INFORMACIJSKI POOBLAŠČENEC
REPUBLIKE SLOVENIJE

'16 Letno poročilo

Informacijskega pooblaščenca
za leto 2016

Spoštovani,

Letno poročilo o delu Informacijskega pooblaščenca za leto 2016 kaže, da je bilo to leto za Informacijskega pooblaščenca prelomno, tako zaradi zakonskih sprememb kot tudi zaradi obsega aktivnosti in števila primerov, ki jih je obravnaval. Izdal je več kot 312 odločb v pritožbenih zadevah s področja dostopa do informacij javnega značaja, kar je največ od začetka njegovega delovanja. Na področju varstva osebnih podatkov je obravnaval 683 inšpekcijskih zadev, zaposleni so odgovorili na več kot 1330 prošenj za pisna mnenja ter več kot 2500-krat svetovali po telefonu posameznikom, podjetjem in drugim organizacijam.

Na področju varstva osebnih podatkov se je leta 2016 s sprejetim svežnjem predpisov Evropske unije v okviru reforme varstva osebnih podatkov zgodil prelomen korak za celotno Evropsko unijo, saj upravljavcem zbirk osebnih podatkov prinaša številne nove obveznosti, posameznikom pravice, Informacijskemu pooblaščencu pa nove naloge in pristojnosti. Področje dostopa do informacij javnega značaja pa je zaznamovala predvsem novela Zakona o dostopu do informacij javnega značaja (ZDIJZ-E), ki je implementirala spremenjeno evropsko direktivo o ponovni uporabi informacij javnega sektorja. Njen namen je vsakomur zagotoviti pravico do enostavne in učinkovite ponovne uporabe prosto dostopnih podatkov javnega sektorja za kateri koli namen. V režim ponovne uporabe so tako od maja 2016 vključeni tudi muzeji, knjižnice in arhivi, in sicer v zvezi s tistim prosto dostopnim gradivom, pri katerem nobena tretja oseba ni imetnik pravic intelektualne lastnine.

Informacijski pooblaščenec je leta 2016 z željo po največjem možnem učinku na pravice posameznikov svoje sile usmeril v izobraževanje, hitro reševanje pritožbenih zadev na področju dostopa do informacij javnega značaja ter učinkovito ukrepanje proti kršitvam na področju varstva osebnih podatkov. Naše glavno vodilo je pravočasno prepoznati ključna področja (na podlagi pritožb, prijav ali inšpekcij po uradni dolžnosti), kjer lahko najučinkovitejše pomagamo posameznikom pri uveljavljanju obeh ustavnih pravic. Ko gre za varstvo osebnih podatkov, je naša prioriteta hitro reševanje nujnih zadev, pri katerih obstaja verjetnost velikega števila prizadetih posameznikov, in tistih, pri katerih gre za občutljive osebne podatke. To pomeni, da imajo ti primeri po hitrosti in nujnosti našega odziva prednost pred posamičnimi prijavami, kjer nevarnosti za zasebnost ni več.

Informacijski pooblaščenec je na področju dostopa do informacij javnega značaja leta 2016 prejel 514 pritožb. Od tega je bilo 316 pritožb zoper zavrnilne odločbe ter 198 pritožb zoper molk organa. Veseli nas, da se je bistveno zmanjšalo število pritožb zaradi t. i. molka organa, se je pa povečalo število prošenj za mnenja in pojasnila. To kaže, da so bili zavezanci to leto bolj aktivni in odzivni kot leto pred tem. Povprečen čas reševanja pritožbenih zadev zoper zavrnilne odločbe, v katerih je bil potreben poseben ugotovitveni postopek, je pri Informacijskem pooblaščencu znašal 47 dni, kar dokazuje, da je naš trud za čim hitrejšo obravnavo pritožbenih zadev obrodil sadove. Največ pritožb smo prejeli zoper zavrnilne odločbe, vložene zoper državne organe, vendar jih je bilo številčno vendarle manj kot leto dni pred tem, znova pa je bilo zaznati porast pritožb zoper zavrnilne odločbe občin.

Kot že leto prej je Informacijski pooblaščenec tudi leta 2016 zaznal porast pritožbenih zadev na področju dostopa do okoljskih informacij. Prav za okoljske podatke naša zakonodaja določa najvišjo stopnjo transparentnosti in pri njih ne pride v poštev praktično nobena zakonska izjema.

