost	29
2.6.9.	Poslovna skrivnost	30
2.6.10.	Tajni podatki, notranje delovanje organa	31
2.6.11.	Tajni podatki, test javnega interesa	33
2.6.12.	Okoljski podatki	34
2.7.	Splošna ocena in priporočila na področju dostopa do informacij javnega značaja	36

**3. DELO NA PODROČJU VARSTVA OSEBNIH PODATKOV**

3.1.	Koncept varstva osebnih podatkov v Republiki Sloveniji	39
3.2.	Dejavnost državnih nadzornikov za varstvo osebnih podatkov	40
3.2.1.	Pravice in dolžnosti državnega nadzornika	40
3.2.2.	Inšpekcijski nadzor	40
3.2.2.1.	Inšpekcijski nadzor v javnem sektorju	41

3.2.2.2. Inšpekcijski nadzor v zasebnem sektorju	42
3.2.3. Storjeni prekrški	44
3.3. Dajanje pisnih mnenj in pojasnil	46
3.4. Dopustnost izvajanja biometrijskih ukrepov	47
3.5. Ugotavljanje ustrezne ravni varstva osebnih podatkov v tretjih državah	50
3.6. Izdajanje dovoljenj za povezovanje javnih evidenc	55
3.7. Seznanitev z lastnimi osebnimi podatki	57
3.8. Zahteve za oceno ustavnosti	59
3.8.1 Odločitev Ustavnega sodišča RS v zvezi z oceno ustavnosti in zakonitosti XIII. poglavja Zakona o elektronskih komunikacijah	59
3.9. Izbrani primeri kršitev varstva osebnih podatkov	60
3.9.1. Ustvarjanje nove zbirke osebnih podatkov iz podatkov, objavljenih na spletu, in njeno trženje	60
3.9.2. Nezakoniti vpogledi oz. preusmeritev e-pošte zaposlenih	62
3.9.3. Posredovanje osebnih podatkov dolžnikov slovenskemu odvetniku, ki je zastopal hrvaško družbo zaradi neplačila parkirnine	63
3.9.4. Zbiranje osebnih podatkov zaposlenih	64
3.9.5. Izvajanje videonadzora v domu upokojencev	65
3.9.6. Izvajanje videonadzora na vhodu v krajinski park	67
3.9.7. Razkrivanje osebnih podatkov učencev ob prijavi na šolski obrok	68
3.10. Splošna ocena stanja varstva osebnih podatkov in priporočila	69

#### **4. DRUGE DEJAVNOSTI INFORMACIJSKEGA POOBLAŠČENCA**

4.1. Sodelovanje pri pripravi zakonov in drugih predpisov	75
4.2. Sodelovanje z javnostmi	77
4.3. Mednarodno sodelovanje	79
4.3.1. Sodelovanje v mednarodnih delovnih telesih	79
4.3.2. Ostale mednarodne dejavnosti	81
4.3.3. Sodelovanje na mednarodnih srečanjih	82



**1** INFORMACIJSKI POOBLAŠČENEC

## 1.1. Nastanek Informacijskega pooblaščenca

Državni zbor RS je 30. 11. 2005 sprejel Zakon o Informacijskem pooblaščenju<sup>1</sup>, s katerim je bil 31. 12. 2005 ustanovljen nov samostojen in neodvisen državni organ. Omenjeni zakon je združil dva organa, in sicer Pooblaščenca za dostop do informacij javnega značaja, ki je imel že prej status neodvisnega organa, in Inšpektorat za varstvo osebnih podatkov, ki je deloval kot organ v sestavi Ministrstva za pravosodje. Ob uveljavitvi ZInfp je Pooblaščenec za dostop do informacij javnega značaja nadaljeval delo kot Informacijski pooblaščenec, ki je prevzel inšpektorje in druge uslužbenke Inšpektorata za varstvo osebnih podatkov, pripadajočo opremo in sredstva. Hkrati je prevzel tudi vse nedokončane zadeve, arhive in evidence, ki jih je vodil Inšpektorat za varstvo osebnih podatkov. S tem so se pristojnosti organa, ki je skrbel za nemoteno izvajanje dostopa do informacij javnega značaja, močno spremenile in se razširile še na 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.

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

Od ustanovitve Informacijskega pooblaščenca do 17. 7. 2014 je bila informacijska pooblaščenka Nataša Pirc Musar. Navedenega dne je predala posle novi informacijski pooblaščenki Mojci Prelesnik, ki je tako nastopila svoj petletni mandat.

## 1.2. Pristojnosti Informacijskega pooblaščenca

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 krtil pravico do dostopa ali ponovne uporabe informacije javnega značaja, ter v okviru postopka na drugi stopnji tudi za nadzor nad izvajanjem zakona, ki ureja dostop do informacij javnega značaja, in za nadzor na 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<sup>2</sup> (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<sup>3</sup>.

<sup>1</sup> Uradni list RS, št. 113/2005, 51/2007 – ZUstS-A; v nadaljevanju ZInfp.

<sup>2</sup> Uradni list RS, št. 110/2006 – uradno prečiščeno besedilo 1, s spremembami; v nadaljevanju ZMed.

<sup>3</sup> Uradni list RS, št. 51/2006 – uradno prečiščeno besedilo 2, s spremembami; v nadaljevanju ZDIJZ.

Na področju varstva osebnih podatkov ima Informacijski pooblaščenec pristojnosti, ki mu jih dajeta Zakon o varstvu osebnih podatkov<sup>4</sup> in 2. člen ZInFP, in sicer:

- 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 planirani – preventivni inšpekcijski nadzor pri upravljavcih osebnih podatkov s področja javnega in zasebnega sektorja) – pristojnost je določena v 2. členu ZInFP;
- odloča o pritožbi posameznika, kadar upravljavec osebnih podatkov ne ugotovi zahtevi posameznika 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);
- vodi postopke o prekrških s področja varstva osebnih podatkov (hitri postopek);
- vodi in vzdržuje register zbirk osebnih podatkov in skrbi, da je register ažuren ter javno dostopen prek svetovnega spleta (28. člen ZVOP-1);
- omogoča vpogled in prepis podatkov iz registra zbirk osebnih podatkov, praviloma isti dan, najpozneje pa v osmih dneh (29. člen ZVOP-1);
- odloča o ugovoru posameznika glede obdelave osebnih podatkov na podlagi četrtega odstavka 9. člena in tretjega odstavka 10. člena ZVOP-1;
- izdaja odločbe o zagotavljanju ustrezne ravni varstva osebnih podatkov v tretjih državah (63. člen ZVOP-1);
- vodi postopke ugotavljanja ustrezne ravni varstva osebnih podatkov v tretjih državah na podlagi ugotovitev inšpekcijskega nadzora in drugih informacij (64. člen ZVOP-1);
- vodi seznam tretjih držav, 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);
- vodi upravne postopke za izdajo dovoljenj o iznosu osebnih podatkov v tretjo državo (70. člen ZVOP-1);
- vodi upravne postopke za izdajo dovoljenj za povezovanje javnih evidenc in javnih knjig, kadar katera od zbirk osebnih podatkov, ki naj bi se jih povezovalo, vsebuje občutljive osebne podatke ali pa je za izvedbo povezovanja potrebna uporaba istega povezovalnega znaka (npr. EMŠO ali davčna številka) – 84. člen ZVOP-1;
- 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);
- sodeluje z državnimi organi, pristojnimi organi EU 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;
- daje in objavlja predhodna mnenja državnim organom ter nosilcem javnih pooblastil o usklajenosti določb predlogov predpisov z zakoni in drugimi predpisi, ki urejajo osebne podatke;
- daje in objavlja neobvezna mnenja o skladnosti kodeksov poklicne etike, splošnih pogojev poslovanja oz. njihovih predlogih s predpisi s področja varstva osebnih podatkov;
- pripravlja, daje in objavlja neobvezna navodila in priporočila glede varstva osebnih podatkov na posameznem področju;
- na spletni strani in na drug ustrezen način objavlja predhodna mnenja o usklajenosti predlogov zakonov in drugih predpisov z zakonom in drugimi predpisi s področja varstva osebnih podatkov ter zahtev 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);
- daje izjave za javnost o opravljanju nadzorih in pripravlja letna poročila o svojem delu v preteklem letu;

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

- 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 členu 29 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 Europol ter v skupini za nadzor Eurodaca).

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

Informacijski pooblaščenec lahko v skladu s 6. alinejo prvega odstavka 23.a člena Zakona o ustavnem sodišču<sup>5</sup> z zahtevo začne postopek za oceno ustavnosti oz. zakonitosti predpisa ali splošnega akta, izdanega za izvrševanje javnih pooblastil, če nastane vprašanje ustavnosti ali zakonitosti v zvezi s postopkom, katerega vodi.

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, vnešenih 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<sup>6</sup>, Zakonu o potnih listinah<sup>7</sup> in Zakonu o osebni izkaznici<sup>8</sup>.

Pristojnosti Informacijskega pooblaščenca na podlagi ZPacP so:

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

Pristojnosti Informacijskega pooblaščenca po ZPLD-1 in ZOIZk-1 so omejene na določbe, ki urejajo, v kakšnih 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<sup>9</sup>:

- podaja soglasja upravljavcem sistema SISBON pred začetkom uporabe pravil sistema iz 1. točke trinajstega odstavka 309.a člena ZBan-1, ki določa, da mora upravljavec sprejeti pravila sistema, v katerih določi tehnične pogoje za dostop članov do sistema in druge ukrepe za zavarovanje osebnih podatkov (štirinajsti odstavek 390.a člena ZBan-1);
- izvaja nadzor nad 309.a členom ZBan-1, ki ureja zbiranje in obdelovanje ter sistem

<sup>5</sup> Uradni list RS, št. 64/2007 – uradno prečiščeno besedilo 1, 109/2012.

<sup>6</sup> Uradni list RS, št. 15/2008; v nadaljevanju ZPacP.

<sup>7</sup> Uradni list RS, št. 29/2011 – uradno prečiščeno besedilo 4; v nadaljevanju ZPLD-1.

<sup>8</sup> Uradni list RS, št. 35/2011; v nadaljevanju ZOIZk-1.

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

izmenjave informacij o boniteti strank (sistem SISBON) in skladno s 397. členom ZBan-1 vodi postopke o prekršku zaradi kršitve določb 309.a člena ZBan-1 (deseti do petnajsti odstavek 397. člena ZBan-1).

Pristojnosti, ki jih je imel Informacijski pooblaščenec na podlagi Zakona o elektronskih komunikacijah<sup>10</sup>, so se s sprejetjem novele zakona konec leta 2012 povečale na:

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

Leta 2013 je Informacijski pooblaščenec s spremembo Zakona o potrošniških kreditih<sup>11</sup> pridobil novo pristojnost. 36. člen ZPotK-1 določa, da Informacijski pooblaščenec opravlja nadzor nad dajalci kreditov glede izvajanja:

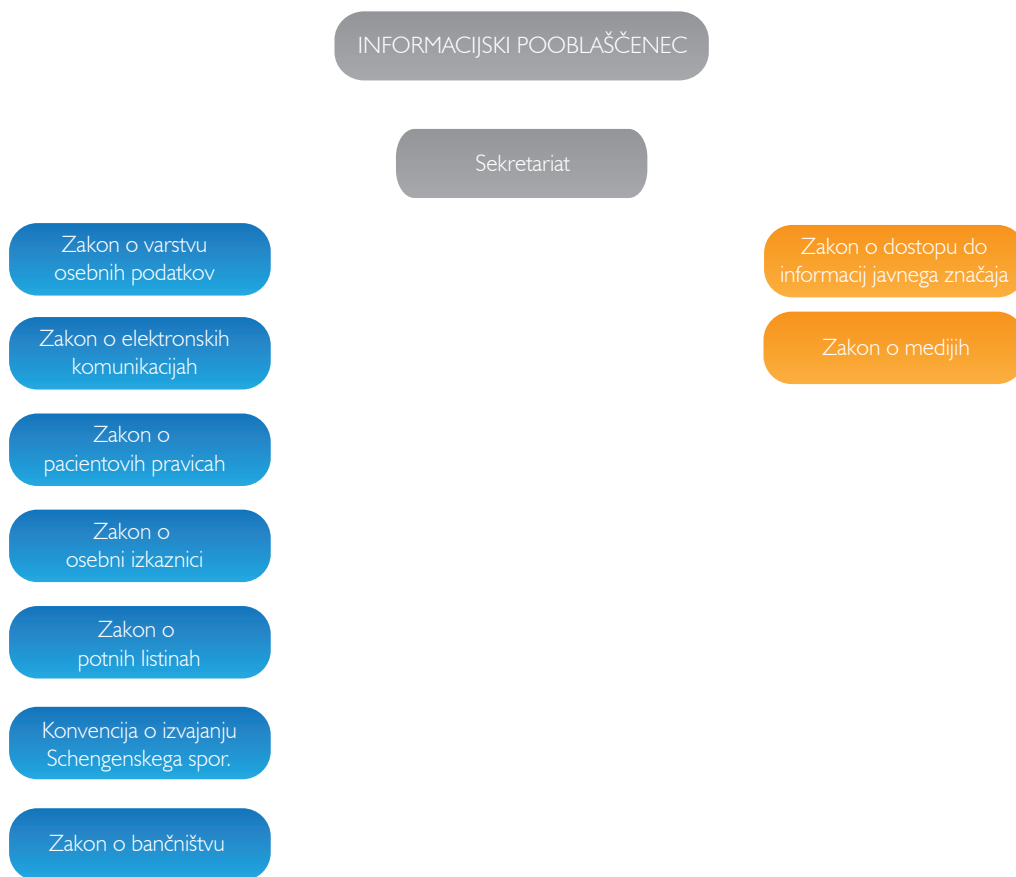
- drugega odstavka 8. člena ZPotK-1, ki določa, da mora dajalec kredita pred sklenitvijo kreditne pogodbe oceniti kreditno sposobnost potrošnika, pri čemer informacije o njegovih prejemkih oz. njegovem premoženjskem stanju pridobi od potrošnika, informacijo o zadolženosti potrošnika pa pridobi iz zbirk osebnih podatkov, ki se vodijo na podlagi zakona, ki ureja bančništvo,
- prvega, drugega in četrtega 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.

<sup>10</sup> Uradni list RS, št. 109/2012; v nadaljevanju ZEKom-1.

<sup>11</sup> Uradni list RS, št. 59/2010 in 30/2013; v nadaljevanju ZPotK-1.



Slika 1: Pristojnosti Informacijskega pooblaščenca.



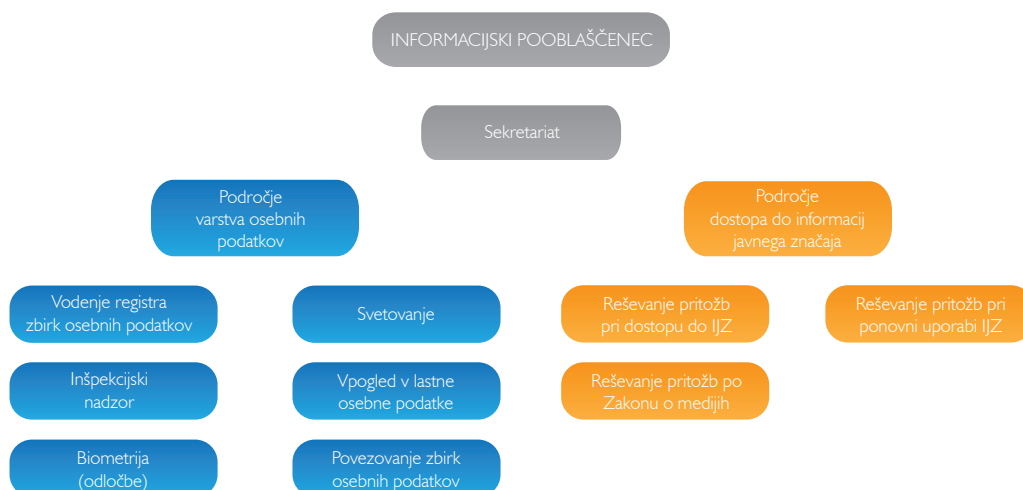
### 1.3. Organiziranost Informacijskega pooblaščenca

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

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 2014 je imel Informacijski pooblaščenec 34 zaposlenih:

- informacijska pooblaščenka,
- namestnica za področje varstva osebnih podatkov,
- namestnica za področje dostopa do informacij javnega značaja,
- namestnik za področje informacijskih tehnologij,
- namestnik – vodja državnih nadzornikov za varstvo osebnih podatkov,
- generalna sekretarka,
- osem svetovalcev,
- asistent svetovalca,
- enajst državnih nadzornikov za varstvo osebnih podatkov,
- svetovalec pooblaščenca za mednarodne odnose,
- trije raziskovalci,
- projektni sodelavec,
- tri administrativno-tehnične sodelavke (finančna referentka, poslovna sekretarka, dokumentalistka).

Preglednica 1: Izobrazbena struktura zaposlenih pri Informacijskem pooblaščenču 31. 12. 2014.

	Srednja izobrazba	Višja strokovna šola	Univerzitetna izobrazba	Magisterij	Doktorat	Skupaj
Pooblaščenka			1			1
Namestniki			2	2		4
Generalna sekretarka				1		1
Svetovalec			8			8
Asistent svetovalca			1			1
Raziskovalci			3			3

Državni nadzorniki za varstvo osebnih podatkov			6	4	1	11
Svetovalec pooblaščenca za mednarodne odnose			1			1
Projektni sodelavec	1					1
Administrativno-tehnični sodelavec		3				3
Skupaj	1	3	22	7	1	34

Na 31. 12. 2014 je bilo pri Informacijskem pooblaščenju zaposlenih 34 oseb, od tega 30 za nedoločen čas ter štiri za določen čas zaradi dela na projektu in nadomeščanj zaposlenih na porodniškem dopustu. Do konca leta 2014 ni nobeden izmed zaposlenih izpolnil pogojev za redno upokožitev. V primerjavi z letom 2013 se je število zaposlenih povečalo za eno osebo. Soglasje za to je podalo Ministrstvo za finance, razlog pa je bil v dodatnih pristojnostih Informacijskega pooblaščenca, povezanih s širitvijo kroga zavezancev za posredovanje informacij javnega značaja, kot izhaja iz novele ZDIJZ-C.

#### 1.4. Finančna sredstva Informacijskega pooblaščenca

Sredstva za delo Informacijskega pooblaščenca se v skladu s 5. členom ZInFP zagotavljajo iz državnega proračuna. Višino sredstev določi Državni zbor RS na predlog Informacijskega pooblaščenca.

Državni zbor RS je za delo Informacijskega pooblaščenca za leto 2014 v državnem proračunu določil integralna sredstva v višini 1.247.110,10 EUR (leta 2013 1.291.210,00 EUR). Ob koncu leta je bilo na postavki plače 1.070.517,32 EUR, materialni stroški 133.893,67 EUR in investicije 42.699,11 EUR.

S sklepom o prerazporeditvi pravic porabe je bilo junija s strani Ministrstva za finance prerazporejenih 17.500,00 EUR za pokrivanje stroškov nove zaposlitve za nedoločen čas zaradi sprememb ZDIJZ in posledično dodatnih pristojnosti, povezanih s širitvijo kroga zavezancev za posredovanje informacij javnega značaja.

Leta 2014 je Informacijski pooblaščenec razpolagal z namenski sredstvi, založenimi sredstvi ter donacijami za sodelovanje v projektih, ki so bili financirani s strani EU, v skupni višini 29.562,62 EUR (prenesenih sredstev iz leta 2013 je bilo 7.063,62 EUR, prejetih sredstev v letu 2014 pa 22.499,00 EUR).

V proračun za leto 2015 je Informacijski pooblaščenec prenesel skupaj 14.107,73 EUR namenskih sredstev in sredstev donacij (8.150,00 EUR namenskih sredstev, 5.611,31 EUR donacij (mednarodna spletna stran, LAPSI 2.0 - Legal Aspects of Public Sector Information in TAIEX) in 346,42 EUR založenih sredstev).

Zaradi proračunskih omejitev in varčevalnih ukrepov, ki jih je sprejela slovenska vlada leta 2014, je Informacijski pooblaščenec omejil izobraževanje zaposlenih, povsem skrčil obseg udeležbe na mednarodnih sestankih ter skrbno in zelo restriktivno porabljal finančna sredstva na postavkah materialni stroški, investicije in plače. Prav tako je Informacijski pooblaščenec bistveno znižal stroške izdaje publikacij, študentskega dela in drugih storitev.

Preglednica 2: Proračun Informacijskega pooblaščenca 2014.

	Veljavni proračun v EUR	Prevzete obveznosti v EUR	Razpoložljiv proračun v EUR konec leta
Informacijski pooblaščenec	1.281.555,80	1.253.100,17	28.455,63
Podprogrami			
<b>OPRAVLJANJE DEJAVNOSTI</b>	<b>1.247.110,10</b>	<b>1.232.728,18</b>	<b>14.381,92</b>
PP 1271 Materialni stroški	133.893,67	120.072,70	13.820,97
PP 1273 Investicije	42.699,11	42.693,23	5,88
PP 1267 Plače	1.070.517,32	1.069.962,25	555,07
<b>NAMENSKA SREDSTVA</b>	<b>14.150,00</b>	<b>6.000,00</b>	<b>8.150,00</b>
PP 7459 Namenska sredstva kupnine	14.150,00	6.000,00	8.150,00
<b>DONACIJE</b>	<b>20.295,70</b>	<b>14.371,99</b>	<b>5.923,71</b>
PP 9958 Mednarodna spletna stran	578,27	362,08	216,19
PP 130130 LAPSI 2.0	8.726,43	4.773,31	3.953,12
PP130134 TAIEX projekt	1.442,00	0,00	1.442,00
PP140084 IP-CRISP	9.549,00	9.236,60	312,40
<b>ZALOŽENA SREDSTVA</b>			
PP 344 Založena sredstva	346,42	0	346,42

Preglednica 3: Namenska sredstva in donacije.

	Prenesena sredstva iz leta 2013	Prilivi v letu 2014	Skupaj sredstva leta 2014
Informacijski pooblaščenec	7.063,62	22.499,00	29.562,62
<b>NAMENSKA SREDSTVA</b>	<b>0,00</b>	<b>8.150,00</b>	<b>8.150,00</b>
PP 7459 Namenska sredstva kupnine	0,00	8.150,00	8.150,00
<b>DONACIJE</b>	<b>6.717,20</b>	<b>4.800,00</b>	<b>11.517,20</b>
PP 9378 EU open privacy space	3,41	0,00	3,41
PP 9586 LAPSI 1.0	349,40	0,00	349,40
PP 9596 Twinning Črna Gora	342,88	0,00	342,88
PP 9950 Twinning Srbija	74,81	0,00	74,81
9958 Mednarodna spletna stran	578,27	0,00	578,27
PP 130130 LAPSI 2.0	3.926,43	4.800,00	8.726,43
PP130134 TAIEX projekt	1.442,00	0,00	1.442,00
<b>ZALOŽENA SREDSTVA</b>	<b>346,42</b>	<b>0</b>	<b>346,42</b>
PP 344 Založena sredstva	346,42	0	346,42
Sredstva se ne prenesajo - tip postavke 80		9.549,00	9.549,00
PP140084 IP-CRISP		9.549,00	9.549,00

Za plače zaposlenih (plače in dodatki, regres za letni dopust, povračila in nadomestila, sredstva za delovno uspešnost iz naslova povečanega obsega dela, prispevki delodajalcev za socialno varnost, prispevki za zdravstveno zavarovanje, prispevki za zaposlovanje in starševsko varstvo, premije kolektivnega dodatnega pokojninskega zavarovanja) je bilo leta 2014 porabljenih 1.069.962,25 EUR (leta 2013 1.047.826,01 EUR, leta 2012 1.138.678,08 EUR in leta 2011 1.139.495,82 EUR). Za izplačilo plač zaposlenim je Informacijski pooblaščenec zagotovil finančna sredstva v višini 27.281,63 EUR s prerazporeditvijo privarčevanih sredstev iz postavke materialni stroški na postavko plače. Junija je Informacijski pooblaščenec v

dogovoru z Ministrstvom za finance dobil dodeljena dodatna finančna sredstva, in sicer 17.500 EUR za eno dodatno zaposlitev za nedoločen čas. Razlog za primanjkljaj sredstev na plačnih postavkah, kljub uvedenim varčevalnim ukrepom, je bila tudi obveznost izplačila tretje četrtine nesorazmerij v osnovnih plačah javnim uslužbencem za obdobje od 1. 10. 2010 do 31. 5. 2015, kot je izhajalo iz Zakona o načinu izplačila razlike v plači zaradi odprave tretje četrtine nesorazmerij v osnovnih plačah javnih uslužbencev<sup>12</sup>. Sredstva za izplačilo razlike je Informacijski pooblaščenec moral zagotoviti iz lastnih sredstev s prerazporeditvijo iz materialnih stroškov. Razpoložljivi proračun oz. ostanek sredstev v višini 555,07 EUR je bil ob koncu leta vrnjen v proračun.

Za materialne stroške je bilo leta 2014 porabljenih 120.072,70 EUR (leta 2013 206.304,91 EUR, leta 2012 252.887,49 EUR in leta 2011 302.103,22 EUR). Poraba sredstev za materialne stroške se že nekaj let zmanjšuje. Ti stroški vključujejo pisarniški material, tisk, čiščenje poslovnih prostorov, spremljanje medijev in arhiviranje – kliping, zdravniške preglede zaposlenih, stroške za energijo, vodo, komunalne storitve in komunikacije, prevozne stroške in vzdrževanje vozil, izdatke za službena potovanja, manjša popravila v poslovnih prostorih, vzdrževanje spletne strani, odmero nadomestila za uporabo stavbnega zemljišča, naročnino za IUS-INFO in prekrškovni portal, plačila sodb sodišč, plačila kvot Javnemu jamstvenemu, preživninskemu in invalidskemu skladu, izdatke za strokovno izobraževanje zaposlenih ter študentsko delo kot nadomeščanje. Na koncu leta je ostanek sredstev glede na veljavni proračun znašal 13.820,97 EUR, in sicer zaradi skrajnih varčevalnih ukrepov, ki jih je Informacijski pooblaščenec izvajal, da bi s tem lahko izplačal drugi obrok nesorazmerij v osnovnih plačah, česar pa vse do konca leta ni mogel izvesti.

Veljavni proračun za investicije je bil 42.699,11 EUR, do konca leta je bilo porabljenih 42.693,23 EUR. Informacijski pooblaščenec je za zagotavljanje delovanja informacijskega sistema, pri katerem so se začele zaradi dotrajanosti pojavljati težave, leta 2014 izvedel nakup oz. naročil storitev njegove prenove v znesku 20.061,68 EUR. Edino prenovo informacijskega sistema je Informacijski pooblaščenec namreč izvedel leta 2007, ko je zaradi povečanih pristojnosti in zapolnitve delovnih mest moral ustrezno povečati zmogljivosti in razpoložljivost informacijskega sistema. Od takrat je poskušal brez dodatnih nakupov in posodobitev z minimalnimi stroški zagotoviti nemoteno delovanje informacijskega sistema, ki je bil že izven amortizacijske dobe, predvsem pa krepko izven garancijske dobe. Zaradi racionalizacije stroškov se je Informacijski pooblaščenec odločil za nakup vozila Audi A4, letnik 2011, v vrednosti 18.990,00 EUR. Staro vozilo Audi A4, letnik 2006, je prodal za 6.000,00 EUR, tako da je bilo iz sredstev investicij za nakup vozila porabljenih 12.990,00 EUR. 2.520,72 EUR je bilo namenjenih za nakup monitorjev in prenosnih računalnikov, 642,00 EUR za nakup mobilnih telefonov, 5.672,19 EUR za sanacijo fasade na objektu ter izdelavo in montažo okna v novem prostoru v pritličju stavbe, 806,64 EUR pa za nakup licenčne programske opreme.

Informacijski pooblaščenec je leta 2014 prodal službeni vozili Audi A4 in Peugeot 607 v skupnem znesku 14.000,00 EUR ter mobilna telefona v znesku 150,00 EUR. Za nakup drugega (rabljenega) vozila Audi A4 je bilo iz namenskih sredstev kupnin porabljeno 6.000,00 EUR. V leto 2015 se je preneslo 8.150,00 EUR.

Leta 2014 so se končali projekti EU Open privacy space, LAPSI 1.0, Twinning Črna Gora, Twinning Srbija. Ostanek sredstev v višini 3,41 EUR, 349,40 EUR, 342,88 EUR in 74,81 EUR s pripadajočimi obrestmi je bil prenesen v proračun Republike Slovenije.

Informacijski pooblaščenec sodeluje v evropskem projektu LAPSI 2.0, ki se je začel leta 2013. Financira ga EU na podlagi pogodbe Evropske komisije z nosilcem projekta Katholieke Universiteit Leuven. Projekt se osredotoča na nadaljevanje projekta LAPSI 1.0, in sicer odkrivanje in odstranjevanje pravnih ovir pri dostopu in ponovni uporabi informacij javnega značaja, ki se postavljajo na področju prava, informatike, intelektualne lastnine, zasebnosti, konkurenčnega prava, upravnega in okoljskega prava ter oblikovanje strategij, kako te ovire

<sup>12</sup> Uradni list RS, št. 100/2013.

preseči. V okviru projekta so organizirani seminarji in konference, ki so namenjeni spodbujanju debate med raziskovalci in drugimi udeleženci na tem področju, namen projekta pa je tudi razširiti diskusijo med širšo javnostjo in dvigniti nivo zavedanja problematike na področju ponovne uporabe informacij javnega značaja. Cilj projekta je priprava dodatnih smernic za Evropsko komisijo, ki bodo pripomogle k učinkovitejšemu izkoriščanju ponovne uporabe informacij javnega značaja. Sodelovanje Informacijskega pooblaščenca kot enega izmed partnerjev projekta vključuje sodelovanje na tematskih konferencah projekta in seminarjih s predstavitvami na izbrane teme, aktualne za informacije javnega značaja. Za sodelovanje v projektu bo Informacijski pooblaščenec s strani EU v letih 2013, 2014 in 2015 skupaj prejel namenska sredstva v višini 16.000,00 EUR. Leta 2013 je prejel 9.600,00 EUR (od tega je leta 2013 porabil 5.673,57 EUR), leta 2014 pa je prejel 4.800,00 EUR. Leta 2014 je tako imel na razpolago 8.726,43 EUR, porabil pa je 4.773,31 EUR za stroške službenih poti v zvezi z udeležbo na sestankih in konferencah v okviru projekta ter izplačilo povečanega obsega dela zaposlenih, ki sodelujejo pri projektu. Ostanek sredstev, 3.953,12 EUR, se je prenesel v leto 2015.

Informacijski pooblaščenec je leta 2014 začel sodelovati v projektu IP CRISP v okviru Sedmega okvirnega programa: THEME [SEC-2013.5.4-1] – Evaluation and certification schemes for security products – Capability, št. pogodbe 607941. Projekt je financiran s strani Evropske komisije, ki jo zastopa Izvajalska agencija za raziskave. Projekt bo predvidoma trajal 36 mesecev in se osredotoča na izboljšanje metodologije za certificiranje varnostnih izdelkov, med drugim upoštevajoč vidike varstva osebnih podatkov. Sodelovanje Informacijskega pooblaščenca vključuje sodelovanje zaposlenih pri pripravi posameznih gradiv, analiz, raziskav in pri drugih aktivnostih projekta ter njihovo napotitev na misije in sestanke v zvezi s projektom, kjer bodo izvajali posamezne naloge s področja varstva osebnih podatkov, ki jih pokriva projekt (npr. predstavitve, seminarje in delavnice za ciljne skupine projekta). Za sodelovanje v projektu bo Informacijski pooblaščenec prejel namenska sredstva v višini 149.230,00 EUR, v okviru rednih aktivnosti za izvajanje projekta v času trajanja projekta bo Informacijskemu pooblaščenca iz integralnih proračunskih sredstev zagotovljeno skupaj 24.890,00 EUR. Sredstva bodo porabljena za pokrivanje stroškov dela zaposlenih in drugih stroškov v zvezi s pripravo in izvedbo aktivnosti ter materialnih stroškov. Leta 2014 je bilo s strani Evropske komisije nakazanih 82.076,50 EUR. S sklepom Vlade RS so bile povečane pravice porabe za leto 2014 za projekt CRISP v znesku 9.549,00 EUR, porabljenih pa je bilo 9.236,60 EUR za materialne stroške in za plače.

Leta 2014 v okviru projekta TAIEX ni bilo porabljenih sredstev. Ostanek sredstev, 1.442,00 EUR, se je prenesel v leto 2015.

Informacijski pooblaščenec je imel na računu tudi sredstva za kratkoročne obveznosti za prejete varščine v znesku 346,42 EUR. Založena sredstva predstavljajo predujem stranke za postavitev izvedenca po Zakonu o splošnem upravnem postopku. Ker leta 2014 ni porabil nobenih sredstev, se njihov preostanek, 346,42 EUR, prenese v leto 2015.





2

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



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

Pravico dostopa do informacij javnega značaja je zakonodajalec zagotovil že z Ustavo Republike Slovenije<sup>1</sup>. Ta v drugem odstavku 39. člena določa, da ima vsakdo pravico dobiti informacijo javnega značaja, za katero ima v zakonu utemeljen pravni interes, razen v primerih, ki jih določa zakon. Čeprav je pravica dostopa do informacij javnega značaja ena od temeljnih človekovih pravic in kot taka tudi zaščiten 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<sup>2</sup>. 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 EU. 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, ter Direktive 2003/98/ES Evropskega parlamenta in Sveta o ponovni uporabi informacij javnega sektorja, ki je začela veljati 17. 11. 2003.

Leta 2005 je bil z novelo ZDIJZ (ZDIJZ-A) 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.

Leta 2014 sta bili sprejeti dve noveli ZDIJZ (ZDIJZ-C<sup>3</sup> in ZDIJZ-D<sup>4</sup>). Najpomembnejša sprememba, ki sta jo prinesli, je, da se je obveznost posredovanja informacij javnega značaja z organov javnega sektorja razširila tudi na gospodarske družbe in druge pravne osebe pod prevladujočim vplivom (oz. v večinski lasti) države, občin ali drugih oseb javnega prava ter da je AJ PES v roku šestih mesecev od uveljavitve ZDIJZ-C vzpostavil spletni Register zavezancev za informacije javnega značaja, ki je javen, podatki v njem pa so dostopni brezplačno. Namen sprememb ZDIJZ je, da se poleg zagotavljanja javnosti in odprtosti delovanja javnega sektorja krepi tudi transparentnost in odgovorno ravnanje pri upravljanju s finančnimi sredstvi poslovnih subjektov, nad katerimi ima javni sektor prevladujoč vpliv. Nadzor javnosti, omejen zgolj na državne organe, občine in širši javni sektor, se je izkazal kot nezadosten. Finančna in gospodarska kriza preteklih let je namreč povečala občutljivost javnosti na korupcijo, zlorabo oblasti in slabo upravljanje. K večji transparentnosti bo prispela tudi proaktivna objava informacij javnega značaja na spletnih straneh, ki jo zahteva novela ZDIJZ-C

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 posredovanje informacij javnega značaja se delijo v dve skupini:

<sup>1</sup> Uradni list RS, št. 33/1991, 42/1997, 66/2000, 24/2003, 69/2004, 68/2006; v nadaljevanju Ustava RS.

<sup>2</sup> Uradni list RS, št. 24/2003, s spremembami; v nadaljevanju ZDIJZ.

<sup>3</sup> Uradni list RS, št. 23/2014.

<sup>4</sup> Uradni list RS, št. 50/2014 in 19/2015.

- organi (državni organi, organi lokalnih skupnosti, javne agencije, javni skladi in druge osebe javnega prava, nosilci javnih pooblastil in izvajalci javnih služb) ter
- poslovni subjekti pod prevladujočim vplivom oseb javnega prava.

Zavezanci so informacije javnega značaja dolžni zagotavljati na dva načina: z objavo na spletu in z omogočanjem dostopa na podlagi individualnih zahtev. Za vsako od skupin zavezanec je pojem »informacija javnega značaja« (torej informacija, ki jo morajo zavezanci praviloma posredovati prosilcu) drugače definiran; pri zavezancih iz druge skupine je ožji. Medtem ko za organe na splošno lahko rečemo, da so vsi dokumenti, zadeve, dosjeji, registri, evidence ali dokumentarna gradiva, s katerimi razpolagajo (ne glede na to, ali jih je organ izdelal sam, v sodelovanju z drugim organom ali jih je pridobil od drugih oseb), informacije javnega značaja, razen izjem, za nove zavezance velja ravno obraten miselni proces – informacije javnega značaja so le tisti dokumenti, zadeve, dosjeji, registri, evidence ali dokumentarna gradiva, ki jih kot take določa ZDIJZ (npr. informacije, povezane s sklenjenimi pravnimi posli, ter informacije o članih poslovnega organa, organa upravljanja in organa nadzora). Za nove zavezance velja tudi časovna omejitev, saj se dolžnost posredovanja nanaša le na informacije, nastale v času pod prevladujočim vplivom. Zavezanci, ki izpolnjujejo kriterije za umestitev v obe skupini (npr. gospodarske družbe v 100 % lasti občine, ki so hkrati tudi izvajalke javne službe), so zavezani posredovati obe vrsti informacij javnega značaja. Tisti poslovni subjekti pod prevladujočim vplivom oseb javnega prava, ki hkrati ne sodijo med organe, lahko uporabijo t. i. poenostavljen postopek odločanja o zahtevah (npr. ne izdajo zavrnilne odločbe, ampak vlagatelja pisno obvestijo o razlogih, zaradi katerih informacije ne bodo posredovali). Ostali zavezanci (npr. nosilci javnih pooblastil, ki so hkrati pod prevladujočim vplivom pravnih oseb javnega prava) so dolžni voditi upravni postopek, kot je določen za organe.

Informacije javnega značaja so prosto dostopne vsem, zato pravnega interesa za njihovo pridobitev ni treba izkazovati, dovolj sta radovednost ter želja po znanju in obveščenosti. Vsak prosilec ima na svojo zahtevo od zavezanca pravico pridobiti informacijo javnega značaja, in sicer tako, da jo dobi na vpogled ali dobi njen prepis, fotokopijo ali elektronski zapis. Zavezanec mora o zahtevi odločiti v 20 delovnih dneh, organi lahko v izjemnih okoliščinah podaljšajo rok na največ 30 delovnih dni. Vpogled v zahtevano informacijo je brezplačen. Za posredovanje prepisa, fotokopije ali elektronskega zapisa zahtevane informacije lahko zavezanec prosilcu zaračuna materialne stroške. Če zavezanec prosilcu ne posreduje zahtevane informacije javnega značaja, ima prosilec v 15 dneh pravico vložiti pritožbo zoper zavrnilno odločbo ali obvestilo, s katerim je zavezanec zahtevo zavrnil. O pritožbi odloča Informacijski pooblaščenec. Prav tako ima prosilec pravico do pritožbe, če mu zavezanec na zahtevo ni odgovoril (oz. je v molku) in če ni dobil informacije v obliki, ki jo je zahteval.

Zavezanec lahko prosilcu dostop do zahtevane informacije zavrne, če se zahteva nanaša na eno izmed izjem, določenih v prvem odstavku 6. člena ZDIJZ (tajni podatek, poslovna skrivnost, osebni podatek, davčna tajnost, sodni postopek, upravni postopek, statistična zaupnost, dokument v izdelavi, notranje delovanje organa, varovanje naravne oz. kulturne vrednote). Kljub navedenim izjemam iz prvega odstavka 6. člena ZDIJZ organ dostop do zahtevane informacije vedno dovoli, če gre za podatke o porabi javnih sredstev ali podatke, povezane z opravljanjem javne funkcije ali z delovnim razmerjem javnega uslužbenca. Zavezanec pod prevladujočim vplivom države prosilcu praviloma ne sme zavrnil dostopa, če gre za absolutno javne informacije (osnovni podatki o poslih, ki se nanašajo na izdatke); razkritju teh podatkov se lahko poslovni subjekt izogne le, če izkaže, da bi to huje škodovalo njegovemu konkurenčnemu položaju na trgu.

Če dokument, ki ga zahteva prosilec, delno vsebuje informacije, ki so izjema od prostega dostopa iz 6. člena ZDIJZ, to ni razlog, da bi organ zavrnil dostop do celotnega dokumenta. Če je te informacije mogoče iz dokumenta izločiti, ne da bi to ogrozilo njihovo zaupnost, se jih prekrije, prosilcu pa se posreduje preostali del informacij javnega značaja. Zavezanec mora namreč v skladu z 21. členom Uredbe o posredovanju in ponovni uporabi informacij

javnega značaja<sup>5</sup> varovane podatke prekri in prosilcu omogočiti vpogled v preostanek dokumenta (fotokopije ali elektronskega zapisa).

Če poda zahtevo za posredovanje informacij medij na podlagi 45. člena ZMed, je postopek nekoliko drugačen, saj informacije po ZMed niso enake informacijam javnega značaja po določbah ZDIJZ. Informacije za medije so širši pojem kot informacije javnega značaja, saj med prve sodi tudi priprava odgovorov na vprašanja (pojasnila, razlage, analize, komentarji). Če medij zahteva odgovor na vprašanje, se njegova vloga obravnava po določbah ZMed, če pa zahteva dostop do dokumenta, se njegova vloga obravnava po ZDIJZ. Medij mora vprašanje vložiti pisno po navadni ali elektronski pošti (digitalno potrdilo ali elektronski podpis nista potrebna), zavezanec pa ga mora o zavrnitvi ali delni zavrnitvi odgovora pisno obvestiti do konca naslednjega delovnega dne. V nasprotnem primeru mora zavezanec odgovor na vprašanje poslati najpozneje v sedmih delovnih dneh od prejema vprašanja, pri čemer sme odgovor zavrniti le, če so zahtevane informacije izvzete iz prostega dostopa po ZDIJZ. Medij lahko po prejemu odgovora zahteva dodatna pojasnila, ki mu jih mora zavezanec posredovati najpozneje v treh dneh. Če zavezanec z informacijo, ki predstavlja odgovor na vprašanje, ne razpolaga v materializirani obliki, se medij ne more pritožiti zoper obvestilo o zavrnitvi ali delni zavrnitvi odgovora. Pritožba pa je dovoljena, kadar odgovor na vprašanje izhaja iz dokumenta.

## 2.2. Število vloženih pritožb in število rešenih zadev

Leta 2014 je Informacijski pooblaščenec prejel 578 pritožb, od tega 320 zoper zavrnilne odločbe in 258 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 vodil 25 postopkov zoper nove zavezanca, tj. pravne osebe pod prevladujočim vplivom države, občin ali drugih oseb javnega prava. Izdal 288 odločb (od tega 53 v zadevah, ki jih je v reševanje prejel pred letom 2014), sedem prosilcev je pritožbo umaknilo, 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 prosilcem zahtevane informacije javnega značaja posredovali. Z odgovorom organa je bil postopek zaradi molka zaključen, prosilci, ki so dobili zavrnilno odločbo, pa so imeli možnost pritožbe Informacijskemu pooblaščenecu zaradi zavrnitve zahteve po dostopu do informacij javnega značaja. V 30 primerih je Informacijski pooblaščenec pritožbo zaradi preuranjenosti ali pomanjkljive vloge s sklepom zavrgel, pet posameznikov je pritožbo umaknilo, ker so prejeli zahtevano dokumentacijo, v sedmih 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 2014 prejel tudi 150 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 oz. odstopil v reševanje organom prve stopnje.

<sup>5</sup> 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 2014 je bilo opravljenih 53 takšnih ogledov.

Leta 2014 je Informacijski pooblaščenec prejel 297 prošenj za pomoč in različnih vprašanj posameznikov glede dostopa do informacij javnega značaja, predvsem o tem, ali je določen dokument informacija javnega značaja. Informacijski pooblaščenec je vsem odgovoril v okviru svojih pristojnosti, največkrat jih je napotil na pristojno institucijo. Informacijski pooblaščenec je namreč drugostopenjski organ, ki odloča o pritožbi, in ni pristojen, da v fazi, ko mora odločati organ prve stopnje, odgovarja na konkretna vprašanja, ali je določen dokument informacija javnega značaja ali ne. V skladu z 32. členom ZDIJZ mnenja na področju dostopa do informacij javnega značaja daje ministrstvo, pristojno za javno upravo.

### 2.3. Število vloženih tožb na Upravnem sodišču RS, število sodb Upravnega in Vrhovnega sodišča RS

Pritožba zoper odločbo Informacijskega pooblaščenca ni dopustna, mogoče pa je sprožiti upravni spor. Leta 2014 je bilo zoper odločbe Informacijskega pooblaščenca na Upravnem sodišču vloženih 29 tožb (zoper 10,1 % izdanih odločb). Delež vloženih tožb je v primerjavi z letom poprej nekoliko narasel, čeprav se je pred tem konstantno zmanjševal. Tako so bile leta 2011 vložene tožbe zoper 13,1 % odločb, ki jih je izdal Informacijski pooblaščenec, leta 2012 10,5 %, leta 2013 pa 8,1 %. Razlog je v novih zavezancih, ki so z obveznostmi, ki jih je prinesla novela ZDIJZ-C, slabše seznanjeni, poleg tega zakonskim obveznostim nasprotujejo. Kljub temu pa je delež sproženih upravnih sporov relativno majhen, kar kaže na uveljavitev transparentnosti in odprtosti javnega sektorja glede njegovega delovanja ter tudi na sprejemanje odločb Informacijskega pooblaščenca s strani organov in prosilcev.

Upravno sodišče je leta 2014 odločilo o 17 tožbah, ki so bile vložene zoper odločbe Informacijskega pooblaščenca, in:

- tožbo zavrnilo (8);
- tožbi ugodilo, izpodbijano odločbo oz. del odločbe odpravilo in zadevo vrnilo Informacijskemu pooblaščenecu v ponovno odločanje (5);
- tožbi ugodilo, odločbo Informacijskega pooblaščenca je delno odpravilo, prav tako odločbo organa prve stopnje in jo v tem delu organu vrnilo v ponoven postopek (2);
- tožbi ugodilo, odločbo prvostopenjskega organa delno odpravilo in mu jo vrnilo v ponovno odločanje (1);
- tožbo zavrglo (1).

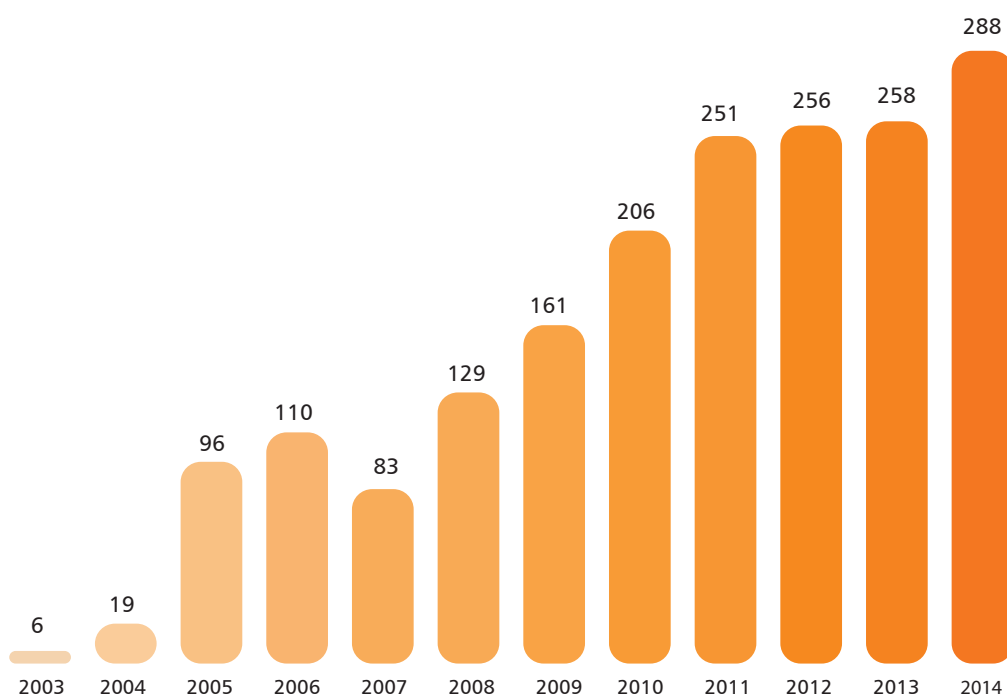
Upravno sodišče je odločilo tudi o predlogu poprave izreka sodbe, ki jo je izdalo leta 2013, in sicer je predlog s sklepom zavrglo.

Leta 2014 sta bili zoper sodbi Upravnega sodišča na Vrhovno sodišče vloženi dve reviziji, o katerih pa Vrhovno sodišče v preteklem letu ni odločilo. Odločilo pa je v postopku iz leta 2013, in sicer je revizijo zavrglo.

## 2.4. Statistika po posameznih področjih ZDIJZ

Število izdanih odločb na področju dostopa do informacij javnega značaja se je v primerjavi s preteklimi leti povečalo. Leta 2011 je bilo izdanih 251 odločb, leta 2012 256, leta 2013 258, leta 2014 pa kar 288.

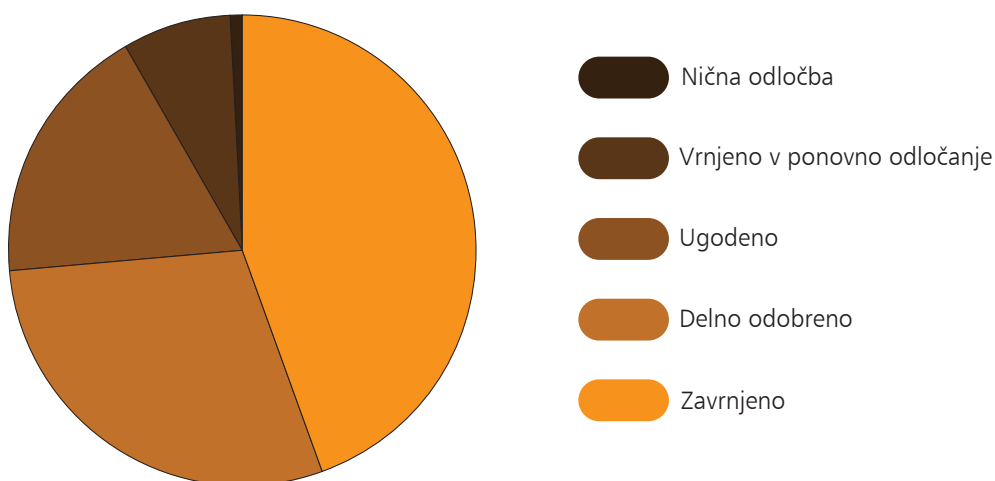
Slika 3: Število izdanih odločb na področju dostopa do informacij javnega značaja med letoma 2003 in 2014.



Informacijski pooblaščenec je v izdanih odločbah:

- pritožbo zavrnil (128);
- dostop do informacije delno odobril (84);
- pritožbi ugodil oz. rešil zadevo v korist prosilca (52);
- zadevo vrnil v ponovno odločanje prvostopenjskemu organu (22);
- odločbo prvostopenjskega organa razglasil za nično (2).

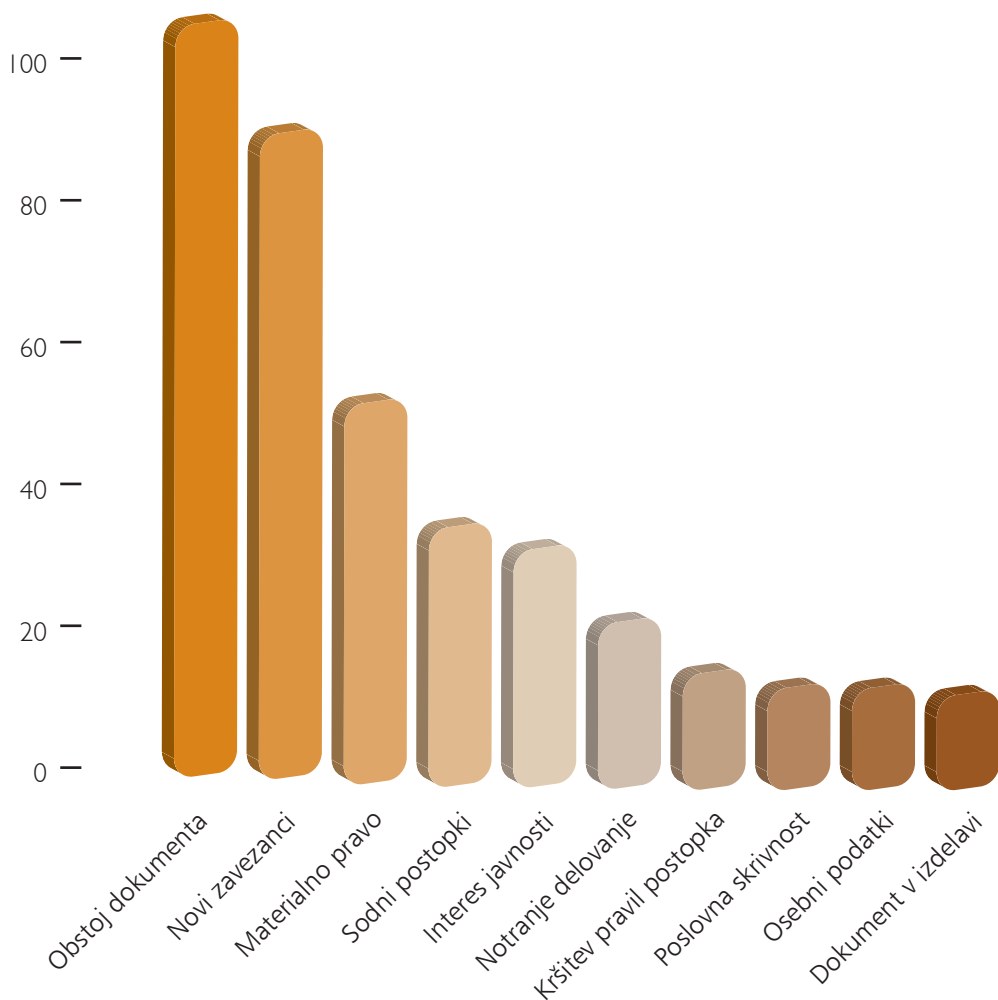
Slika 4: Odločitve Informacijskega pooblaščenca glede prejetih pritožb.



Informacijski pooblaščenec je v odločbah vsebinsko odločal oz. presojal:

- ali zavezanec sploh ima dokument oz. informacijo javnega značaja, ki jo je prosilec zahteval (106);
- ali zahtevani dokumenti vsebujejo osebne podatke, katerih razkritje bi pomenilo kršitev varstva osebnih podatkov v skladu z ZVOP-1 (91);
- ali prosilci zahtevajo informacije oz. podatke, ki so v skladu z zakonom, ki ureja gospodarske družbe, opredeljeni kot poslovna skrivnost (54);
- ali gre za kršitev pravil postopka (37);
- ali so zahtevane informacije podatki iz dokumenta, ki je bil sestavljen v zvezi z notranjim delovanjem oz. dejavnostjo organov, in bi njegovo razkritje povzročilo motnje v delovanju oz. dejavnosti organa (34);
- ali je interes javnosti glede razkritja močnejši od javnega interesa ali interesa drugih oseb za omejitev dostopa do zahtevane informacije (24);
- ali so zahtevane informacije podatki, ki so bili pridobljeni ali sestavljeni zaradi pravnega, nepravdnega ali drugega sodnega postopka, in bi njihovo razkritje škodovalo njegovi izvedbi (17);
- ali gre za kršitev materialnega prava (15);
- ali gre za novega zavezanca (poslovni subjekt pod prevladujočim vplivom oseb javnega prava) (15);
- 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 (14);
- izdaja odločbe v postopku, ko je prosilec zahteval dokument iz postopka javnega naročanja (14);
- ali zahtevani dokument izpolnjuje pogoje za obstoj informacije javnega značaja v skladu s prvim odstavkom 4. člena ZDIJZ (13);
- ali se zahtevane informacije nanašajo na delo in osebne podatke javnih uslužbencev in funkcionarjev (11);
- ali je organ pravilno zaračunal stroške posredovanja informacij javnega značaja (11);
- 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 (11);
- ali gre za delovno področje organa (10);
- 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);
- ali je organ, na katerega je bila zahteva po dostopu do informacije javnega značaja naslovljena, sploh zavezanec v skladu s prvim odstavkom 1. člena ZDIJZ (9);
- ali so zahtevane informacije podatki, ki so bili pridobljeni ali sestavljeni zaradi upravnega postopka, in bi njihovo razkritje škodovalo njegovi izvedbi (9);
- ali gre za ponovno uporabo informacije javnega značaja (8);
- ali so zahtevane informacije podatki, ki so na podlagi zakona, ki ureja tajne podatke, opredeljeni kot tajni (8);
- 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 (6);
- ali gre za zlorabo pravice po ZDIJZ (6);
- ali so zahtevane informacije podatki, katerih razkritje bi pomenilo kršitev zaupnosti davčnega postopka ali davčne tajnosti skladno z zakonom, ki ureja davčni postopek (4);
- ali gre za okoljske podatke (4);
- ali gre za proaktivno objavo informacij (4);
- izdaja odločbe v postopku, ko je prosilec zahteval dokument z delovnega področja organov EU (1);
- ali gre za podatek, glede katerega zakon določa varovanje tajnosti vira (1).

Slika 5: Odločbe na področju ZDIJZ glede na različne izjeme. (Opomba: ena odločba se lahko nanaša na več izjem.) - najpogostejših 10 izjem.

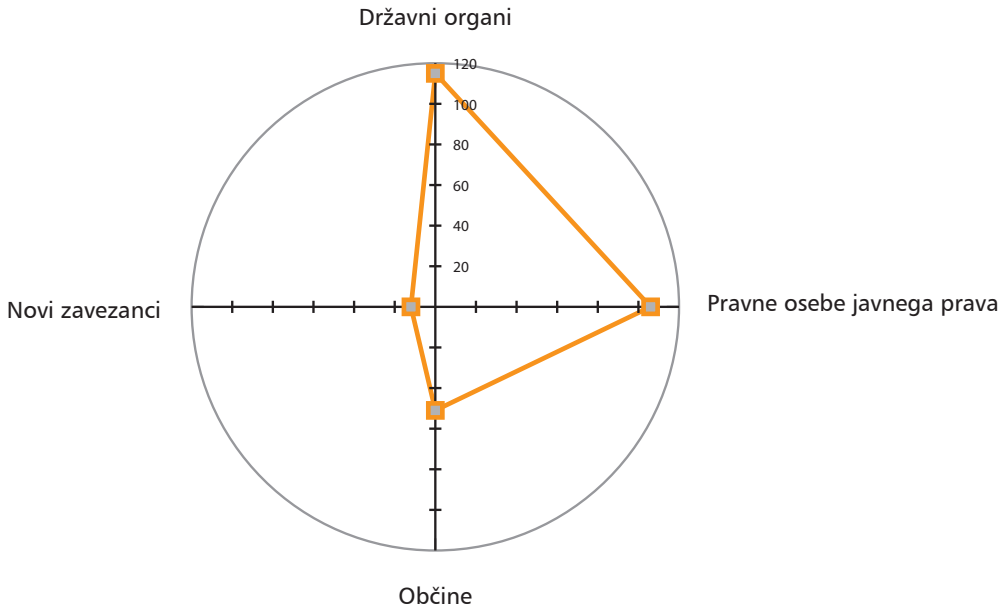


Pritožbe prosilcev zaradi zavrnitve dostopa do informacij javnega značaja, o katerih je Informacijski pooblaščenec odločil z odločbo, so zadevale naslednje skupine zavezancev:

- državni organi 115, od tega ministrstva in organi v sestavi ter upravne enote 73, sodišča, vrhovno državno tožilstvo, državno pravobranilstvo pa 29,
- javni skladi, zavodi, agencije, izvajalci javnih služb, nosilci javnih pooblastil in druge pravne osebe javnega prava 106,
- občine 51,
- novi zavezanci (poslovni subjekti pod prevladujočim vplivom države, občin ali drugih oseb javnega prava) 12.

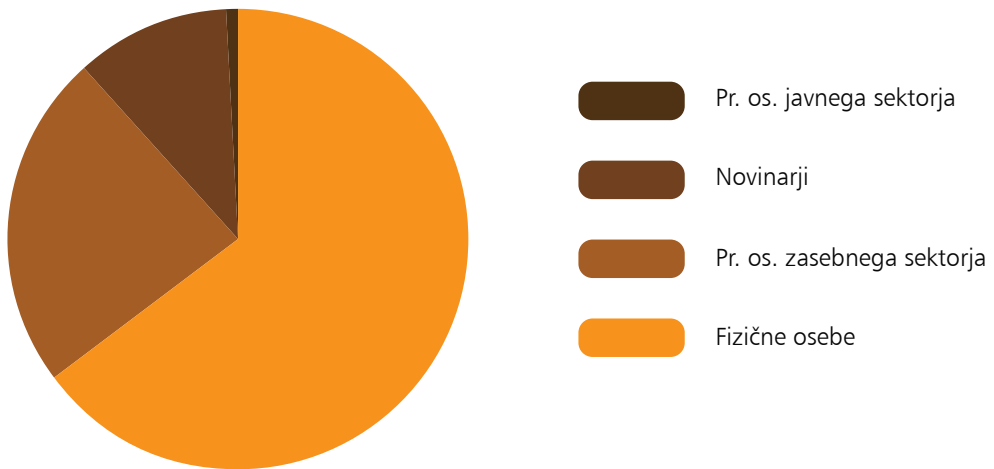
Štiri pritožbe so se nanašale na pravne osebe zasebnega sektorja, za katere pa je bilo ugotovljeno, da niso zavezanci po ZDIJZ.

Slika 6: Pritožbe prosilcev glede na zavezanca.



V 187 primerih so bili prosilci fizične osebe, v 68 primerih so se pritožile pravne osebe zasebnega sektorja, novinarji so se pritožili 31-krat, pravne osebe javnega sektorja pa dvakrat.

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



## 2.5. Storjeni prekrški po ZDIJZ, ZInfP in ZMed

Leta 2014 sta bila uvedena dva postopka o prekršku, in sicer zaradi storitve prekrška po prvem odstavku 15. člena ZInfP, ker organ Informacijskemu pooblaščenču ni posredoval zahtevanih dokumentov, ki so bili potrebni za odločitev v pritožbenem postopku. Informacijski pooblaščenec je kršiteljem v obeh primerih izrekel globo; en kršitelj je vložil zahtevo za sodno varstvo.



Informacijski pooblaščenec je izrekel eno opozorilo po Zakonu o prekrških<sup>6</sup> zaradi kršitve 1. točke šestega odstavka ZMed oz. storitve prekrška po 1. točki drugega odstavka 147. člena ZMed.

Informacijski pooblaščenec je na Inšpektorat za javni sektor prijavil kršitev določb Zakona o splošnem postopku v povezavi z ZDIJZ.

## 2.6. Predstavitev najodmevnejših in precedenčnih primerov po področjih

V nadaljevanju je predstavljenih nekaj najzahtevnejših in najzanimivejših odločb iz leta 2014, ki so razvrščene po področjih.

### 2.6.1. Stresni testi, poslovna skrivnost

Z odločbo št. 090-225/2013/4 z dne 13. 1. 2014 je Informacijski pooblaščenec delno odpravil odločbo Banke Slovenije in ji naložil, da prosilcu omogoči vpogled in fotokopiranje pogodb, ki jih je Banka Slovenije sklenila za stresne teste in AQR s podjetji Ernst & Young, Deloitte, Oliver Wyman in Roland Berger, pri čemer naj v posredovanih dokumentih prekrije podatke, ki predstavljajo varovane osebne podatke, poslovno skrivnost in podatke o notranjem delovanju organa.

Banka Slovenije (organ) je z navedeno odločbo prosilcu delno ugodila, zavrnila pa je njegovo zahtevo v delu, ki se nanaša na varovane osebne podatke, poslovno skrivnost in podatke o notranjem delovanju organa. Informacijski pooblaščenec je v pritožbenem postopku ugotovil, da vsi podatki, do katerih je organ prosilcu dostop zavrnil, ne izpolnjujejo pogojev za obstoj navedenih izjem od dostopa po 2., 3. oz. 11. točki prvega odstavka 6. člena ZDIJZ in da je treba dostop do njih dopustiti.

Informacijski pooblaščenec je ugotovil, da poslovne skrivnosti ne predstavljajo podatki o višini plačila, odstotku stroškov od plačila, višini odškodnine, predmetu pogodbe, finančnih pogojih, dinamiki plačil ter o ceni, ki jo bo organ za opravljeno storitev stranskemu udeležencu plačal iz javnih sredstev. Gre namreč za podatke o porabi javnih sredstev, ki glede na določbo 1. alineje tretjega odstavka 6. člena ZDIJZ, določbe Zakona o javnem naročanju na področju obrambe in varnosti<sup>7</sup> ter določbo tretjega odstavka 39. člena Zakona o gospodarskih družbah<sup>8</sup> ne morejo predstavljati poslovne skrivnosti. Hkrati je Informacijski pooblaščenec za nekatere dokumente, kot so splošni pogoji gospodarskega subjekta in določbe o tem, na kakšen način bo naročnik končno poročilo izvajalca uporabil, ne izpolnjujejo pogojev za obstoj poslovne skrivnosti po objektivnem kriteriju (drugem odstavku 39. člena ZGD-1). Ne organ ne stranski udeleženci namreč niso uspeli izkazati, da bi z razkritjem teh dokumentov stranskim udeležencem lahko nastala občutna škoda.

V zvezi z zatrjevano izjemo varstva osebnih podatkov po 3. točki prvega odstavka 6. člena ZDIJZ je organ pravilno ugotovil, da ime, priimek in naziv skrbnika pogodbe in kontaktne osebe na strani stranskega udeleženca predstavljajo varovane osebne podatke. Po drugi strani pa podatki o direktorju stranskega udeleženca, kot podpisniku pogodbe, ne predstavljajo varovanih osebnih podatkov. Podatki o osebah, pooblaščenih za zastopanje gospodarskih subjektov, so namreč javno dostopni že na podlagi veljavne zakonodaje o vpisu teh subjektov v sodni oz. poslovni register (Zakon o sodnem registru<sup>9</sup>, Zakon o Poslovnem

<sup>6</sup> Uradni list RS, št. 29/2011 – uradno prečiščeno besedilo 8 s spremembami; v nadaljevanju ZP-1.

<sup>7</sup> Uradni list RS, št. 90/2012 in 90/2014; v nadaljevanju ZJNPOV.

<sup>8</sup> Uradni list RS, št. 65/2009 - uradno prečiščeno besedilo 3 s spremembami; v nadaljevanju ZGD-1.

<sup>9</sup> Uradni list RS, št. 54/2007 – uradno prečiščeno besedilo 2 s spremembami, v nadaljevanju ZSReg.

registru<sup>10</sup> in ZGD-1). Prav tako na osnovi varstva osebnih podatkov ni mogoče zavrniti dostopa do podatkov o tem, kdo je v imenu in za račun organa (Banke Slovenije) sklenil pogodbo ter kdo je njegova kontaktna oseba. Gre namreč za guvernerja in direktorja oddelka za nadzor bančnega poslovanja in oba v zahtevanih dokumentih nastopata v tej funkciji. Njuni podatki so tudi javno objavljeni v AJPES.

Informacijski pooblaščenec je v pritožbenem postopku ugotovil še, da je organ uspel izkazati obstoj izjeme notranjega delovanja organa glede dokumenta priloge 2, Splošnih pogojev Banke Slovenije – Appendix 2: Copy of Bank of Slovenia Terms of Reference. Navedeni dokument je bil namreč sestavljen za notranje potrebe organa, saj je nastal ob oblikovanju politike oz. razmišljanja organa, mnenj, stališč in navodil, vezanih na projekt AQR. Dokument ni namenjen tretjim osebam oz. javnosti, temveč internemu delovanju organa in naj bi določal delovanje organa v projektu AQR. Hkrati dokument vsebuje podrobne elemente metodologije izvajanja projekta AQR, katerih razkritje bi nedvomno ogrozilo izvedbo projekta. Informacijski pooblaščenec je tako ugotovil, da je treba dostop do tega dokumenta zavrniti. Glede zatrjevane izjeme notranjega delovanja organa pri določenem delu dokumenta (Splošni pogoji Banke Slovenije – Top - down challenge of bottom up stress tests results by an independent consulting firm – BoS Terms of Reference), je Informacijski pooblaščenec ugotovil, da navedeni dokument sicer izpolnjuje prvi kriterij te izjeme, saj je bil sestavljen v zvezi z notranjim delovanjem organa, vendar pa organ ni uspel izkazati, da bi razkritje določenega dela dokumenta (prvi in drugi odstavek točke 1. Introduction and objectives, zadnji odstavek na strani 4 ter celotna točka 6. Final results) povzročilo motnje pri delovanju oz. dejavnosti organa (t. i. specifični škodni test). Besedo »motnje« je namreč treba razlagati v smislu, da bi razkritje podatka pomenilo resno oviro za nadaljnje delo organa oz. bi bilo to delo bistveno drugače (po kvaliteti slabše), kot je bilo pred razkritjem oz. kakršno bi bilo, če do razkritja dokumenta ne bi prišlo. Dokazni standard glede izkazovanja motnje organa je dokazni standard »onkraj dvoma«, kar je potrdilo tudi Upravno sodišče RS.<sup>11</sup> Glede navedenih delov splošnih pogojev organa tako škoda ni izkazana in ti podatki predstavljajo prosto dostopno informacijo.

### 2.6.2. Ponovna uporaba

Informacijski pooblaščenec je z odločbo št. 090-263/2013/5 z dne 27. 1. 2014 odpravil sklep o zavrnjenju Agencije RS za javnopravne evidence in storitve (AJPES) in organu naložil, da prosilcu posreduje kopijo izvoza najnovejše mesečne celotne baze Poslovnega registra Slovenije (PRS), širši nabor, v tekstovni obliki, s priloženo kopijo najnovejše različice dokumenta „Strukture podatkov iz Poslovnega registra Slovenije za posredovanje uporabnikom“ za ponovno uporabo v nepridobitne namene.

Prosilec je zahteval kopijo vseh podatkov iz PRS, pri čemer je navedel, da podatke potrebuje za nepridobitne namene informiranja javnosti z raziskavo s področja dostopa do informacij javnega značaja. V PRS objavljeni podatki namreč prosilcu za te namene ne zadostujejo.

Organ je prosilca dvakrat pozval, da zahtevo dopolni. Ker prosilec tega ni storil, je organ njegovo zahtevo kot nepopolno zavrgel s sklepom. Ob tem je organ navedel, da v zahtevi prosilca ni natančno navedeno, kdo je naročnik podatkov, kateremu naj izda odločbo, prav tako prosilec ni dovolj jasno opredelil načina ponovne uporabe informacij, ki jih zahteva, in ni navedel razlogov, zaradi katerih podatke potrebuje.

Informacijski pooblaščenec je ugotovil, da organ ni imel zakonske podlage za pozivanje prosilca k dopolnitvi vloge. Iz nje je bilo namreč jasno razvidno, katere informacije prosilec želi (PRS v elektronski obliki), na kakšen način želi zahtevane informacije prevzeti (prenosljivi na USB pomnilnik ali prenosni disk) in za kakšen namen želi informacijo ponovno uporabiti (nepridobitni namen, za informiranje javnosti z raziskavo s področja dostopa do informacij javnega značaja, v okviru katere sodeluje z mednarodno organizacijo Access

<sup>10</sup> Uradni list RS, št. 49/2006 s spremembami; v nadaljevanju ZPRS-1.

<sup>11</sup> Sodba Upravnega sodišča RS št. I U 1176/2010-13 z dne 30. 11. 2011.

Info). Iz slednjega tudi jasno izhaja, na kakšen način bodo zahtevane informacije na voljo javnosti. Zahteva prosilca je tako v celoti zrela za meritorno obravnavo. Pri vprašanju, katere podatke organ od prosilca v primeru zahteve za ponovno uporabo lahko zahteva, je treba izhajati iz četrtega odstavka 17. člena ZDIJZ v povezavi s 5. členom ZDIJZ. Slednji določa uporabo načela prostega dostopa, po katerem so informacije javnega značaja fizičnim in pravnim osebam prosto dostopne, in pomeni, da se za dostop do informacij javnega značaja pravnega ali kakršnega koli drugega interesa ne zahteva, organ pa nima podlage, da bi ugotavljal te okoliščine v postopku. Organ torej ni ravnal pravilno, ko je od prosilca v pozivu k dopolnitvi zahteve terjal, naj natančneje navede predvideni način ponovne uporabe informacij za nepridobitne namene ter razloge, zaradi katerih potrebuje vse podatke PRS oz. iz kakšnega izdelka bo razvidna uporaba teh podatkov.

Informacijski pooblaščenec je tudi ugotovil, da ni podana nobena od izjem iz šestega odstavka 6. člena ZDIJZ, zaradi katerih bi bilo treba zahtevo prosilca za ponovno uporabo zavrniti.

V odločbi je Informacijski pooblaščenec tudi opozoril, da je prosilec pri nadaljnji uporabi dolžan upoštevati omejitve glede obdelave osebnih podatkov, ki izhajajo iz zakona, ki ureja sodni register, in zakona, ki ureja varstvo osebnih podatkov. Konkretno mora prosilec glede podatkov o lastniških deležih gospodarskih družb, ki v skladu s 3. alinejo 8. člena ZPRS-1 izvirajo iz sodnega registra, upoštevati tudi omejitve iz 50. člena ZSReg. Pri ponovni uporabi zadevnih podatkov jih prosilec javnosti ne sme ponuditi na način, ki bi dovolil ugotovitev, ali je določena oseba v določenem subjektu vpisa ustanovitelj, družbenik ali član nadzornega sveta, oz. ugotovitev, v katerih subjektih vpisa je določena oseba ustanovitelj, družbenik oz. član nadzornega sveta. Dostop do teh podatkov je lahko omogočen zgolj posredno, prek dostopa do posameznega subjekta vpisa. V skladu s 26. členom Uredbe o posredovanju in ponovni uporabi informacij javnega značaja<sup>12</sup> mora prosilec pri ponovni uporabi podatkov navesti tudi vir podatkov (Javne informacije AJPES).

### 2.6.3. Osebnih podatki

Z odločbo št. 090-255/2013/9 z dne 14. 2. 2014 je Informacijski pooblaščenec odpravil odločbo Družbe za avtoceste v Republiki Sloveniji (DARS) in ji naložil, da prosilcu omogoči vpogled v Pravno mnenje izpolnjevanje pogoja delovnih izkušenj za izbiro kandidata na javnem razpisu.

Organ je v celoti zavrnil zahtevo prosilca, da mu po elektronski pošti posreduje pravno mnenje, ki ga je naročil organ in ki je pokazalo, da ima določen kandidat ustrezne izkušnje za zasedbo delovnega mesta člana uprave organa. Pri zavrnitvi se je organ skliceval na izjemo iz 8. točke prvega odstavka 6. člena ZDIJZ in navajal, da bi razkritje zahtevanega dokumenta lahko škodilo sodnemu postopku, za katerega je bil zahtevani dokument izdelan. Prav tako se je organ skliceval na izjemo iz 3. točke prvega odstavka 6. člena ZDIJZ, ker naj bi dokument vseboval varovane osebne podatke.

V pritožbenem postopku je izdelovalka zahtevanega pravnega mnenja kot stranska udeleženka navedla, da bi z razkritjem kršili določbe Zakona o odvetništvu<sup>13</sup> glede dolžnosti odvetnika, da varuje poklicno tajnost. Po njenem mnenju gre za kolizijo ZDIJZ in ZOdv, pri čemer je slednji specialnejši in ga je treba upoštevati pred ZDIJZ.

Informacijski pooblaščenec je v pritožbenem postopku izpostavil, da stransko udeleženko ZOdv sicer res zavezuje k varovanju zaupnosti podatkov strank in vsebine odvetnikovega spisa. Vendar je v danem primeru zahtevani dokument s tem, ko je bil izdelan in izročen zavezancu za dostop do informacij javnega značaja, postal del njegove dokumentacije. Pravica do informacije, s katero razpolaga organ, pa je posebej urejena v ZDIJZ. Poleg tega ZOdv ne zavezuje k molčečnosti organa, zato do kolizije med predpisoma ne pride.

<sup>12</sup> Uradni list RS, št. 76/2005 s spremembami; v nadaljevanju Uredba.

<sup>13</sup> Uradni list RS, št. 18/1993 s spremembami; v nadaljevanju ZOdv.

V zvezi z zatrjevano izjemo iz 8. točke prvega odstavka 6. člena ZDIJZ je Informacijski pooblaščenec ugotovil, da je sodni postopek, na katerega se sklicuje organ, še vedno v teku, vendar pa ne organ ne pristojno sodišče nista izkazala, da bi z njegovim razkritjem nastala škoda za izvedbo postopka. Sodišče se v pojasnilih Informacijskemu pooblaščenec ni opredelilo do tega vprašanja, kar pa ne more biti razlog za zavrnitev dostopa do zahtevane informacije. Hkrati je organ v izpodbijani odločbi zgolj navedel, da bi z razkritjem informacij nastala škoda za sodni postopek, nič pa se ni opredelil do ključnih elementov škode in ni izkazal verjetnosti nastanka škode. S takšnim pavšalnim zatrjevanjem škode organ ni izpolnil dokaznega bremena, ki ga zahteva izjema iz 8. točke prvega odstavka 6. člena ZDIJZ. Posledično velja predpostavka, da javni interes po zagotavljanju javnosti, odprtosti (transparentnosti) in čim večje obveščenosti javnosti, tudi javni nadzor nad delovanjem javnopравnih subjektov, pretehtata.<sup>14</sup> Poleg tega je Informacijski pooblaščenec ugotovil, da razkritje zahtevanega dokumenta ne more povzročiti škode za sodni postopek. Zahtevani dokument je organ v sodnem postopku predložil sodišču in je z njim seznanjena tudi nasprotna stranka. Organ zato z razkritjem dokumenta ne bi bil postavljen v neenakopraven položaj kot stranka, ki v postopku varuje svoje pravice in interese. Poleg tega izvensodno izdelano pravno mnenje predstavlja zgolj določeno zatrjevanje stranke, odločitev pa je vselej v pristojnosti sodišča. Sodišče je dolžno preveriti pravilnost trditev strank in odločiti na podlagi listin, ki jih stranke vložijo, njihovih argumentov in na podlagi zakona, ne glede na to, katere informacije iz sodnega spisa so javno prosto dostopne. Svoboda informiranja in razvito javno mnenje sta namreč izredno pomembna za preprečevanje zlorab in za demokratično izvrševanje državne oblasti. To pa pomeni, da se o tem razpravlja tudi izven sodišča, v obliki javnega mnenja, vendar to ne more in ne sme vplivati na strokovno delo sodnikov, na njihovo neodvisnost in nepristranskost. Informacijski pooblaščenec je tako ugotovil, da izjema iz 8. točke prvega odstavka 6. člena ZDIJZ ni podana, saj ni izkazano, da bi z razkritjem zahtevanega dokumenta nastala škoda za sodni postopek.

Informacijski pooblaščenec je ugotovil tudi, da zahtevani dokument ne vsebuje varovanih osebnih podatkov, saj v njem ni nobenih konkretnih podatkov o posamezniku. Gre le za splošne ugotovitve izdelovalca pravnega mnenja, kako pravno interpretirati delovne izkušnje na vodilnih delovnih položajih in kako jih izkazati. Poleg tega so v postopku imenovanja članov uprave družbe v večinski lasti države izredno pomembni strokovnost in izkušnje ljudi, ki jih vodijo, da bi omogočili njihovo kakovostno upravljanje. Zato je pri vprašanju, ali država zaposluje ustrezno usposobljene ljudi oz. katere delovne izkušnje država šteje za ustrezne za zasedbo najpomembnejših delovnih mest v podjetju v njeni 100-odstotni lasti, nedvomno podan tudi javni interes. Sklicevanje na izjemo po 3. točki prvega odstavka 6. člena ZDIJZ pri zavrnitvi dostopa do zahtevane informacije tako ni utemeljeno.