Ugotavljamo, da se pričakovanja glede učinkovite uporabe modernih tehnologij v javnem sektorju odražajo tudi v pritožbah v zvezi z dostopom do informacij javnega značaja. Največ pritožbenih primerov se tako leta 2016 ni nanašalo na izjemo varstva osebnih podatkov (kot pred tem več let zapored), ampak na vprašanje, ali zahtevana informacija sploh obstaja. V času hitrega razvoja informacijske tehnologije prosilci od zavezancev pričakujejo, da bodo ti razpolagali z različnimi statističnimi podatki in z možnostjo iskanja po informacijah po različnih zahtevanih kriterijih, v praksi pa se pogosto izkaže, da temu ni tako. Informacijski pooblaščenec zato pozdravlja rešitev, ki

jo je prinesla novela ZDIJZ-E v 10.b členu: zakonodajalec je zavezancem naložil, da s posredovanjem informacij v svetovni splet in na portal odprtih podatkov sami proaktivno zagotavljajo odprte podatke za ponovno uporabo, s čimer se posredno zagotavlja bistveno večja transparentnost.

Na področju varstva osebnih podatkov je Informacijski pooblaščenec poleg inšpekcijskih in prekrškovnih postopkov ter obravnave mnenj, vlog za izdajo dovoljenja za povezovanje zbirk osebnih podatkov in vlog za izdajo dovoljenja za izvajanje biometričnih ukrepov obravnaval tudi kar 53 vlog za izdajo dovoljenja za iznos osebnih podatkov v države izven Evropske unije ter 91 pritožb zaradi zavrnitve zahteve za seznanitev z lastnimi osebnimi podatki.

Število prijav zaradi suma kršitev predpisov s področja varstva osebnih podatkov, ki jih je Informacijski pooblaščenec prejel leta 2016, je bilo podobno kot v preteklih letih, še vedno so prevladovale prijave zaradi posredovanja osebnih podatkov nepooblaščenim uporabnikom, izvajanja videonadzora (zlasti v delovnih prostorih), prijave zaradi uporabe osebnih podatkov za namene neposrednega trženja (zlasti zaradi suma nezakonitega pridobivanja osebnih podatkov za te namene ter neupoštevanja zahteve posameznika po prenehanju uporabe osebnih podatkov za te namene), prijave zaradi preusmeritve in posledično branja elektronske pošte, ki prihaja na službeni elektronski naslov zaposlenih, prijave zaradi objave osebnih podatkov na spletnih straneh ter prijave zaradi pomanjkljivega zavarovanja osebnih podatkov. Informacijski pooblaščenec je leta 2016 s ciljem zagotavljanja čim višje možne ravni varstva vsem prebivalcem Slovenije okrepil izvajanje t. i. načrtovanih ex offo *inšpekcijskih nadzorov, ki se vsako leto izvajajo skladno s sprejetim letnim načrtom. Načrtovani inšpekcijski nadzor nad spoštovanjem določb ZVOP-1 se je leta 2016 največ izvajal v policiji, zdravstvenih zavodih, bankah in hranilnicah, pri dajalcih potrošniških kreditov, zavarovalnicah, organih lokalne samouprave, v visokošolskih zavodih, srednjih šolah ter energetskih družbah.*

Kot smo ugotavljali že v letnem poročilu za leto 2015, se je v zadnjih desetih letih delovanja Informacijskega pooblaščenca bistveno izboljšala ozaveščenost tako splošne kot strokovne javnosti glede zasebnosti in varstva osebnih podatkov. Še vedno pa je pri upravljavcih podatkov in njihovih obdelovalcih na nekaterih področjih mogoče zaslediti pomanjkljivosti in nepravilnosti.

Vse v postopkih inšpekcijskega nadzora ugotovljene nepravilnosti in pomanjkljivosti so zavezanci dolžni odpraviti, pri čemer je treba poudariti, da zavezanci to praviloma prostovoljno hitro uredijo že na podlagi opozorila državnega nadzornika. Velik problem pri opravljanju inšpekcijskega nadzora pa na žalost še vedno predstavljajo zavezanci, ki nimajo poslovnih prostorov, temveč le poštni nabiralnik, ter zavezanci, ki imajo v Poslovni register kot pooblaščene osebe za zastopanje vpisane tuje državljane. Večinoma gre za zavezance, ki se ukvarjajo s spletno prodajo, ter osebne podatke zbirajo in uporabljajo za vsiljivo neposredno trženje. Trenutno stanje zavezancem omogoča nezakonito ravnanje ter izogibanje odgovornosti za kršitve. Na pobudo Informacijskega pooblaščenca je to problematiko obravnaval Inšpekcijski svet, ki bo na podlagi prejetih predlogov rešitev inšpekcijskih organov pripravil predlog rešitev za pristojni ministrstvi, za Ministrstvo za gospodarski razvoj in tehnologijo ter Ministrstvo za pravosodje.