Ker pa zahtevani dokument predstavlja avtorsko delo po določbah Zakona o avtorski in sorodnih pravicah<sup>15</sup>, pri čemer je imetnik avtorskih pravic avtor dokumenta (in ne organ), je Informacijski pooblaščenec v skladu z določbo drugega odstavka 25. člena ZDIJZ zavrnil pravico prosilca do prejema elektronske ali fizične kopije dokumenta. Prosilec ima pravico le do vpogleda v zahtevani dokument.

#### 2.6.4. Poslovna skrivnost

Informacijski pooblaščenec je z odločbo št. 090-1/2014/12 z dne 25. 3. 2014 odpravil odločbo Ministrstva za finance, s katero je ta zavrnil zahtevo prosilke po posredovanju podatkov o tem, kdo je kupec 15. 11. 2013 izdanih državnih obveznic. Ministrstvu je Informacijski pooblaščenec naložil, da prosilki posreduje zahtevano informacijo.

Organ je v izpodbijani odločbi zatrjeval, da zahtevani podatek predstavlja izjemo od dostopa po 2. in 11. točki prvega odstavka 6. člena ZDIJZ.

<sup>14</sup> Glej sodbi Upravnega sodišča RS v zadevah U 2423/2007 z dne 12. 5. 2010 in U 1976/2008-26 z dne 26. 5. 2010.

<sup>15</sup> Uradni list RS, št. 16/2007 – uradno prečiščeno besedilo, s spremembami; v nadaljevanju ZASP.

Glede zatrjevane izjeme poslovne skrivnosti je Informacijski pooblaščenec ugotovil, da organ sodi v izvršilno vejo oblasti in kot tak ne sodi med gospodarske subjekte (gospodarske družbe) po ZGD-1. Ker je predmet presoje dokument, ki ga je ustvaril organ, tako ni mogoče, da bi bil glede tega dokumenta izpolnjen subjektivni kriterij za obstoj poslovne skrivnosti iz prvega odstavka 39. člena ZGD-1. Z vidika izpolnjenosti objektivnega kriterija iz drugega odstavka 39. člena ZGD-1 za obstoj poslovne skrivnosti pa je v konkretnem primeru bistveno vprašanje, ali bi z razkritjem zahtevane informacije nastala občutna škoda kupcu dne obveznic in ne državi. Organ se je pri utemeljevanju obstoja objektivnega kriterija zgolj na splošno skliceval, da so tovrstni podatki za finančne institucije zaupni, ob tem pa spregledal, da gre pri večini tovrstnih poslov, ko gre za vprašanje prodaje obveznic države, za odprte postopke, saj je jasno, da je podan širši interes javnosti, da se tovrstni postopki vodijo transparentno in da javnosti niso dostopni le podatki, za koliko se mora država zadolžiti, temveč tudi, kdo je pripravljen v državo na ta način investirati. Zahtevana informacija izkazuje, ali država gospodarno razpolaga z javnimi sredstvi, saj gre za razpolaganje z denarjem davkoplačevalcev. Poleg tega je kupec obveznic v pritožbenem postopku sam navedel, da njegova identiteta v vlogi investitorja v novembrsko zaprto izdajo obveznic zanj ne predstavlja poslovne skrivnosti ter da ne nasprotuje razkritju svoje identitete.

Treba pa je upoštevati tudi dejstvo, da glede na določbe Zakona o javnih financah<sup>16</sup> o sklepanju poslov v zvezi z zadolževanjem države in upravljanjem z državnimi dolgovi odloča minister za finance na podlagi letnega programa financiranja proračuna, ki ga sprejme vlada. Minister za finance torej sam odloča o vrsti dolgoročnega instrumenta zadolževanja, njegovi ročnosti in dinamiki izdaje, prav tako v okviru določenih vrednosti odloča o višini potrebnih sredstev. V konkretnem primeru se je minister za finance odločil za izdajo obveznic, v okviru bilateralnega pogajanja z enim potencialnim kupcem, s čimer je odstopil od sicer običajne prakse javne izdaje državnih obveznic. Sam postopek izdaje obveznic sicer ni normativno določen, temveč je odvisen od tržne prakse in poslovnih običajev države, v kateri se obveznice izdajajo. Zgolj dejstvo, da tržna praksa predvideva, da se podatka o investitorjih ne razkriva, še ne pomeni, da je slednje mogoče vedno upoštevati v primerih, kadar je izdajatelj obveznic država. V primeru državne izdaje obveznic je izdajatelj subjekt javnega prava, za katerega veljajo drugačna pravila, saj upravlja z javnimi sredstvi, zato je tudi podan širši interes javnosti, da se tovrstni postopki vodijo transparentno, gospodarno in da javnosti niso dostopni samo podatki, za koliko se mora država zadolžiti, temveč tudi, kdo je pripravljen v državo na ta način investirati. Razlika med javno izdajo državnih obveznic in zasebnim plasmajem obveznic je v tem, da imajo v prvem primeru državne obveznice možnost kupiti vsi potencialni investitorji ter da se država odloči za tistega, ki ponudi najvišjo ceno in najugodnejše pogoje, pri zasebni izdaji državnih obveznic, pa se država pogaja z enim samim investitorjem, pri čemer ni mogoče brez dvoma vedeti, ali je država iztržila boljše pogoje in ugodnejšo ceno, kot bi jo z javno ponudbo svojih obveznic. Izdaje obveznic na podlagi dogovorov med državo in enim investitorjem (oz. ožjim krogom investitorjev) morajo zato biti toliko bolj transparentne in obrazložene.

V zvezi z zatrjevano izjemo iz 11. točke prvega odstavka 6. člena ZDIJZ je Informacijski pooblaščenec ugotovil, da ni izpolnjen niti prvi pogoj za obstoj te izjeme. Zahtevani podatek namreč ni akt beleženja notranjega delovanja oz. postopka oblikovanja odločitev organa, saj ne vsebuje podatkov oz. informacij o tem, kako je organ oblikoval svojo politiko oz. kako je potekal postopek notranjega razmišljanja organa, preden je prišel do odločitve, ki je zabeležena v njem. Poleg tega je zahtevani dokument ni namenjen le organu, temveč tudi tretji osebi – banki, saj vsebuje bistvene podatke o mandatu, ki je bil s strani države podeljen banki. Hkrati se zahtevani dokument posreduje tudi borzi, na kateri izdane državne obveznice kotirajo. Organ tudi ni uspel izkazati drugega pogoja za obstoj navedene izjeme, torej da bi razkritje dokumenta povzročilo škodo za notranje delovanje organa. Sklicevanje organa na to, da se bodo zaradi razkritja dokumenta potencialni bodoči investitorji na trgu obnašali drugače in ne bodo želeli investirati v Republiko Slovenijo, saj bi bila ob tem njihova investicija razkrita javnosti, je neutemeljeno. Razkritje konkretnega investitorja, glede na to, da je odločitev o podelitvi mandata banki že sprejeta, da so bile obveznice na podlagi tega mandata že prodane ter da investitor ne nasprotuje razkritju svoje identitete, nikakor ne more povzročiti motenj v delovanju oz. dejavnosti organa.

<sup>16</sup>

Uradni list RS, št. 11/2011 – uradno prečiščeno besedilo 4; s spremembami, v nadaljevanju ZJF.

Informacijski pooblaščenec pa je podredno ugotovil tudi, da je v konkretnem primeru javni interes glede razkritja zahtevanega dokumenta močnejši od javnega interesa ali interesa drugih oseb za omejitev dostopa do zahtevanega dokumenta. Slednji je namreč povezan z medijsko zelo odmevnimi temami, zadolževanje države pa je postalo predmet širše javne razprave, ki se navezuje tudi na način izdaje obveznic v konkretnem primeru, saj je država pri izdaji predmetnih obveznic odstopila od svoje prakse in obveznic ni izdala z javno ponudbo, temveč v okviru zaprte ponudbe. Za to prakso se tudi druge države redko odločajo. Javni interes se zato kaže v širši razpravi o tem, ali so bila ravnanja organa v zvezi z izdajo obveznic v zaprti izdaji za državo finančno smotna in primerna ter ali netransparentnost izdaje obveznic ne daje vtisa, da je bilo morda z izdajo teh obveznic morebiti povezano še kaj drugega ter da smo kupcu obveznic morda obljubili nekaj, česar ne bi smeli, oz. da bi se država morda uspela zadolžiti ugodneje, če bi svoje obveznice ponudila javno, vsem pod enakimi pogoji ter bi izbrala najugodnejšega ponudnika. Zneski, za katere se je država zadolžila, so tako visoki, da ne bodo bremenili le današnje generacije, temveč tudi prihodnje, zato mora biti taka zadolžitev pregledna in ustrezno razkrita javnosti, saj so državljani tisti, ki so to zadolžitev dolžni financirati. Zadolževanje in vrnitev teh sredstev z obrestmi dnevno terja zmanjševanje socialnih in drugih pravic državljanov, kar posledično pomeni tudi zmanjšanje kakovosti življenja, zdravja in varnosti posameznikov. Problematika s tega področja se tako ne dotika le prosilke, temveč vseh pravnih in fizičnih oseb, ki so zavezane za plačevanje davkov in prispevkov v Republiki Sloveniji, kot tudi preostale širše javnosti. Javni interes se torej kaže v zahtevi po preglednem, odprtem delovanju organov, v potrebi po tem, da delujejo odgovorno in skrbno, kadar se odločajo o javnem zadolževanju.

#### 2.6.5. Proaktivna objava

Z odločbo št. 090-46/2014/8 z dne 12. 4. 2014 je Informacijski pooblaščenec opravil odločbo Banke Slovenije in prosilca napotil na spletno stran, kjer so bili objavljeni dokumenti, ki jih je zahteval.

Banka Slovenije je z izpodbijano odločbo delno ugodila zahtevi prosilca po odločbah, s katerimi so prenehale obveznice z ISIN oznako XS0283183084 in XS0325446903, in odločbah Banke Slovenije o izrednih ukrepih zoper vseh pet poslovnih bank. Zahtevane odločbe je organ prosilcu posredoval, vendar je v njih prekril dele odločb, ki predstavljajo izjeme po 2., 3., 7. in 11. točki prvega odstavka 6. člena ZDIJZ.

Glede zahtevanih odločb o izrednih ukrepih je Informacijski pooblaščenec v pritožbenem postopku ugotovil, da jih je organ v celoti objavil na svoji spletni strani, na povezavi <https://www.bsi.si/nadzor-bank.asp?Mapald=1600>. Tam je organ odločbe o izrednih ukrepih objavil tako, da je levo objavljena odločba o izrednih ukrepih s prekritimi podatki, kot jo je prosilec prejel na podlagi izpodbijane odločbe, desno pa celotna vsebina odločbe o izrednih ukrepih. Takšen način objave omogoča primerjavo celotne odločbe o izrednih ukrepih z odločbo o izrednih ukrepih v obliki delnega dostopa. Po pojasnilih organa so odločbe na spletni strani objavljene v izvorni obliki, umaknjena je le oznaka »strogo zaupno«, da pri objavi odločbe ne bi prišlo do kršitev predpisov, ki urejajo varovanje zaupnosti. Ker so bile odločbe o izrednih ukrepih v celoti objavljene na spletu s strani organa, je Informacijski pooblaščenec ugotovil, da ugotavljanje obstoja izjem od dostopa do zahtevanih dokumentov ni potrebno. Ker objavljene odločbe o izrednih ukrepih na spletni strani organa v celoti razkrivajo vsebino, je prosilec z vpogledom vanje tudi v celoti seznanjen z zahtevanimi dokumenti in je s tem dosežen namen zahteve prosilca, ki ga ZDIJZ zasleduje. Na podlagi petega odstavka 6. člena ZDIJZ je zato Informacijski pooblaščenec prosilca napotil na spletno stran organa, kjer so objavljene zahtevane odločbe o izrednih ukrepih.

Informacijski pooblaščenec je v pritožbenem postopku ugotovil še, da je organ prosilcu posredoval tudi odločbi o prenehanju obveznosti iz obveznic št. 24.20-022/13-009 in št. 24.20-023/13-009, obe z dne 17. 12. 2013, ki ju je zahteval prosilec. Tudi navedeni odločbi sta objavljeni na že omenjeni spletni strani.

V zvezi z navedbami prosilca, da mu organ ni obrazložil razlike med odločbo, v kateri ni omenjena obveznica z ISIN oznako XS0283183084, in uradnim obvestilom na spletni strani Abanke, kjer je obveznica z ISIN oznako XS0283183084 omenjena, je Informacijski pooblaščenec izpostavil, da se prost dostop lahko zagotovi le do informacij, ki dejansko že obstajajo. Organi, ki so zavezani po ZDIJZ, so dolžni omogočiti dostop le do že obstoječih informacij in na podlagi zahteve za dostop do informacij javnega značaja niso dolžni ustvariti novega dokumenta ter za prosilca pripravljati pojasnil ali razlag. Pritožbeni postopek ni in ne more biti namenjen prisili ustvarjanja informacij ali ugotovitvi, da bi določene informacije morale obstajati. Informacijski pooblaščenec zato organu ne more naložiti, naj prosilcu posreduje dokumentacijo, s katero ne razpolaga (npr. z razlago ali pojasnilom glede obveznic).

### 2.6.6. Dokument v izdelavi

Informacijski pooblaščenec je z odločbo št. 090-116/2014/3 z dne 12. 6. 2014 odpravil odločbo Ministrstva za pravosodje in mu naložil, da prosilcu posreduje zahtevana strokovna mnenja v zvezi z ratifikacijo Konvencije Sveta Evrope o preprečevanju nasilja nad ženskami in nasilja v družini ter boja proti njima.

Organ je z izpodbijano odločbo zahtevo prosilca v celoti zavrnil, pri čemer se je skliceval na obstoj izjeme iz 9. točke prvega odstavka 6. člena ZDIJZ. Navedel je, da še ni dokončno oblikoval stališča glede ratifikacije predmetne konvencije. Razkritje do zdaj prejetih mnenj bi zato prejudiciralo končno mnenje organa, saj so zahtevana mnenja precej različna. Zahtevani dokumenti so torej predmet »posvetovanja« v organu, saj mora pristojna notranja organizacijska enota mnenje šele dokončno izdelati. Posredovanje strokovnih mnenj bi lahko povzročilo napačno razumevanje ter posledično nepotrebne zaplete, ki so zaradi kompleksnosti in obsežne problematike obravnavane zadeve še toliko verjetnejši.

Informacijski pooblaščenec je v pritožbenem postopku ugotovil, da ni mogoče slediti navedbam organa, da zahtevani dokument ne obstaja, ker organ še ni sprejel končnega mnenja glede ratifikacije konvencije. Prosilec namreč ni zahteval končnega mnenja organa, temveč strokovna mnenja, ki jih je v postopku priprave svojega mnenja pridobil organ. Vsa zahtevana mnenja so zaključena, podpisana s strani odgovornih oseb in posredovana organu, zato ne gre več za dokumente v nastajanju v smislu izjeme iz 9. točke prvega odstavka 6. člena ZDIJZ. Iz mnenj izhaja, da je njihova vsebina zaključena in da so inštitucije, ki so mnenja posredovale, že izoblikovale svoja stališča glede ratifikacije t. i. Istanbulske konvencije in jih posredovale organu. Dejstvo, da organ še ni sprejel »končnega« mnenja, ne pomeni, da so dokumenti, na podlagi katerih bo to mnenje (med drugim) temeljilo, še v postopku izdelave. Tudi če bi inštitucije, ki so svoja mnenja že posredovale organu, pozneje ta mnenja spremenile oz. dopolnile, ne bi mogli reči, da so že posredovani dokumenti še v fazi nastajanja. Dejstvo je namreč, da je dokument izdelan, ko ga podpiše oseba, ki je pri določenem organu oz. drugem subjektu pooblaščen za odločanje, ta kriterij pa je v konkretnem primeru glede vseh posredovanih mnenj izpolnjen. Vsak dokument – prejeto mnenje – torej predstavlja samostojen dokument, ki je izdelan v smislu ZDIJZ, zato za obstoj izjeme iz 9. točke prvega odstavka 6. člena ZDIJZ že prvi pogoj (da je dokument še v postopku izdelave pri organu) ni izpolnjen. Ker zahtevana mnenja niso več predmet posvetovanja pri organih oz. inštitucijah, ki so jih podali (seveda pa so lahko predmet posvetovanja pri drugem organu, vendar je to posvetovanje namenjeno izdelavi novega dokumenta v smislu ZDIJZ, to je končnega mnenja organa, ki ga ta še pripravlja), tudi drugi pogoj za obstoj izjeme po 9. točki prvega odstavka 6. člena ni izpolnjen.

Prav tako ni izpolnjen tretji kriterij, ki izhaja iz 9. točke prvega odstavka 6. člena ZDIJZ, saj organ ni izkazal, da bi razkritje zahtevanih dokumentov povzročilo škodo v smislu napačnega razumevanja njihove vsebine. Upošteva dejstvo, da prosilec ni zahteval mnenja organa, ampak mnenja inštitucij, od katerih je mnenja pridobil organ, Informacijski pooblaščenec ne vidi možnosti, da bi razkritje teh mnenj (katerih vsebina je zaključena) lahko povzročilo možnost njihovega napačnega razumevanja. Ker so si zahtevana mnenja med seboj

nasprotujoča in vsebujejo razloge za in proti ratifikaciji konvencije, je še toliko pomembnejše, da se javnost z njimi seznani. Pri tako pomembnem vprašanju, kot je ratifikacija mednarodne konvencije, ima javnost namreč pravico sodelovati v najširši meri, posledično pa se ima tudi pravico seznaniti z vsemi argumenti, ki govorijo ratifikaciji v prid ali proti njej. ZDIJZ je v tem pogledu izjemno naklonjen transparentnosti, saj v 2. točki prvega odstavka 10. člena določa, da je vsak organ dolžan v svetovni splet posredovati programe, strategije, stališča, mnenja in navodila, ki so splošnega pomena ali so pomembna za poslovanje organa s fizičnimi in pravnimi osebami oz. za odločanje o njihovih pravicah ali obveznostih, študije in druge podobne dokumente, ki se nanašajo na delovno področje organa. Med te dokumente praviloma sodijo tudi mnenja, ki jih organi izdajajo v določeni fazi postopka odločanja glede ratifikacije mednarodnih konvencij, pa čeprav so po svojem smislu le predlogi oz. rešitve, ki še ne predstavljajo končne odločitve. Ne nazadnje so zahtevana mnenja izdelale inštitucije, ki so tudi same pravne osebe javnega prava in s tem zavezane postopati po ZDIJZ, zato tudi njih zavezuje načelo odprtosti delovanja iz 2. člena ZDIJZ. Posledično zahtevani dokumenti tudi zanje ne predstavljajo nobene izmed zakonskih izjem, zaradi katerih se dostop do informacij javnega značaja lahko zavrne.

### 2.6.7. Notranje delovanje organa

Z odločbo št. 090-61/2014/6 z dne 13. 6. 2014 je Informacijski pooblaščenec odpravil odločbo Državnega izpitnega centra in mu naložil, da prosilcu iz baze podatkov vseh osnovnih šol posreduje podatke o povprečnih dosežkih učencev in učenk pri nacionalnem preverjanju znanja za angleščino, slovenščino, matematiko, biologijo in geografijo za šolska leta 2010/2011, 2011/2012 in 2012/2013.

Organ je z izpodbijano odločbo zavrnil zahtevo prosilca in navedel, da zahtevani dokument ne obstaja v obliki, kot jo zahteva prosilec. Dokument oz. informacija, kjer bi bili zahtevani podatki zbrani skupaj, pri organu ne obstaja. Grafi, ki so javno objavljeni v Letnem poročilu o izvedbi nacionalnega preverjanja znanja, so rezultat programske kode, ki je povezana neposredno z dosežki posameznih učencev v podatkovni bazi in v kateri ni imen šol. Nikjer v podatkovni bazi organa tudi ni povprečnih dosežkov šol.

Informacijski pooblaščenec je v pritožbenem postopku ugotovil, da navedbe organa, da z zahtevanimi informacijami ne razpolaga, ne držijo. Zato je, upoštevaje določbo drugega odstavka 164. člena zakona o splošnem upravnem postopku<sup>17</sup>, kot dokazno sredstvo uporabil zapisnik o ogledu in camera, ki je bil izdelan v zadevi št. 090-214/2012, saj je predmet zahteve v obeh zadevah identičen. Razlika med obema zahtevama je le v tem, da je v obravnavani zahtevi prosilec zahteval podatke za več let in za več osnovnošolskih predmetov. Če bi Informacijski pooblaščenec odločil v nasprotju s svojim stališčem v odločbi št. 090-214/2012/4 z dne 5. 12. 2012 in s stališčem, ki ga je Upravno sodišče RS zavzelo v sodbi št. I U 44/2013-14 z dne 16. 10. 2013, bi prišlo do kršitve enakega varstva pravic (22. člen Ustave RS) in načela zaupanja v pravo (2. člen Ustave RS).

Iz zapisnika o ogledu in camera v zadevi št. 090-214/2012 izhaja, da organ dokumenta oz. podatka, iz katerega izhaja povprečna uspešnost konkretne osnovne šole pri nacionalnem preverjanju znanja pri slovenščini (oz. angleščini) nima, ga pa lahko prikljče iz svoje baze podatkov. Organ je zelo hitro pridobil (prikljal) podatek o povprečni uspešnosti določene šole pri nacionalnem preverjanju znanja pri slovenščini leta 2010/2011. Enake podatke lahko organ prikljče tudi za angleščino. Glede na to, da organ v konkretni zadevi ni zanikal, da bi bilo na enak način mogoče prikljcati tudi podatke, ki so predmet obravnavanih zahtev prosilca, je Informacijski pooblaščenec ugotovil, da je istovrstne podatke mogoče hitro in preprosto prikljcati tudi za leta 2012 in 2013 ter za matematiko, biologijo in geografijo. Argument organa, da bi priklj ob obravnavanih podatkov za organ pomenil nesorazmeren napor zunaj preprostega postopka, torej ne zdrži resne pravne presoje. Posledično tudi ne držijo navedbe organa, da takšen priklj podatkov predstavlja izdelavo novega dokumenta

<sup>17</sup> Uradni list RS, št. 24/2006 – uradno prečiščeno besedilo 2 s spremembami, v nadaljevanju ZUP.



v smislu ZDIJZ. Organi, zavezanci po ZDIJZ, so dolžni omogočiti dostop le do že obstoječih informacij in niso dolžni ustvariti novega dokumenta, zbirati informacij, opravljati raziskav ali analizirati podatkov, da bi zadostili zahtevi prosilca. Izjema od napisanega so le informacije, ki so v računalniških bazah, nastalih v zvezi z dejavnostjo organa. Dolžnost posredovanja informacij se namreč nanaša le na t. i. surove informacije.<sup>18</sup> V duhu namena zakona, da se zagotovi javnost in odprtost delovanja organov ter se omogoči uresničevanje pravice posameznikov in pravnih oseb, da pridobijo informacijo javnega značaja, je torej pri dokumentih ali podatkih, ki so v informacijskih bazah organa, potreben relativiziran pristop. V praksi se je tako izoblikovalo stališče, da mora organ zavezanec omogočiti dostop do dokumentov, ki so v računalniških bazah, čeprav priklic iz zbirke, tehnično gledano, pomeni nastanek (ustvarjanje) novega dokumenta.

Informacijski pooblaščenec se zaveda, da je v določenih primerih za priklic podatkov iz računalniške baze lahko potreben določen čas. Vendar je pri tem treba upoštevati, da mora organ narediti vse, kar je od njega mogoče razumno pričakovati, da zadosti zahtevam za dostop do informacij javnega značaja. Organi so po ZDIJZ prosilcu dolžni posredovati zahtevane informacije v zahtevani obliki ob predpostavki, da razpolagajo tako z informacijo kot tudi z ustreznimi napravami ter strokovnim znanjem, da je takšen priklic informacij mogoč. Pri tem ni pomembno, ali organi z zahtevanimi podatki že razpolagajo v obliki datoteke, temveč je pomembno, ali informacijo lahko prikličejo iz svojega informacijskega sistema. Takšen priklic informacije pa ne pomeni nastanka novega dokumenta.

Informacijski pooblaščenec je tako ugotovil, da zahtevani dokumenti obstajajo in izpolnjujejo vse zakonske kriterije za informacijo javnega značaja, kot izhaja iz prvega odstavka 4. člena ZDIJZ, pri čemer ne vsebujejo podatkov, ki bi bili izjema od prostega dostopa do informacij javnega značaja. Zahtevi prosilca je zato treba ugoditi.

### 2.6.8. Poslovni subjekt pod prevladujočim vplivom, poslovna skrivnost

Informacijski pooblaščenec je z odločbo št. 0902-6/2014/4 z dne 9. 7. 2014 Zavarovalnici Triglav (zavezanec) naložil, da prosilki posreduje pogodbe z Goldman Sachs, Strelsko zvezo Slovenije, Motivo, d. o. o., in Pristop, d. o. o., v delu, ki se nanaša na zneske in datume pogodb ter storitve, ki so bile opravljene na podlagi teh pogodb.

Zavezanec je zahtevo prosilke zavrnil, ker naj ne bi šlo za informacije javnega značaja, kot jih opredeljuje novela ZDIJZ-C. Določene informacije, ki jih je zahtevala prosilka, sicer ustrezajo definiciji informacije javnega značaja, vendar predstavljajo poslovno skrivnost, zaradi česar se dostop do njih zavrne. V naknadnih pojasnilih je zavezanec oporekal skladnosti novele ZDIJZ-C z Ustavo RS, dodal pa je še, da je prosilka zahtevala odgovore na vprašanja in ne dokumente. Če bi jih posredoval dokumente, bi kršil načelo zakonitosti, saj je informacija javnega značaja lahko v skladu z določbo 4. člena le dokument oz. dokumentarno gradivo v fizični obliki. Ker se zahteva prosilke nanaša na informacije, ki so nastale pred 17. 4. 2014, ko je začela veljati novela ZDIJZ-C, bi bila ugoditev zahtevi prosilke v nasprotju z načelom prepovedi retroaktivne veljavnosti predpisov.

V zvezi z navedbami organa glede neustavnosti ZDIJZ-C je Informacijski pooblaščenec izpostavil, da ni zaznal nikakršnih neskladnosti določb ZDIJZ z Ustavo RS, zaradi česar tudi ni sprožil postopka za presojo ustavnosti navedenega predpisa. Glede očitane nasprotovanja načelu prepovedi retroaktivne veljavnosti predpisov, se je Informacijski pooblaščenec v odločbi skliceval na določbo petega odstavka 1.a člena, po kateri je poslovni subjekt pod prevladujočim vplivom oseb javnega prava zavezanec za dostop do informacij javnega značaja iz 4.a člena tega zakona, ki so nastale kadar koli v času, ko je bil pod prevladujočim vplivom oseb javnega prava. V to obdobje torej sodijo tudi informacije, ki jih zahteva prosilka.

<sup>18</sup> Več: Komentar Zakona o dostopu do informacij javnega značaja, doc. dr. Senko Pličanič s soavtorji, Inštitut za javno upravo pri Pravni fakulteti v Ljubljani, 2005, str. 83.

Glede navedb zavezanca, da je prosilka zahtevala odgovore na vprašanja in ne dokumentov, je Informacijski pooblaščenec zavezancu pritrnil, da mu ni treba na novo ustvariti informacije javnega značaja, če z njo še ne razpolaga – ni mu torej treba odgovarjati na vprašanja prosilcev in analizirati ali uparjati podatkov. Vendar pa mora prosilcu posredovati podatke, ki so v dokumentu (ali zadevi, dosjeju, registru, evidenci ali drugem dokumentarnem gradivu), s katerim razpolaga (in ga je izdelal sam, v sodelovanju z drugim organom ali ga je pridobil od drugih oseb), ne glede na to, ali je prosilec zahtevo formuliral v obliki vprašanja. Če torej zavezanec razpolaga z dokumentom, iz katerega je razviden odgovor na vprašanje prosilke, v materializirani obliki, ga mora prosilki posredovati. V konkretnem primeru je Informacijski pooblaščenec ugotovil, da organ razpolaga z dokumenti – pogodbami, iz katerih so razvidni odgovori na prosilčina vprašanja.

Vse zahtevane pogodbe sodijo v delovno področje zavezanca. ZDIJZ delovnih področij, glede katerih so poslovni subjekti pod prevladujočim vplivom oseb javnega prava zavezanci za dostop do informacij javnega značaja, ni opredelil glede na tip pogodbe po civilnopravni opredelitvi (oz. glede na pravno kvalifikacijo po Obligacijskem zakoniku), ampak jih je v tretjem odstavku 6.a člena ZDIJZ izrecno navedel. Izpolnjenost kriterijev delovnega področja se torej presoja glede na vsebinski učinek, ki ga pogodba dosega, in ne glede na civilnopravno kvalifikacijo tipa obveznosti. Argument, da pogodba ne sodi v domet tretjega odstavka 6.a člena, ker je podjemna pogodba, je v postopku dostopa do informacij javnega značaja tako pravno povsem irelevanten. Bistveno je vprašanje, ali določena storitev, opravljena na podlagi takšne pogodbe, dosega učinek storitev, kot jih dosegajo pogodbe, našteje v tretjem odstavku 6.a člena ZDIJZ. Namen, ki ga ZDIJZ zasleduje, je krepitev transparentnosti in odgovornega ravnanja pri upravljanju s finančnimi sredstvi poslovnih subjektov pod prevladujočim vplivom oseb javnega prava, zato je tudi jasno določil, kateri podatki iz katerih pogodb so absolutno javni. Interes javnosti je očitno prepoznal že zakonodajalec s sprejemom ZDIJZ-C, zato Informacijski pooblaščenec niti nima pristojnosti, da bi glede podatkov, ki jih je zahtevala prosilka in jih ZDIJZ opredeljuje v tretjem odstavku 6.a člena v povezavi s prvim odstavkom 6.a člena, tehtal med interesom prosilke za dostop do informacij javnega značaja in interesom zavezanca, da ščiti svoje poslovne interese, ker je tehtanje glede osnovnih podatkov o pogodbi predhodno opravil že zakonodajalec.

Informacijski pooblaščenec je v pritožbenem postopku ugotovil, da podatki, ki jih je zahtevala prosilka, izhajajo iz pogodb, s katerimi zavezanec razpolaga v materializirani obliki, in dosegajo učinke, opredeljene v tretjem odstavku 6.a člena ZDIJZ. Hkrati zahtevani podatki ne predstavljajo izjeme od prostega dostopa, ampak absolutno javne podatke, taksativno navedene v prvem odstavku 6.a člena ZDIJZ, zato je treba dostop do njih dopustiti.

### 2.6.9. Poslovna skrivnost

Z odločbo št. 090-103/2014/6 z dne 15. 7. 2014 je Informacijski pooblaščenec Družbi za upravljanje terjatev bank naložil, da prosilki posreduje zahtevane fotokopije zapisnikov sej upravnega odbora od ustanovitve organa naprej v delih, ki se nanašajo na sklepanje zunanjih svetovalnih pogodb.

Organ je zahtevo prosilke v celoti zavrnil zaradi izjeme varstva poslovne skrivnosti po 2. točki prvega odstavka 6. člena ZDIJZ, pri čemer se je skliceval na drugi odstavek 39. člena ZGD-1 (objektivni kriterij).

Prosilka se je pritožila glede zavrnitve njene zahteve po pridobitvi fotokopij zapisnikov sej upravnega odbora organa v delih, ki se nanašajo na sklepanje zunanjih svetovalnih pogodb. O preostalih delih zapisnikov Informacijski pooblaščenec zato, ob upoštevanju 247. člena ZUP Informacijski pooblaščenec, ni odločal.

Informacijski pooblaščenec je ugotovil, da je organ napačno uporabil določbe 2. točke prvega odstavka 6. člena ZDIJZ, hkrati pa pri odločanju ni upošteval določbe 7. člena ZDIJZ. S tem, ko je ugotovil, da so zapisniki dokumenti, ki so jih drugi poslovni subjekti označili za

poslovne skrivnosti, je tudi zmotno ugotovil dejstva. Z vpogledom v zapisnike je Informacijski pooblaščenec namreč ugotovil, da nobeden od dokumentov ni označen kot poslovna skrivnost, akt o varovanju poslovne skrivnosti pa je bil sprejet šele po njihovem nastanku. Posledično subjektivni kriterij za obstoj poslovne skrivnosti ni izpolnjen. Prav tako je Informacijski pooblaščenec ugotovil, da glede zahtevanih dokumentov ni izpolnjen objektivni kriterij za obstoj poslovne skrivnosti. Deli zapisnikov, ki se nanašajo na zunanje svetovalce oz. druge izvajalce, ne vsebujejo nič takega, kar bi kazalo na najmanjšo možnost nastanka kakršne koli škode, če bi za te podatke izvedela nepooblaščen oseba, še manj, da bi bila ta škoda potencialno lahko občutna, nikakor pa to ni očitno. Gre zgolj za pogovore in odločitve upravnega odbora, ki kažejo zlasti na modus operandi upravnega odbora pri odločanju za angažiranje zunanjih izvajalcev oz. svetovalcev in pri njihovi izbiri. Na določenih mestih je neločljiv del same diskusije tudi razlog za angažma zunanjih svetovalcev oz. izvajalcev. Ti deli nikakor ne morejo vplivati na položaj organa na trgu, še manj na poslovne subjekte, glede katerih se je upravni odbor pogovarjal in se nanje nanašajo nekatere odločitve o izbiri.

Uvodni in zaključni deli zapisnikov neposredno sicer res ne pomenijo pogovorov oz. odločitev o izbiri zunanjih izvajalcev, kar je zahtevala prosilka, vendar so ti podatki bistveni za zahtevane podatke – kdaj se je upravni odbor pogovarjal o izbiri oz. kdaj je odločal o zunanjih izvajalcih in kateri člani upravnega odbora so bili prisotni na seji, torej podatek o tem, kdo konkretno je odločal o zunanjih izvajalcih. V vseh dokumentih so navedena tudi imena in priimki članov upravnega odbora in vodilnih oseb organa. Ne glede na to, da gre za njihove osebne podatke, ti niso varovani, saj so bodisi javni na podlagi zakona (ZGD-1) bodisi gre za porabo javnih sredstev (ker so zaposleni pri organu in nastopajo v imenu odločevalcev o (potencialni) porabi javnih sredstev). V enem od dokumentov je bilo sicer navedeno tudi ime in priimek posameznika, ki ni noben od navedenih posameznikov, vendar gre za izbiro posameznika, ki je bil pozneje v zvezi z organom prepoznan kot relativno javna osebnost (o njem so veliko poročali mediji) in glede na to, da je bil izbran za opravljanje določenih funkcij in zanje tudi plačan, gre pri odločanju o njegovi izbiri tudi za porabo javnih sredstev. Enako velja za ime in priimek posameznika, ki sicer ni noben od navedenih posameznikov, vendar gre za angažiranje posameznika, ki dejavnost, za katero naj bi ga organ angažiral, opravlja kot registriran samostojni podjetnik posameznik, zato v tej zvezi njegovi osebni podatki niso varovani.

Organ bi lahko iz 12 zapisnikov prosilki omogočil seznanitev le z deli, ki jih je zahtevala, kar bi lahko storil s prekritjem preostalih delov, ob smiselnem upoštevanju določbe 7. člena ZDIJZ in Uredbe o posredovanju in ponovni uporabi informacij javnega značaja. Do drugih delov 12 zapisnikov, ki jih prosilka ni zahtevala, se Informacijski pooblaščenec ni opredelil, ker niso bili predmet zahteve, izpodbijane odločbe in pritožbe.

### 2.6.10. Tajni podatki, notranje delovanje organa

Informacijski pooblaščenec je z odločbo št. 090-231/2014/7 z dne 21. 10. 2014 odločil, da mora Vlada RS iz magnetograma 69. redne seje Vlade RS z dne 31. 7. 2014, na kateri je odločala o imenovanju kandidatke za evropsko komisarko, umakniti stopnjo tajnosti INTERNO in magnetogram v elektronski obliki posredovati na elektronski naslov prosilca.

Organ se je pri zavrnitvi dostopa do magnetograma skliceval na izjemo po 11. točki prvega odstavka 6. člena ZDIJZ, vendar je Informacijski pooblaščenec po uradni dolžnosti preverjal najprej, ali gre za podatek, ki je na podlagi Zakona o tajnih podatkih<sup>19</sup> opredeljen kot tajen. Na ogledu in camera je bilo namreč ugotovljeno, da je ta dokument označen s stopnjo tajnosti INTERNO, v zvezi z njim pa obstajata dve pisni oceni možnih škodljivih posledic, in sicer ocena generalne sekretarke vlade z dne 12. 8. 2014 in ocena generalnega sekretarja vlade z dne 10. 10. 2014.

<sup>19</sup> Uradni list RS, št. 50/2006 – uradno prečiščeno besedilo 2 s spremembami, v nadaljevanju ZTP.

Informacijski pooblaščenec je v pritožbenem postopku ugotovil, da nobena izmed navedenih ocen ne izpolnjuje vseh kriterijev, ki jih določa ZTP za tajne podatke, in zato obravnavani magnetogram ne more biti označen kot tajni podatek. Pri tem je ugotovil, da sta izpolnjena le dva elementa, ki sta predpisana za formalni kriterij za določitev podatka za tajnega – v skladu z določbo 17. člena ZTP je dokument vidno označen s stopnjo tajnosti (INTERNO), oceno možnih škodljivih posledic pa je, v skladu z določbo 10. člena ZTP, podpisala za to pooblaščenca oseba: generalni sekretar vlade na podlagi pooblastila predsednika vlade. Ni pa izpolnjen tretji element za formalni kriterij, saj ocena škodljivih posledic ne izpolnjuje pogojev iz 11. člena ZTP – ne vsebuje navedbe in konkretizacije možnih škodljivih posledic, ki naj bi nastale z razkritjem dokumenta za delovanje ali izvajanje nalog organa. Poleg tega omenjeni oceni ne izpolnjujeta pogojev iz prvega oz. četrtega odstavka 11. člena ZTP, saj sta bili izdani prepozno. Informacijski pooblaščenec je zaključil, da eden izmed elementov, ki morajo biti kumulativno podani za opredelitev obstoja formalnega kriterija za klasifikacijo podatka za tajni podatek, ni izpolnjen.

Prav tako je Informacijski pooblaščenec ugotovil, da ni podan materialni kriterij za določitev zahtevanega dokumenta za tajnega po ZTP, saj organ ni uspel izkazati, da bi z razkritjem zahtevanega dokumenta nastale, ali bi očitno lahko nastale, škodljive posledice za varnost države ali za njene politične in gospodarske koristi, konkretno za delovanje ali izvajanje nalog organa na enem izmed področij, navedenih v 5. členu ZTP. Da ne gre za podatke, katerih razkritje bi povzročilo omenjene škodljive posledice, potrjuje tudi dejstvo, da niti gradivo, ki je bilo podlaga za razpravo na obravnavani seji, niti magnetogram v trenutku nastanka nista bila označena z nobeno stopnjo tajnosti, kot je sicer običajna praksa Vlade RS, kadar so na dnevnem redu seje tajni podatki. Informacijski pooblaščenec tudi ni sledil navedbam organa, da bi razkritje magnetograma nepooblaščenim osebam lahko povzročilo pritisk javnosti na posameznega člana vlade ali posamezno politično stranko in bi lahko povsem spremenilo način dela Vlade RS. Razpravljavci bi bili namreč ob sprejemanju odločitev pod pritiskom, da bodo njihove razprave pozneje predmet javnih debat in morebitnih očitkov. Informacijski pooblaščenec je v odločbi poudaril, da je že sama narava dela članov Vlade RS takšna, da je njihovo delo izpostavljeno presoji javnosti, zato omenjeni argumenti organa ne zdržijo resne pravne presoje. Dejstva, da je razprava, ki se odvija v vladi, predmet javne debate in kritike, zato nikakor ni mogoče upoštevati v smislu škodljivih posledic za politične koristi države, kot jih določa ZTP. Zahtevani magnetogram torej ne vsebuje podatkov, katerih razkritje bi lahko povzročilo nastanek škodljivih posledic za politične koristi države, ki se nanašajo na zunanje zadeve, zaradi česar tudi materialni kriterij za določitev stopnje tajnosti podatkov v obravnavanem dokumentu ni izpolnjen.

Informacijski pooblaščenec je tako v pritožbenem postopku ugotovil, da ni podana izjema po 1. točki prvega odstavka 6. člena ZDIJZ. Ker iz tretjega odstavka 17. člena ZTP izhaja, da se mora podatek oz. dokument obravnavati kot tajen, če je označen le s stopnjo tajnosti (torej, če je izpolnjen le eden izmed formalnih elementov), je Informacijski pooblaščenec organu naložil, da z magnetograma 69. redne seje umakne stopnjo tajnosti.

V pritožbenem postopku pa je Informacijski pooblaščenec ugotovil tudi, da ni podana izjema po 11. točki prvega odstavka 6. člena ZDIJZ. Pri tem ni sporno, da je bil zahtevani magnetogram sestavljen v zvezi z notranjim delovanjem organa, vendar pa je Informacijski pooblaščenec ugotovil, da ni izpolnjen drugi pogoj za obstoj te izjeme: da bi razkritje povzročilo motnje pri delovanju oz. dejavnosti organa. Argument organa o velikem psihičnem pritisku nad razpravljavci v primeru razkritja zahtevanega magnetograma namreč ni utemeljen. Gre za javne funkcionarje, katerih delovanje ne pomeni samo sprejema končne odločitve, temveč tudi ravnanje pred sprejemom te odločitve. Zato se morajo ves čas svojega delovanja zavedati, da so v službi ljudstva, ki nima enotnih stališč, zaradi česar so določeni pritiski, ki jih doživljajo, nekaj povsem običajnega in jih ni mogoče šteti za »motnje«, ki so pravno upoštevne pri utemeljevanju izjeme od prostega dostopa do informacij javnega značaja. Besedo »motnje« je treba tolmačiti v smislu, da bi razkritje podatka (dokumenta) pomenilo resno oviro za nadaljnje delo organa oz. bi bilo to delo bistveno drugače (po kvaliteti slabše), kot je bilo pred razkritjem oz. kakršno bi bilo, če do razkritja dokumenta ne bi prišlo. Da bi bil namreč škodni test izpolnjen, bi morale razkritje

dokumenta ne samo ogroziti varovano pravno dobrino, ampak že resno ogroziti proces odločanja institucije; šele takrat bi bil dostop do dokumentov lahko zavržen.

V obravnavanem primeru torej nista kumulativno izpolnjena oba pogoja, ki ju za obstoj izjeme po 11. točki prvega odstavka 6. člena določa ZDIJZ, kar pomeni, da ta izjema glede obravnavanega dokumenta ni podana.

### 2.6.11. Tajni podatki, test javnega interesa

Z odločbo št. 090-164/2014 z dne 21. 11. 2014 je Informacijski pooblaščenec Policiji naložil, da umakne stopnjo tajnosti INTERNO s seznama o letni statistiki uporabe IMSI-lovilcev, skupno in po posameznih kaznivih dejanjih, ter seznam posreduje prosilcu.

Organ je zahtevo prosilca po posredovanju skupne letne statistike uporabe IMSI-lovilcev in letni statistiki uporabe, ločeni po posameznih kaznivih dejanjih, zavrnil, s sklicevanjem na izjemi po 1. in po 11. točki prvega odstavka 6. člena ZDIJZ.

Informacijski pooblaščenec je ugotovil, da organ razpolaga z dvema dokumentoma, iz katerih so razvidni podatki, ki jih je zahteval prosilec, oba imata oznako INTERNO. Za oba dokumenta je organ predložil pisni oceni škodljivih posledic, podpisani s strani generalnega direktorja Policije, ki je za določanje tajnih podatkov pooblaščen po zakonu (ZTP). V konkretnem primeru so torej izpolnjeni vsi formalni pogoji za določitev obeh dokumentov za tajna. Hkrati se podatki, ki so označeni kot tajni, nanašajo na javno varnost, kar je eno izmed področij, naštetih v 5. členu ZTP, s čimer je izpolnjen tudi materialni kriterij za tajne podatke. Zahtevana statistika se namreč nanaša na področje uporabe IMSI-lovilcev, ki spadajo na področje uporabe prikritih preiskovalnih metod in ukrepov dela policije pri odkrivanju, preiskovanju in dokazovanju kaznivih dejanj. Navedeno izhaja tudi iz pisnih ocen škodljivih posledic, iz katerih sledi, da so objekt varstva podatki o uporabi naprave IMSI-lovilec v povezavi s konkretnimi operativnimi komunikacijami, v katerih Policija izvaja prikrite preiskovalne ukrepe. Podatki o konkretnih operativnih kombinacijah, kot tudi o taktiki in metodiki dela kriminalistične policije pri izvajanju prikritih preiskovalnih ukrepov, so že zaradi narave dela tajni. Na podlagi vsega navedenega je Informacijski pooblaščenec ugotovil, da sta zahtevana dokumenta označena kot tajna na podlagi ZTP, ker sta izpolnjena tako materialni kot formalni kriterij. V skladu s tem gre za izjemo od prosto dostopnih informacij javnega značaja po 1. točki prvega odstavka 6. člena ZDIJZ.

Vendar pa je Informacijski pooblaščenec upošteval tudi določbo drugega odstavka 6. člena ZDIJZ, po katerem se dostop do zahtevanih podatkov dovoli, če je javni interes glede razkritja močnejši od javnega interesa ali interesa drugih oseb za omejitev dostopa do zahtevane informacije. Navedene določbe se ne more uporabiti v primeru tajnih podatkov, ki so označeni z najvišjima dvema stopnjama tajnosti (TAJNO in STROGO TAJNO). V konkretnem primeru so predmet presoje informacije, ki so označene z oznako INTERNO (najnižja stopnja tajnosti), zato je Izvajanje testa interesa javnosti glede teh podatkov dovoljeno.

Informacijski pooblaščenec je ugotovil, da je treba dostop do letne statistike uporabe IMSI-lovilcev dovoliti, ker se z njihovo uporabo posega v ustavno varovano pravico do zasebnosti posameznikov (38. člen Ustave RS), in sicer ne samo tistih, zoper katere Policija ta ukrep neposredno izvaja, ampak tudi drugih, ki so lahko le naključno na območju komunikacij, ki jih zajame lovilec. Hkrati uporaba IMSI-lovilcev zakonsko (še) ni regulirana, zato za posameznike ni predvidljiva. Če so statistični podatki o letni uporabi IMSI-lovilcev tajni, v javnosti pa so o tem nasprotujoče si informacije, posamezniki nimajo možnosti oceniti, katero njihovo ravnanje bi jih izpostavilo nevarnosti (policijskega) nadzora in pod kakšnimi pogoji bi se ta nadzor izvajal. Uporaba tehničnih sredstev in metod, ki se jih poslužuje Policija pri odkrivanju kaznivih dejanj, bi morala biti sorazmerna storjenemu kaznivemu dejanju, stopnja posega v varstvo osebnih podatkov tretjih oseb pa minimalna. Ob tem je uporaba tajnih metod in sredstev v predkazenskem postopku ravno iz tega razloga zakonsko natančno regulirana. Tudi glede drugih prikritih ukrepov, ki jih izvaja oz. jih je izvajal

organ skupaj z uporabo IMSI-lovilcev, Zakon o kazenskem postopku<sup>20</sup> določa, pod kakšnimi pogoji in za preiskovanje katerih kaznivih dejanj se jih lahko uporabi. Iz navedenega tako sledi, da lahko posamezniki (tudi morebitni storilci kaznivih dejanj) že na podlagi samega zakona predvidevajo, pri katerih kaznivih dejanjih policija uporablja posebne preiskovalne ukrepe in kakšne metode uporablja. Sklicevanje organa na dejstvo, da bi se z razkritjem teh podatkov zmanjšala uspešnost in učinkovitost policije pri izvajanju nalog, ker bi se morebitni storilci kaznivih dejanj tovrstnemu delovanju policije prilagodili, je tako neutemeljeno. Posameznik mora imeti namreč že na podlagi samega zakona jasno predstavbo, pri katerih kaznivih dejanjih policija uporablja posebne metode in sredstva ter do kakšnih posegov v njegovo zasebnost ob tem lahko pride. V takšnem prepričanju utrjuje tudi dejstvo, da je bila v okviru priprave spremembe ZKP (novela ZKP-M<sup>21</sup>) v predlog zakona dodana določba glede uporabe IMSI-lovilcev, iz katere bi jasno izhajalo, kdaj in pod kakšnimi pogoji ter pri preiskovanju katerih kaznivih dejanj lahko policija uporablja IMSI-lovilce. Upošteva ta vidik pa postane sklicevanje organa na dejstvo, da »bodo morebitni storilci seznanjeni s tem, pri preiskovanju katerih kaznivih dejanj policija lovilce uporablja in da se bodo temu prilagodili« povsem brezpredmetno.

Poleg tega je Informacijski pooblaščenec ugotovil, da gre za najmanj dve leti stare statistične podatke, iz katerih niso določljivi niti konkretni postopki niti konkretni posamezniki, zoper katere ti postopki tečejo. Zgolj na podlagi letnih statističnih podatkov brez podrobnejše lokacije dejanja (kraj ali vsaj regija) in časa storitve kaznivega dejanja, se morebitni storilci kaznivih dejanj nikakor ne morejo določiti, kar pomeni, da se tudi ne morejo prepoznati, kot navaja organ. Na drugi strani pa za razkritje teh statističnih podatkov obstaja močan javni interes. S primerjavo letnih statističnih podatkov uporabe po kaznivih dejanjih se namreč da ugotoviti, zoper storilce katerih kaznivih dejanj se dejansko uporablja lovilce, te naj bi se namreč uporabljalo le pri preiskovanju hujših kaznivih dejanj. V interesu javnosti je, da v demokratični družbi javnost razpolaga z nepristranskimi, objektivnimi informacijami, na podlagi katerih se lahko informirano odloča v/o javnopravnih zadevah in s tem vrši nadzor v skladu s 3. členom Ustave RS. Področje uporabe IMSI-lovilcev pa je področje, ki v javnosti sproža številne razprave, še posebej upošteva dejstvo, da se vprašanje (glede na to, da je že bila v pripravi novela ZKP-M) očitno namerava zakonsko urediti. O vprašanju sorazmernosti, nujnosti in učinkovitosti teh (novih) represivnih metod policijskega dela, bi morala skozi javno razpravo odločati tudi (strokovna in laična) javnost. Le dobro in izdatno ter nepristransko obveščena javnost pa lahko uresničuje pravico iz 39. člena Ustave RS: o zadevni zadevi zakonodajalcu izraža mnenje in s tem hkrati uresničuje svojo oblastno pravico iz 3. člena Ustave RS. Nadzor javnosti nad delom represivnega aparata je v demokratični družbi integralnega pomena, zato je seznanitev z zahtevanimi podatki nedvomno v interesu javnosti.

Na podlagi vsega navedenega je Informacijski pooblaščenec ugotovil, da so v obravnavanem primeru izrazito močno izražene okoliščine, ki so v prid interesu javnosti, tehtanje vseh okoliščin v danem primeru pa pripelje do zaključka, da je interes javnosti za razkritje zahtevanih informacij močnejši od interesa, da se ti podatki zavarujejo zaradi varovanja tajnih podatkov, s katerimi se v konkretnem primeru varuje delovanje Policije na področju prikritih preiskovalnih ukrepov. Zahtevane podatke je zato treba razkriti.

### 2.6.12. Okoljski podatki

Informacijski pooblaščenec je z odločbo št. 090-263/2014 z dne 28. 11. 2014 Občini Ilirska Bistrica naložil, da prosilcu omogoči vpogled in posreduje študijo vplivov hrupa na okolje in zdravje prebivalcev v Občini Ilirska Bistrica.

Organ se je v izpodbijani odločbi pri zavrnitvi zahteve prosilca skliceval na izjemo iz 9. točke prvega odstavka 6. člena ZDIJZ. S takim dokončnim dokumentom, kot ga je zahteval prosilec, organ namreč ne razpolaga oz. ga v času zahteve nima; obstoječi dokument se še

<sup>20</sup> Uradni list RS, št. 32/2012 – uradno prečiščeno besedilo 8 s spremembami, v nadaljevanju ZKP.

<sup>21</sup> Uradni list RS, št. 87/2014.

dopolnjuje. Razkritje bi lahko povzročilo napačne predstavitve in razumevanje podatkov in pritiske javnosti, otežena bi bila tudi morebitna nadaljnja nadgraditev dokumenta.

V pritožbenem postopku je Informacijski pooblaščenec ugotovil, da organ razpolaga s študijo vplivov hrupa na okolje in zdravje prebivalcev v Občini Ilirska Bistrica v materializirani obliki. Informacijo javnega značaja v smislu 4. člena ZDIJZ predstavlja kakršna koli vsebina – informacija v materializirani obliki, tudi če je ta npr. še v fazi nezaključenega dokumenta, osnutka, neformalnega zapisa, zabeleške ... Zahtevana informacija tako izpolnjuje kriterije za obstoj informacije javnega značaja po 4. členu ZDIJZ.

V zvezi z zatrjevano izjemo iz 9. točke prvega odstavka 6. člena ZDIJZ je Informacijski pooblaščenec ugotovil, da je zahtevana študija zaključena, podane so določene ugotovitve, študijo so tudi podpisale odgovorne osebe izvajalca in posredovana je bila organu, zato ne gre več za dokument v nastajanju v smislu navedene izjeme. Poleg tega gre za dokument, ki ga je Zavod za zdravstveno varstvo Koper, kot pripravljavec in avtor dokumenta, že v celoti zaključil in posredoval organu. Avtor študije je zunanji izvajalec, pri čemer organ ni predviden kot (so)avtor oz. (so)pripravljavec dokumenta niti ni predvideno, da bi organ dokument lahko vsebinsko sam dopolnjeval, zato ta že po naravi stvari ni v postopku izdelave pri organu, prav tako pa ni predmet posvetovanja v organu. Argument, da bo organ potencialno izdal naročilo za dopolnitev študije, če in ko bo imel za to razpoložljiva denarna sredstva (ko bo sprejet proračun za leto 2014), pa ne zdrži resne pravne presoje. Tudi če bo organ izdal naročilo za nove, dodatne študije, bo vsaka nova študija predstavljala nov, samostojen dokument, nikakor pa ne bo šlo za nadgraditev oz. dopolnitev dokumenta, ki je predmet presoje v konkretni zadevi. Ta je bil namreč s tem, ko je bil podpisan s strani osebe, pooblaščen za njegovo pripravo in posredovan organu, vsebinsko zaključen. Vsebina konkretne študije, ki jo je organ prejel, je zaključena in bo ostala ista. Tudi, če bi inštitucija, ki je študijo posredovala organu, kasneje tako študijo dopolnila, spremenila oz. izdala nove ugotovitve, ne bi mogli reči, da je že posredovana študija še vedno v fazi nastajanja. Dejstvo je namreč, da je dokument zaključen s podpisom osebe, ki je pri določenem organu oz. drugem subjektu pooblaščen za odločanje, ta kriterij pa je v konkretnem primeru glede zahtevane študije izpolnjen. Vsak dokument – prejeta študija – torej predstavlja samostojen dokument, ki je zaključen v smislu ZDIJZ. V konkretnem primeru tako nista izpolnjeni že prvi dve predpostavki za obstoj izjeme po 9. točki prvega odstavka 6. člena ZDIJZ, organu pa v postopku tudi ni uspelo izkazati, da je izpolnjena tretja predpostavka, to je, da bi razkritje dokumenta povzročilo napačno razumevanje njegove vsebine. Organ namreč ni konkretno pojasnil možnosti nastanka škode, še posebej upošteva dejstvo, da so v študiji zbrani in obdelani podatki iz javnih zdravstvenih statistik in nekaterih drugih javnosti dostopnih dokumentov. Morebitno dejstvo, da se organ z izsledki študije ne strinja oz. da bi takšni izsledki lahko povzročili pritisk javnosti na organ, pa tudi ni upošteveno. Takšni pritiski so namreč legitimni. Informacije o vplivih hrupa na zdravje lokalnega prebivalstva, na kar se nanaša zahtevana študija, so zagotovo v javnem interesu, prebivalci zadevnega območja pa se imajo pravico seznaniti z vsemi informacijami, ki so s tem povezane. Kadar gre za informacije, ki se nanašajo na področja delovanja, ki so v javnem interesu (npr. področje javnega zdravja, vplivov na okolje, porabe javnega denarja ...), morajo zavezanci še prav posebej postopati transparentno (kar izhaja že iz drugega odstavka 2. člena ZDIJZ).

ZDIJZ je v tem pogledu izjemno naklonjen transparentnosti, saj v 2. točki prvega odstavka 10. člena (med drugim) določa, da je vsak organ dolžan v svetovni splet posredovati tudi študije in druge podobne dokumente, ki se nanašajo na delovno področje organa. Med take dokumente nedvomno spada tudi zahtevana študija. Povedano drugače, upošteva določbo 10. člena ZDIJZ, bi organ moral zahtevani dokument že sam proaktivno objaviti na svoji spletni strani, tudi brez zahteve prosilca.

Upošteva vse navedeno je Informacijski pooblaščenec ugotovil, da izjema iz 9. točke prvega odstavka 6. člena ZDIJZ glede zahtevanega dokumenta ni podana in da je treba zahtevani dokument posredovati prosilcu.

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

Informacijski pooblaščenec je leta 2014 na področju dostopa do informacij javnega značaja prejel v reševanje 578 pritožbenih zadev, od tega 320 pritožb zoper zavrnilne odločbe in 258 pritožb zaradi molka organa. Prosilci in zavezanci so se na Informacijskega pooblaščenca v 297 primerih obrnili s prošnjo za mnenje oz. pojasnilo. Skupaj je bilo tako obravnavanih 875 zadev. Glede na leto 2013 se je povečalo število prejetih pritožb zoper zavrnilne odločbe (leta 2013 je bilo 271 pritožb) in zmanjšalo število prejetih pritožb zaradi molka organa (leta 2013 je bilo teh pritožb 339). Po oceni Informacijskega pooblaščenca je zmanjšanje števila pritožb zaradi molka organa pozitiven kazalnik, ki kaže na večjo odzivnost prvostopenjskih organov, porast števila pritožbenih zadev zoper zavrnilne odločitve pa gre pripisati predvsem noveli ZDIJZ-C in širjenju kroga zavezancev.

Aprila 2014 je namreč začela veljati novela ZDIJZ-C, ki je razširila krog zavezancev za posredovanje informacij javnega značaja tudi na poslovne subjekte pod prevladujočim vplivom. Prevladujoč vpliv je podan, kadar Republika Slovenija, samoupravne lokalne skupnosti ali druge osebe javnega prava, posamično ali skupaj:

- v gospodarski družbi, neposredno ali posredno prek druge gospodarske družbe ali druge pravne osebe zasebnega prava, lahko izvajajo prevladujoč vpliv na podlagi večinskega deleža vpisanega kapitala, ali imajo pravico nadzora večine, ali lahko imenujejo več kot polovico članov poslovnega ali nadzornega organa, ali
- v drugi pravni osebi zasebnega prava, ki ni gospodarska družba, neposredno ali posredno prek druge gospodarske družbe ali druge pravne osebe zasebnega prava nastopajo kot ustanovitelji.

Posledično se je leta 2014 obseg dela Informacijskega pooblaščenca na področju dostopa do informacij javnega značaja povečal. Informacijski pooblaščenec je v zvezi z izvajanjem zakona pri t. i. novih zavezancih ugotovil, da so ti z zakonskimi obveznostmi, ki jih prinaša ZDIJZ-C, slabo seznanjeni in da jim nasprotujejo. Rezultat tega so pritožbeni postopki pred Informacijskim pooblaščencom, ki se v večini primerov nadaljujejo v upravnem sporu pred Upravnim sodiščem RS. Glede na to, da je ZDIJZ-C začel veljati aprila 2014, ti sodni postopki še niso zaključeni.

Leta 2014 je Informacijski pooblaščenec zaznal tudi porast pritožbenih zadev zoper zavezance iz 1. člena ZDIJZ, ki so pravne osebe javnega prava, izpolnjujejo pa tudi zakonske kriterije za poslovne subjekte pod prevladujočim vplivom (primer: DUTB, javna podjetja). Za te subjekte zakon predvideva, da se v delu, ki se nanaša na izvajanje javnih pooblastil ali javne službe, uporabljajo določbe ZDIJZ, ki urejajo dostop do informacij za organe, sicer pa določbe, ki urejajo dostop do informacij za poslovne subjekte pod prevladujočim vplivom oseb javnega prava. Za te subjekte torej ne velja določba 26.a člena, ki ureja poseben, poenostavljen postopek pri poslovnih subjektih pod prevladujočim vplivom, ampak morajo izdati odločbo po 22. členu ZDIJZ.

Glede na številne novosti, ki jih prinaša ZDIJZ-C, Informacijski pooblaščenec ocenjuje, da je treba (še) več napora vložiti v promocijo pravice dostopa do informacij javnega značaja in v usposabljanje zavezancev za uporabo zakona v praksi. Na to kaže tudi število vprašanj in prošenj za pojasnila, ki je tudi leta 2014 naraslo. Ne le poslovni subjekte pod prevladujočim vplivom, tudi občine in organi širšega javnega sektorja (javni zavodi s področja šolstva, zdravstva, druge pravne osebe javnega prava) ter izvajalci javnih služb in nosilci javnih pooblastil, ki so pravne osebe zasebnega prava, so z obveznostmi, ki jim jih nalaga ZDIJZ, še vedno slabo seznanjeni. Tudi leta 2014 je Informacijski pooblaščenec zato izvajal pedagoške dejavnosti, ki so enake poslanstvu katerega koli pritožbenega organa, da upošteva svoje pristojnosti in načelo nepristranskosti svetuje tako organom kot prosilcem ter s tem preprečuje nepotrebne pritožbene postopke, ki bi izvirali zgolj iz nezadostne komunikacije med proslcem in organom zavezancev ali iz nezadostnega poznavanja



posebnosti prava dostopa do informacij javnega značaja pri organu. Po oceni Informacijskega pooblaščenca so prosilci s pravico dostopa do informacij dobro seznanjeni in jo v praksi pogosto uresničujejo, na drugi strani pa je pri zavezancih (tudi zaradi pomanjkanja kadrovske in finančne vire) še vedno zaznati nepoznavanje oz. neseznanjenost z obveznostmi, ki jih prinaša ZDIJZ. Informacijski pooblaščenec je zato za zavezance izvedel več brezplačnih delavnic in predstavitev. V sodelovanju z Ministrstvom za javno upravo je bila pripravljena tudi brošura za nove zavezance o tem, kaj prinaša novela ZDIJZ-C.

Informacijski pooblaščenec, kot od 2009. vsako leto, tudi tokrat opozarja na problematiko zaračunavanja stroškov dela v postopku dostopa do informacij javnega značaja. Pravica dostopa do informacij javnega značaja je temeljna človekova pravica, ki jo zagotavlja Ustava RS. Informacijski pooblaščenec zato meni, da mora višina stroškov izvrševanja te pravice ostati najnižja možna ter ne sme nesorazmerno ovirati dostopa do informacij javnega značaja. Ravno iz tega razloga so vse vloge v postopku dostopa do informacij javnega značaja oproščene plačila upravne takse. Nesprejemljivo je, da se stroški dela »prevallijo« na novinarje in druge prosilce. Ob tem Informacijski pooblaščenec poudarja, da dostop do informacij javnega značaja ni v celoti brezplačen, problematično pa je zaračunavanje stroškov dela javnih uslužbencev po urnih postavkah. Iz veljavne ureditve izhaja, da se za posredovanje informacij javnega značaja (fotokopije, elektronskega zapisa, prepisa) lahko zaračunajo le materialni stroški, med te pa stroški dela javnih uslužbencev brez dvoma ne sodijo. Povsem nesprejemljivo je namreč stališče, da bi morali prosilci dodatno, po urnih postavkah, plačevati stroške javnih uslužbencev, ki že prejemajo plačo iz proračuna. Glede na izkušnje zadnjih nekaj let Informacijski pooblaščenec tudi opozarja, da je zaračunavanje stroškov dela javnih uslužbencev po urnih postavkah lahko zelo arbitrarno, v pritožbenem postopku pa ni mogoče preveriti, ali je organ stroške zaračunal upravičeno ali ne (odvisno od hitrosti javnih uslužbencev, organizacije dela ter (ne)urejenosti poslovanja z dokumentarnim gradivom pri organih zavezancih). V skladu z novelo ZDIJZ-C, ki je začela veljati aprila 2014, bi morala Vlada RS, po pridobitvi predhodnega mnenja Informacijskega pooblaščenca, nov, enotni stroškovnik sprejeti najpozneje do sredine oktobra 2014, a ga do izdaje tega letnega poročila še nismo prejeli v usklajevanje. Ker to v praksi predstavlja velik problem, vnovič pozivamo Ministrstvo za javno upravo in Vlado RS, naj nemudoma pristopita k oblikovanju enotnega stroškovnika in oblikujeta način zaračunavanja materialnih stroškov, po katerem organi zavezanci administrativnega bremena (iskanja po (ne) urejeni dokumentaciji) ne bodo v celoti »prevallili« na prosilce.

Na področju ponovne uporabe informacij javnega značaja je Informacijski pooblaščenec leta 2014 obravnaval osem pritožbenih zadev, kar je več kot leta 2013 (šest pritožb). Relativno majhno število pritožb na tem področju kaže, da so prosilci slabo seznanjeni s pravnimi možnostmi, ki jih imajo v primeru, če jim zavezanci vlogo za ponovno uporabo zavrnejo. Področje ponovne uporabe informacij javnega značaja ima pomemben gospodarski potencial, ki pa v praksi ostaja premalo izkoriščen.

V okviru mednarodnega sodelovanja na področju dostopa do informacij je Informacijski pooblaščenec tudi leta 2014 sodeloval v mednarodnem konzorciju pri projektu LAPSI 2.0, ki pa se z iztekom tega leta končuje.



**3**

**DELO NA PODROČJU VARSTVA  
OSEBNIH PODATKOV**

### 3.1. Koncept varstva osebnih podatkov v Republiki Sloveniji

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

Za normativno urejanje varstva osebnih podatkov je zlasti pomemben drugi odstavek 38. člena Ustave 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<sup>22</sup>, 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 EU 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<sup>23</sup>.

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 up-

<sup>22</sup> Uradni list RS, št. 86/2004; v nadaljevanju ZVOP-1.

<sup>23</sup> Uradni list Evropskih skupnosti, št. L 281, 23. 11. 1995.

orablajo tudi določbe Konvencije o varstvu posameznikov glede na avtomatsko obdelavo osebnih podatkov, ki je bila ratificirana in objavljena leta 1994<sup>24</sup>. Namen omenjene konvencije Sveta Evrope je na ozemlju vsake pogodbenice vsakemu posamezniku, ne glede na njegovo državljanstvo in prebivališče, zagotoviti spoštovanje njegovih pravic in temeljnih svoboščin ter v okviru tega še posebej spoštovanje pravice do zasebnosti v primeru avtomatske obdelave njegovih osebnih podatkov.

Julija 2007 je bila sprejeta novela ZVOP-1, to je Zakon o spremembah in dopolnitvah zakona o varstvu osebnih podatkov<sup>25</sup>. ZVOP-1A je uvedel dve pomembni novosti – poleg nekaterih 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 tudi finančno razbremenitev upravljavcev osebnih podatkov.

Določbe ZVOP-1A so bile usklajene s spremembami Zakona o prekrških<sup>26</sup> iz leta 2006 ter so upoštevale uvedbo evra kot plačilnega sredstva v Republiki Sloveniji s 1. 1. 2007.

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

### 3.2. Dejavnost državnih nadzornikov za varstvo osebnih podatkov

#### 3.2.1. Pravice in dolžnosti državnega nadzornika

Državni nadzornik za varstvo osebnih podatkov opravlja inšpekcijski nadzor nad izvajanjem določb ZVOP-1 in je pri opravljanju svojih nalog v skladu s svojimi pooblastili samostojen. Naloge opravlja v okviru in na podlagi Ustave RS 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<sup>27</sup>, specifične pristojnosti državnega nadzornika pa so določene v 53. členu ZVOP-1.

#### 3.2.2. Inšpekcijski nadzor

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

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

Informacijski pooblaščenec je leta 2014 zaradi suma kršitev določb ZVOP-1 vodil 628 inšpekcijskih zadev, kar je manj kot v preteklih letih (leta 2013 je bilo takih zadev 712, leta 2012 še nekaj več, 725), od tega 206 v javnem in 422 v zasebnem sektorju. Zoper pravne osebe javnega sektorja je na podlagi prijav odprl 195 inšpekcijskih zadev, 11 postopkov pa je uvedel po uradni dolžnosti, npr. če je na podlagi objav v medijih zaznal sum kršitve

<sup>24</sup> Uradni list RS, št. 11/1994 – Mednarodne pogodbe št. 3/1994.

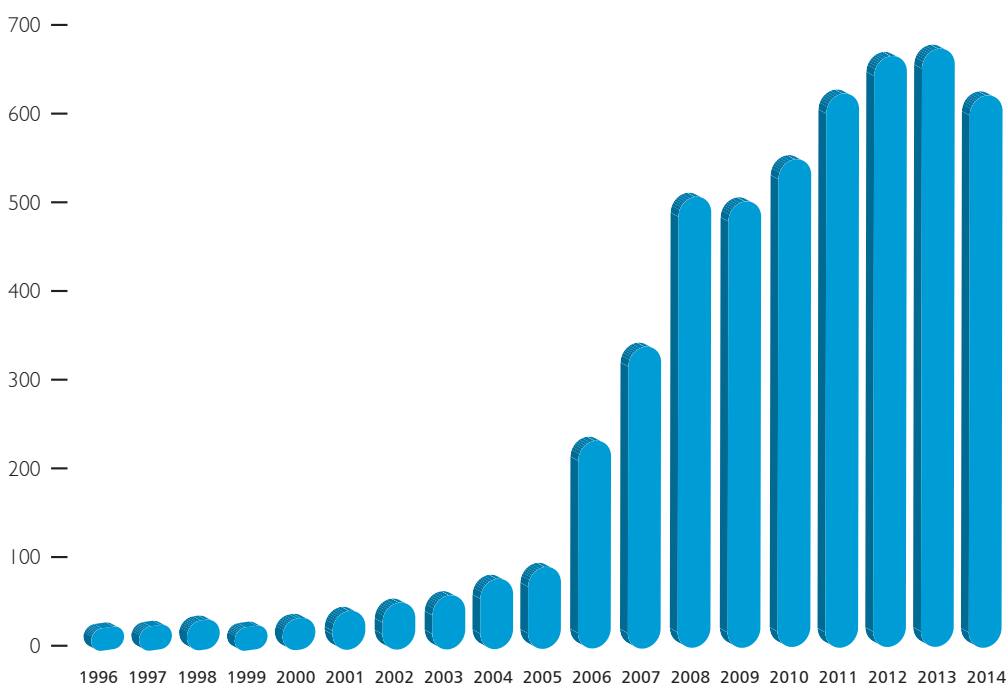
<sup>25</sup> Uradni list RS, št. 67/2007; v nadaljevanju ZVOP-1A.

<sup>26</sup> Uradni list RS, št. 29/2011 – uradno prečiščeno besedilo 8, s spremembami; v nadaljevanju ZP-1.

<sup>27</sup> Uradni list RS, št. 43/2007 – uradno prečiščeno besedilo 1 in 40/2014; v nadaljevanju ZIN.

varstva osebnih podatkov ali v okviru načrtovanih ogledov. Zoper zavezanca v zasebnem sektorju je na podlagi prijav odprl 410 inšpekcijskih zadev, 12 postopkov je začel po uradni dolžnosti. Število prijav in pritožb zaradi suma kršitev določb ZVOP-1 se je v primerjavi z letom 2013 nekoliko zmanjšalo, in sicer jih je bilo 722 (leta 2013 jih je bilo 852, leta 2012 pa 747), posledično se je zmanjšalo skupno število inšpekcijskih zadev. Število prijav, ki jih je prejel Informacijski pooblaščenec, je večje od števila odprtih inšpekcijskih zadev oz. uvedenih inšpekcijskih postopkov, ker je zoper določene zavezanca prejel več prijav. Tako je Informacijski pooblaščenec leta 2014 zoper zavezanca v javnem sektorju prejel 200 prijav (leta 2013 jih je prejel 241, leta 2012 pa 237), zoper zavezanca v zasebnem sektorju pa 522 prijav (leta 2013 jih je bilo 611 in leta 2012 510). Večje število prijav zoper posamezne zavezanca je opaznejše v zasebnem sektorju, zlasti zoper zavezanca, ki izvajajo neposredno trženje in svoje ponudbe pošiljajo velikemu številu posameznikov.

*Slika 8: Število inšpekcijskih zadev, ki jih je zaradi suma kršitev določb ZVOP-1 vodil Informacijski pooblaščenec (na podlagi prijav) med letoma 1996 in 2014.*



### 3.2.2.1. Inšpekcijski nadzor v javnem sektorju

Informacijski pooblaščenec je zaradi suma kršitev določb ZVOP-1 zoper pravne osebe javnega sektorja na podlagi prijav odprl 195 inšpekcijskih zadev. V 70 primerih so državni nadzorniki prijaviteljem pisno pojasnili, zakaj uvedba postopka inšpekcijskega nadzora ne bi bila smiselna oz. zakaj v prijavi opisano dejanje ne pomeni kršitve določb ZVOP-1. Leta 2014 je bilo izdanih še pet obvestil o neuvedbi inšpekcijskega postopka za prijave, prejete konec leta 2013. V štirih primerih Informacijski pooblaščenec ni uvedel postopkov, ker prijavitelji niso posredovali svojih podatkov, zaradi česar jih ni mogel pozvati za posredovanje dodatnih podatkov, ki so potrebni za uvedbo inšpekcijskega postopka. Na podlagi šestih prijav je Informacijski pooblaščenec takoj izrekel ukrep v skladu z zakonom, ki ureja prekrške, ker je po preučitvi prijav zaključil, da uvedba inšpekcijskih postopkov ne bi bila smiselna, saj je šlo za enkratna dejanja v preteklosti, ki jih z inšpekcijskimi ukrepi za nazaj ni več možno preprečiti ali odpraviti, in ker je bilo prijavi priloženih dovolj dokazov o storitvi prekrška. Informacijski pooblaščenec je tri prijave odstopil v reševanje pristojnim institucijam. Po preučitvi prejetih prijav je bilo leta 2014 začelih 112 inšpekcijskih postopkov, 11 pa še po uradni dolžnosti, skupaj torej 123. V okviru inšpekcijskih postopkov v javnem sektorju je bilo opravljenih 47 inšpekcijskih pregledov. Za odpravo ugotovljenih nepravilnosti je bilo izrečenih 12 opozoril na zapisnik in izdanih pet odločb.

Leta 2014 je bilo zaključenih 113 inšpekcijskih postopkov. 107 jih je bilo zaključenih s sklepom o ustavitvi postopka, od tega 64 iz preteklih let. Z odločbo so se zaključile štiri zadeve (zoper eno odložbo je zavezanec vložil tožbo), z zaznamkom v zapisniku o inšpekcijskem nadzoru pa sta bila ustavljena dva postopka. V 58 inšpekcijskih postopkih (od tega jih je bilo 33 iz leta 2013) Informacijski pooblaščenec ni zaznal kršitev določb ZVOP-1.

Leta 2014 je Upravno sodišče RS odločilo v enem upravnem sporu, ki ga je sprožil zavezanec zoper odločbo, s katero je Informacijski pooblaščenec odredil odpravo ugotovljenih nepravilnosti. Sodišče je tožbi ugodilo, odločbo Informacijskega pooblaščenca odpravilo in mu zadevo vrnilo v ponoven postopek.

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 – 73,
- nezakonito zbiranje oz. zahtevanje osebnih podatkov – 52;
- neustrezno zavarovanje osebnih podatkov – 16,
- nezakonito izvajanje videonadzora in sporna uporaba videoposnetkov – 14,
- neposredno trženje – 5,
- razno: pogodbeno 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 – 46.

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

- javne sklade, zavode, agencije in druge osebe javnega prava – 106, od tega 35 zoper vzgojno-izobraževalne ustanove in 25 zoper zdravstvene ustanove,
- državne organe – 58, od tega sodišča, tožilstva, pravobranilstvo – 9,
- občine – 42.

### 3.2.2.2. Inšpekcijski nadzor v zasebnem sektorju

Informacijski pooblaščenec je leta 2014 zoper zavezance v zasebnem sektorju na podlagi prijav odprl 410 zadev. V 127 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 niso posredovali dovolj podatkov za uvedbo inšpekcijskega postopka. V 14 primerih Informacijski pooblaščenec postopka ni mogel uvesti, ker je bilo v prijavi premalo podatkov in ker prijaviteljev zaradi anonimnosti ni mogel pozvati k dopolnitvi prijavi. Informacijski pooblaščenec je pet 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 14 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 ukrepi za nazaj ni več mogoče preprečiti ali odpraviti, in ker je bilo prijavi priloženih dovolj dokazov o storitvi prekrška. 12 prijav je posredoval v reševanje pristojnim institucijam in o tem obvestil prijavitelja. Izdal je še osem obvestil o neuvedbi inšpekcijskega postopka, ki so se nanašala na prijave, prejete konec leta 2013.

Tako je bilo leta 2014 na podlagi prejetih prijav začelih 238 postopkov inšpekcijskega nadzora, 12 jih je bilo uvedenih po uradni dolžnosti, skupaj torej 250. Državni nadzorniki za varstvo osebnih podatkov so v zasebnem sektorju opravili 97 inšpekcijskih ogledov na terenu. Zaradi ugotovljenih nepravilnosti so izrekli 31 opozoril v zapisniku o inšpekcijskem nadzoru in izdali 17 ureditvenih odločb. Poleg inšpekcijskih ogledov na terenu so državni nadzorniki opravili tudi 32 ogledov spletnih strani (večinoma v zvezi s piškotki), pri čemer

so zaradi ugotovljenih nepravilnosti v zapisnikih o inšpekcijskem nadzoru izrekli 24 opozoril za odpravo ugotovljenih nepravilnosti.

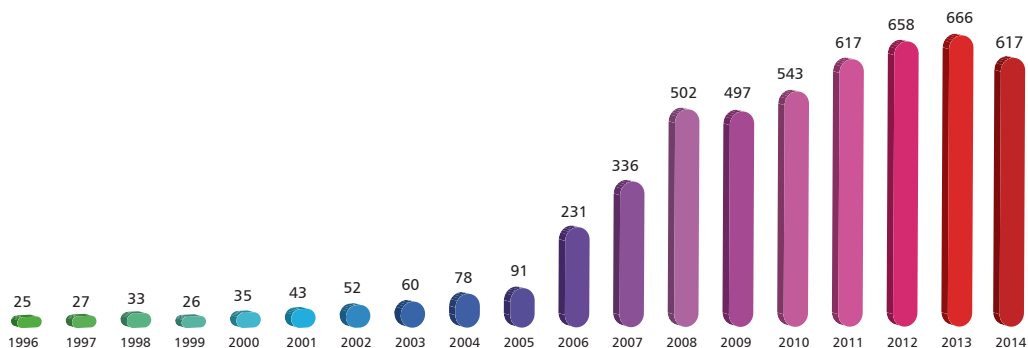
En zavezanec je zoper prejeto odločbo sprožil upravni spor z vložitvijo tožbe na Upravno sodišče RS. Omenjeno sodišče je leta 2014 odločilo v dveh upravnih sporih, ki sta ju sprožila zavezanca zoper odločbi, s katerima je Informacijski pooblaščenec odredil odpravo ugotovljenih nepravilnosti. Sodišče je eno tožbo zavrnilo, eni tožbi pa ugodilo, odločbo Informacijskega pooblaščenca odpravilo in mu zadevo vrnilo v ponoven postopek.