Veliko povečanje obsega in razmah množičnosti obdelave osebnih podatkov smo opazili tudi na področju pametnih telefonov, saj očitno postajajo enotna točka za identifikacijo posameznika, vstopno sredstvo do različnih sistemov in storitev ter nadomeščajo druge naprave. Evropska Splošna uredba o varstvu osebnih podatkov v povezavi s pametnimi napravami priznava pomen različnih spletnih identifikatorjev, nevarnosti naraščajočega profiliranja in avtomatiziranega odločanja. Pred upravljavce bo postavila več zahtev po preventivnem delovanju, saj vsebuje mehanizme potrjevanja, zahteve za imenovanje pooblaščenih odgovornih oseb za varstvo osebnih podatkov, ocene učinkov, načela vgrajene in privzete zasebnosti ter odgovornosti (angl. accountability*). Ocenjujemo, da je pri obravnavi varstva osebnih podatkov pravilno poudarjanje preventive in proaktivnosti, vsekakor pa to za upravljavce pomeni veliko spremembo pristopa.*

Trendi, ki smo jih identificirali v predhodnih poročilih, se nadaljujejo: pospešena digitalizacija na vseh področjih življenja, t. i. big data, *profiliranje in razvoj umetne inteligence ter internet stvari. Na prav tako pomembnih področjih genetskih in biometrijskih podatkov bo državam članicam Evropske unije Splošna uredba o varstvu podatkov prepustila več možnosti za ohranitev ali določitev pravil. Internet stvari prinaša predvsem izzive z varnostnega vidika, saj mnogim razvijalcem ni najpomembnejše, kako zavarovati nove povezane točke, temveč v internet povezujejo vse več stvari, ne glede na to, ali tja sodijo ali ne (povezujejo pametne žarnice, hladilnike, športne ure in v zadnjem času pospešeno avtomobile). Po nekaterih ocenah naj bi bilo do leta 2020 v internet stvari povezanih celo do 30 milijard naprav, čeprav imamo glede varstva zasebnosti velike težave*

že z obstoječimi napravami; tudi največji upravljavci imajo namreč ranljive sisteme, beležijo vdore v strežnike in se soočajo z izgubo podatkov.

Zavedati se moramo, da spremembe na področju zasebnosti hitro potekajo. Področij, kjer nihče ne zbira podatkov o nas, je vse manj, pa tega v vsakdanjem življenju niti ne opazimo. Zbrani podatki predstavljajo predvsem moč odločanja, in ta se pospešeno seli od nas k drugim – k trgovcem, operaterjem, državi, obveščevalnim agencijam, organom pregona.

Posebno pozornost je Informacijski pooblaščenec zato tudi leta 2016 posvetil preventivnim vidikom svojega delovanja. S ciljem izobraževanja upravljavcev in drugih zavezancev smo izvedli 96 brezplačnih predavanj domačim slušateljem, če upoštevamo tudi predavanja gostom iz tujine, pa je bilo brezplačnih predavanj več kot 100. V stalnem stiku smo z upravljavci, obdelovalci in predlagatelji predpisov, da bi lahko pravočasno naslavljali različne dileme glede novih načinov zbiranja in obdelave osebnih podatkov ter iskanja zasebnosti prijaznih zakonskih rešitev ob uvajanju novih tehnologij ter povečevanju učinkovitosti. Med drugim smo zato na vseh ministrstvih izvedli predavanja za strokovnjake, ki pripravljajo zakonske in podzakonske predpise, ki se dotikajo področja varstva osebnih podatkov, podali pa smo tudi več kot 120 mnenj na predloge zakonov in drugih predpisov, ki se nanašajo na različne vidike urejanja zbiranja in obdelave osebnih podatkov.

Informacijski pooblaščenec omogoča tudi neformalno izvedbo ocen učinkov na varstvo osebnih podatkov kot eno temeljnih preventivnih orodij za pravočasni pristop k varstvu osebnih podatkov. Leta 2016 se je na nas obrnilo več kot 100 upravljavcev in obdelovalcev iz javnega in zasebnega sektorja, ki so pripravljali zakonodajo, rešitve ali projekte, in so se želeli o tveganjih pravočasno posvetovati ter se tako izogniti kršitvam. Izdali smo tudi štiri nove smernice ter napotke za upravljavce brezpilotnih letalnikov glede izvedbe ocen učinkov na varstvo osebnih podatkov.