Leta 2014 je Informacijski pooblaščenec izdal 202 sklepa o ustavitvi postopka, od tega je 105 sklepov izdal v postopkih, ki so bili začeti pred letom 2014. Šest postopkov je bilo ustavljenih z zaznamkom v zapisniku o inšpekcijskem nadzoru. V 87 inšpekcijskih postopkih (41 iz leta 2014) Informacijski pooblaščenec ni zaznal kršitev določb ZVOP-1.

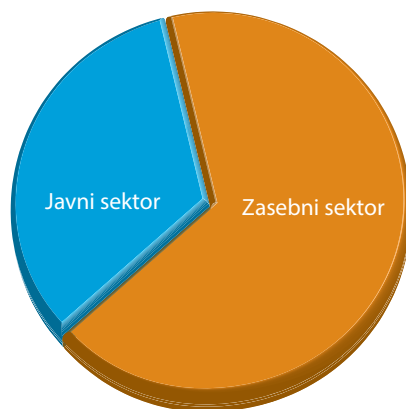
Sumi kršitve določb ZVOP-1 so se nanašali na:

- 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 – 109,
- zlorabe osebnih podatkov za namene neposrednega trženja – 86,
- nezakonito zbiranje oz. zahtevanje osebnih podatkov – 75,
- nezakonito izvajanje videonadzora in sporna uporaba posnetkov – 59,
- neustrezno zavarovanje osebnih podatkov – 17,
- piškotki – 15,
- ostalo: predčasno uničenje osebnih podatkov, zavrnitev posredovanja osebnih podatkov, obdelava netočnih in neažurnih osebnih podatkov, obdelava osebnih podatkov v nasprotju z namenom zbiranja, pogodbeno obdelava, obdelava osebnih podatkov po preteku roka hrambe – 61.

Slika 9: Število zadev na podlagi prejetih prijav zaradi suma kršitev določb ZVOP-1 med letoma 2006 in 2014.



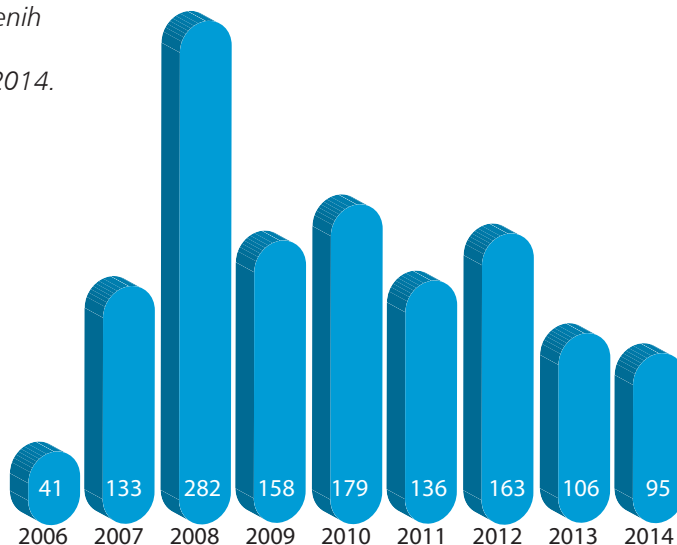
Slika 10: Sumi nezakonite obdelave osebnih podatkov leta 2014, primerjava med javnim in zasebnim sektorjem.



### 3.2.3. Storjeni prekrški

Zaradi kršitev določb ZVOP-1 je bilo leta 2014 uvedenih 95 postopkov o prekršku (leta 2013 106 in leta 2012 163), od tega 52 postopkov zoper pravne osebe zasebnega sektorja in njihove odgovorne osebe, 22 postopkov zoper pravne osebe javnega sektorja in njihove odgovorne osebe ter 21 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 izreče opozorilo, če je storjeni prekršek neznaten in če pooblaščen uradna oseba oceni, da je glede na pomen dejanja opozorilo zadosten ukrep. Če je storjen hujši prekršek, prekrškovni organ izda odločbo o prekršku, s katero kršitelju izreče sankcijo. V skladu s 4. členom ZP-1 sta sankciji za prekršek globa in opomin, glede na 57. člen ZP-1 pa se lahko globa izreče tudi v obliki plačilnega naloga.

Slika 11: Število uvedenih postopkov o prekršku med letoma 2006 in 2014.



V prekrškovnih postopkih, vključno z odprtimi postopki iz preteklih let, je Informacijski pooblaščenec leta 2014 izdal:

- 19 opozoril,
- 76 odločb o prekršku (26 opominov in 50 glob).

Število izdanih odločb o prekršku je v primerjavi z letom 2013 ostalo skoraj nespremenjeno (takrat jih je bilo 72), manj je bilo izrečenih opominov (leta 2013 jih je bilo 36) in več glob (leta 2013 36).

Poleg opozoril, ki so bila izrečena v prekrškovnih postopkih, je Informacijski pooblaščenec v skladu z načelom ekonomičnosti tudi v okviru postopkov inšpekcijskega nadzora izrekel 55 opozoril po 53. členu ZP-1 za manjše kršitve, kar je manj kot prejšnja leta (leta 2013 90, leta 2012 87), in sicer 19 (leta 2013 25, leta 2012 24) v javnem in 36 (leta 2013 65, leta 2012 63) v zasebnem sektorju.

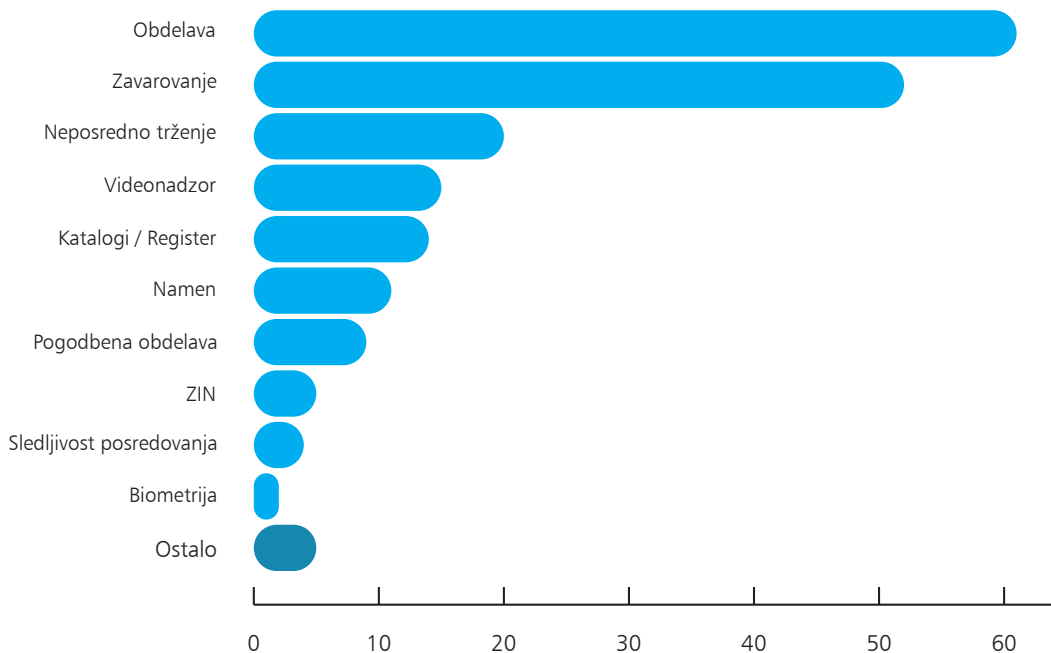
Kršitelji so zoper izdane odločbe o prekršku vložili deset zahtev za sodno varstvo oz. zoper 13,3 % izdanih odločb (leta 2013 je bil ta delež 16,7 %, leta 2012 pa 25,2 %). Vse zahteve za sodno varstvo so bile vložene zoper odločbe, s katerimi je Informacijski pooblaščenec kršiteljem izrekel globe. To je posledica dejstva, da so globe po ZVOP-1 zelo visoke, če gre za stek prekrškov. Informacijski pooblaščenec izreka globe v primerih, ko gre za prekrške, s katerimi je bilo občutno poseženo v pravico do varstva osebnih podatkov oškodovanca, ali v primerih zlorabe osebnih podatkov s strani pooblaščenih oseb znotraj določenega upravljavca, ki so dostop do osebnih podatkov v določeni zbirki pridobili za potrebe opravljanja svojega dela. Relativno majhen delež vloženi zahtev za sodno varstvo kaže na to, da se storilci zavedajo teže prekrškov, ki so jih storili.



Kršitve (v okviru enega postopka je lahko več kršitev) so zadevale:

- nezakonito obdelavo osebnih podatkov: 8. člen ZVOP-1 (61),
- neustrezno zavarovanje osebnih podatkov: 24. in 25. člen ZVOP-1 (52),
- kršitev določb o neposrednem trženju: 72. in 73. člen ZVOP-1 (20),
- nezakonito izvajanje videonadzora: 74., 75., 76. in 77. člen ZVOP-1 (15),
- nepravilnosti v zvezi z vzpostavitvijo katalogov zbirk osebnih podatkov in posredovanjem podatkov v register zbirk osebnih podatkov: 26. in 27. člen ZVOP-1 (14),
- nezakonit namen zbiranja in nadaljnje obdelave osebnih podatkov: 16. člen ZVOP-1 (11),
- neustrezno pogodbeno obdelavo: 11. člen ZVOP-1 (9),
- neizpolnjevanje ukrepov, izrečenih v postopkih inšpekcijskega nadzora, kršitve določb ZIN (5),
- neustrezno sledljivost posredovanja osebnih podatkov: tretji odstavek 22. člena ZVOP-1 (4),
- nezakonito izvajanje biometrijskih ukrepov v zasebnem sektorju: 80. člen ZVOP-1 (2),
- sporno dopolnitev, popravek, blokiranje ali izbris osebnih podatkov: 33. člen ZVOP-1 (1),
- prekomeren rok hrambe osebnih podatkov: 21. člen ZVOP-1 (1),
- neustrezno obveščanje posameznika o obdelavi osebnih podatkov: 19. člen (1),
- nezakonito obdelavo občutljivih osebnih podatkov: 13. člen ZVOP-1 (1),
- nezakonito kopiranje osebnih dokumentov: 4.a člen ZPLD (1).

Slika 12: Najpogostejše kršitve določb ZVOP-1 leta 2014.



Leta 2014 je Informacijski pooblaščenec prejel 19 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:

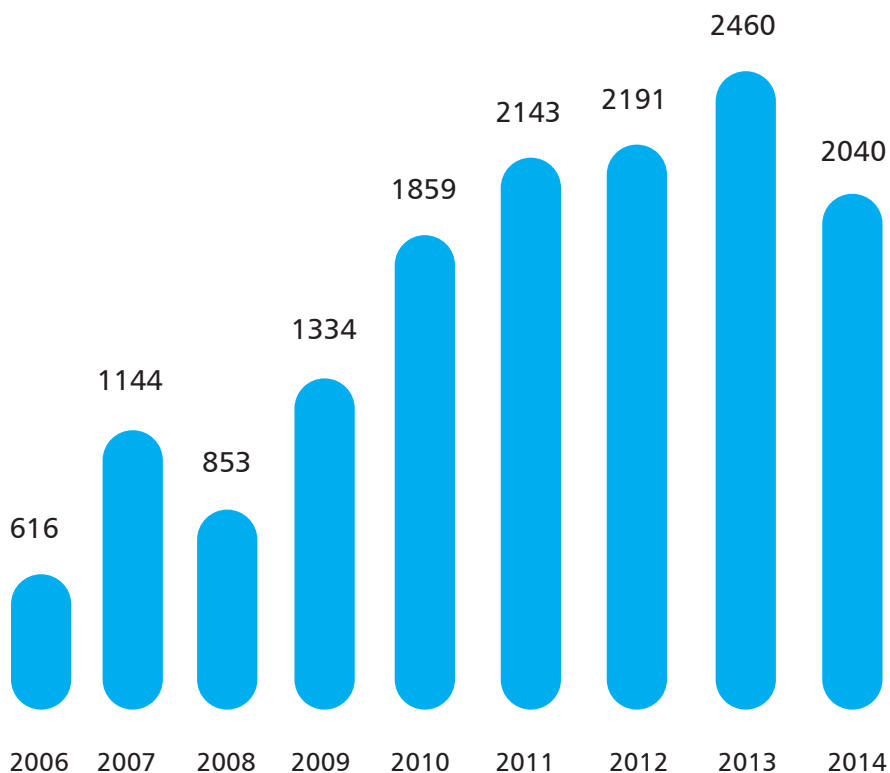
- zahtevi za sodno varstvo je bilo ugodeno v delu, ki se nanaša na izrečeno sankcijo, tako da se je storilec za prekršek spremenila sankcija ali višina globe, sicer je bila zahteva za sodno varstvo zavržena kot neutemeljena – 7,
- zahteva za sodno varstvo je bila zavržena kot neutemeljena, odločba Informacijskega pooblaščenca pa potrjena – 5,
- zahtevi za sodno varstvo je bilo ugodeno, odločba Informacijskega pooblaščenca odpravljena, postopek o prekršku pa ustavljen – 5,
- zahteva za sodno varstvo je bila zavržena – 2.

Informacijski pooblaščenec je v enem primeru, ko je okrajno sodišče postopek o prekršku ustavilo, zoper odločitev sodišča vložil pritožbo na višje sodišče. Sodišče do izdaje pričujočega letnega poročila o pritožbi še ni odločilo.

### 3.3. Dajanje pisnih mnenj in pojasnil

Neposredna pravna podlaga za dajanje neobveznih mnenj, pojasnil, stališč, navodil in priporočil s področja varstva osebnih podatkov so določbe 49. člena ZVOP-1. Informacijski pooblaščenec je leta 2014 prejel 2.040 prošelj za podajo pisnega pojasnila ali mnenja v zvezi s konkretnimi vprašanji. Število prošelj se je lani po več letih stalnega naraščanja njihovega števila nekoliko zmanjšalo (leta 2013 jih je bilo 2.460, leta 2012 2.191). Zaposila za mnenja in pojasnila so vsebinsko zahtevnejša, kar lahko pripisemo 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 49 mnenj in pojasnil, medtem ko je posameznikom, ki so zastavili vprašanja, na katera je v preteklosti že odgovarjal, posredoval krajši odgovor oz. jih je le napotil na že izdelano mnenje; kratkih odgovorov in napotitev je bilo 1.991. Informacijski pooblaščenec je dajal tudi ustna mnenja in pojasnila. V uradu je namreč vsak dan na voljo dežurni državni nadzornik, ki na vprašanja odgovarja po telefonu.

Slika 13: Število zaprosil za mnenja med letoma 2006 in 2014.



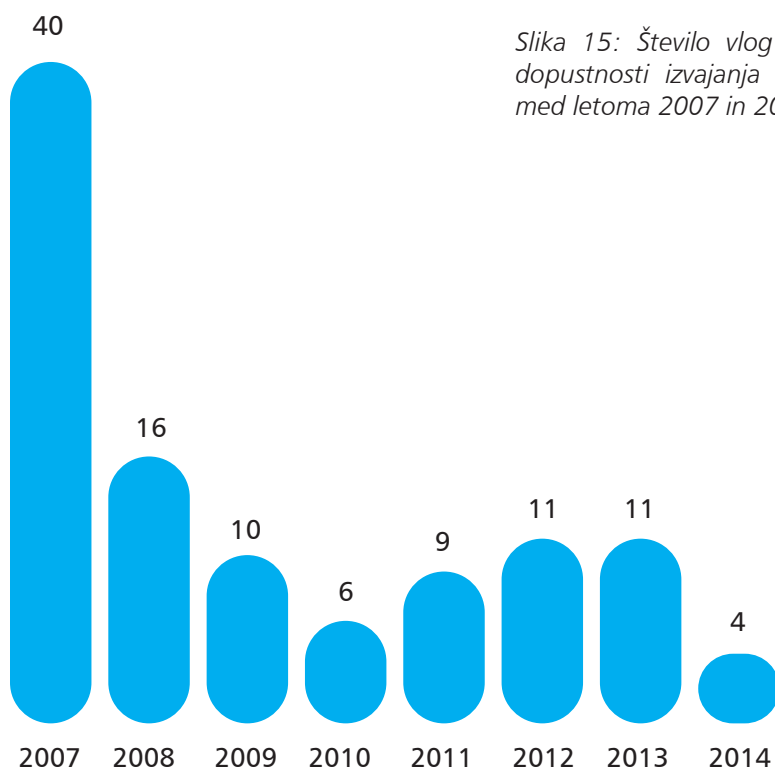
Zaposila za mnenja in pojasnila so zadevala različna področja. Informacijski pooblaščenec izdala mnenja razvršča v 47 področij (npr. bančništvo, biometrija, davčni postopki, delovna razmerja, društva, elektronska pošta, enotna matična številka občana in davčna številka, iznos osebnih podatkov v tretje države, knjižničarstvo, mediji, moderne tehnologije, neposredno trženje in nagradne igre, občine, pogodbeno 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-osebni-podatkov/iskalniki-po-odlocbah-in-mnenjih/odlocbe-in-mnenja-varstvo-osebni-podatkov/>.

### 3.4. Dopustnost izvajanja biometrijskih ukrepov

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

Po določbi tretjega odstavka 80. člena ZVOP-1 mora Informacijski pooblaščenec pri odločanju o tem, ali je nameravana uvedba biometrijskih ukrepov v zasebnem sektorju v skladu z določbami ZVOP-1, predvsem ugotoviti, ali je izvajanje biometrijskih ukrepov nujno za opravljanje dejavnosti, za varnost ljudi ali premoženja ali za zavarovanje 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 doseg namena, Informacijski pooblaščenec ugotavlja, ali bi namen, ki ga zasleduje vlagatelj, lahko dosegel s postopki in ukrepi za zavarovanje, ki manj posegajo v zasebnost zaposlenih oz. ne vključujejo biometrijskih ukrepov. Pri uvajanju slednjih je namreč treba upoštevati, da predstavljajo 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, torej za avtentikacijo, ali za ugotavljanje identitete, torej za identifikacijo).



Slika 15: Število vlog za izdajo odločbe o dopustnosti izvajanja biometrijskih ukrepov med letoma 2007 in 2014.

Informacijski pooblaščenec je leta 2014 prejel štiri vloge (tako leta 2013 kot 2012 jih je prejel 11) za izdajo dovoljenja za uvedbo biometrijskih ukrepov. Izdal je devet odločb, v katerih je presojal in odločil o dopustnosti izvajanja biometrijskih ukrepov, od tega jih je bilo pet izdanih v postopkih, začeti leta 2013. V štirih primerih je Informacijski pooblaščenec vlogam za izvajanje biometrijskih ukrepov delno ugodil, v štirih primerih je zahteve zavrnil, v enem primeru pa je zahtevi v celoti ugodil.

Informacijski pooblaščenec je vlagatelju dovolil, da za namen varovanja tajnih podatkov in premoženja izvaja biometrijske ukrepe z uporabo enaintridesetih čitalnikov prstnih odtisov in treh čitalcev očesne šarenice nad zaposlenimi, ki imajo pooblastilo za vstop v varovane prostore. Gre za prostore, ki so bili s sklepom razglašeni za varnostna območja I. oz. II. stopnje na podlagi Zakona o tajnih podatkih<sup>28</sup> in Uredbe o varovanju tajnih podatkov<sup>29</sup>, v katerih se hranijo tajni podatki (nacionalni tajni podatki najvišjih stopenj tajnosti ter tajni podatki zveze Nato in EU) in komunikacijsko-informacijska tehnologija za prenos tajnih podatkov, ki je ključna za delovanje obrambnega sistema države. Informacijski pooblaščenec je presodil, da je izvajanje biometrijskih ukrepov sorazmerno in da varovanje tajnih podatkov in premoženja v konkretnem primeru odtehta poseg v informacijsko zasebnost zaposlenih. Pri tem je upošteval predvsem težo in obseg posledic uničenja, zlorabe ali drugačnega nepooblaščenega ravnanja s temi podatki. Vlagatelj bo biometrijske ukrepe izvajal le nad ožjim krogom zaposlenih (149 od 8503 zaposlenih), ki so posebej pooblaščen za vstopanje v varovane prostore (imajo z zakonom predpisano dovoljenje za dostop do tajnih podatkov določene stopnje) ter usposobljeni za dela in naloge, ki se odvijajo v teh prostorih.

Zahtevam štirih vlagateljev (štirim povezanim podjetjem), ki imajo poslovne prostore v istem poslovnem objektu oz. pri opravljanju dejavnosti uporabljajo iste poslovne prostore, je Informacijski pooblaščenec ugodil delno. Ker gre kljub povezanosti vlagateljev za samostojne pravne osebe in kot take tudi za samostojne upravljavce osebnih podatkov, ki se bodo obdelovali pri izvajanju biometrijskih ukrepov, je Informacijski pooblaščenec vsakemu izdal posebno odločbo. Vsem je dovolil, da za namen varovanja poslovnih skrivnosti in premoženja (strežnikov) izvajajo biometrijske ukrepe z uporabo čitalnikov prstnih odtisov za vstopanje v pisarne direktorjev, in sicer le nad tistimi zaposlenimi, ki so pooblaščen za vstopanje v te pisarne.

Informacijski pooblaščenec je zavrnil zahteve v delu, ki se je nanašal na izvajanje biometrijskih ukrepov:

- na glavnem vhodu v poslovni objekt, ker je iz navedb vlagateljev izhajalo, da bi bilo mogoče skozi ta vhod vstopati tudi na druge načine (npr. z brezkontaktno kartico ali celo brez nje) in ne samo z izvajanjem biometrijskih ukrepov. Ob takšnem dvojnem sistemu vstopanja bi izvajanje biometrijskih ukrepov izgubilo smisel, saj ne bi v ničemer prispevalo k stopnji varovanja. Biometrijski ukrepi na glavnem vhodu bi se lahko izvajali le, če bi bil celoten poslovni objekt opredeljen kot varovano območje (in ne le določeni prostori), kar pa bi pomenilo tudi, da bi moral biti ustrezno omejen krog oseb, ki lahko vanj vstopajo. V konkretnem primeru pa lahko v objekt vstopajo vsi zaposleni in tudi zunanji obiskovalci.
- na vhodih v prostore proizvodnje, ker vlagatelji niso izkazali, da proizvodni proces ali njegovi deli predstavljajo poslovne skrivnosti po ZGD-1, prav tako niso opredelili premoženja, ki bi ga bilo treba posebej varovati, in niso izkazali, da bi bilo zaradi vstopa nepooblaščenih oseb v te prostore ogroženo življenje in zdravje ljudi. Informacijski pooblaščenec je poudaril, da se navedbe vlagateljev, da je treba izvajati biometrijske ukrepe nad vsemi zaposlenimi, ki opravljajo dela v proizvodnih prostorih, ne ujemajo s samim pojmom poslovne skrivnosti v ZGD-1, katere temeljni element oz. pogoj je, da je znana samo omejenemu krogu posameznikov. Poleg tega bi bil vstop v proizvodnjo mogoč še z brezkontaktnimi karticami, kar pomeni, da izvajanje biometrijskih ukrepov ni nujno, ker obstaja milejši ukrep. Biometrijski ukrepi so namreč učinkoviti samo, če predstavljajo edini način vstopanja v varovane prostore.

<sup>28</sup> Uradni list RS, št. 50/2006 – uradno prečiščeno besedilo 2, s spremembami; v nadaljevanju ZTP.

<sup>29</sup> Uradni list RS, št. 74/2005, s spremembami.

- na vhodih v pisarne pred pisarnami direktorjev, ker naj bi v njih hranili pomembno dokumentacijo, ki naj bi vsebovala tudi poslovne skrivnosti, česar pa vlagatelj niso izkazali.
- na vhodih v moške in ženske garderobe, ker osebne stvari, ki jih zaposleni pustijo v službeni garderobi, ne predstavljajo premoženja take vrste, narave ali vrednosti, ki bi ga bilo treba varovati z biometrijskimi ukrepi. Varovanje osebnih stvari zaposlenih je mogoče zagotoviti z drugimi postopki in ukrepi, ki tudi zagotavljajo učinkovito varovanje, a ne posegajo v informacijsko zasebnost zaposlenih (npr. zaklepanje prostorov, vstop vanje le s ključi ali brezkontaktnimi karticami, posebej zaklenjene omare ali prostori, v katere bi zaposleni lahko shranili vrednejše predmete itd).

Informacijski pooblaščenec je v celoti zavrnil štiri zahteve za izvajanje biometrijskih ukrepov:

Tri zahteve so se nanašale na med seboj povezane družbe oz. vlagatelje (lastnik poslovnih prostorov in poslovna partnerja, ki zanj opravljata storitvene dejavnosti, npr. hišniška opravila in vzdrževalno-obnovitvena dela ter servisiranje strojev in opreme, pomoč pri proizvodnji), ki so nameravali biometrijske ukrepe izvajati s čitalcem prstnih odtisov na vhodu v poslovne prostore. Biometrijske ukrepe naj bi izvajal lastnik prostorov, in sicer nad svojimi zaposlenimi in nad zaposlenimi pri poslovnih partnerjih, ki v delajo v njegovih prostorih. Lastnik v teh prostorih opravlja specifično dejavnost sestavljanja in montaže električnih in strojnih komponent za tirna vozila (lokomotive, vlaki, super hitri vlaki) za nemško podjetje, zato naj bi bili v njih tudi specifični načrti in specifični materiali zalog in polizdelkov.

Informacijski pooblaščenec je zaključil, da vlagatelj niso izkazali, zakaj in kako bi bila lahko ogrožena njihova dejavnost, ljudje ali premoženje ter poslovne skrivnosti ali tajni podatki, če prisotnosti zaposlenih ne bi evidentirali z biometrijskimi ukrepi, ampak na drug način. Informacijski pooblaščenec je poleg tega ugotovil, da bi, četudi bi se ugotovilo, da je za varstvo katere od pravnih dobrin iz 80. člena ZVOP-1 evidentiranje prisotnosti zaposlenih nujen ukrep, za ta namen zadostovala uporaba brezkontaktnih kartic ali drugih primerljivih sredstev, ki predstavljajo manjši poseg v zasebnost posameznika kot uvedba biometrijskih ukrepov. Uvedba biometrijskih ukrepov namreč ni utemeljena in tudi ne nujno potrebna, če jih vlagatelj uvaja zgolj zaradi priročnosti oz. odsotnosti skrbi ob npr. uporabi brezkontaktnih kartic, ki predstavljajo alternativno rešitev preprečevanja vstopa nepooblaščenim osebam v prostor.

Vlogo vlagatelja, ki je navedel, da namerava biometrijske čitalce namestiti na vhodnih vratih v poslovne prostore in vratih v posamezne pisarne, v prostore s strežniki, dvigalo, pa tudi ob vhodu na parkirišče z namenom nadzora dostopa zaposlenih, varovanja premoženja ter preprečevanja vstopa nepooblaščenim osebam. Z izvajanjem biometrijskih ukrepov naj bi vlagatelj preprečil morebitno razkritje ali krajo intelektualne lastnine, marketinških podatkov in premoženja zaposlenih, preprečil pa naj bi tudi nevarnost izrednih dogodkov (požar, sabotaza) ter hkrati poskrbel za nemoten in varen delovni proces. Vlagatelj je pojasnil, da je njegova osnovna dejavnost upravljanje z oglaševalskimi proračuni naročnikov (kar zajema npr. pripravo in izvedbo oglaševalskih strategij za različne blagovne znamke ter analiziranje marketinških in oglaševalskih podatkov) in da pri svojem delu uporablja številne dragocene podatke o naročnikih in slovenskem oglaševalskem trgu, ki jih mora v skladu s pogodbami najstrožje varovati. Neustrezno zavarovanje podatkov bi lahko povzročilo odpoved pogodbe, kar bi mu povzročilo nepopravljivo poslovno škodo. Kot dejavnik tveganja je vlagatelj izpostavil številne obiske predstavnikov medijev, naročnikov in drugih poslovnih partnerjev, pa tudi vse večje število nezaželenih obiskovalcev.

Glede lokacij postavitve čitalcev je Informacijski pooblaščenec zaključil, da je vlagatelj območja varovanja opredelil preširoko oz. da ni navedel, kje konkretno (v katerem prostoru in kje znotraj prostora) naj bi hranil poslovne skrivnosti in vrednejše premoženje, katerega varovanje bi zahtevalo uvedbo biometrijskih ukrepov. Vlagatelj tudi ni predložil dokazov o tem, da razpolaga s poslovnimi skrivnostmi po ZGD-1, in ni izkazal, zakaj svoje dejavnosti ne bi mogel normalno opravljati, če za nadzor vstopa v poslovne prostore ne bi izvajal biometrijskih ukrepov. Poleg tega ni navedel, kakšne ukrepe je že sprejel za varovanje na-

vedenih dobrin. Navedel je le, da so nekateri postopki in ukrepi zavarovanja neustrezni in neprimerni, saj naj bi bili preveč tvegani (razpolaganje zaposlenih s ključi do prostorov) ali naj bi preveč ovirali njegovo normalno delo (najavljanje obiskov, sprotno odpiranje vrat) ali pa naj bi bili dovzetni za zlorabe (kartice, osebna gesla).

Informacijski pooblaščenec je pojasnil, da je z uporabo različnih postopkov in ukrepov (npr. uporaba ključev, brezkontaktnih kartic, osebnih gesel), zlasti pa z njihovo kombinacijo, mogoče doseči povsem primerljivo stopnjo zavarovanja ljudi, premoženja in podatkov kot z izvajanjem biometrijskih ukrepov, in to ob znatno manjšem posegu v informacijsko zasebnost zaposlenih ali celo brez njega. Možnosti zlorab teh načinov zavarovanja seveda ni mogoče povsem izključiti, vendar to velja tudi pri uporabi biometrijskih ukrepov (npr. zaposleni, ki s pomočjo svoje biometrijske značilnosti vstopa v varovani prostor, lahko nepooblaščenim posameznikom omogoči, da v prostor vstopijo skupaj z njim).

Informacijski pooblaščenec je vlagatelje opozoril na napačno razumevanje določbe 80. člena ZVOP-1, v skladu s katero se biometrijski ukrepi lahko izvajajo le nad zaposlenimi, med katere se štejejo samo tisti posamezniki, ki z vlagatelji kot delodajalci sklenejo pogodbo o zaposlitvi iz 11. člena Zakona o delovnih razmerjih<sup>30</sup>. Posameznikov, ki za vlagatelje opravljajo dela na kaki drugi pravni podlagi (podjemne pogodbe, pogodbe o sodelovanju, študentsko delo) ni mogoče šteti med zaposlene, zato nad njimi ni dopustno izvajati biometrijskih ukrepov.

### 3.5. Ugotavljanje ustreznih 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 ustreznih ravni varstva osebnih podatkov v tretjih državah (63. člen);
- vodenje postopkov ugotavljanja ustreznih 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 ustrežno raven varstva osebnih podatkov ali da te nimajo zagotovljene; če je ugotovljeno, da tretja država ustrežno raven varstva osebnih podatkov zagotavlja le delno, je v seznamu navedeno tudi, v katerem delu je ustrežna raven zagotovljena (66. člen);
- vodenje upravnih postopkov za izdajo posebnih dovoljenj za iznos osebnih podatkov v tretjo državo (70. člen).

Informacijski pooblaščenec mora kot pristojni nadzorni organ za varstvo osebnih podatkov glede na določbe 7. točke prvega odstavka 70. člena ZVOP-1 v postopku odločanja o dovolitvi iznosa osebnih podatkov v tretjo državo preveriti, ali upravljavec osebnih podatkov (izvoznik podatkov) zagotavlja ustrezne postopke in ukrepe zavarovanja osebnih podatkov ter preveriti, ali je v določbah pogodb ali v splošnih pogojih poslovanja navedel ustrezne možnosti njihovega uresničevanja in varstva. Poleg tega mora Informacijski pooblaščenec pri odločanju o izdaji posebne odločbe glede iznosa osebnih podatkov v tretje države opraviti tudi vsebinski preizkus o tem, ali za posredovanje oz. 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 pooblaščenцу nalagata ZVOP-1 in ZInfP.

Informacijski pooblaščenec je leta 2014 prejel 11 vlog (leta 2013 jih je prejel 14, leta 2012

<sup>30</sup> Uradni list RS, št. 21/2013 in 78/2013.

pa pet) za iznos osebnih podatkov. Izdal je 13 odločb, od tega dve v zadevah, ki jih je prejel v reševanje leta 2013. Vsem vlagateljem je iznos osebnih podatkov dovolil:

- Podružnicam treh farmacevtskih družb je dovolil, da po prejemu odločb osebne podatke sodelavcev, potrošnikov, poslovnih strank in drugih deležnikov, dobaviteljev in poslovnih partnerjev ter posameznikov, ki sodelujejo ali prispevajo k raziskavam in farmakovigilanci, za namene zagotavljanja informacijske infrastrukture in upravljanja podatkovnih baz iznašajo v Indijo in jih tam posredujejo svojim pogodbenim obdelovalcem.

- Podružnici družbe, ki se ukvarja s trženjem zdravil, je dovolil, da po prejemu odločbe osebne podatke trenutnih in nekdanjih zaposlenih in pogodbenih sodelavcev za namene zagotavljanja izvajanja podpornih storitev s področja upravljanja s človeškimi viri iznaša v Srbijo in jih tam posreduje svojemu pogodbenemu obdelovalcu.

- Podjetju za proizvodnjo armatur ter podjetju za proizvodnjo in prodajo jeklolitin (izvoznika podatkov) je dovolil, da po sklenitvi standardnih pogodbenih klavzul (z obema dodatkom), kot sta jih v svojih vlogah predložila Informacijskemu pooblaščenca, osebne podatke zaposlenih, izvajalcev in nekdanjih zaposlenih iz zbirke človeških virov PeopleSoft ter osebne podatke zaposlenih, posameznikov, ki pošiljajo e-pošto izvozniku ali jo od njega prejemajo, in posameznikov, navedenih v e-poštnih sporočilih ali znotraj funkcije koledarja ali katere koli druge funkcije sistema izmenjave informacij, ki izhajajo iz podatkovne zbirke sistema Microsoft Exchange, za namene koriščenja gostovanja in upravljanja podatkovne zbirke PeopleSoft in sistema za izmenjavo e-pošte Microsoft Exchange iznašata v Združene države Amerike (ZDA) in jih tam posredujejo svojim pogodbenim obdelovalcem.

- Družbi za davčno in družbi za poslovno svetovanje (izvoznika podatkov) je dovolil, da po prejemu odločbe drugim upravljavcem osebnih podatkov v tretjih državah – članom mreže, za katere nadzor in upravljanje je zadolžena družba iz Velike Britanije, katere člana sta izvoznika podatkov, iznašata in posredujejo osebne podatke sedanjih in nekdanjih uslužbencev, partnerjev, upravljavcev in direktorjev družbe, prijaviteljev, vzdrževalcev, pogodbenih delavcev in izvajalcev del, strank, kupcev in prodajalcev. Pravno podlago za iznos podatkov predstavljajo zavezujoča poslovna pravila, podatki pa se bodo obdelovali za namene globalnega poslovanja članov mreže: globalnega upravljanja zaposlovanja, programa osebnega razvojnega upravljanja uslužbencev, standardiziranja procesa komuniciranja s strankami, globalnega računovodenja v zvezi z uslužbenci, dobavitelji, pogodbenimi delavci in strankami, ocene poslovnih odnosov in preverjanja, s katerimi družba zagotavlja, da članice mreže sledijo njihovim in lokalnim pravilom, nadzora kvalitete storitev, zagotavljanja opozoril glede potovanj za uslužbence in poročil o izrednih situacijah, kadar so ta potrebna, globalnega spremljanja delovnega časa in stroškov uslužbencev, vzdrževanja centralne zbirke podatkov pogodbenih delavcev, ki opravljajo oz. so opravljali storitve za družbo na področju Evrope, Bližnjega vzhoda, Indije in Afrike.

- Družbi za promet s farmacevtskimi izdelki (izvoznik podatkov) je dovolil, da po prejemu odločbe drugim upravljavcem osebnih podatkov v tretjih državah – članom skupine podjetij, za katere nadzor in upravljanje je zadolžena družba iz Velike Britanije, katere član je izvoznik podatkov, iznaša in posreduje osebne podatke trenutnih, preteklih in prihodnjih zaposlenih ali dopolnilnih delavcev ter njihovih zakoncev in vzdrževanih družinskih članov, če je to potrebno, ter osebne podatke zunanjih zdravnikov in drugih strokovnih zdravstvenih delavcev, ki sodelujejo pri raziskavah in razvoju, ter kandidatov ali posameznikov, ki sodelujejo pri raziskovalnih aktivnostih, ali posameznikov, ki jemljejo proizvode ali zdravila in katerih osebne podatke izvoznik obdeluje v procesih farmakovigilance. Podatki se bodo iznašali na podlagi zavezujočih poslovnih pravil z namenom centralizacije obdelave osebnih podatkov in zagotavljanja enake stopnje kakovosti ter upravljanja tveganj v zvezi z obdelavo osebnih podatkov znotraj skupine, tako za potrebe upravljanja s človeškimi viri kot tudi za potrebe raziskav in razvoja.

- Družbi za trženje medicinske in laboratorijske opreme (izvoznik podatkov) je dovolil, da po prejemu odločbe drugim upravljavcem osebnih podatkov v tretjih državah

– povezanim družbam znotraj koncerna, katerega član je tudi izvoznik podatkov, iznaša in posreduje osebne podatke zaposlenih v družbi, kupcev, dobaviteljev ter drugih poslovnih in pogodbenih partnerjev na podlagi zavezujočih poslovnih pravil. Izvoznik podatkov namerava osebne podatke posredovati z namenom povezovanja aktivnosti med povezanimi družbami znotraj koncerna – za namene iskanja kadrov, administracije človeških virov in razvoja zaposlenih, za namene skladnosti poslovanja, za izvajanje in implementacijo nalog in projektov za zunanje in notranje partnerje, za obdelavo naročil in delovnih nalogov z dobavitelji in ponudniki storitev, za izpolnjevanje nalog v zvezi s poročanjem, za izpolnjevanje obveznosti do dobaviteljev in izterjavo dolgov kupcev, za računovodske namene, za namene interne komunikacije, za namene konsolidacije in združevanja IT-postopkov v določenih regijah s ciljem zniževanja stroškov ter tudi v povezavi s sodelovanjem in koordinacijo družb skupine na nivoju divizij ali regij ali pa na globalnem nivoju v toku poslovnih transakcij in projektov.

· Družbi, katere dejavnost je prodaja kozmetičnih izdelkov, je Informacijski pooblaščenec kot članici mednarodne korporacije dovolil, da po prejemu odločbe osebne podatke:

1. lastnikov, partnerjev in družbenikov tretje stranke kot posrednika in morebitne matične družbe tretje stranke kot posrednika, če ta obstaja,
2. direktorjev, vodilnih oseb, zaposlenih in morebitnih prihodnjih zaposlenih tretje stranke kot posrednika,
3. bližjih sorodnikov lastnikov, partnerjev in družbenikov tretje stranke kot posrednika in njegove morebitne matične družbe, če ta obstaja, in direktorjev, vodilnih oseb, zaposlenih in morebitnih prihodnjih zaposlenih tretje stranke kot posrednika,
4. poslovnih družabnikov lastnikov, partnerjev in delničarjev tretje stranke kot posrednika in njene morebitne matične družbe, če ta obstaja, in direktorjev, vodilnih oseb, zaposlenih in morebitnih prihodnjih zaposlenih tretje stranke kot posrednika,
5. vladnih uradnikov, ki jim tretja stranka kot posrednik plačuje nadomestilo, in
6. zastopnikov ali agentov, podpogodbениkov, hčerinskih družb, povezanih podjetij, partnerjev ali mešanih družb, ki jih najame tretja stranka kot posrednik,
7. posreduje svoji matični družbi v ZDA in povezani družbi v Hongkong zaradi izpolnjevanja pravnih zahtev in obveznosti vodenja evidenc in poročanja, za izvedbo revizij in poizvedb o preteklosti oseb, za upoštevanje vladnih inšpekcij in drugih zahtev vlade ali drugih javnih organov, za odzivanje na sodne postopke, za uveljavljanje zakonskih pravic in pravnih sredstev, za obrambo v pravnih sporih in reševanje morebitnih internih pritožb ali zahtevkov ter za upoštevanje internih politik in postopkov.