Informacijski pooblaščenec je leta 2016 okrepil sodelovanje z deležniki, s čimer dosegamo sinergijske in multiplikativne učinke. Na področju ozaveščanja o varni rabi interneta delujemo v projektu Safe-si, sodelujemo z Inštitutom za korporativne varnostne študije (ICS) ter z Agencijo za komunikacijska omrežja in storitve, leta 2016 pa smo podpisali dogovor o sodelovanju s SI-CERT, nacionalnim odzivnim centrom za obravnavo incidentov s področja varnosti elektronskih omrežij in informacij, ter pristopili k sklepanju dogovora z Združenjem bank Slovenije in Zvezo potrošnikov Slovenije. Tesno sodelujemo tudi z Javno agencijo za civilno letalstvo pri izobraževanjih operaterjev brezpilotnih letalnikov.

S ciljem učinkovitega komuniciranja z vsemi našimi javnostmi smo leta 2016 prenovili spletno stran Informacijskega pooblaščenca. Del preventivnega delovanja Informacijskega pooblaščenca predstavljajo tudi strokovno sodelovanje v medresorskih delovnih skupinah in nastopi na različnih konferencah, strokovnih dogodkih, posvetih ter okroglih mizah, kot so INFOSEK 2016, Cryptoparty 2016, CSA CEE Cloud Security Summit, Moskovska mednarodna konferenca o varstvu podatkov, 24. mednarodna konferenca o revidiranju, 7. mednarodna konferenca Dnevi korporativne varnosti, Varnost mobilnih telefonov, XV. dnevi delovnega prava in socialne varnosti, Okrogla miza z naslovom Pravica do zasebnosti in nove tehnologije, Dnevi kazenskega prava, posvet Priložnost digitalne preobrazbe za Slovenijo, Festival odprtih podatkov ...

Vse navedeno kaže, da nas tudi leta 2017 čakajo odgovorne naloge, med katerimi bo ena prednostnih učinkovita priprava na začetek uporabe Splošne uredbe o varstvu osebnih podatkov. Z veseljem ugotavljamo, da so se tudi številni večji upravljavci že začeli pripravljati na njeno uporabo, saj je določene prilagoditvene aktivnosti nujno začeti dovolj zgodaj – prilagoditi bo treba poslovne procese, angažirati ustrezne kadre in podrobno preveriti obstoječe ravni varstva osebnih podatkov. Naloga zakonodajalca pa je ustrezno urediti tista področja, kjer uredba državam članicam pri urejanju dopušča nekaj več svobode (npr. pravila glede zdravstvenih, biometrijskih in genetskih podatkov). Trend eksponentnega naraščanja pristojnosti se bo nadaljeval, saj bo Splošni uredbi o varstvu podatkov leta 2017 sledila še evropska uredba o e-zasebnosti na enotnem digitalnem trgu, poleg tega pa že sama narava modernih tehnologij in zahteve družbe prispevajo k temu, da se pristojnosti Informacijskega pooblaščenca kot varuha zasebnosti in transparentnosti nenehno množijo. Vse to pomeni za nas veliko odgovornost, zato se bomo svoje kadrovske in finančne vire trudili uporabiti čim bolj učinkovito in seveda s ciljem zagotavljanja najvišje možne ravni varstva obeh ustavnih pravic prebivalcev Republike Slovenije.

Mojca Prelesnik,
informacijska pooblaščenka

1. O INFORMACIJSKEM POOBLAŠČENCU

1.1. Nastanek Informacijskega pooblaščenca 9
1.2. Pristojnosti Informacijskega pooblaščenca 9
1.3. Organiziranost Informacijskega pooblaščenca 13
1.4. Finančna sredstva Informacijskega pooblaščenca 14

2. DELO NA PODROČJU DOSTOPA DO INFORMACIJ JAVNEGA ZNAČAJA

2.1. Pravna ureditev na področju dostopa do informacij javnega značaja v Republiki Sloveniji 18
2.2. Število vloženih pritožb in število rešenih zadev 20
2.3. Število vloženih tožb na Upravnem sodišču, število sodb Upravnega in Vrhovnega sodišča 21
2.4. Statistika po posameznih področjih ZDIJZ 21
2.5. Storjeni prekrški po ZDIJZ, ZInfP in ZMed 24
2.6. Predstavitev najodmevnejših in precedenčnih primerov po področjih 25
2.6.1. Okoljski podatki, varstvo upravnega postopka 25
2.6.2. Mediji, javni uslužbenci, delovno področje organa 25
2.6.3. Dokument v izdelavi 26
2.6.4. Poslovni subjekt pod prevladujočim vplivom 26
2.6.5. Poslovna skrivnost, poraba javnih sredstev 27
2.6.6. Okoljski podatki 27
2.6.7. Tajni podatki 27
2.6.8. Tajnost vira 28
2.6.9. Mediji, varstvo kazenskega pregona 28
2.6.10. Ali je organ zavezanec? 29
2.6.11. Notranje delovanje organa, poslovna skrivnost 29
2.6.12. Ponovna uporaba 30
2.6.13. Tajni podatki, umik stopnje tajnosti 30
2.6.14. Poslovna skrivnost, avtorsko delo 31
2.7. Splošna ocena in priporočila na področju dostopa do informacij javnega značaja 32