· Družbi za računalništvo in informatiko (izvoznik podatkov) je dovolil, da po prejemu odločbe:

1. osebne podatke, ki se nanašajo na upravljanje s človeškimi viri: osebni podatki trenutnih in nekdanjih zaposlenih pri izvozniku, neodvisnih zunanjih izvajalcev, občasnih delavcev in pripravnikov, ki so zaposleni pri ali opravljajo delo za izvoznika, in družinskih članov navedenih oseb;
2. osebne podatke, ki se nanašajo na zaposlovanje: osebni podatki kandidatov in potencialnih kandidatov za zaposlitev pri izvozniku;
3. osebne podatke, ki se nanašajo na finančno poslovanje: osebni podatki izvoznikovih strank, pogodbenikov, dobaviteljev, prodajalcev, potencialnih strank in partnerjev;
4. osebne podatke, ki se nanašajo na poslovne stike: osebni podatki izvoznikovih poslovnih strank, vključno z obstoječimi in potencialnimi poslovnimi strankami, distributerjev, (pod)pogodbениkov, prodajalcev in poslovnih partnerjev;

iznaša v ZDA in jih tam posreduje drugemu upravljavcu osebnih podatkov v mednarodni korporaciji (uvozniku podatkov), katere član je izvoznik podatkov. Uvoznik podatkov bo osebne podatke obdeloval za potrebe izvoznika in za lastne potrebe, zlasti za zagotavljanje učinkovitega delovanja korporacije, za usklajevanje poslovanja povezanih družb in za izvrševanje upravljanja nad povezanimi družbami.

· Družbi za kurirske storitve (izvoznik podatkov) je dovolil, da po prejemu odločbe:

1. drugim družbam v mednarodni skupini s sedeži v tretjih državah posreduje osebne



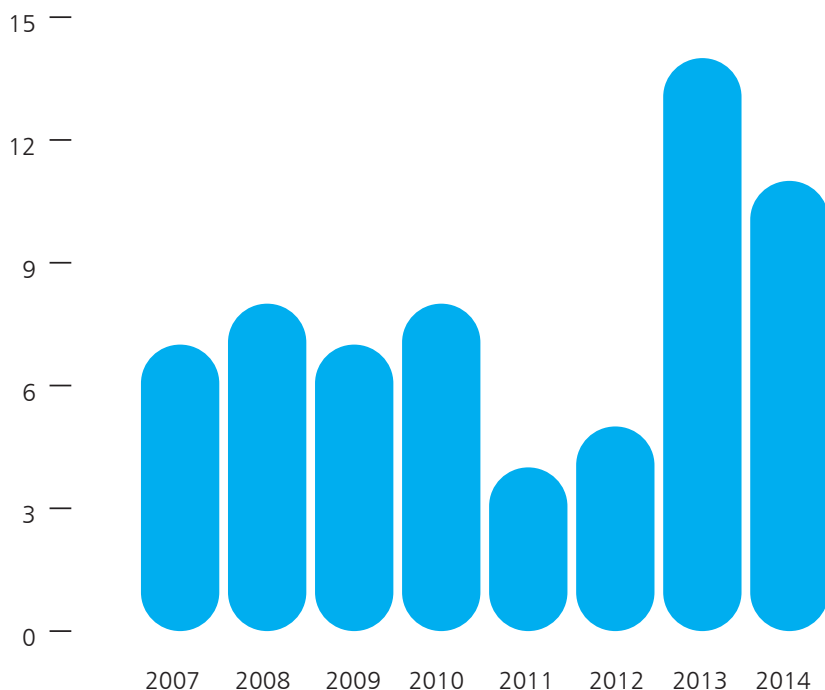
- podatke strank, zaposlenih pri strankah, pošiljatelj in prejemnikov pošiljk ter zaposlenih pri izvozniku podatkov za namen zagotavljanja seznama zaposlenih, kakor tudi za SharePoint in druga orodja za lažjo in boljše komunikacijo med družbami v skupini, za namen centraliziranega upravljanja strank in odnosov s strankami, učinkovitejšega zagotavljanja storitev in hitrejšega sprejemanja poslovnih odločitev, urejanja in načrtovanja dostave pošiljk, pošiljanja in sledenja naročil, upravljanja z napakami in izgubljenimi pošiljkami, centraliziranega in koordiniranega oglaševanja in odnosov z javnostmi, poslovnih analiz in priprave poročil ter za namen zagotavljanja skladnosti z veljavno zakonodajo in internimi politikami;
2. svoji matični družbi posreduje osebne podatke zaposlenih za namen izvajanja rešitev upravljanja s človeškimi viri, izvajanja sistema PRISM – notranje baze podatkov z dokumentacijo o kadrih, izvajanja sistema Satisfaction-Feedback-Action, upravljanja e-izobraževanja zaposlenih, upravljanja s kariernim portalom, zagotavljanja seznama zaposlenih, kakor tudi za SharePoint in druga orodja za lažjo in boljše komunikacijo med družbami v skupini; osebne podatke strank, zaposlenih pri strankah, pošiljatelj in prejemnikov pošiljk za namen upravljanja odnosov s strankami, hitrejšega sprejemanja poslovnih odločitev, upravljanja z IT-sistemi in orodji za upravljanje pošiljk, njihovo sledenje in dostavo, centraliziranega in koordiniranega oglaševanja in odnosov z javnostmi, poslovnih analiz in priprave poročil ter zagotavljanja skladnosti z veljavno zakonodajo in internimi politikami; osebne podatke dobaviteljev in zaposlenih pri dobaviteljih za namen izvajanja pogodbenih odnosov (postopek odobritve računov);
  3. svojemu pogodbenemu obdelovalcu v ZDA za namen izvajanja storitev gostovanja in zagotavljanja vzdrževanja in posodabljanja programske opreme ter upravljanja s strukturo podatkov posreduje osebne podatke zaposlenih, strank, pošiljatelj in prejemnikov pošiljk ter dobaviteljev;
  4. svojemu pogodbenemu obdelovalcu v ZDA za namen razvijanja vzdušja zaposlovanja in analize zasedenosti delovnih mest, spremljanja zaposlovanja in ad hoc poročanja ter načrtovanja odzivov na dobljene povratne informacije posreduje osebne podatke zaposlenih.

V primeru iznosa osebnih podatkov pogodbenim obdelovalcem (uvoznikom podatkov), ki bodo osebne podatke obdelovali v imenu in za račun upravljavcev osebnih podatkov (izvoznikov podatkov), se kot pravna podlaga za posredovanje osebnih podatkov 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 in 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 ter osebnih podatkov ne sme obdelovati za noben drug namen. Medsebojne pravice in obveznosti se uredijo s pogodbo, ki mora biti sklenjena v pisni obliki in mora vsebovati tudi dogovor o postopkih in ukrepih iz 24. člena tega zakona. Informacijski pooblaščenec je po pregledu pogodb s standardnimi pogodbenimi klavzulami, ki so jih predložili izvozniki podatkov, ugotovil, da so izvozniki in uvozniki podatkov uporabili in sprejeli model standardnih pogodbenih klavzul in oba dodatka iz Sklepa Komisije z dne 5. 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 drugi 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 hkrati zadostijo tudi vsem zahtevam iz 11. člena ZVOP-1, saj štejejo kot pisna pogodba med upravljavcem osebnih podatkov in pogodbenim obdelovalcem, iz katere so razvidne medsebojne pravice in obveznosti, poleg tega pa sprejete klavzule z obema dodatkoma in prej omenjeno pogodbo vsebujejo tudi dogovor o postopkih in ukrepih za zavarovanje osebnih podatkov iz 24. člena ZVOP-1.

Pri posredovanju osebnih podatkov na podlagi zavezujočih poslovnih pravil (BCR - Binding Corporate Rules) je Informacijski pooblaščenec 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 člena 29, 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 navede možnosti njihovega uresničevanja ali varstva, skladno 7. točko prvega odstavka 70. člena ZVOP-1. Postopek sprejema zavezujočih poslovnih pravil zajema postopek pred vodilnim organom za varstvo osebnih podatkov glede na sedež ustrezne članice v EU (v obravnavanih primerih sta bila to organa Velike Britanije in Nemčije), 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 preostali organi iz relevantnih držav članic EU.

V primeru posredovanja osebnih podatkov drugim upravljavcem osebnih podatkov v tretjih državah je Informacijski pooblaščenec preverjal pravne podlage za iznos osebnih podatkov in pri tem ugotovil, da je pravna podlaga za posredovanje osebnih podatkov zaposlenih 48. člen ZDR-1, saj je posredovanje osebnih podatkov potrebno zaradi uresničevanja pravic in obveznosti iz delovnega razmerja. Če se delavec zaposli v mednarodnem podjetju, ki je sestavni del korporacije, v okviru katere mora biti delovanje povezanih družb usklajeno, centralnega upravljanja s kadri nedvomno ni mogoče zagotoviti drugače, kot da se podatki o zaposlenih posredujejo določeni družbi znotraj skupine. Pravno podlago za iznos osebnih podatkov kandidatov in strank predstavljajo osebne privolitve, osebni podatki poslovnih partnerjev pa se bodo posredovali na podlagi drugega odstavka 10. člena ZVOP-1, saj je obdelava osebnih podatkov nujno potrebna med pogajanjem ter za poslovanje in sklepanje pogodb. Ker so izvozniki osebnih podatkov nameravali iznesti osebne podatke v tretjo državo tudi na podlagi 7. točke prvega odstavka 70. člena ZVOP-1, so morali pridobiti odločbo Informacijskega pooblaščenca. Ta je opravil skrben pregled pogodb, ki so jih predložili izvozniki podatkov, in pri tem ugotovil, da so izvozniki in uvozniki podatkov v pogodbah v celoti uporabili standardne pogodbene klavzule ter obe prilogi (Načela obdelave podatkov in Opis prenosa) iz Odločbe Komisije Evropskih skupnosti z dne 27. 12. 2004 o spremembi Odločbe 2001/497/ES glede uvedbe alternativnega sklopa standardnih pogodbenih klavzul za prenos osebnih podatkov v tretje države (notificirana pod dokumentarno številko K(2004) 5271), ki veljajo za prenos osebnih podatkov od upravljavca k upravljavcu. Uporabljene standardne pogodbene klavzule zagotavljajo primerne zaščitne ukrepe glede varstva zasebnosti ter temeljnih pravic in svoboščin posameznikov in glede uveljavljanja ustreznih pravic, kakor zahteva drugi odstavek 26. člena Direktive 95/46/ES Evropskega Parlamenta in Sveta z dne 24. 10. 1995 o zaščiti posameznikov pri obdelavi osebnih podatkov in pri prostem gibanju takih podatkov.

Slika 16: Število vlog za izdajo odločbe glede iznosa osebnih podatkov med letoma 2007 in 2014.



### 3.6. 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 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 oz. 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.).

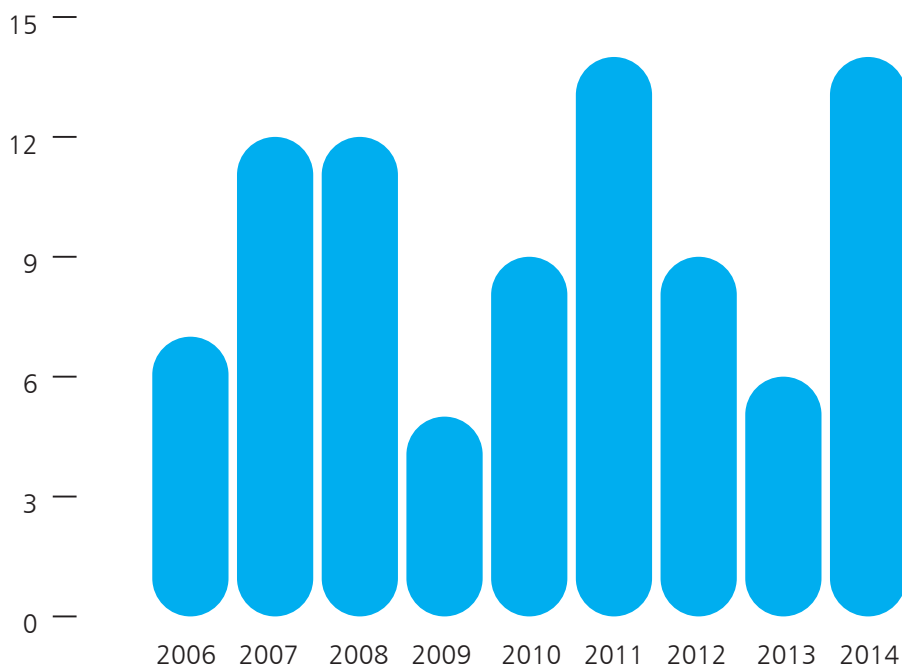
Zoper odločbo Informacijskega pooblaščenca pritožba ni mogoča, dovoljen pa je upravni spor.

Informacijski pooblaščenec je leta 2014 prejel 14 vlog (leta 2013 šest in leta 2012 devet) za pridobitev dovoljenja za povezovanje zbirk osebnih podatkov. Izdal je devet odločb, s katerimi je dovolil povezovanje zbirk osebnih podatkov. En vlagatelj je svojo vlogo umaknil.

Informacijski pooblaščenec je dovolil povezovanje naslednjih zbirk osebnih podatkov:

1. Zavodu za pokojninsko in invalidsko zavarovanje Slovenije ter Agenciji RS za javno-pravne evidence in storitve je dovolil vzpostavitev neposredne računalniške povezave med Matično evidenco zavarovancev in uživalcev pravic iz obveznega pokojninskega in invalidskega zavarovanja ter Poslovnim registrom Slovenije. Povezava med zbirkama se izvede z uporabo EMŠO.
2. Javnemu, jamstvenemu, preživninskemu in invalidskemu skladu RS je dovolil, da Evidenco o pravicah z naslova insolventnosti delodajalca in Evidenco o nadomestilih preživnine poveže s Centralnim registrom prebivalstva, katerega upravljavec je Ministrstvo za notranje zadeve. Kot povezovalni znak se uporabi EMŠO.
3. Vrhovnemu sodišču RS je dovolil, da Informacijski sistem e-INS poveže z Davčnim registrom, katerega upravljavec je Ministrstvo za finance, Davčna uprava RS. Povezava med zbirkama se izvede z uporabo davčne številke.
4. Zavodu za pokojninsko in invalidsko zavarovanje Slovenije je dovolil, da Matično evidenco zavarovancev in uživalcev pravic iz obveznega pokojninskega in invalidskega zavarovanja poveže z Evidenco davkov in prispevkov ter s Knjigovodsko evidenco, katerih upravljavec je Ministrstvo za finance, Davčna uprava RS. Kot povezovalni znak se uporabijo EMŠO, davčna številka in identifikacijska številka zavarovanca.
5. Ministrstvu za pravosodje je dovolil, da Imenik sodnih izvedencev, sodnih cenilcev in sodnih tolmačev poveže s Centralnim registrom prebivalstva, katerega upravljavec je Ministrstvo za notranje zadeve. Kot povezovalni znak se uporabi EMŠO.
6. Ministrstvu za izobraževanje znanost in šport je dovolil, da Evidenčni in analitski sistem visokega šolstva v RS (eVŠ) poveže z Evidenco prijavljenih za vpis in vpisanih študentov višjih strokovnih šol, ki jo vodi izvajalec višješolske prijavnne službe. Povezava med zbirkama se izvede z uporabo EMŠO.
7. Ministrstvu za izobraževanje znanost in šport je dovolil, da eVŠ poveže s Centralno evidenco udeležencev vzgoje in izobraževanja (CEUVIZ). Povezava med zbirkama se izvede z uporabo EMŠO.
8. Zavodu za pokojninsko in invalidsko zavarovanje Slovenije je dovolil, da Matično evidenco zavarovancev in uživalcev pravic iz obveznega pokojninskega in invalidskega zavarovanja in Matično evidenco o zavarovancih neposredno računalniško poveže z eVŠ - Evidenco študentov in diplomantov ter s CEUVIZ, katerih upravljavec je Ministrstvo za izobraževanje, znanost in šport. Kot povezovalni znak se uporabi EMŠO.
9. Ministrstvu za pravosodje, Upravi RS za izvrševanje kazenskih sankcij je dovolil, da Centralno evidenco pripornikov RS in Centralno evidenco o osebah na prestajanju kazni zapora poveže s Centralnim registrom prebivalstva, katerega upravljavec je Ministrstvo za notranje zadeve. Kot povezovalni znak se uporabi EMŠO.

Slika 17: Število vlog za izdajo odločbe glede povezljivosti zbirk osebnih podatkov med letoma 2006 in 2014.



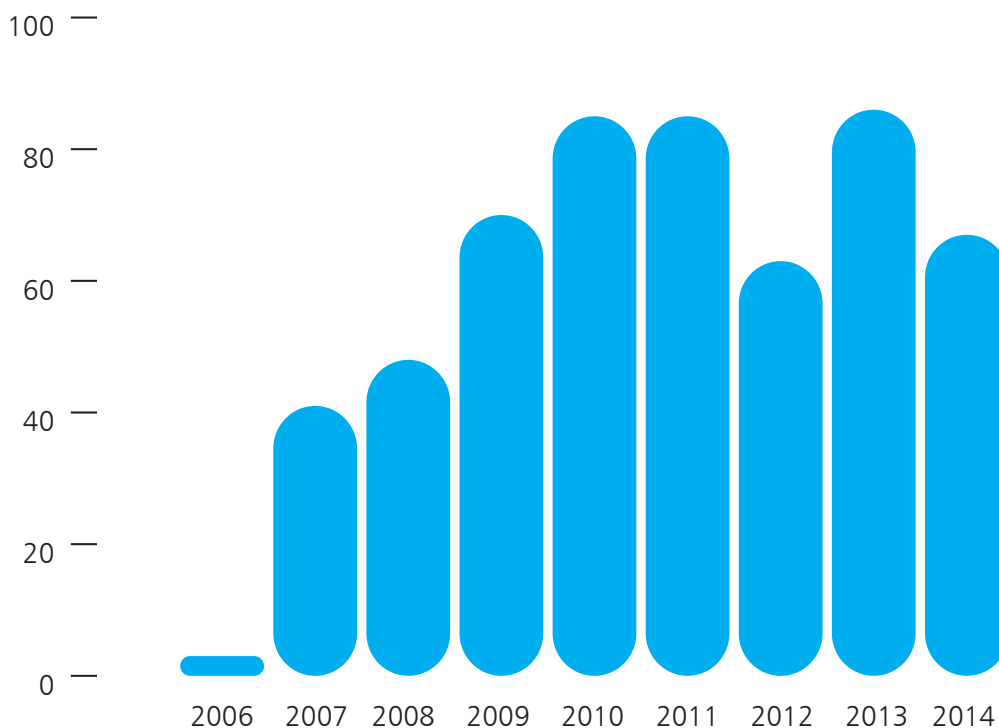
### 3.7. Seznanitev z lastnimi osebnimi podatki

V skladu s tretjim odstavkom 38. člena Ustave RS je posamezniku zagotovljena pravica do seznanitve z zbranimi osebnimi podatki, ki se nanašajo nanj. Omenjena 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 2014 prejel 67 pritožb v zvezi s pravico do seznanitve z lastnimi osebnimi podatki (leta 2013 jih je prejel 68, leta 2012 pa 63). V okviru pritožbenih postopkov je Informacijski pooblaščenec reševal tudi pritožbe, ko posamezniki niso pridobili zdravstvene dokumentacije po ZPacP. Teh je bilo pet (leta 2010 so bile štiri, leta 2011 jih je bilo 18, leta 2012 deset, leta 2013 pa 11).

Informacijski pooblaščenec je po preučitvi pritožb ugotovil, da se je v primerjavi s preteklimi leti delež molka upravljavcev osebnih podatkov, ko ti na zahtevo posameznika po seznanitvi z lastnimi osebnimi podatki sploh niso odgovorili, malenkost zmanjšal – znašal je 49,2 % (leta 2013 52 %). Posameznik lahko v primeru molka upravljavca, pa tudi v primeru zavrnitve seznanitve, vloži pritožbo Informacijskemu pooblaščenču.

Slika 18: Število pritožb v zvezi s pravico do seznanitve z lastnimi osebnimi podatki med letoma 2006 in 2014.



Vložene pritožbe so v 39 primerih (58 %) zadevale državne organe (večinoma ministrstva in organe v njihovi sestavi), medtem ko so se ostale pritožbe nanašale na različne skupine upravljalcev osebnih podatkov, med katerimi nobena ni številčno posebej izstopala (občine, društva, banke, zavarovalnice, zdravstvene in izobraževalne ustanove, centri za socialno delo).

Informacijski pooblaščenec je po prejemu pritožbe upravljalca osebnih podatkov vedno najprej pozval, da pojasni, zakaj posamezniku ni odgovoril ali zakaj mu ni omogočil seznanitve z lastnimi osebnimi podatki. V 19 primerih so upravljalci 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 upravljalcev osebnih podatkov po prejemu zahteve posameznika je bil v večini primerov nepoznavanje pravice do seznanitve z lastnimi osebnimi podatki in njihovih dolžnosti v zvezi z njenim izvrševanjem. Če upravljalci osebnih podatkov posameznikom niso omogočili seznanitve, je Informacijski pooblaščenec o pravici posameznika odločil z odločbo. Tako je izdal štiri odločbe, s katerimi je upravljavcem naložil, da morajo posameznikom omogočiti seznanitev z njihovimi osebnimi podatki, od tega je v dveh odločbah zahtevi posameznika ugodil delno. Zaradi potrebe po popolni ugotovitvi dejanskega stanja (ogled razpoložljivega dokumentarnega gradiva) je Informacijski pooblaščenec v prostorih upravljalcev osebnih podatkov opravil dva oglada, na katera so bili vabljeni tudi posamezniki, ki so vložili pritožbe. Informacijski pooblaščenec je z odločbo zavrnil dve pritožbi, eno pritožbo pa je s sklepom zavrgel. Pritožbi je zavrnil, ker vsebinsko nista predstavljali pritožbe zaradi zavrnitve seznanitve z lastnimi osebnimi podatki, zavrgel pa ker pritožnik svoje vloge po pozivu ni dopolnil. Informacijski pooblaščenec je 14 posameznikom svetoval, kako naj postopajo, osem pritožb je odstopil v reševanje pristojnim organom, trije posamezniki pa so svoje pritožbe umaknili.

Leta 2014 je bila zoper eno odločbo Informacijskega pooblaščenca vložena tožba na Upravno sodišče RS. To je tožbo kot neutemeljeno zavrnilo.

### 3.8. Zahteve za oceno ustavnosti

Informacijski pooblaščenec lahko z zahtevo začne postopek za oceno ustavnosti oz. zakonitosti predpisov na podlagi 23.a člena Zakona o Ustavnem sodišču<sup>31</sup>, 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 2014 Informacijski pooblaščenec ni vložil nobene zahteve za oceno ustavnosti.

#### 3.8.1. Odločitev Ustavnega sodišča RS v zvezi z oceno ustavnosti in zakonitosti XIII. poglavja (hramba podatkov) – 162., 163., 164., 165., 166., 167., 168. in 169. člena Zakona o elektronskih komunikacijah<sup>32</sup>

Informacijski pooblaščenec je prejel sodbo Ustavnega sodišča RS v zvezi z zahtevo za oceno ustavnosti določb XIII. poglavja ZEKom-1 o obvezni hrambi podatkov o prometu elektronskih komunikacij zatrjujoč nesorazmernost ukrepa, ki posega v zasebnost slehrega posameznika in ki s strani uporabnikov teh podatkov (policije, varnostnih in obveščevalnih služb) ni omejen na hujša kazniva dejanja, kot je opredeljeno v Direktivi 2006/24/ES kot temelju za nacionalno zakonsko ureditev.

Ustavno sodišče RS je konec septembra 2013 postopek za oceno ustavnosti prekinilo do odločitve Sodišča EU v zadevah C-293/12 in C-594/12, ker je glavni očitke neustavnosti temeljil na obvezni hrambi podatkov, kot naj bi izhajala iz Direktive 2006/24/ES. Sodišče EU je 8. 4. 2014 sprejelo odločbo, s katero je Direktivo razglasilo za neveljavno, češ da je zakonodajalec z njenim sprejetjem prekoračil meje, ki jih zahteva spoštovanje načela sorazmernosti iz Evropske listine o temeljnih pravicah.

Ustavno sodišče RS je o zahtevi Informacijskega pooblaščenca odločilo z odločbo U-I-65/13-19 z dne 3. 7. 2014, tako da je razveljavilo 162., 163., 164., 165., 166., 167., 168. in 169. člen ZEKom-1, poleg tega pa je – da bi preprečilo nadaljnje nesorazmerne posege v pravico do varstva osebnih podatkov – operaterjem naložilo uničenje vseh podatkov, ki jih hranijo na podlagi izpodbijanih določb, takoj po objavi odločbe v uradnem listu RS. Ustavno sodišče RS je ukrep obvezne hrambe prepoznalo kot nesorazmeren z več vidikov:

- ker neselektivna in vnaprejšnja hramba prometnih podatkov nujno v prevladujočem delu pomeni poseg v pravice tistega dela prebivalstva, ki ni dala povoda za takšen poseg, in ne omogoča anonimne uporabe komunikacijskih sredstev za vse tiste primere, ko je zaupna in nesledljiva uporaba komunikacijskih sredstev nujna za doseg njenega namena (npr. telefonske storitve za pomoč v duševni stiski);
- ker razlogi za relativno dolgo hrambo podatkov (14 mesecev za podatke v zvezi s telefonskimi storitvami in 8 mesecev za vse druge podatke) iz zakonodajnega gradiva niso razvidni;
- ker izpodbijane določbe obdelave obvezno hranjenih prometnih podatkov niso omejile na zgolj določena (huda kazniva) dejanja, za katere bi ocenili, da zaradi njihove teže hramba podatkov oz. dostop do njih opravičujeta poseg v zasebnost posameznika.

Informacijski pooblaščenec je odločitev Ustavnega sodišča RS sprejel z velikim zadovoljstvom kot izjemno pomemben korak v varstvu pravic posameznikov do zasebnosti. Sodišče je prepoznalo pomen varstva osebnih podatkov v odnosu do modernih komunikacijskih tehnologij, še posebej kadar so te uporabljene s strani samih državnih (represivnih) organov oz. za namen izvajanja njihovih pristojnosti.

<sup>31</sup> Uradni list RS, št. 64/2007 – uradno prečiščeno besedilo 1, s spremembami.

<sup>32</sup> Uradni list RS, št. 109/2012; v nadaljevanju ZEKom-1.

### 3.9. Izbrani primeri kršitev varstva osebnih podatkov

V nadaljevanju je predstavljenih sedem odločitev Informacijskega pooblaščenca v postopkih, ki jih je vodil leta 2014.

#### 3.9.1. Ustvarjanje nove zbirke osebnih podatkov iz podatkov, objavljenih na spletu, in njeno trženje

Informacijski pooblaščenec je uvedel postopek zaradi suma nezakonite obdelave osebnih podatkov – zbirke 40.000 e-naslovov posameznikov, ki jo je zavezanec proti plačilu ponujal na spletu.

V skladu s 1. točko 6. člena ZVOP-1 je osebni podatek kateri koli podatek, ki se nanaša na posameznika, ne glede na obliko, v kateri je izražen, pri čemer je posameznik v skladu z 2. točko 6. člena ZVOP-1 določena ali določljiva fizična oseba, na katero se osebni podatek nanaša. Tudi e-naslov je osebni podatek takrat, kadar določi posameznika oz. ga naredi določljivega (tudi če ne vsebuje imena in priimka posameznika). Informacijski pooblaščenec je pridobil kopijo sporne zbirke in ugotovil, da so določeni e-naslovi v zbirki vsebovali ime in priimek (oz. so bili tipa ime.priimek@podjetje.si, ime.priimek@ponudnik.com ipd.) ter tako zagotovo predstavljali osebne podatke, ki so varovani z določbami ZVOP-1, saj so bili imetniki teh e-naslovov na enostaven način določljivi. Zato jim ni mogoče odreči pravic, ki jih posameznikom glede njihovih osebnih podatkov daje ZVOP-1, med katerimi je treba izpostaviti zlasti pravico do seznanitve (30. člen ZVOP-1), pravico do dopolnitve, popravka, blokiranja, izbrisa in ugovora (32. člen ZVOP-1) ter pravico do prepovedi obdelave e-naslava za namene neposrednega trženja (73. člen ZVOP-1). V omenjeni zbirki e-naslovov osebnih podatkov niso predstavljali le tisti e-naslovi, ki so pripadali pravnim osebam, torej e-naslovi tipa info@podjetje.si, podjetje@siol.net ipd. Takšni e-naslovi niso varovani z določbami ZVOP-1.

Ker je bilo z vpogledom v omenjeno zbirko e-naslovov, ki je dejansko vsebovala 36.093 e-naslovov, ugotovljeno, da vsebuje tudi z ZVOP-1 varovane osebne podatke, je bilo bistveno vprašanje, ali ima zavezanec pravno podlago za njihovo obdelavo (pridobivanje, uporabo, hrambo, razkrivanje, sporočanje, dajanje na razpolago ipd.).

Splošne pravne podlage za obdelavo osebnih podatkov so podane v 8. členu ZVOP-1, pravne podlage za obdelavo osebnih podatkov v zasebnem sektorju pa navaja 10. člen ZVOP-1, ki določa, da se osebni podatki lahko obdelujejo, če obdelavo osebnih podatkov in osebne podatke, ki se obdelujejo, določa zakon ali če je za obdelavo določenih osebnih podatkov podana osebna privolitev posameznika, če je obdelava osebnih podatkov potrebna in primerna za izvedbo pogajanj za sklenitev pogodbe ali za izpolnjevanje pogodbe ali če je to nujno zaradi uresničevanja zakonitih interesov zasebnega sektorja.

V konkretnem primeru je bilo treba upoštevati tudi določbe ZEKom-1, ki ureja področje trženja z uporabo elektronskih komunikacij, in v 158. členu določa, da je uporaba e-pošte za namene neposrednega trženja dovoljena samo na podlagi naročnikovega ali uporabnikovega predhodnega soglasja (t. i. načelo opt-in). Izjemoma je uporaba e-naslava za neposredno trženje dovoljena v tistih primerih, ko fizična ali pravna oseba e-naslov posameznika pridobi od kupca svojih izdelkov ali storitev in ta naslov uporablja za neposredno trženje svojih podobnih izdelkov ali storitev.

Po določbi 16. člena ZVOP-1 se lahko osebni podatki zbirajo le za določene in zakonite namene ter se ne smejo nadalje obdelovati tako, da bi bila njihova obdelava v neskladju s temi nameni, če zakon ne določa drugače. V zvezi z zavezančevimi navedbami, da je določene e-naslave pridobil iz javno dostopnih virov, je Informacijski pooblaščenec ugotovil, da bi bila njihova nadaljnja obdelava dopustna le v primerih oz. pod pogoji, ki jih



določa ZVOP-1 v 10. členu. Brez obstoja pravne podlage pomeni vsaka obdelava (zbiranje, pridobivanje, urejanje, shranjevanje, razkrivanje, sporočanje, širjenje ali povezovanje osebnih podatkov) brez vnaprejšnje seznanitve posameznika in podane osebne privolitve posameznika poseg v pravico iz 38. člena Ustave RS (prvi odstavek prepoveduje uporabo osebnih podatkov v nasprotju z namenom njihovega zbiranja) ter kršitev določb ZVOP-1. Vzpostavitev nove zbirke osebnih podatkov in uporaba teh za pridobitne namene oz. trženje namreč pomeni uporabo osebnih podatkov izven namenov javne objave podatkov na spletnih straneh oz. izven namenov uporabe osebnih podatkov svojih strank za izvajanje neposrednega trženja svojih izdelkov in storitev.

Dejstvo, da so bili določeni osebni podatki predhodno javno objavljeni ali vključeni v posamezno javno objavljeno zbirko osebnih podatkov (npr. BIZI), torej še ne pomeni, da se lahko takšni osebni podatki brez pravne podlage povežejo in uporabijo za vzpostavitev in vodenje nove zbirke osebnih podatkov, kot je to naredil zavezanec. Sklicevanje na predhodno javno objavo uporabljenih osebnih podatkov je brezpredmetno, saj 10. člen ZVOP-1, ki določa pravne podlage za zakonito obdelavo osebnih podatkov v zasebnem sektorju, glede tega ne določa nobene izjeme. Obdelavo osebnih podatkov (v konkretnem primeru uporabo podatkov za vzpostavitev nove zbirke in njeno trženje oz. dajanje na razpolgo drugim uporabnikom) mora določati poseben zakon, če take zakonske podlage ni, pa mora biti podana osebna privolitev posameznika. Takšno stališče je zavzelo tudi Upravno sodišče RS v sodbi št. U 2477/2005-48 z dne 10. 10. 2007, ki se je nanašala na ponovno uporabo javno objavljenih podatkov o zastopnikih, članih vodstev, ustanoviteljih ali članih nadzornih svetov v poslovnih subjektih. Enako stališče je Upravno sodišče RS zavzelo tudi v sodbi št. I U 1047/2010-19 z dne 14. 7. 2011, v upravnem sporu, ki se je nanašal na vzpostavitev in trženje nove zbirke osebnih podatkov zdravnikov, in sicer na podlagi javno objavljenih podatkov.

Glede osebnih podatkov, za katere je zavezanec navedel, da jih je pridobil prek svojega telefonskega studia oz. od svojih naročnikov, je Informacijski pooblaščenec zaključil, da bi zavezanec lahko izkazal kvečjemu obstoj privolitve posameznikov za neposredno trženje svojih podobnih izdelkov ali storitev (drugi odstavek 158. člena ZEKom-1), česar pa ni storil. Prav tako mu takšen način pridobitve e-naslovov ni dal pravne podlage za to, da jih je vključil v novo zbirko, ki jo je za namene neposrednega trženja proti plačilu ponujal drugim pravnim in fizičnim osebam. Če bi želel zavezanec zbirko svojih naročnikov za potrebe neposrednega trženja posredovati drugim uporabnikom osebnih podatkov, bi moral za takšno posredovanje pridobiti pisno privolitev vsakega posameznika, katerega osebni podatki so bili v zbirki, in sicer na način, določen v četrtem odstavku 72. člena ZVOP-1.

Ker je Informacijski pooblaščenec ugotovil, da je zavezanec zbirko e-naslovov tržil tudi leta 2014 (ali pa je celo ustvaril novo zbirko osebnih podatkov), čeprav je vedel, da tega ne bi smel, mu je izrekel globo v znesku 300.000 evrov. Informacijski pooblaščenec je namreč zavezancu že leta 2012 z upravo odločbo, v kateri mu je podrobno in obširno pojasnil nezakonnost njegovega ravnanja, odredil, da mora iz zbirke 36.093 e-naslovov, ki jo je proti plačilu ponujal na spletu in prek določenega e-naslava, izbrisati vse e-naslave, ki vsebujejo ime in/ali priimek fizične osebe. Zavezanec je takrat izjavil, da je bazo nehal prodajati in da je e-naslave izbrisal. Gre za najvišjo možno globo, ki jo lahko prekrškovni organ v skladu z ZP-1 izreče samostojnemu podjetniku posamezniku. Kljub temu da je celotna zbirka vsebovala 36.093 e-naslovov, je Informacijski pooblaščenec sledeč načelu ekonomičnosti svojo odločbo oprl le na prvih 95 osebnih podatkov, ki jih je zbirka osebnih podatkov vsebovala, saj je že s tem številom osebnih podatkov presegel največjo dovoljeno mero enotne sankcije, ki se lahko izreče samostojnemu podjetniku posamezniku. Pri določitvi steka je Informacijski pooblaščenec upošteval sodbo Vrhovnega sodišča RS št. IV Ips 51/2011, z dne 21. 6. 2011, v kateri je sodišče navedlo, da je »pri tovrstnih prekrških toliko prekrškov, kolikor je oškodovancev« in še, da »vsak poseg v posameznikovo pravico do informacijske zasebnosti predstavlja samostojen prekršek.«

### 3.9.2. Nezakoniti vpogledi oz. preusmeritev e-pošte zaposlenih

Informacijski pooblaščenec je prejel prijavo zoper določenega delodajalca, ker je vsebino e-pošte predala, ki je pripadal nekanjemu zaposlenemu, preusmeril na drug e-naslov.

Glede na opredelitev osebnega podatka v ZVOP-1, je Informacijski pooblaščenec ugotovil, da so ime, priimek, naslov e-pošte ter (nekdanja) zaposlitev, ki se da razbrati iz naslova e-pošte, nedvomno osebni podatki. Informacijski pooblaščenec je poudaril, da pri preusmeritvi e-pošte ne gre le za osebne podatke in poseg v zasebnost posameznika, ki je nosilec poštnega naslova, temveč tudi za vse posameznike, ki jim je ta posameznik pošto poslal oz. pošto od njih prejel. Posameznik, ki posreduje e-sporočilo na službeni e-naslov posameznika, namreč utemeljeno pričakuje, da se bo z njegovim sporočilom in osebnimi podatki seznanila oseba, ki ji je bil dodeljen takšen e-naslov ter ji je sporočilo namenjeno, in ne neka druga oseba, na katere e-naslov je njegovo sporočilo preusmerjeno.

Obdelava osebnih podatkov je v skladu s 3. točko 6. člena ZVOP-1 kakršno koli delovanje ali niz delovanj, ki se izvaja v zvezi z osebnimi podatki, ki so avtomatizirano obdelani ali ki so pri ročni obdelavi del zbirke osebnih podatkov ali so namenjeni vključitvi v zbirko osebnih podatkov. To pomeni, da je tudi preusmeritev e-pošte mogoče šteti kot obdelavo osebnih podatkov.

Informacijski pooblaščenec je pri odločitvi upošteval pravne podlage v prvem odstavku 8. člena in v 10. členu ZVOP-1 ter 48. člen Zakona o delovnih razmerjih, ki določa, da se osebni podatki delavcev lahko zbirajo, obdelujejo, uporabljajo in posredujejo tretjim osebam samo, če je to določeno s tem ali drugim zakonom ali če je to potrebno zaradi uresničevanja pravic in obveznosti iz delovnega razmerja ali v zvezi z delovnim razmerjem, ter da se morajo osebni podatki delavcev, za zbiranje katerih ne obstoji več zakonska podlaga, takoj zbrisati in nehati uporabljati.

Informacijski pooblaščenec je na podlagi navedenih določb zaključil, da delodajalec ni imel zakonske podlage za preusmeritev e-pošte nekdanjega zaposlenega, takšna preusmeritev pa tudi ni bila nujno potrebna za zagotavljanje nadaljnjega nemotenega dela, saj bi ga lahko zagotovil na način, da bi blokiral e-naslov posameznika ter vklopil samodejni odzivnik, da posameznik ni več dosegljiv in da naj pošiljatelj pošto pošljejo na splošen e-naslov (ali drugi osebi) – takšno ravnanje je tudi najpogostejše v praksi in z vidika ZVOP-1 nesporno. Ker torej obstaja vsaj še en način rešitve konkretne situacije ob odhodu zaposlenega, je moč zaključiti, da je preusmeritev e-pošte na drug naslov z vidika tretjega odstavka 10. člena ZVOP-1 nedvomno nepotrebna in nenujna ter da posega v ustavno pravico do varstva osebnih podatkov posameznika. Kot pravno podlago za obdelavo osebnih podatkov ni mogoče šteti niti osebne privolitve, ki naj bi jo po mnenju delodajalca podal posameznik s podpisom pogodbe o zaposlitvi, saj bi bila glede na določbe ZVOP-1 in ZDR-1 privolitev v pogodbi o zaposlitvi nezakonita. Edina možna privolitev bi bila prostovoljna (torej ne izsiljena, kar je v praksi s strani delodajalca težko dokazati) privolitev posameznika ob zaključku delovnega razmerja.

Zaradi večjega števila prijav, ki so se nanašale na nezakonito obdelavo osebnih podatkov ob ravnanju z e-poštnimi predali zaposlenih, je Informacijski pooblaščenec v sporočilu za javnost delodajalce opozoril, da pri preusmerjanju in prebiranju e-pošte veljajo stroge zakonske določbe in da bo zaradi nezakonite preusmeritve e-pošte (nekdanjega) zaposlenega na drug naslov v podjetju v prihodnje izrekal globe.

Pregledovanje oz. prebiranje (službene) e-pošte ne pomeni le hude kršitve ZVOP-1, temveč je tudi temelj za kazensko in odškodninsko odgovornost (kršitev tajnosti občil). Upoštevati je namreč treba, da lahko zaposleni v službeni e-poštni predal prejemajo sporočila svojih prijateljev, odvetnikov, zdravnikov in druga sporočila zasebne in občutljive narave, za katera bi bilo nedopustno, da se z njimi seznanijo tretje osebe. Zato je Informacijski pooblaščenec delodajalcem in delavcem svetoval, da vprašanje prebiranja in »čiščenja« službene e-pošte po zaključku delovnega razmerja opravijo sporazumno. V nasprotnem primeru namreč

obe strani tvegata – na eni strani gre za poseg v delavčevo zasebnost, na drugi strani pa za njegovo odgovornost, če delodajalcu ne preda vseh službenih podatkov. Delodajalec lahko v izjemnih primerih (npr. smrt delavca) vpogleda v e-pošto, vendar mora pri tem upoštevati načelo sorazmernosti in odpreti samo tisto e-pošto, iz katere je že ne prvi pogled (npr. iz »Zadeve«) možno razbrati, da gre za službeno e-pošto. Zaradi morebitnega poznejšega dokazovanja Informacijski pooblaščenec priporoča, da vpogled opravi posebna (za to imenovana) komisija, v kateri naj bo tudi predstavnik zaposlenih ali sindikata, če ta pri delodajalcu deluje. Po zaključku delovnega razmerja mora delodajalec e-naslov delavca nemudoma blokirati in ga narediti nedostopnega, lahko pa (kar je tudi priporočljiva in pogosta rešitev v praksi) v nastavitvah e-predala uredi samodejni odzivnik, ki pošiljatelja e-pošte obvesti, da delavec ni več dosegljiv (delovanje odzivnika naj bo omejeno na določen čas, npr. 3–6 mesecev) ali da e-naslov ne obstaja več in da naj pošiljatelj pošlje e-pošto na drug naslov (po navadi je to splošni e-naslov delodajalca). V nobenem primeru pa delodajalec ne sme več obdelovati osebnih podatkov nekdanjega delavca (npr. preusmeriti e-pošto).

### 3.9.3. Posredovanje osebnih podatkov dolžnikov slovenskemu odvetniku, ki je zastopal hrvaško družbo zaradi neplačila parkirnine

V okviru postopka inšpekcijskega nadzora zoper odvetniško družbo je Informacijski pooblaščenec ugotavljal zakonitost obdelave osebnih podatkov lastnikov motornih vozil, katerim je odvetniška družba v imenu hrvaških podjetij zaradi izterjave neplačane parkirnine poslala pisanje Poziv za plačilo pred sodno izterjavo.

Informacijski pooblaščenec je ugotovil, da je odvetniška družba na podlagi pooblastil dveh hrvaških družb, sklicujoč se na 10. člen Zakona o odvetništvu, iz evidence registriranih vozil od različnih upravnih enot pridobila osebne podatke o lastnikih vozil. Na podlagi tako pridobljenih osebnih podatkov je poslala dopise, v katerih je od posameznih lastnikov motornih vozil zahtevala plačilo parkirnine ter stroškov opomina. Odvetniška družba je bila pooblaščenec za izterjavo civilnopravnih obveznosti, saj je šlo za dolžniško-upniško razmerje oz. terjatev, ki jo je hrvaška družba uveljavljala zoper posamezne lastnike motornih vozil, ki niso poravnali parkirnine ob parkiranju na javnih plačljivih parkiriščih, s katerimi upravlja. Ob tem je Informacijski pooblaščenec poudaril, da vprašanje utemeljenosti zahtevka oz. obstoja terjatve, katere plačilo zahteva odvetniška družba v imenu hrvaških družb, ni predmet inšpekcijskega postopka, saj odločanje ali podajanje vrednostnih sodb o protipravnosti oz. (ne)utemeljenosti upnikovega zahtevka ni v njegovi pristojnosti. O tem in o potencialnih vračilih neupravičeno pridobljene koristi zaradi protipravnega pobiranja parkirnine lahko odloči le pristojno sodišče. Z vidika posredovanja osebnih podatkov je pravno relevantno predvsem dejstvo, da lahko upnik izpolnitev celotne obveznosti načeloma zahteva le od lastnika vozila in da za izterjavo potrebuje podatke, ki mu omogočijo vložitev popolne zahteve.

Odvetniška družba je podatke o lastnikih vozil zahtevala pri različnih upravnih enotah na podlagi registrskih števil motornih vozil. V vsaki zahtevi je navedla registrsko številko vozila, v zvezi s katerim naj bi nastala terjatev, opredelila je nabor osebnih podatkov, ki jih potrebuje, ter točen datum nastanka izterjevane obveznosti (datum parkiranja). Informacijski pooblaščenec je ugotovil, da se registrske številke, navedene v zahtevi in pooblastilu, ki ju je odvetniška družba predložila upravni enoti, v vseh primerih ujemajo s podatki s fotografij, ki jih je predložila v postopku.

Glede na navedeno je Informacijski pooblaščenec zaključil, da je v obravnavanih primerih za pridobivanje in nadaljnjo obdelavo osebnih podatkov domnevnih dolžnikov hrvaških družb obstajala ustrezna pravna podlaga ter da posredovanje podatkov s strani upravnih enot kot tudi pridobivanje le-teh s strani odvetniške družbe ni predstavljalo kršitve ZVOP-1. Osebnih podatki se skladno s prvim odstavkom 8. člena ZVOP-1 lahko obdelujejo le, če obdelavo osebnih podatkov in osebne podatke, ki se obdelujejo, določa zakon ali če je za obdelavo določenih podatkov podana osebna privolitev. V javnem sektorju, kamor sodijo upravne enote, se lahko osebni podatki obdelujejo (tj. posredujejo), če obdelavo osebnih

podatkov in osebne podatke, ki se obdelujejo, določa zakon, z zakonom pa se lahko določi, da se določeni osebni podatki obdelujejo le na podlagi osebne privolitve posameznika (prvi odstavek 9. člena ZVOP-1). Enako pa lahko podlago za obdelavo osebnih podatkov (tj. pridobivanje) v zasebnem sektorju, v katerega sodijo odvetniki, skladno s prvim odstavkom 10. člena ZVOP-1, predstavlja zakon. Zakon, na podlagi katerega morajo državni oz. upravni organi posredovati osebne podatke posameznikov odvetnikom, je ZOdv. Ta v 10. členu določa, da so državni organi, organi samoupravnih lokalnih skupnosti ter nosilci javnih pooblastil dolžni brez privolitve posameznika, na katerega se osebni podatki nanašajo, brezplačno dati odvetniku podatke, ki jih potrebuje pri opravljanju odvetniškega poklica v posamični zadevi, in sicer v roku 15 dni od dneva, ko prejmejo pisno zahtevo odvetnika, ne glede na določbe drugih zakonov, ki določajo posredovanje osebnih podatkov upravljavcem osebnih podatkov in uporabnikom osebnih podatkov. Odvetnik te pravice nima, če gre za osebne podatke, ki so na podlagi posebnih zakonskih določb dostopni le pooblaščenim organom. Za podatke o lastništvu vozila niti Zakon o motornih vozilih niti kak drug zakon ne določa omejitev v smislu drugega odstavka 10. člena ZOdv, zato se tudi za vprašanja posredovanja podatkov iz evidence registriranih vozil odvetniku smiselno uporablja prvi odstavek 10. člena ZOdv.

### 3.9.4. Zbiranje osebnih podatkov zaposlenih

Informacijski pooblaščenec je na podlagi prijave, v kateri je bilo navedeno, da je delodajalec (zavezanec) začel zbirati osebne podatke delavcev (ali je delavec samohranilec, ali je delavec druga (ali več) generacija v podjetju), uvedel inšpekcijski postopek zaradi suma nezakonite obdelave osebnih podatkov.

V postopku je Informacijski pooblaščenec ugotovil, da je zbiranje osebnih podatkov že končano, vendar zavezanec podatka o tem, koliko delavcev je posredovalo svoje podatke, ni imel, ker so bili vsi zbrani podatki še vedno v zaprtih kuvertah v pisarni vodje kadrovske službe. Zavezanec je osebne podatke delavcev zbral na zahtevo nadrejene družbe za namen statistične obdelave strukture kadrov v skupini, za zbiranje osebnih podatkov pa je pripravil poseben obrazec oz. izjavo. Izjavo je poslal organizatorjem dela, ki so jih razdelili delavcem, zbrali izpolnjene izjave in jih v zaprti kuverti poslali v kadrovsko službo. V skladu z navodili so morali organizatorji dela zbrane osebne podatke delavcev in datum seznanitve z izjavo vnesti tudi v pripravljene preglednice z osebnimi imeni delavcev. Zavezanec je navedel, da posredovanje podatkov ni bilo obvezno.

Čeprav ZVOP-1 razlikuje med pravnimi podlagami v javnem in zasebnem sektorju, je obdelava osebnih podatkov na delovnopravnem področju omejena in urejena z Zakonom o evidencah na področju dela in socialne varnosti ter Zakonom o delovnih razmerjih. ZEPDSV v 12. členu določa vrste in vsebino evidenc s področja dela in socialne varnosti, ki jih morajo voditi delodajalci, ZDR-1 pa v 48. členu določa, da se osebni podatki delavcev lahko zbirajo, obdelujejo, uporabljajo in posredujejo tretjim osebam samo, če je to določeno s tem ali drugim zakonom ali če je to potrebno zaradi uresničevanja pravic in obveznosti iz delovnega razmerja ali v zvezi z delovnim razmerjem. Osebne podatke delavcev lahko zbira, obdeluje, uporablja in posreduje tretjim osebam samo delodajalec ali delavec, ki ga delodajalec za to posebej pooblasti. Osebni podatki delavcev, za zbiranje katerih ne obstoji več zakonska podlaga, se morajo takoj izbrisati in nehati uporabljati. Delodajalec torej lahko obdeluje tiste delavčeve osebne podatke, ki jih določa ZEPDSV in za katere izkaže, da jih potrebuje zaradi uresničevanja pravic in obveznosti iz delovnega razmerja ali v zvezi z delovnim razmerjem. Pri tem so mišljene pravice in obveznosti obeh, torej delavca in delodajalca.

Zbiranje osebnih podatkov delavcev na podlagi osebne privolitve je dovoljeno v primerih, ko gre za osebne podatke, ki niso potrebni za uresničevanje pravic in obveznosti iz delovnega razmerja. Takšen je bil tudi obravnavani primer.

Osebná privolitěv je po 14. točki 6. členu ZVOP-1 prostovoljná izjava volje posameznika, da se lahko njegovi osebni podatki obdelujejo za določen namen, in je dana na podlagi informacij, ki mu jih mora zagotoviti upravljavec. Osebná privolitěv posameznika je lahko pisná, ustná ali druga ustrezná privolitěv. Kot pravná podlaga za obdelavo osebnih podatkov se osebná privolitěv šteje, če je jasná in nedvoumná izjava volje, če je dana prostovoljnó in za konkretnó obdelavo osebnih podatkov (ne na splošno) ter če je informirána. Pravila glede obveščanja posameznika o obdelavi osebnih podatkov določá 19. člen ZVOP-1, ki predstavlja odraz temeljnega načela pri obdelavi osebnih podatkov, to je načela zakonitosti in poštenosti. Dolžnost obveščanja ni vezána na zahtevo posameznika, upravljavec jo mora izpolniti avtomatično. Informacije morajo biti jasné in razumljivé, saj se bo posameznik lahko le na podlagi takšnih informacij odločil, ali bo za obdelavo osebnih podatkov podal svojo privolitěv oz. ali bo svoje osebne podatke posredoval upravljavcu osebnih podatkov. Posamezniku mora upravljavec dati vse potrebne informacije pred začetkom zbiranja osebnih podatkov, to je informacije iz prvega in drugega odstavka 19. členu (npr. kdo bo upravljavec osebnih podatkov in kakšen je namen njihove obdelave). Nameni morajo biti nedvoumni in čim natančneje definirani, saj neopredeljen namen obdelave osebnih podatkov pomeni, da se zbrani podatki lahko uporabljajo za različné, posameznikom, ki so svoje podatke dali, neznane namene, kar je v nasprotju z ZVOP-1. To pomeni, da odprta privolitěv brez natančne navedbe namena obdelave ni sprejemljiva. Poleg tega je privolitěv lahko veljavná le, če ima posameznik, na katerega se osebni podatki nanašajo, resnično izbiro ter ne obstaja nevarnost zavajanja, ustrahovanja, prisiljevanja ali znatnih negativnih posledic, če posameznik privolitěv ne da. Če posledice privolitěv ogrožajo svobodno izbiro posameznikov, privolitěv ni prostovoljná. To lahko velja tudi v primeru delovnega razmerja, ko je delavec odvisen od delodajalca zaradi narave razmerja in ga je strah, da bo obravnaván drugače, če v obdelavo podatkov ne bo privolil.

Privolitěv je torej lahko veljavná le, če je svobodná, prostovoljná in dana na podlagi informacij iz prvega in drugega odstavka 19. členu ZVOP-1. V konkretnem primeru je Informacijski pooblaščenec ugotovil, da zavezanec delavcem pred zbiranjem osebnih podatkov ni posredoval dovolj informacij. V izjavi ni natančno navedel, kdo bo upravljavec zbirke osebnih podatkov, namen obdelave osebnih podatkov je bil presplošen, delavec ni bil seznanjen s tem, ali je zbiranje osebnih podatkov obvezno ali prostovoljnó ter z možnimi posledicami, če ne bo prostovoljnó podal podatkov, prav tako ni bil seznanjen z informacijo o pravici do vpogleda, prepisa, kopiranja, dopolnitve, popravka, blokiranja in izbrisa osebnih podatkov, ki se nanašajo nanj. Informacijski pooblaščenec je ob upoštevanju zgoraj navedenega zaključil, da so bili osebni podatki delavcev zbrani na podlagi nepopolnih informacij iz prvega in drugega odstavka 19. členu ZVOP-1, zaradi česar osebnih privolitěv delavcev ni bilo mogoče šteti za veljavné. Zato je zavezancu z odločbo odredil, da mora uničiti izjave, ki so jih podali delavci, ter preglednice, v katere so organizatorji dela vnesli osebne podatke delavcev iz omenjenih izjav. Zavezanec je odrejena ukrepa izvršil.

### 3.9.5. Izvajanje videonadzora v domu upokoencev

V postopku inšpekcijskega nadzora je bilo ugotovljeno, da zavezanec izvaja videonadzor nad prostori in okolico doma starejših občanov ter da so praktično vsi delovni prostori, prostori za stanovalce (razen njihovih sob), okolica doma ter prostori, v katerih zavezanec opravlja tržno dejavnost (fitnes, lokal, telovadnica), videonadzorovani.

Zavezanec naj bi videonadzor izvajal z namenom, da se zaščiti pred tem, da bi se v prostorih znotraj zavoda in v njegovi neposredni okolici dogajale kraje in fizični napadi na stanovalce ali zaposlene. Zato je kamere namestil na vse dostope in vhode v varovane oddelke in terapevtski park, ki je »zunanji del varovanega oddelka«, pa tudi v centru za zdravje (na vstopu v bazen, ob bazenu, v telovadnici in fitnesu) z namenom zagotavljanja varnosti uporabnikov storitev, ki so večinoma zunanje stranke in ne stanovalci doma. Izvajanje videonadzora naj bi doprineslo tudi k lepšemu vedenju zaposlenih do strank, poleg tega naj bi bil namen videonadzora spremljanje tehničnih procesov v kuhinjah. Videonadzor nad prostori doma za starejše naj bi bil zavezanec dolžan izvajati na podlagi določb 6. členu

Pravilnika o kadrovskih, tehničnih in prostorskih pogojih za izvajanje nalog na področju duševnega zdravja za izvajalce institucionalnega varstva ter centre za socialno delo ter o postopku njihove verifikacije .

ZVOP-1 določa izvajanje videonadzora v 74.–77. členu (splošne določbe, videonadzor dostopa v uradne službene in poslovne prostore, videonadzor v večstanovanjskih stavbah in videonadzor znotaj delovnih prostorov). V 75. členu ZVOP-1 določa, da lahko javni in zasebni sektor izvajata videonadzor dostopa v uradne službene oz. poslovne prostore, če je to potrebno za varnost ljudi ali premoženja, zaradi zagotavljanja nadzora vstopa v ali službene oz. poslovne prostore ali izstopa iz njih ali če zaradi narave dela obstaja možnost ogrožanja zaposlenih. Videonadzor znotraj delovnih prostorov se lahko v skladu s 77. členom ZVOP-1 izvaja le v izjemnih primerih, kadar je to nujno potrebno za varnost ljudi ali premoženja ali za varovanje tajnih podatkov ter poslovnih skrivnosti, tega namena pa ni mogoče doseči z milejšimi sredstvi.

Informacijski pooblaščenec je na podlagi ugotovitev v inšpekcijskem postopku zavezancu z odločbo odredil, da mora na dveh lokacijah prenehati izvajati videonadzor in odstraniti 54 (od 63) kamer, s katerimi je snemal hodnike, stopnišča, pralnico, vhod v bazen in bazen, telovadnico, fitnes, kavarno, čakalnico pred ambulanto, dnevni prostor za druženje, vhod v kuhinjo in kuhinjo, smeti zunaj, prostor za delovno terapijo, park pred stavbo, cesto, ki vodi do prostorov doma, dostavo in prevzem v kleti, teraso, jedilnico, ker za izvajanje videonadzora ni imel pravne podlage oz. je bil videonadzor v nasprotju z določbami 8., 9., 75. in 77. člena ZVOP-1. Poleg tega je videonadzor, kot ga je vzpostavil zavezanec, predstavljal pretiran poseg v zasebnost ne le stanovalcev, temveč tudi zaposlenih, zavezanec pa bi lahko namene uvedbe videonadzora dosegel z milejšimi sredstvi.

V konkretnem primeru ob upoštevanju določb 77. člena ZVOP-1 ni bilo mogoče govoriti o dopustnem izvajanju videonadzora znotraj delovnih prostorov, saj ta ni bil nujno potreben zaradi varovanja ljudi, premoženja, tajnih podatkov ali poslovne skrivnosti. Upravičenost uvedbe videonadzora se namreč vedno presoja od primera do primera, kar pomeni, da mora biti osnovno vodilo pri uvedbi videonadzora načelo, da se ta uvede, kadar ni na razpolago drugega milejšega ukrepa za zagotovitev ciljev. V konkretnem primeru je bila pomembna narava dela zavezanca, ki je takšna, da mora zagotoviti 24-urno prisotnost zaposlenih, ki skrbijo za varnost stanovalcev in hkrati za premoženje, zato videonadzor za ta dva namena ni bil potreben. Videonadzor namreč ne more preprečiti kraj ali tega, da bi se kateri od oskrbovancev izgubil, zašel v del doma, ki ga ne pozna, se poškodoval ipd. Videonadzor varovancev dejansko ne varuje, saj omogoča le naknaden pregled posnetkov in s tem eventualno olajša ugotavljanje poteka preteklega (neželenega) dogodka. Poleg tega je zavezanec namen varovanja premoženja dosegal že z izvajanjem videonadzora vstopov v prostore doma za starejše in izstopov iz njega (kamere snemajo glavni vhod in recepcijo ter druge vhode v stavbo), ki je v skladu s 75. členom ZVOP-1.

V zvezi z uporabo videonadzora za nadzor nad zaposlenimi (ugotavljanje, ali se zaposleni lepo vedejo do strank, saj bi nasprotno predstavljalo kršitev delovnih obveznosti in povod za uvedbo disciplinskega postopka) je Informacijski pooblaščenec zaključil, da gre za nezakonit namen, saj niti ZVOP-1 niti kateri koli drug zakon takšnega videonadzora ne dopušča. Za nadzor nad delom zaposlenih so namreč zadolženi njihovi nadrejeni.

Glede na določbe Pravilnika bi zavezanec v posebej varovanih oddelkih lahko izvajal videonadzor, s katerim bi dodatno poskrbel za varnost stanovalcev, ki imajo zaradi težav v duševnem zdravju omejeno oz. nadzorovano gibanje po prostorih in morajo biti zaradi tega nepretrgoma deležni posebne zaščite in varstva, izhodi iz teh prostorov pa morajo biti nenehno nadzirani. V skladu s Pravilnikom mora biti varovanje na teh oddelkih zagotovljeno s stalno prisotnostjo ustrezno usposobljene osebe za delo z osebami z demenco, v nočnem času pa je lahko nadzor skupnih prostorov urejen tudi s tehničnimi sredstvi, npr. z videonadzorom. Zavezanec v inšpekcijskem postopku ni izkazal, da ima posebej varovan oddenek, ampak je trdil, da zanj varovani oddenek predstavlja celotno območje doma. To pa ni v skladu s Pravilnikom, ki jasno določa, kaj so varovani oddelki v socialnovarstvenih

inštitucijah in kakšen je postopek pridobitve verifikacije za takšne oddelke. Zato je Informacijski pooblaščenec zaključil, da Pravilnik ne more predstavljati pravne podlage za izvajanje videonadzora v prostorih in okolici doma za starejše.

Zavezanec je zoper odločbo Informacijskega pooblaščenca sprožil upravni spor oz. vložil tožbo na Upravno sodišče RS, ki pa jo je zavrnilo kot neutemeljeno.

### 3.9.6. Izvajanje videonadzora na vhodu v krajinski park

Informacijski pooblaščenec je z odločbo prepovedal izvajanje videonadzora tudi zavezancu, ki je izvajal videonadzor na vhodu v krajinski park.

V inšpekcijskem postopku je bilo ugotovljeno, da zavezanec nad vstopi v krajinski park izvaja videonadzor s tremi kamerami, ki jih je namestil na drog luči, ki osvetljuje javno cesto, ki vodi v park. Z vpogledom v videonadzorni sistem je bilo ugotovljeno, da ena kamera pokriva dostop do vhoda, ki je varovan z zapornico, druga kamera je usmerjena na vratarnico oz. prostor za pobiralce vstopnine, tretja pa na področje pred zapornico, kjer vozniki ustavijo, da plačajo vstopnino. Zavezanec je uvedel videonadzor z namenom občasne kontrole prometa, občasne kontrole pobiranja vstopnine, pridobitve evidence prometa v sezoni, ko se ne pobira vstopnina, ter snemanja dnevne slike stanja vremena za potrebe Arso in turizma. Zavezanec je na vhodu v krajinski park na stavbo vratarnice oz. recepcije namestil obvestilo o izvajanju videonadzora z vsemi informacijami, ki jih določa ZVOP-1 v 74. členu.

ZVOP-1 daje neposredno pravno podlago le za izvajanje videonadzora dostopa v uradne službene oz. poslovne prostore (75. člen), videonadzora večstanovanjskih stavb (76. člen) ter videonadzora delovnih prostorov (77. člen), kar pomeni, da navedene določbe v obravnavanem primeru ne morejo predstavljati pravne podlage za uvedbo in izvajanje videonadzora. Ta je na drugih mestih dopusten le pod pogoji, če je tako določeno v drugem zakonu ali če so za izvajanje videonadzora izpolnjeni pogoji iz tretjega odstavka 10. člena ali četrtega odstavka 9. člena ZVOP-1. Ker gre v obravnavanem primeru za izvajalca videonadzora iz zasebnega sektorja, je treba upoštevati tretji odstavek 10. člena, ki določa, da se v zasebnem sektorju lahko obdelujejo tisti osebni podatki, ki so nujni za izvrševanje zakonitih pristojnosti, nalog ali obveznosti zasebnega sektorja, če se s to obdelavo ne poseže v upravičen interes posameznika, na katerega se osebni podatki nanašajo.

Informacijski pooblaščenec je zato tehtal interese zasebnega sektorja na eni strani in interese posameznika, na katerega se nanašajo osebni podatki, na drugi. Kot vodilo je uporabil test, ki ga je v Mnenju št. 06/2014 predstavila Delovna skupina za varstvo podatkov iz člena 29 (Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC) kot odziv na potrebo po harmonizirani interpretaciji določbe 7.(f) člena direktive 95/46/ES. Ta določa, da se lahko osebni podatki obdelujejo tudi, če je obdelava potrebna zaradi zakonitih interesov, za katere si prizadeva upravljavec ali tretja stranka ali stranke, ki so jim osebni podatki posredovani, razen kadar nad takimi interesi prevladajo temeljne pravice in svoboščine posameznika, na katerega se osebni podatki nanašajo, ki se varujejo na podlagi Direktive 95/46/ES, ta pa je bila prenesena v slovenski pravni red v tretjem odstavku 10. člena ZVOP-1.

Informacijski pooblaščenec je ocenil, da z videonadzorom na vhodu v krajinski park zavezanec ne izvršuje nobenih zakonitih interesov (nadzor nad pobiranjem vstopnine v krajinski park bi lahko zagotovil s postavitvijo avtomata za plačilo vstopnine pri zapornici), ki bi prevladali nad interesi posameznikov, ki obiskujejo krajinski park, in da bi lahko vse namene dosegel z milejšimi ukrepi, s katerimi ne pride do obdelave osebnih podatkov in do posegov v zasebnost obiskovalcev krajinskega parka. Varovanje premoženja, ki bi ga želeli varovati lastniki zemljišč v krajinskem parku, je mogoče zavarovati z videonadzorom nad konkretnim premoženjem (vsak lastnik nad svojim premoženjem) in ne z videonadzorom nad vstopno cesto in zapornico pred vhodom v dolino, saj je takšen videonadzor glede na namen nesorazmeren. Vse ostale namene, ki jih je navedel zavezanec, pa lahko doseže s t. i. pan-

oramskimi kamerami, ki bi prikazovale npr. vreme, razmere v gorah. V zvezi z zavezančovo navedbo, da mu kamere služijo tudi za nadzor zaposlenih pobiralcev vstopnine ob vstopu v krajinski park, pa je Informacijski pooblaščenec poudaril, da gre nedvomno za izvajanje videonadzora, kakršnega ZVOP-1 ali kateri koli drug zakon ne dopušča. Za nadzor nad delom zaposlenih so namreč zadolženi njihovi nadrejeni.

### 3.9.7. Razkrivanje osebnih podatkov učencev ob prijavi na šolski obrok

Informacijski pooblaščenec je v okviru svojih pristojnosti (zadevo je preveril tudi Inšpektorat RS za izobraževanje, znanost in šport) preveril navedbe v številnih medijskih objavah, prejel pa je tudi prijave, da določena osnovna šola nezakonito razkriva osebne podatke učencev, saj se je pri učencih, ki so v jedilnico prišli na obrok, v primeru neplačane položnice za šolsko prehrano pojavilo zvočno opozorilo.

V inšpekcijskem postopku je bil opravljen pregled sistema Abonent za registriranje in vodenje evidence šolske prehrane. Zavezanec je sistem uvedel že v šolskem letu 2007/08, ker je bolj preprost in zanesljiv kot uporaba blokcev. Sistem je namenjen izključno evidentiranju kosil, drugi obroki so urejeni drugače. Računalnik s programom Abonent je bil nameščen na steni pred delilnim pultom, monitor je bil obrnjen v kuhinjo, tako da je imelo vpogled nanj le kuhinjsko osebje, ne pa tudi učenci. Na monitorju so se ob registraciji z individualnim ključkom upravičencev do prehrane prikazali podatki o imenu, priimku in razredu učenca ter zeleno oz. rdeče polje v obliki kvadrata z izpisom razloga zavrjenega dostopa. Razlog zavrnitve zaradi neplačila je bil označen kot »porabljeni obroki«. V primeru neuspešne registracije učenca iz tehničnega razloga je vodja kuhinje učenca opozoril na neuspešno registracijo, ki jo je otrok vnovič opravil, v primeru neuspešne registracije iz drugih razlogov (npr. registracija z nepoznanim obeskom, ob odpovedanem obroku, zunaj časa obroka, dvojna registracija) pa se je pojavil tudi opozorilni pisk na aparatu, nameščenem pod računalnikom in blizu kuhinjskega osebja. Pisk je bil komaj slišen in enak v vseh programsko predvidenih primerih. Zavezanec je pojasnil, da je učenec tudi v primeru neplačila oz. porabljenih obrokov dobil kosilo, vodja kuhinje pa ga je napotil v tajništvo (kjer se je programsko zabeležila registracija za posamezen obrok, pa tudi razlog neuspešne registracije) po pojasnilo in za eventualno obvestilo (opomin) staršem o plačilu dolga. Pri računalniku je bila tudi tipkovnica, ki je bila namenjena zgolj izklopu sproženega piska iz predprogramiranega razloga.

Informacijski pooblaščenec je ugotovil nepravilnosti pri obdelavi osebnih podatkov učencev, prijavljenih na šolsko prehrano, saj so bili ob razdeljevanju kosil s prikazom na monitorju in z opozorilnim piskom v računalniškem programu Abonent nepooblaščenim osebam razkriti podatki o imenu in priimku ter o številu plačanih obrokov oz. o porabljenem plačilu. To je v nasprotju z določbami 24. in 25. člena ZVOP-1 o zavarovanju osebnih podatkov ter 17. člena Zakona o šolski prehrani, ki med drugim določa osebne podatke v evidenci šolske prehrane in namene njihove obdelave ter pravila dostopa do podatkov v evidenci. Zavezanec je poudaril, da nikdar ni imel namena nikogar stigmatizirati ali diskriminirati, zato je takoj po opozorilu državnega nadzornika, že v času inšpekcijskega ogleda, sam prostovoljno odpravil nepravilnosti glede zavarovanja osebnih podatkov, tako da je izklopil računalniški zaslon in opozorilni pisk v računalniškem programu Abonent ob razdeljevanju kosil, naknadno pa je pogodbeni izvajalec tudi programsko onemogočil prikaz osebnih podatkov iz evidence šolske prehrane na monitorju v šolski kuhinji. Zavezanec je preklical tudi pooblastilo vodji šolske kuhinje za uporabo osebnih podatkov o naročnikih šolske prehrane ter pooblastilo omejil na obdelavo osebnih podatkov o naročnikih šolske prehrane, ki potrebujejo dietno prehrano, kar je skladno z načelom sorazmernosti iz 3. člena ZVOP-1.



### 3.10. Splošna ocena stanja varstva osebnih podatkov in priporočila

Informacijski pooblaščenec je leta 2014 na področju varstva osebnih podatkov vodil skupaj 628 inšpekcijskih postopkov, od tega 206 na področju javnega sektorja in 422 na področju zasebnega sektorja (leta 2013 jih je bilo skupaj 712, leta 2012 jih je bilo 725, leta 2011 jih je bilo 682, leta 2010 pa 599) ter 95 prekrškovnih postopkov (leta 2013 jih je bilo 106, 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 2014 prejel še 2.040 zaprosil za mnenja in pojasnila s področja varstva osebnih podatkov (leta 2013 je bilo takih zaprosil 2.460, leta 2012 jih je bilo 2.191, leta 2011 jih je bilo 2.143, leta 2010 pa 1.859), 14 vlog za izdajo dovoljenja za povezovanje zbirk osebnih podatkov (leta 2013 jih je bilo šest, leta 2012 jih je bilo devet, leta 2011 jih je bilo 14, leta 2010 pa devet), štiri vloge za izdajo dovoljenja za izvajanje biometričnih ukrepov (leta 2013 in 2012 je prejel 11 takih vlog, leta 2011 devet, leta 2010 pa šest), 11 vlog za izdajo dovoljenja za iznos osebnih podatkov (leta 2013 jih je bilo 14, leta 2012 pet, leta 2011 je prejel štiri, leta 2010 pa osem), 67 pritožb zaradi zavrnitve zahteve za seznanitev z lastnimi osebnimi podatki (leta 2013 jih je bilo 68, leta 2012 63, leta 2011 in 2010 pa po 85).

Iz navedenih podatkov je razvidno, da se je število prijav, ki jih zaradi suma kršitve predpisov vsako leto prejme Informacijski pooblaščenec, umirilo oz. se je leta 2014 glede na prejšnja leta celo nekoliko zmanjšalo. Zaradi tega je Informacijski pooblaščenec leta 2014 lahko več pozornosti posvetil t. i. planiranemu ex offo inšpekcijskemu nadzoru, ki ga vsako leto izvaja skladno s sprejetim letnim načrtom. Planirani inšpekcijski nadzor nad spoštovanjem določb ZVOP-1 se je leta 2014 izvajal na področju lokalne samouprave, socialnega in zdravstvenega varstva, dajanja potrošniških kreditov, obrambe ter policije. Pri izvajanju tega nadzora Informacijski pooblaščenec ni ugotovil večjih kršitev, ugotovljene nepravilnosti in pomanjkljivosti pa so se nanašale zlasti na površno predpisane postopke in ukrepe za zavarovanje osebnih podatkov in njihovo nedosledno izvajanje.

Podobno kot v preteklih letih je Informacijski pooblaščenec tudi leta 2014 prejel največ prijav suma nezakonitega posredovanja oz. objave osebnih podatkov (182), med katerimi je bilo veliko takih, ki so se nanašale na objavo različnih osebnih podatkov na družbenih omrežjih (predvsem Facebook). Informacijski pooblaščenec v večini primerov zaradi nepristojnosti ni ukrepal, ker je šlo za objavo osebnih podatkov (npr. fotografij), ki ne izhajajo iz zbirk osebnih podatkov. ZVOP-1 namreč varuje le tiste osebne podatke, ki so del zbirk osebnih podatkov. To pa ne pomeni, da prizadeti posameznik nima pravnega varstva, saj lahko, če meni, da je bilo z objavo njegovih osebnih podatkov poseženo v njegove osebnostne pravice, po Obligacijskem zakoniku ali Kazenskem zakoniku svoje pravice sam uveljavlja na sodišču.

Zelo veliko prijav je bilo v zvezi z izvajanjem neposrednega trženja (91). Pri obravnavi teh prijav so bile ugotovljene zlasti kršitve zaradi nezakonitega pridobivanja in uporabe osebnih podatkov, zaradi neobveščanja posameznikov o njihovih pravicah do prepovedi uporabe osebnih podatkov za namene neposrednega trženja in nespoštovanja te pravice, še vedno pa so pogoste tudi kršitve zaradi razkrivanja elektronskih naslovov vsem prejemnikom sporočila, ko pošiljatelj elektronske naslove prejemnikov zapiše v rubriko »Za« ali »Kp«, namesto da bi jih zapisal v rubriko »Skp« oz. skrita kopija.

Informacijski pooblaščenec je prejel tudi veliko prijav (73) v zvezi z izvajanjem videonadzora, zlasti zoper izvajalce v zasebnem sektorju. Pri obravnavi teh prijav je Informacijski pooblaščenec ugotovil predvsem kršitve v zvezi z izvajanjem videonadzora na mestih, kjer ta, glede na stroge določbe ZVOP-1, ni upravičen (npr. na tistih javnih površinah in znotraj tistih delovnih prostorov, kjer izvajanje videonadzora ni nujno potrebno zaradi varovanja ljudi, premoženja ali tajnih in drugih varovanih podatkov ter bi se ta namen lahko dosegel z milejšimi sredstvi), pogoste pa so bile tudi kršitve v zvezi z evidentiranjem pregledovanja in posredovanja posnetkov, z njihovim pomanjkljivim zavarovanjem ter neustreznim oz. pomanjkljivim obveščanjem o izvajanju videonadzora.

V številnih prijavih, ki so se nanašale na zbiranje osebnih podatkov, so posamezniki trdili, da so različni organi pridobili njihove osebne podatke, ki so jih obdelovali za namen vodenja postopkov (npr. prekrškovnih postopkov) nezakonito, in da so pridobili podatke, ki jih v postopku ne potrebujejo. Informacijski pooblaščenec v zvezi s tem pojasnjuje, da ni pristojen preverjati, ali pooblaščen uradna oseba določenega organa zakonito vodi in odloča v določenem postopku, saj bi s tem, kot izhaja iz sklepa Ustavnega sodišča RS št. U-I-92/12-13 z dne 10. 10. 2013, prekoračil svoja pooblastila. To pomeni, da mora posameznik, katerega osebne podatke naj bi določen organ obdeloval v nasprotju z zakonom, svoje pravice uveljavljati oz. varovati pred pristojnimi inštančnimi organi na način, določen s predpisi, ki urejajo posamezno področje, in ne prek Informacijskega pooblaščenca.

Informacijski pooblaščenec je tudi leta 2014 prejel nekaj prijav zaradi preusmeritve in posledično branja e-pošte zaposlenih, do česar prihaja zlasti po prekinitvi delovnega razmerja, ko delodajalci namesto ukinitve e-naslova nekdanjega zaposlenega, e-pošto, ki prihaja na njegov e-naslov, preusmerijo na drug e-naslov. Informacijski pooblaščenec je na takšno prakso delodajalcev opozoril že v poročilu za leto 2013, vendar je nekateri delodajalci kljub temu niso opustili. Informacijski pooblaščenec je zato pripravil in 5. 9. 2014 objavil posebno sporočilo za javnost. Informacijski pooblaščenec meni, da je omenjena praksa delodajalcev v precejšnji meri posledica nedorečene zakonodaje na tem področju, zaradi česar je že večkrat pozval k sprejetju zakona, ki bi celostno uredil področje zasebnosti na delovnem mestu, ter pristojnemu ministrstvu pred leti celo poslal predlog Zakona o zasebnosti na delovnem mestu, vendar to področje zaradi pomanjkanja politične volje še vedno ni ustrezno urejeno.

Informacijski pooblaščenec je, potem ko je leta 2013 prejel 35 prijav v zvezi s piškotki, ki so se nanašale na 141 zavezancev (upravljalcev spletnih strani), pri čemer se je ena prijava nanašala na 50 različnih spletnih strani in s tem na 50 različnih zavezancev, leta 2014 prejel le še 15 prijav, trend upadanja prijav na tem področju pa se še nadaljuje. Informacijski pooblaščenec je glede na veliko količino prejetih prijav in omejeno število državnih nadzornikov za varstvo osebnih podatkov prejete prijave v zvezi s piškotki obravnaval glede na prioritete in razpoložljive resurse. Do konca leta 2014 je uspešno zaključil 52 inšpekcijskih postopkov. Pri tem je treba poudariti, da je postopke vodil zelo ekonomično in učinkovito, saj so vsi zavezanci ugotovljene nepravilnosti odpravili še pred izdajo inšpekcijske odločbe. Glede na stanje po drugih državah EU, kjer je inšpekcijski nadzor na tem področju zelo okrnjen, lahko z gotovostjo trdimo, da je inšpekcijski nadzor učinkovit in da so rezultati jasno opazni. Številni zavezanci so izboljšali svoje prakse in o uporabi spletnih piškotkov podrobno obveščajo obiskovalce svojih spletnih strani, prav tako pa so uporabnikom na številnih spletnih mestih na voljo mehanizmi za podajo privolitve v uporabo t. i. sledilnih oz. invazivnih piškotkov. Informacijski pooblaščenec bo glede na prioritete in resurse z izvajanjem inšpekcijskih postopkov nadaljeval tudi leta 2015.

Informacijski pooblaščenec je leta 2014 izdal nekaj pomembnih smernic, ki dajejo napotke upravljavcem osebnih podatkov, in sicer:

- Smernice o varstvu osebnih podatkov pri uporabi GPS-naprav,
- Smernice za varstvo osebnih podatkov pri izvajanju internih tržnih raziskav,
- smernice Presoje vplivov na zasebnost pri uvajanju novih policijskih pooblastil.