3. DELO NA PODROČJU VARSTVA OSEBNIH PODATKOV

3.1. Koncept varstva osebnih podatkov v Republiki Sloveniji 35
3.2. Dejavnost državnih nadzornikov za varstvo osebnih podatkov 36
3.2.1. Pravice in dolžnosti državnega nadzornika 36
3.2.2. Inšpekcijski nadzor 36
3.2.2.1. Inšpekcijski nadzor v javnem sektorju 37
3.2.2.2. Inšpekcijski nadzor v zasebnem sektorju 38
3.2.3. Storjeni prekrški 39
3.3. Dajanje mnenj in pojasnil 41
3.4. Dopustnost izvajanja biometrijskih ukrepov 41
3.5. Ugotavljanje ustrezne ravni varstva osebnih podatkov v tretjih državah 44
3.6. Izdajanje dovoljenj za povezovanje javnih evidenc 47
3.7. Pravica do seznanitve z lastnimi osebnimi podatki 48

3.8.	Pravica do dopolnitve, popravka, blokiranja, izbrisa in ugovora	50
3.9.	Zahteve za oceno ustavnosti	51
3.9.1.	Odločitev Ustavnega sodišča RS v zvezi z zahtevo za presojo ustavnosti Zakona o davčnem postopku	52
3.10.	Izbrani primeri kršitev varstva osebnih podatkov	52
3.10.1.	Izvajanje videonadzora nad dovozno potjo	53
3.10.2.	Zbiranje osebnih podatkov za namen izterjave parkirnin	53
3.10.3.	Uporaba telesnega skenerja na letališču	54
3.10.4.	Neustrezno zavarovanje osebnih podatkov uporabnikov storitev na strežnikih telekomunikacijskega operaterja	55
3.10.5.	Neustrezno zavarovanje osebnih podatkov pacientov in zaposlenih na spletni strani	56
3.10.6.	Nezakonita pridobitev osebnih podatkov za namen neposrednega trženja	56
3.10.7.	Razkrivanje podatkov o osebnem stečaju na poštnih ovojnicah	57
3.10.8.	Nezakonito posredovanje osebnih podatkov v zvezi z zaračunavanjem stroškov kopiranja	58
3.11.	Splošna ocena stanja varstva osebnih podatkov in priporočila	60

4. DRUGE DEJAVNOSTI INFORMACIJSKEGA POOBLAŠČENCA

4.1.	Sodelovanje pri pripravi zakonov in drugih predpisov	68
4.2.	Sodelovanje z javnostmi	70
4.3.	Mednarodno sodelovanje	73
4.3.1.	Sodelovanje v mednarodnih delovnih telesih	73
4.3.2.	Ostale mednarodne dejavnosti	75
4.3.3.	Sodelovanje na mednarodnih srečanjih	75
4.3.4.	Projekti Informacijskega pooblaščenca	75
4.3.4.1.	Projekt CRISP	76
4.3.4.2.	Projekt ARCADES	77