Izdaja Smernic o varstvu osebnih podatkov pri uporabi GPS-naprav se je izkazala kot nujna – Informacijski pooblaščenec je namreč prejemal vse več vprašanj glede uporabe GPS-naprav. GPS sodi med najbolj uveljavljene tehnologije za pozicioniranje, sledenje in nadzor oseb, predmetov ter vozil in na Informacijskega pooblaščenca so se tako že obrnila številna podjetja in inštitucije, ki jih je zanimala uporaba GPS za sledenje tovornjakov, delovnih strojev, taksijev in drugih službenih vozil, sledenje opravljanja dela občinskih redarjev, poštarjev in raznašalcev časopisov, lociranje dementnih upokojenec v domovih za starejše. GPS-tehnologije so načrtovane tudi v raznih programih spremljanja in varovanja otrok, starejših in bolnih oseb, planincev in pohodnikov. Glede na to, da lociranje vozil in ljudi neizogibno pomeni obdelavo osebnih podatkov, smernice pojasnjujejo, na kaj je treba biti pozoren in kako uporabljati GPS-naprave skladno z zakonodajo, ki ureja varstvo osebnih podatkov.

Skladno s politiko čim večje uporabnosti smernic za ciljne publike smernice vsebujejo tudi enostranski hitri vodič, ki opisuje osnovne korake, ki jih je treba upoštevati, ko se odločamo za uporabo GPS-naprav.

Smernice za varstvo osebnih podatkov pri izvajanju internih tržnih raziskav je Informacijski pooblaščenec pripravil na pobudo izvajalcev tržnih raziskav, ki so se pri svojem delu soočali s številnimi dilemami. Z njimi nadaljuje s prakso sodelovanja z zainteresiranimi strokovnimi javnostmi in drugimi deležniki, saj lahko s skupnimi znanji in resursi pripravijo bolj kakovostne smernice. Po smernicah glede računalništva v oblaku so to naslednje smernice, kjer je Informacijski pooblaščenec pritegnil znanje in sodelovanje drugih deležnikov. Namen tržnih raziskav je pridobiti podatke, s katerimi lahko podjetje natančneje spozna svoje stranke, s tem pa tudi izboljša svoje procese, ponudbo in storitve za večjo uspešnost. Pri tem pa s strani podjetij oz. ponudnikov blaga in storitev na trgu, izvajalcev tržnih raziskav in drugih marketinških aktivnosti, odgovornih za upravljanje odnosov s strankami (CRM), poslovnih analitikov in zunanjih pogodbenih obdelovalcev praktično neizogibno pride do zajema in nadaljnje obdelave osebnih podatkov, zato je bistveno, da vsi navedeni dobro poznajo določbe ZVOP-1. Smernice podajajo usmeritve in odgovore na najpogosteje zastavljena vprašanja ponudnikov blaga in storitev na trgu, ki se nanašajo na zbiranje osebnih podatkov posameznikov pri izvajanju internih tržnih raziskav in nadgradnji podatkov, ki se zbirajo v okviru klubov in kartic ugodnosti.

Informacijski pooblaščenec je še posebej veliko energije vložil v pripravo smernic Presoje vplivov na zasebnost pri uvajanju novih policijskih pooblastil. Kot je izpostavil v predhodnih letnih poročilih, je namreč pri uvajanju novih policijskih pooblastil v preteklosti prihajalo do predlogov, ki niso bili deležni potrebne strokovne razprave. Posledično so se pojavile težave z rabo ukrepov v praksi (izločitvijo zbranih dokazov), neredko tudi v velikih, pomembnih in medijsko zelo odmevnih primerih, ter občasno izrazit odpor splošne in strokovne javnosti pri uvajanju novih pooblastil. Stanje na področju uvajanja novih pooblastil organov pregona je bilo z vidika posegov v pravico do zasebnosti skrb vzbujajoče. V zadnjih nekaj letih smo bili priča uvajanju novih pooblastil brez uporabe primerne metodologije, ki bi:

- omogočila izvedbo presoje vplivov na zasebnost,
- upravičila nujnost, primernost in učinkovitost ter sorazmernost uvajanja novih pooblastil,
- analizirala tveganja glede uvajanja novih pooblastil,
- celostno obravnavala identificirana tveganja,
- ponudila primerne kriterije za izvedbo naknadnih analiz učinkov.

Običajno je k uvajanju novih pooblastil vodila dostopnost določene nove tehnologije na trgu (npr. brezpilotni letalniki, IMSI-lovilci) oz. zmanjšanje učinkovitosti organov pregona zaradi uporabe novih tehnologij na strani osumljencev oz. preiskovancev (npr. večja uporaba šifriranih komunikacij s strani storilcev kaznivih dejanj, uporaba predplačniških SIM-kartic ipd.). Temu je običajno sledila takojšnja priprava pravnih podlag, ki naj bi z novimi pooblastili policiji nevtralizirale navidezno prednost potencialnih storilcev kaznivih dejanj pri rabi informacijskih tehnologij. Predhodne analize nujnosti, primernosti in učinkovitosti ter sorazmernosti takih pooblastil praviloma niso bile izvedene, naknadne analize pa ne predvidene. Obrazložitev so bile skope, pogosto oprte na neprepričljive argumente in včasih celo zavajajoče. Obrazložitev sorazmernosti posegov v pravico do zasebnosti in pravico do varstva osebnih podatkov, skupaj z ostalimi analizami, pa je izostala. Ker takšno tehtanje ni bilo opravljeno, so bili predlagatelji soočeni z vprašljivo sorazmernostjo ukrepov ter nemalokrat tudi z negativnim odzivom splošne in strokovne javnosti. Posledice neizvajanja ustreznih analiz so pogosto dolgoročne – javna razprava je onemogočena ali vsaj okrnjena, naknadno ukinjanje novih pooblastil je praktično nerealno, sfera zasebnosti se oži, ob odsotnosti predhodnih analiz primernosti in naknadnih analiz učinkovitosti predpisov pa stroške neučinkovitosti novih pooblastil nosi celotna družba. V izogib vsemu navedenemu se je Informacijski pooblaščenec odločil za pripravo omenjenih smernic. Smernice Informacijskega pooblaščenca za presojo vplivov na zasebnost pri uvajanju novih policijskih pooblastil zato predstavljajo metodološki okvir za preudarno, smiselno in legitimno uvajanje novih policijskih pooblastil, zlasti tistih s tehnološkim značajem. Po prejetih odzivih

ugotavljamo, da gre za koristno in pomembno orodje, ki ga redko zasledimo pri drugih nadzornih organih za varstvo zasebnosti in osebnih podatkov. Informacijski pooblaščenec z veseljem ugotavlja, da so se k uporabi smernic javno zavezali tudi visoki predstavniki službe generalnega direktorja policije.

Na področju sodobnih informacijsko-komunikacijskih tehnologij, se poleg trendov, ki smo jih obravnavali v predhodnih poročilih (računalništvo v oblaku, t. i. big data), nadaljujejo novi izzivi za varstvo osebnih podatkov. Soočeni smo z dejstvom, da se številna naša področja življenja v informacijski družbi digitalizirajo. Uvajajo se pametni števcji porabe električne energije. Digitalna televizija zaradi dvosmerne komunikacije omogoča zajem podrobnih podatkov o tem, katere televizijske kanale gledamo in kdaj. V t. i. internet stvari se vključuje čedalje več naprav, ki jih vsak dan uporabljamo. Zavarovalnice zanimajo črne skrinjice v vozilih, ki bi spremljale, kako (ne)varno vozimo, in omogočale prilagajanje avtomobilskih zavarovanj posameznim profilom voznikov. Z digitalizacijo družbe se seveda soočamo z dejstvom, da se o nas lahko hitreje zbere več podatkov in da se o nas lahko sprejemajo različne odločitve, pri čemer se dogaja, da o njih sploh nismo ustrezno obveščeni. Tako se npr. verjetno le redki zavedajo, da se vsak naš pritisk na TV-daljinec sporoči ponudniku TV-programa. Svojevrstni ščit zasebnosti, ki ga je nudila analognost (nedolgo nazaj so npr. operaterji morali posebej plačati določenemu panelu gospodinjestev, da so jim ta zaupala, katere TV-kanale gledajo), z digitalizacijo izginja. Nova orodja za varstvo zasebnosti, kot so presoje vplivov na zasebnost in koncept vgrajene zasebnosti, bodo ob posodobljenem evropskem zakonodajnem okviru in ustreznem inšpekcijskem nadzoru nujna, da v informacijski družbi ohranimo osnovni element informacijske zasebnosti, tj. pravico do odločanja, komu bomo zaupali katere podatke in za katere namene. Če pri temu kot družba ne bomo uspešni, se bomo soočili s tem, da bomo imeli kot posamezniki vse manj možnosti za odločanje o svoji usodi ter bomo vse bolj postajali predmet profiliranja in prilagajanja storitev glede na naš profil tako v zasebnem kot v javnem sektorju.

Med trende, ki bi jih želeli posebej izpostaviti, sodi uporaba brezpilotnih letalnikov (popularno imenovani tudi droni ali troji). Če smo leta 2013 le bežno omenjali porast uporabe brezpilotnih letalnikov, smo bili leta 2014 soočeni s hitro rastjo njihove uporabe. Brezpilotni letalniki omogočajo številne koristne možnosti uporabe za npr. hitro in varno ukrepanje pri naravnih nesrečah (požari, poplave, plazovi ipd.), izvajanje geodetskih storitev, nadzor nad infrastrukturnimi objekti (rafinerije, daljnovodi, plinovodi, jezovi in podobno), medijsko poročanje, umetniško ustvarjanje, naloge s področja policije, obrambe in obveščevalne dejavnosti ter številne druge uporabe. Vendar brezpilotni letalniki obenem omogočajo prikrita, težko zaznavna in obsežna zbiranja osebnih podatkov ter s tem občutne posege v zasebnost, saj se lahko opremijo z zelo različnimi senzorstvi, ki omogočajo zajem videa, slike, zvoka, podatkov o temperaturi, gibanju, lokaciji. Na brezpilotne letalnike se lahko namestijo tudi zelo invazivni sistemi, kot so sistemi biometrijske prepoznave obrazov, infrardeče, termo in UV-kamere, t. i. IMSI-lovilci (lažne bazne postaje za zajem mobilnih telefonskih števil), radarji, sistemi avtomatske prepoznave registrskih tablic in merjenja hitrosti vozil, prav tako pa omogočajo namestitvev sistemov za oborožitev in pasivizacijo (solzilec ipd.), kar pa prinaša pomembne posledice na cel spekter ustavno varovanih človekovih pravic.

Uporaba brezpilotnih letalnikov, ki so opremljeni z navedenimi sistemi, lahko posega v pravico do svobode gibanja (32. člen Ustave RS), splošno pravico do zasebnosti (35. člen Ustave RS), pravico do nedotakljivosti stanovanja (36. člen Ustave RS), pravico do komunikacijske zasebnosti (37. člen Ustave RS), pravico do informacijske zasebnosti (varstvo osebnih podatkov, 38. člen Ustave), pravico do svobode izražanja (39. člen Ustave RS), pravico do zbiranja in združevanja (42. člen Ustave RS) in druge temeljne človekove pravice. Trenutno še neregulirana uporaba takih letalnikov zato predstavlja grožnjo varnosti, enakopravnemu nastopanju na trgu, vpliva pa lahko tudi na pravice do varstva osebnih podatkov in zasebnosti. Informacijski pooblaščenec podobno kot drugi organi za varstvo osebnih podatkov v EU, ki smo zbrani v Delovni skupini iz člena 29 (Article 29 Working Party), ocenjuje, da je nujno treba pripraviti zakonske pogoje za dopustnost uporabe brezpilotnih letalnikov, kar je precej držav EU že storilo. Nadzorni organi za varstvo osebnih podatkov

so v drugih državah EU pri pripravi predpisov tesno sodelovali z nacionalnimi agencijami za civilno letalstvo ter resornimi ministrstvi; pri pripravi predpisov nam lahko tako pomagajo tudi njihove izkušnje. Informacijski pooblaščenec se je oktobra 2014 obrnil na Javno agencijo za civilno letalstvo in ji ponudil vso strokovno pomoč s področja varstva osebnih podatkov, ki mora biti v predpisih o uporabi brezpilotnih letalnikov ustrezno obravnavano, pobudo za strokovno sodelovanje pa smo naslovili tudi na Ministrstvo za infrastrukturo. Do konca leta 2014 žal nismo prejeli nobenega odziva. Informacijski pooblaščenec meni, da je pravočasna priprava omenjenih pravnih podlag nujna, po eni strani zaradi nenadzorovane uporabe brezpilotnih letalnikov, ki predstavlja posege v pravici do varstva osebnih podatkov in zasebnosti, prav tako pa nas tudi kot državljane skrbijo varnostni vidiki. Trenutno lahko namreč te naprave nad gosto naseljenimi območji uporablja kdor koli, morebitna nesreča pa bi lahko imela zelo daljnosežne posledice in bi zavrla številne koristne možnosti uporabe brezpilotnih letalnikov ob ustreznem upoštevanju temeljnih človekovih pravic.



# 4

## DRUGE DEJAVNOSTI INFORMACIJSKEGA POOBLAŠČENCA

#### 4.1. Sodelovanje pri pripravi zakonov in drugih predpisov

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

Informacijski pooblaščenec je leta 2014 znova zaznal skrb vzbujajoče veliko število predlogov sprememb zakonov oz. predlogov novih zakonov, ki prinašajo posege v zasebnost posameznikov z vidika obdelave osebnih podatkov, a se sprejemajo po hitrem postopku brez ustreznih analiz in ocen njihovih posledic za zagotavljanje ustavno zagotovljenega varstva zasebnosti in osebnih podatkov posameznikov.

Leta 2014 je Informacijski pooblaščenec podal mnenje, pripombe oz. sodeloval pri pripravi naslednjih predpisov:

- Sporazum med Vlado Republike Slovenije in Vlado Republike Srbije o sodelovanju pri delu skupnih preiskovalnih skupin, čezmejnem tajnem opazovanju oz. sledenju, pošiljanju in primerjavi profilov DNK in drugega identifikacijskega materiala ter uradnikih za zvezo,
- Uredba o podatkih o lastnostih nepremičnin v registru nepremičnin,
- Zakon o spremembah in dopolnitvah Zakona o vodah,
- Zakon o spremembah Zakona o kmetijskih zemljiščih,
- Predlog 379. člena Energetskega zakona,
- Predlog Pravilnika o spremembah in dopolnitvah Pravilnika o kartici zdravstvenega zavarovanja,
- Sporazum med Republiko Slovenijo in Republiko Korejo o socialni varnosti,
- Zakon o spremembi Zakona o elektronskem poslovanju na trgu,
- Uredba Evropskega parlamenta in Sveta o zahtevah za homologacijo za uvedbo avtomobilskega sistema eCall in spremembi Direktive 2007/46/ES,
- Zakon o spremembah in dopolnitvah Zakona o varstvu potrošnikov,
- Pravilnik o vsebini, obliki in načinu vročanja sklepov o izvršbi v elektronski obliki, drugih pravnih aktov, dokumentov in informacij,
- Zakon o spremembah in dopolnitvah Zakona o motornih vozilih,
- Predlog Zakona o spremembah in dopolnitvah Zakona o kazenskem postopku,
- Predlog Zakona o spremembah in dopolnitvah Zakona o subvencioniranju študentske prehrane,
- Zakon o spremembah in dopolnitvah Zakona o investicijskih skladih in družbah za upravljanje,
- Sprememba Zakona o ohranjanju narave,
- Predlog Zakona o spremembah in dopolnitvah Zakona o varstvu pred ionizirajočimi sevanji in jedrski varnosti,
- Predlog Zakona o napotitvi oseb v mednarodne civilne misije in mednarodne organizacije,
- Novela Zakona o dostopu do informacij javnega značaja – ZDIJZ-D,
- Predlog Zakona o spremembah in dopolnitvah Zakona o referendumski in ljudski iniciativi,
- Predlog Sporazuma o organizaciji skupnih letov za vračanje tujcev in predlog Protokola za izvajanje Sporazuma o organizaciji skupnih letov za vračanje tujcev,
- Pravilnik o vsebini in o obrazcih poročil o zbranih in porabljenih sredstvih za volilno in referendumsko kampanjo,
- Predlog Zakona o začasnem in občasnem delu dijakov in študentov,
- Predlog sprememb Zakona o inšpekcijskem nadzoru,
- Predlog Zakona o gospodarjenju z gozdovi v lasti Republike Slovenije,
- Predlog sprememb Zakona o igrah na srečo,
- Predlog Zakona o partnerski skupnosti,
- Zakon o spremembah in dopolnitvah Zakona o političnih strankah,
- Predlog Zakona o cestninjenju,

- Predlog Pravilnika o strokovnem usposabljanju, obdobjem izpopolnjevanju ter preizkusu znanja občinskih redarjev,
- Zakon o spremembah in dopolnitvah Zakona o knjižničarstvu,
- Predlog Direktive EP in Sveta o spremembah Direktive 2007/36/ES glede spodbujanja dolgoročnega sodelovanja delničarjev in Direktive 2013/34/EU glede določenih elementov izjave o upravljanju podjetij,
- Predlog sprememb Zakona o šolski prehrani,
- Pravilnik o vsebini in načinu predložitve letnega poročila političnih strank,
- Direktiva o družbah z omejeno odgovornostjo z enim družbenikom,
- Predlog Zakona o odvzemu in presaditvi delov človeškega telesa zaradi zdravljenja,
- Uredba o dopolnilnih dejavnostih na kmetiji,
- Predlog Pravilnika o službeni izkaznici inšpektorja in Pravilnika o službeni izkaznici občinskega redarja,
- Pravilnik o priznanju organizaciji proizvajalcev v sektorju sadja in zelenjave, oljčnega olja in namiznih oljk ter hmelja,
- Spremembe in dopolnitve Letnega programa statističnih raziskovanj za leto 2014,
- Pravilnik o nacionalni športni kartici,
- Pravilnik o subvencioniranju študentske prehrane,
- Zakon o spremembah in dopolnitvah Zakona o gospodarskih družbah,
- Pobuda za sklenitev sporazuma med Vlado Republike Slovenije in Svetom ministrov Bosne in Hercegovine o policijskem sodelovanju,
- Zakon o davku na dodano vrednost,
- Pravilnik o registru kmetijskih gospodarstev,
- Predlog Pravilnika o objavah pogodb s področja javnega naročanja in koncesij,
- Zakon o nematerializiranih vrednostnih papirjih,
- Sporazum med Vlado Republike Slovenije in Vlado Republike Makedonije o policijskem sodelovanju,
- Pravilnik o obratovalnem monitoringu stanja podzemnih voda,
- Zakon o spremembah in dopolnitvah Zakona o Poslovnem registru Slovenije,
- Letni program statističnih raziskovanj 2015,
- Predlog sprememb Zakona o bančništvu,
- Predlog Zakona o zavarovalništvu,
- Zakon o spremembah in dopolnitvah Zakona o delovnem času in obveznih počitkih mobilnih delavcev ter zapisovalni opremi v cestnih prevozih,
- Predlog Pravilnika o osebnem dopolnilnem delu,
- Predlog Zakona o spremembah in dopolnitvah Zakona o sodnem registru,
- Poročilo o zakonodajnem okviru za nadzor obveščevalnih in varnostnih služb,
- Zakon o upravljavcih alternativnih investicijskih skladov,
- Uredba o sofinanciranju zavarovalnih premij za zavarovanje primarne kmetijske proizvodnje in ribištva,
- Predlog Zakona o zbirkah podatkov s področja zdravstvenega varstva,
- Zakon o brezplačni pravni pomoči,
- Pravilnik o diplomatski, konzularni in službeni izkaznici,
- Zakon o športu,
- Predlog Državnopravobranilskega reda,
- Predlog Pravilnika o vzpostavitvi in vodenju registra zavezancev za informacije javnega značaja,
- Pravilnik o zbiranju podatkov o plačilnih transakcijah zavezancev za informacije javnega značaja,
- Osnutek Pravilnika o določitvi strokovnega spremstva pri udejstvovanjih lovskih gostov na skupnih lovih.



## 4.2. Sodelovanje z javnostmi

Informacijski pooblaščenec je leta 2014 veskozi skrbel za javnost svojega dela ter za 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](http://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, 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 oz. obrazce, namenjene fizičnim osebam za uveljavljanje njihovih pravic (zahteva za dostop do informacij javnega značaja, pritožba zoper molk ali zavrnilno odločbo organa, zahteva za ponovno uporabo informacij javnega značaja, prijava zlorabe osebnih podatkov, pritožba zaradi kršitve pravice do seznanitve z lastnimi osebnimi podatki, zahteva za seznanitev s podatki v Nacionalnem schengenskem informacijskem sistemu v Sloveniji) in upravljavcem zbirk osebnih podatkov za lažje delo pri vlaganju različnih zahtev in zagotovitvi ustreznega varovanja osebnih podatkov (zahteva za izdajo odločbe glede povezljivosti evidenc, obvestilo o povezovanju evidenc, prijava biometrijskih ukrepov pred njihovo uvedbo, vloga za iznos osebnih podatkov v tretje države, katalogi zbirk osebnih podatkov, pravilnik o zavarovanju osebnih podatkov, pogodba za potrebe pogodbene obdelave osebnih podatkov po 11. členu ZVOP-1, opozorila in obvestila ob neposrednem trženju),
- ažurno objavo izdanih mnenj s področja varstva osebnih podatkov,
- ažurno objavo vseh odločb, s katerimi odloča 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 in 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.

Podobno kot prejšnja leta je Informacijski pooblaščenec tudi leta 2014 v okviru preventivnega delovanja na področju varstva osebnih podatkov sodeloval z upravljavci osebnih podatkov, odgovarjal na pisna in ustna vprašanja posameznikov in upravljavcev osebnih podatkov ter sproti obveščal javnost o vseh pomembnejših ugotovitvah in dogodkih s tega področja.

Informacijski pooblaščenec je bil leta 2014 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 2014 je Informacijski pooblaščenec ob evropskem Dnevu varstva osebnih podatkov (28. januarja) pripravil dogodek, s katerim je želel doprinesti k javni razpravi glede vprašanja pomena in vloge zasebnosti v luči razkritij o obsežnem nadzoru posameznikov s strani varnostnoobveščevalnih služb ter vse večjih apetitov policije po uporabi sredstev, ki omogočajo skoraj vseobsegajoč nadzor posameznikov. Osrednji del dogodka je bila okrogla miza z naslovom Zasebnost po Snowdenu, na kateri so svoje poglede na vlogo varnostnoobveščevalnih agencij in organov pregona v razmerju do varstva zasebnosti pod vodstvom informacijske pooblaščenke Nataše Pirc Musar soočili dr. Katja Šugman Stubbs, profesorica za kazensko pravo na Pravni fakulteti Univerze v Ljubljani, dr. Ciril Ribičič, profesor za ustavno pravo na Pravni fakulteti Univerze v Ljubljani in bivši ustavni sodnik, dr. Damir Črnčec, nekdanji direktor Sove in docent za obrambni in varnostni sistem na Fakulteti za državne in evropske študije, mag. Tatjana Bobnar, namestnica generalnega direktorja policije, Vuk Čosić, digitalni strateg, in mag. Andrej Tomšič, namestnik informacijske pooblaščenke. Strokovnjaki so podali odgovore na aktualna vprašanja v povezavi z množičnim zbiranjem podatkov, ki naj bi nam zagotavljalo večjo varnost (npr. Kako so Snowdenova razkritja o obsežnem nadzoru posameznikov s strani varnostno obveščevalnih služb vplivala na pomen in dojetje zasebnosti? Koliko nadzora je preveč in kje je meja med zagotavljanjem varnosti in kršenjem temeljnih človekovih pravic? Kako razumeti vse večje apetite policije po uporabi sredstev, ki omogočajo skoraj vseobsegajoč nadzor posameznikov? Imamo posamezniki sploh možnost vplivati na omejitve posegov države v našo zasebnost? Kdo je odgovoren za boj za zasebnosti – država, politika, vsak posameznik posebej?).

Že tradicionalno je Informacijski pooblaščenec podelil nagrado za dobro prakso na področju varstva osebnih podatkov. Nagrado je prejel Kreditni biro SISBON, ki je v okviru inšpekcijskega postopka, ki ga je vodil Informacijski pooblaščenec, izkazal zavidljivo raven varovanja osebnih podatkov. Posebna priznanja je podelil tudi družbam, ki so leta 2013 pridobila certifikat po standardu za varovanje informacij ISO/IEC 27001 in s tem izkazala visoko raven varovanja osebnih podatkov: CDE, nove tehnologije, d. o. o., iz Ljubljane, FMC, d. o. o., iz Ljubljane, HRC, d. o. o., iz Žalca, SMART COM, d. o. o., iz Ljubljane, ELEKTRO MARIBOR, d. d., COMLAND, d. o. o., iz Ljubljane, MARAND, d. o. o., iz Ljubljane ter Intermatic inženiring & consulting, d. o. o., iz Ljubljane.

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. Informacijski pooblaščenec je organiziral okroglo mizo z naslovom Ali večja transparentnost krepi zaupanje v pravno državo?, s katero je želel opozoriti na pomen transparentnosti pri krepitvi odgovornosti delovanja javnega sektorja ter zagotavljanju pogojev za učinkovitejše sodelovanje državljanov pri odločanju o skupnih zadevah. Informacijski pooblaščenec je prepričan, da večja transparentnost krepi zaupanje v pravno državo, vendar bi se v praksi lahko storilo še marsikaj, da bi bil ta učinek izrazitejši. Predvsem bi moral biti vsakomur omogočen neoviran, hiter in čim cenejši (po možnosti pa brezplačen) dostop do informacij javnega značaja. Takšno stanje bi zagotovo odstrlo marsikatero tančico dvoma glede delovanja pravne države, poleg tega pa bi pripomoglo h krepitvi demokratične družbe v širšem smislu. Na okrogli mizi so svoje poglede na to temo pod vodstvom informacijske pooblaščenke Mojce Prelesnik soočili strokovnjaki Goran Forbici, direktor Centra za informiranje, sodelovanje in razvoj nevladnih organizacij, dr. Pavel Gantar, bivši minister za informacijsko družbo, prof. dr. Erik Kerševan, izredni profesor na Katedri za upravno pravo na Pravni fakulteti Univerze v Ljubljani, dr. Anamarija Musa, informacijska pooblaščenka Republike Hrvaške, Vlasta Nussdorfer, varuhinja človekovih pravic, in dr. Gregor Virant, bivši minister, pristojen za javno upravo.

Informacijski pooblaščenec je prvič podelil priznanje za dobro prakso na področju dostopa do informacij javnega značaja ambasador transparentnosti. Prejelo jo je Ministrstvo za notranje zadeve, Policija.

Informacijski pooblaščenec je tudi leta 2014 nadaljeval preventivno delo in je veliko pozornosti namenil nadaljnji širitvi orodij in pripomočkov za dvig ozaveščenosti. Zaradi varčevalnih ukrepov je zelo omejil tisk svojih publikacij in tiskovin, izdal je le Letno poročilo Informacijskega pooblaščenca za leto 2013 v slovenščini. Ostale publikacije in letno poročilo za leto 2013 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 prav tako niso bile natisnjene, in sicer Smernice za varstvo osebnih podatkov pri izvajanju internih tržnih raziskav, Uporaba GPS-sledilnih naprav in varstvo osebnih podatkov ter Presoja vplivov na zasebnost pri uvajanju novih policijskih pooblastil. 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 jasn, 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 pooblaščenca daje 49. člen ZVOP-1, ki med drugim določa, da Informacijski pooblaščenec daje neobvezna mnenja, pojasnila in stališča o vprašanih s področja varstva osebnih podatkov in jih objavlja na spletni strani ali na drug primeren način ter pripravlja in daje neobvezna navodila in priporočila glede varstva osebnih podatkov na posameznem področju.

Zaradi novele ZDIJZ-C je Informacijski pooblaščenec v sodelovanju z Ministrstvom za notranje zadeve pripravil spletno brošuro s priporočili o tem, na kakšen način naj poslovni subjekti pod prevladujočim vplivom države, lokalnih skupnosti ali drugih oseb javnega prava izvajajo določbe te novele. Priročnik z naslovom Obveznosti podjetij pod prevladujočim vplivom države, lokalnih skupnosti ali drugih oseb javnega prava je dostopen na spletni strani Informacijskega pooblaščenca.

Skupnost informacijskih pooblaščenecv 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 pooblaščenecv. To zahtevno nalogo so zaupali slovenskemu Informacijskemu pooblaščenca, ki je tako prevzel iniciativo in ustvaril spletno stran [info-commissioners.org](http://info-commissioners.org). Vsebina spletne strani je zanimiva tako za informacijske pooblaščenca kot za širšo zainteresirano javnost, saj ponuja osnovne informacije o vseh informacijskih pooblaščencah po svetu, povezave do njihovih spletnih strani, poleg tega pa zajema tudi vse zakone o dostopu do informacij javnega značaja držav, ki so jih te do zdaj sprejele, letna poročila pooblaščenecv, novice o njihovem delovanju, informacije o pomembnih dogodkih, sprejetih prelomnih odločitvah itd. Informacijski pooblaščenec je za delovanje te spletne strani skrbel tudi leta 2014.

## 4.3. Mednarodno sodelovanje

### 4.3.1. Sodelovanje v mednarodnih delovnih telesih

Informacijski pooblaščenec kot nacionalni 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 zmanjšanja proračunskih sredstev se je Informacijski pooblaščenec – tako kot že leta 2013 – tudi v letu 2014 na ravni EU udeležil le najnujnejših plenarnih sestankov ter občasno še sestankov štirih izmed številnih podskupin Delovne skupine za varstvo osebnih podatkov po 29. členu Direktive 95/46/ES. Informacijski pooblaščenec je tako sodeloval v sedmih

delovnih telesih EU, ki se ukvarjajo z nadzorom nad izvajanjem varstva osebnih podatkov v okviru posameznih področij EU, in sicer:

- v Delovni skupini po 29. členu ter štirih njenih podskupinah (v podskupini Future of Privacy, Tehnološki podskupini, podskupini BCR in podskupini BTLE),
- v Skupnem nadzornem organu za Europol,
- v Skupnem nadzornem organu za 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, poleg tega je sprejela naslednja pomembna mnenja: Mnenje o uporabi konceptov nujnosti in sorazmernosti ter varstva podatkov v sektorju kazenskega pregona, Mnenje o referenčnem dokumentu za zahteve za zavezujoča poslovna pravila, predložena nacionalnim organom za varstvo podatkov v EU, in pravila o varovanju zasebnosti pri čezmejnem prenosu podatkov, predložena odgovornim zastopnikom skupine APEC za pravila o varovanju zasebnosti pri čezmejnem prenosu podatkov, Mnenje o obveščanju o kršitvah varnosti osebnih podatkov, Mnenje o nadzoru elektronskih komunikacij v obveščevalne namene in namene nacionalne varnosti, Mnenje o anonimizacijskih tehnikah, Mnenje o pojmu zakonitih interesov upravljavca podatkov v skladu s 7. členom Direktive 95/46/ES, Mnenje o razvoju dogodkov na področju interneta stvari ter Mnenje o uporabi Direktive 2002/58/ES glede naprav za odvzem prstnih odtisov.

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 varstva 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 2014 nadaljevala razprave in pripravo mnenj za Delovno skupino po 29. členu glede reformnih predlogov za varstvo osebnih podatkov ter pripravila pomembne smernice glede izvrševanja pravice do umika rezultatov spletnega iskanja po osebnem imenu. Predstavniki Informacijskega pooblaščenca so v okviru Tehnološke podskupine aktivno sodelovali v okviru problemskih sklopov, ki se dotikajo zasebnosti na spletu, zlasti regulacije spletnih piškotkov in ugotavljanja identitete uporabnikov spleta s pomočjo t. i. digitalnih prstnih odtisov. Del pozornosti je skupina namenila vprašanju (ne) ustrezne implementacije tehničnih in uporabniških novosti s strani informacijskih gigantov, konkretno Google, Microsofta in Facebooka. Strokovna skupina se je v določenem obsegu posvečala tudi vprašanju v zvezi s tehnikami anonimizacije na spletu, z internetom stvari in z brezpilotnimi letalniki. Podskupina BTLE je pripravila mnenje o nadzoru elektronskih komunikacij v obveščevalne namene in namene nacionalne varnosti, poleg tega pa še spremljevalni dokument tega mnenja z obsežno pravno analizo možnosti zakonitega poseganja v komunikacijsko zasebnosti s strani varnostnoobveščevalnih služb in izmenjave podatkov. Poleg tega se je podskupina leta 2014 še naprej 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, 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 Nataša Pirc Musar je do junija 2014 nadaljevala svoj mandat predsednice Skupnega nadzornega organa za Europol. Aprila 2014 je predstavnik

Informacijskega pooblaščenca sodeloval v mednarodni inšpekcijski skupini, ki je na sedežu v Haagu opravila nadzor nad varstvom osebnih podatkov na Europolu.

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 pooblaščenec in organov za varstvo osebnih podatkov in zasebnosti s celega sveta. Delovna skupina je na zasedanjih v Berlinu in Skopju sprejela naslednja dokumenta: Working Paper on Privacy and Security Risks with the Use of “Own Devices” in Corporate Networks in Working Paper on Big Data and Privacy, Privacy principles under pressure in the age of Big Data analytics.

V okviru Sveta Evrope je predstavnik Informacijskega pooblaščenca tudi leta 2014 sodeloval kot član Posvetovalnega odbora (T-PD) po Konvenciji Sveta Evrope o varstvu posameznikov glede na avtomatsko obdelavo osebnih podatkov (Konvencija 108). Odbor se je lani še naprej posvečal oblikovanju sprememb besedila v procesu posodabljanja Konvencije 108, ki vzporedno poteka tudi v okviru posebnega ad hoc Odbora za varstvo osebnih podatkov Sveta Evrope (CAHDATA). Odbor T-PD je pripravil tudi obrazložitveno poročilo modernizirane konvencije, obravnava sprememb Konvencije 108 pa je namenil tudi pretežni del svojega 31. plenarnega zasedanja junija 2014. Le-temu je neposredno sledila letna konferenca evropskih organov za varstvo osebnih podatkov na temo mednarodnega sodelovanja na tem področju. Med drugimi pomembnimi nalogami odbora v lanskem letu velja poudariti posodabljanje Priporočila Sveta Evrope o zaščiti medicinskih podatkov, pri čemer je Informacijski pooblaščenec s pomembnim vsebinskim in organizacijskim prispevkom sodeloval v obširni anketi, izvedeni na tem področju.

#### 4.3.2. Ostale mednarodne dejavnosti

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 2014 Informacijski pooblaščenec ni prejel nobene pritožbe glede izvajanja te pravice na prvi stopnji.

Informacijski pooblaščenec je leta 2014 gostil predstavnike sorodnih institucij iz Bosne in Hercegovine, Hrvaške, Albanije, Romunije, Črne gore in Ukrajine ter jim predstavil svoje delovanje in dobre prakse s področij, za katera je pristojen.

Informacijski pooblaščenec je leta 2014 pripravil odgovore na 49 vprašanj in vprašalnikov tujih organov za varstvo osebnih podatkov, mednarodnih organizacij in tujih nevladnih organizacij.

Aprila 2014 se je pričel izvajati triletni projekt CRISP, ki ga financira Evropske komisije, ki se osredotoča na izboljšanje metodologije za certificiranje varnostnih izdelkov, med drugim upoštevajoč vidike zasebnosti in varstva osebnih podatkov. Sodelovanje Informacijskega pooblaščenca kot enega izmed partnerjev projekta vključuje sodelovanje zaposlenih pri pripravi različnih pravnih analiz in raziskav na temo projekta.

Novembra 2014 je Informacijski pooblaščenec postal partner v evropskem projektu ARCADES. Projekt je namenjen vnosu vsebin na temo varstva osebnih podatkov in varstva zasebnosti v kurikulum osnovnih in srednjih šol. V okviru projekta bodo partnerji na ravni EU pripravili poenotena gradiva in orodja, ki jih bodo učitelji v osnovnih in srednjih šolah lahko uporabili za seznanjanje učencev in dijakov z omenjenimi temami. Projekt bo potekal do aprila 2016.

Glede mednarodnega sodelovanja na področju dostopa do informacij javnega značaja velja omeniti, da se je decembra 2014 zaključil evropski projekt LAPSI 2.0 (Legal Aspects of Public Sector Information 2.0), v katerem je Informacijski pooblaščenec sodeloval od začetka, tj. od januarja 2013. Projekt se je osredotočal na odkrivanje in odstranjevanje pravnih ovir pri proaktivni objavi in ponovni uporabi informacij javnega značaja na evropskem trgu, na oblikovanje ukrepov in orodij za premagovanje ter odstranjevanje teh ovir ter na stimuliranje evropskega trga k odprtim podatkom. V okviru projekta se je Informacijski pooblaščenec leta 2014 udeležil vseh sestankov delovnih skupin projekta in aktivno sodeloval pri pripravi gradiv skupine. Predstavniki Informacijskega pooblaščenca so tudi aktivno sodelovali na novembrski mednarodni konferenci v Bruslju.

#### 4.3.3. Sodelovanje na mednarodnih srečanjih

Leta 2014 so se zaposleni pri Informacijskem pooblaščenca poleg sestankov v okviru že navedenih mednarodnih dejavnosti (delovne skupine EU, projekti) udeležili zgolj najnujnejših mednarodnih konferenc. Na večini spodaj navedenih srečanj so sodelovali s svojimi prispevki, udeležili pa so se jih na povabilo organizatorjev, ki so tudi v celoti ali delno krili stroške udeležbe.

- 28. februar 2014, Beograd, Srbija: Deveti evropski pravni i politički forum: Slobodan pristup informacijama od javnog značaja, Zakon o zaštiti podataka o ličnosti: kako osigurati transparentnost pravosuđa i drugih institucija;
- 3.–5. marec 2014, Bruselj, Belgija: Zaključna konferenca SMART,
- 2.–3. april 2014, Skopje, Makedonija: Central Eastern Europe Data Protection Authorities 16th meeting,
- 29. maj 2015, Zagreb, Hrvaška: Pravo na pristup informacijama i njegova ograničenja u europskom demokratskom društvu,
- 5. junij 2014, Strasbourg, Francija: European Conference od Data Protection Authorities,
- 16.–18. september 2014, Priština, Kosovo: Freedom of Public Information – Evolving Practices in the Western Balkan Region,
- 24. september 2014, Zagreb, Hrvaška: Pristup informacijama u Republici Hrvatskoj: Novi izazovi nova rješenja,
- 6.–7. oktober 2014, Skopje, Makedonija: XXVI Case Handling Workshop,
- 16.–17. oktober 2014, Skopje, Makedonija: South East Europe Media Forum,
- 3.–5. november 2014, Edinburg, Škotska: Information Commissioner's European Regional Meeting and Conference,
- 8. december 2014, Pariz, Francija: Conference of the European Data Governance Forum: Privacy, innovation, surveillance: which ethical framework for Europe.



Odgovorna urednica:

**Mojca Prelesnik, informacijska pooblaščenka**

Avtorji besedil:

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

**Jože Bogataj**, namestnik informacijske pooblaščenke

**Eva Kalan**, državna nadzornica za varstvo osebnih podatkov

**Kristina Kotnik Šumah**, namestnica informacijske pooblaščenke

**Maja Lubarda**, svetovalka

**mag. Andrej Tomšič**, namestnik informacijske pooblaščenke

Oblikovanje:

**Bons d.o.o. in Klemen Kraigher Mišič**

Fotografije:

**Klemen Kraigher Mišič in Fotolia**

Lektorirala:

**Katja Klopčič Lavrenčič**

*Informacijski pooblaščenec Republike Slovenije*

*Zaloška cesta 59*

*1000 Ljubljana*

*[www.ip-rs.si](http://www.ip-rs.si)*

*[gp.ip@ip-rs.si](mailto:gp.ip@ip-rs.si)*

Ljubljana, maj 2015

ISSN 1854-9500