LETO 2016 V ŠTEVILKAH

32
ZAPOSLENIH ZA NEDOLOČEN ČAS

1.432.399 EUR
PRORAČUN

VARSTVO OSEBNIH PODATKOV

683
INŠPEKCIJSKIH POSTOPKOV

83
PREKRŠKOVNIH POSTOPKOV

1330
PISNIH MNENJ

1884
USTNIH MNENJ

INFORMACIJE JAVNEGA ZNAČAJA

514
VLOŽENIH PRITOŽB

312
IZDANIH ODLOČB

198
POZIVOV ZARADI MOLKA

76
IN CAMERA OGLEDOV

308
PISNIH PROŠENJ ZA POJASNILA

OSTALO

4
SMERNICE

98
PRO BONO PREDAVANJ

SODELOVANJE PRI PRIPRAVI **100** PREDPISOV

O INFORMACIJSKEM POOBLAŠČENCU

1.1. Nastanek Informacijskega pooblaščenca

Državni zbor Republike Slovenije je 30. 11. 2005 sprejel Zakon o Informacijskem pooblaščencu[1], s katerim je bil 31. 12. 2005 ustanovljen nov samostojen in neodvisen državni organ. Omenjeni zakon je združil dva organa, in sicer Pooblaščenca za dostop do informacij javnega značaja, ki je imel že prej status neodvisnega organa, in Inšpektorat za varstvo osebnih podatkov, ki je deloval kot organ v sestavi Ministrstva za pravosodje. Ob uveljavitvi ZInfP je Pooblaščenec za dostop do informacij javnega značaja nadaljeval delo kot Informacijski pooblaščenec, ki je prevzel inšpektorje in druge uslužbence Inšpektorata za varstvo osebnih podatkov, pripadajočo opremo in sredstva. Hkrati je prevzel tudi vse nedokončane zadeve, arhive in evidence, ki jih je vodil Inšpektorat za varstvo osebnih podatkov. S tem so se pristojnosti organa, ki je skrbel za nemoteno izvajanje dostopa do informacij javnega značaja, močno spremenile in se razširile še na pravno področje varstva osebnih podatkov. Informacijski pooblaščenec je tako postal tudi državni nadzorni organ za varstvo osebnih podatkov. Delo je začel 1. 1. 2006.

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

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 17. 7. 2014 Informacijskega pooblaščenca vodi Mojca Prelesnik.

1.2. Pristojnosti Informacijskega pooblaščenca

Informacijski pooblaščenec svoje z zakonom določene naloge in pristojnosti opravlja na dveh področjih:

- na področju dostopa do informacij javnega značaja in
- na področju varstva osebnih podatkov.

Na področju dostopa do informacij javnega značaja, ki je urejeno z Zakonom o dostopu do informacij javnega značaja[2], ima Informacijski pooblaščenec pristojnosti pritožbenega organa (pristojnost je določena v 2. členu ZInfP). To pomeni, da odloča o pritožbi prosilca, če je zavezanec za dostop do informacij javnega značaja:

1. zahtevo za dostop do informacij javnega značaja zavrnil ali zavrgel;
2. na zahtevo ni odgovoril v predpisanem roku (je v molku);
3. omogočil dostop v drugi obliki, kot jo je prosilec zahteval;
4. posredoval informacijo, ki je prosilec ni zahteval;
5. neupravičeno zaračunal stroške za posredovanje informacij ali pa je zaračunal previsoke stroške;
6. ni ugodil zahtevi za umik stopnje tajnosti s podatkov, ki so s stopnjo tajnosti označeni v nasprotju z zakonom, ki ureja tajne podatke;
7. zavrnil, zavrgel ali ni odgovoril na zahtevo za ponovno uporabo informacij javnega značaja.

Informacijski pooblaščenec je tudi pristojen za vodenje evidence vseh podeljenih izključnih pravic na področju ponovne uporabe informacij (peti odstavek 36.a člena ZDIJZ).
Na področju dostopa do informacij javnega značaja ima Informacijski pooblaščenec tudi pristojnosti, ki mu jih podeljuje Zakon o medijih[3] (45. člen). Po ZMed se zavrnilni odgovor zavezanca na vprašanje, ki ga zastavi predstavnik medija, šteje kot zavrnilna odločba. Molk zavezanca ob takem vprašanju je prekršek in hkrati tudi razlog za pritožbo, o kateri odloča Informacijski pooblaščenec po določbah ZDIJZ.

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

Na področju varstva osebnih podatkov ima Informacijski pooblaščenec pristojnosti, ki mu jih dajeta Zakon o varstvu osebnih podatkov[4] in 2. člen ZinfP, in sicer:

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

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

Informacijski pooblaščenec lahko v skladu s 6. alinejo prvega odstavka 23.a člena Zakona o ustavnem sodišču[5] z zahtevo začne postopek za oceno ustavnosti oziroma 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; je neodvisen 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 nadzora podatkovnih zbirk nacionalnega dela Schengenskega informacijskega sistema (SIS) in za preverjanje, da obdelava in uporaba podatkov, vnesenih v SIS, ne pomenita kršenja pravic oseb, na katere se podatki nanašajo.

Informacijski pooblaščenec ima tudi pristojnosti po Zakonu o pacientovih pravicah[6], Zakonu o potnih listinah[7], Zakonu o osebni izkaznici[8], Zakonu o elektronskih komunikacijah[9], Zakonu o centralnem kreditnem registru[10] ter po Zakonu o potrošniških kreditih[11].

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 oziroma osebne izkaznice ter način hrambe kopij (4. 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 s 27. členom ZOIzk-1 in 34.b členom ZPLD-1).

Pristojnosti Informacijskega pooblaščenca na podlagi ZEKom-1:
- izvajanje inšpekcijskega nadzora nad izvajanjem določb 149. člena ZEKom-1, ki ureja notranje postopke o odzivanju na zahteve pristojnih organov za dostop do osebnih podatkov uporabnikov na podlagi področnih zakonov;
- najmanj enkrat na leto opravljanje inšpekcijskega nadzora nad obdelavo podatkov iz 153. člena ZEKom-1, ki določa pogoje in postopke za posredovanje prometnih in lokacijskih podatkov v primerih varovanja življenja in telesa posameznika;
- izvajanje inšpekcijskega nadzora nad izvajanjem določb 155. člena ZEKom-1, ki ureja sledenje zlonamernih ali nadležnih klicev na pisno zahtevo posameznika, ki klice prejema, in postopke glede posredovanja podatkov, ki razkrijejo identiteto kličočega;
- 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 kršitvah ZEKom-1 in na njegovi podlagi izdanih predpisov kot prekrškovni organ v skladu z zakonom, ki ureja prekrške (232. do 236. člen ZEKom-1).

5 Uradni list RS, št. 64/2007 – uradno prečiščeno besedilo 1 in 109/2012.
6 Uradni list RS, št. 15/2008; v nadaljevanju ZPacP.
7 Uradni list RS, št. 29/2011 – uradno prečiščeno besedilo 4; v nadaljevanju ZPLD-1.
8 Uradni list RS, št. 35/2011; v nadaljevanju ZOIzk-1.
9 Uradni list RS, št. 109/2012, s spremembami; v nadaljevanju ZEKom-1.
10 Uradni list RS, št. 77/2016; v nadaljevanju ZCKR.
11 Uradni list RS, št. 77/2016; v nadaljevanju ZPotK-2.

Leta 2016 je bil sprejet ZCKR, ki po novem vsebinsko ureja vzpostavitev centralnega kreditnega registra kot osrednje nacionalne zbirke podatkov o zadolženosti fizičnih oseb in poslovnih subjektov. Del tega registra je tudi sistem izmenjave informacij o zadolženosti posameznih fizičnih oseb, poznan kot SISBON. Tako register kot sistem izmenjave informacij upravlja Banka Slovenije, ki je v skladu s 366. in 400. členom Zakona o bančništvu[12] vzpostavljeni sistem izmenjave informacij o boniteti strank prevzela s 1. 1. 2016. V skladu s 26. členom ZCKR Banka Slovenije v zvezi z vzpostavitvijo in upravljanjem sistema izmenjave informacij določi tehnične pogoje, ki jih morajo izpolnjevati člani sistema in vključeni dajalci kreditov za članstvo oziroma vključitev v sistem izmenjave informacij ter za zagotavljanje zaupnosti podatkov, ki se zbirajo v sistemu izmenjave informacij. Pred določitvijo teh aktov Banka Slovenije pridobi mnenje Informacijskega pooblaščenca, ki izvaja inšpekcijski nadzor v zvezi z zbiranjem in obdelavo osebnih podatkov v centralnem kreditnem registru in sistemu izmenjave informacij v skladu z ZVOP-1[13]. V skladu z 31. členom ZCKR Informacijski pooblaščenec z namenom preprečevanja in odvračanja ravnanj, ki pomenijo nezakonito obdelavo osebnih podatkov, javno objavi informacije v zvezi z ukrepi nadzora in sankcijami zaradi prekrška, ki jih je izrekel.

Leta 2016 je bil sprejet tudi nov ZPotK-2, ki v 78. členu ohranja leta 2013 dodeljeno pristojnost Informacijskega pooblaščenca v zvezi z izvajanjem nadzora nad dajalci kreditov in kreditnimi posredniki glede izvajanja 10. in 42. člena v delu, ki se nanaša na informiranje, zbiranje in obdelavo osebnih podatkov pri izvedbi ocene kreditne sposobnosti potrošnika, ki jo mora dajalec kredita opraviti pred sklenitvijo kreditne pogodbe in pred sklenitvijo kreditne pogodbe za nepremičnino, ter 11. in 44. člena ZPotK-2, ki določata dostop do osebnih podatkov iz sistema izmenjave informacij o boniteti oziroma zadolženosti fizičnih oseb in zavarovanje teh podatkov.

Slika 1: Pristojnosti Informacijskega pooblaščenca.

[12] Uradni list RS, št. 25/2015, s spremembami; v nadaljevanju ZBan-2.

[13] Pred uveljavitvijo ZCKR je Informacijski pooblaščenec izvajal inšpekcijski nadzor v zvezi z zbiranjem in obdelavo osebnih podatkov v sistemu SISBON in je bil prekrškovni organ za kršitve določenih členov ZBan-2.

1.3. Organiziranost Informacijskega pooblaščenca

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

Na dan 31. 12. 2016 je imel Informacijski pooblaščenec 33 zaposlenih, od tega 32 za nedoločen in enega za določen čas zaradi nadomeščanja. V primerjavi z letom 2015 se je skupno število zaposlenih zmanjšalo za tri, hkrati pa se je število redno zaposlenih povečalo za eno osebo. Struktura zaposlenih je bila naslednja:

- 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,
- sedem svetovalcev,
- štirje asistenti svetovalca,
- enajst državnih nadzornikov za varstvo osebnih podatkov,
- svetovalec pooblaščenca za mednarodne odnose,
- raziskovalec,
- tri administrativno-tehnične sodelavke (finančna referentka, poslovna sekretarka, dokumentalistka).

Preglednica 1: Izobrazbena struktura zaposlenih pri Informacijskem pooblaščencu 31. 12. 2016.

	Višja strokovna šola	1. bolonjska stopnja	Univerzitetna izobrazba	Magisterij	Doktorat	Skupaj
Informacijska pooblaščenka			1			1
Namestniki			2	2		4
Generalna sekretarka				1		1
Svetovalci			6	1		7
Asistenti svetovalca			4			4
Raziskovalci		1				1
Državni nadzorniki za varstvo osebnih podatkov			4	6	1	11
Svetovalci pooblaščenca za mednarodne odnose			1			1
Administrativno-tehnični sodelavci	3					3
Skupaj	3	1	18	10	1	33

1.4. Finančna sredstva Informacijskega pooblaščenca

Finančna sredstva za delo Informacijskega pooblaščenca se v skladu s 5. členom ZInfP zagotavljajo iz državnega proračuna in jih določi Državni zbor RS na predlog Informacijskega pooblaščenca.

Na dan 31. 12. 2016 so bila Informacijskemu pooblaščencu dodeljena integralna sredstva v višini 1.335.457,02 EUR, od tega na postavki plače 1.206.489,02 EUR, na postavki materialni stroški 123.920,07 EUR in na postavki investicije 5.047,93 EUR. Evidentiranih odredb je bilo na dan 31. 12. 2016 1.331.901,96 EUR, na postavki plače 1.204.845,68 EUR, na postavki materialni stroški 122.008,95 EUR in na postavki investicije 5.047,33 EUR.

Informacijski pooblaščenec je leta 2016 razpolagal z namenskimi sredstvi v znesku 8.150,00 EUR in donacijami za sodelovanje v projektih, financiranih s strani EU, v višini 88.792,14 EUR. Porabljenih je bilo 68.373,61 EUR namenskih sredstev in donacij. V proračun leta 2017 je Informacijski pooblaščenec prenesel skupno 7.321,05 EUR namenskih sredstev in sredstev donacij (7.317,92 EUR namenskih sredstev ter donacij, mednarodna spletna stran 0,14 EUR, projekt TAIEX 2,99 EUR).

Iz postavke »Tekoča proračunska rezerva« pri Ministrstvu za finance so bila s sklepom Vlade leta 2016 prerazporejena sredstva v znesku 5.100,00 EUR na integralno postavko plače Informacijskega pooblaščenca.

Zaradi proračunskih omejitev in varčevalnih ukrepov, ki jih je sprejela Vlada RS leta 2016, je Informacijski pooblaščenec omejil izobraževanje zaposlenih, 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 2016 (v EUR).

	Veljavni proračun v EUR	Evidentirane odredbe v EUR	Razpoložljiv proračun v EUR konec leta
INFORMACIJSKI POOBLAŠČENEC	1.432.399,16	1.401.107,65	31.291,51
Podprogrami			
OPRAVLJANJE DEJAVNOSTI	1.335.457,02	1.331.901,96	3.555,06
Materialni stroški	123.920,07	122.008,95	1.911,12
Investicije	5.047,93	5.047,33	0,60
Plače	1.206.489,02	1.204.845,68	1.643,34
NAMENSKA SREDSTVA	8.150,00	832,08	7.317,92
Namenska sredstva kupnine	8.150,00	832,08	7.317,92
DONACIJE	88.792,14	68.373,61	20.418,53
Mednarodna spletna stran	0,14	0,00	0,14
Projekt TAIEX	2.692,00	2.689,01	2,99
Projekt IP-CRISP	63.020,00	62.850,63	169,37
Projekt IP-ARCADES	23.080,00	2.833,97	20.246,03

Za **materialne stroške** je bilo leta 2016 porabljenih **122.008,95 EUR**. Ti stroški vključujejo pisarniški material, tisk, čiščenje poslovnih prostorov, spremljanje medijev in arhiviranje – kliping, zdravniške preglede zaposlenih, stroške za energijo, vodo, komunalne storitve, pošto in komunikacijo, prevozne stroške in vzdrževanje dveh službenih vozil, taksi storitve, izdatke za službena potovanja, stroške za tekoče vzdrževanje (namestitev zaščitne mreže proti golobom, vzdrževanje evidence prisotnosti zaposlenih in spletne strani, manjša popravila v poslovnih prostorih, vzdrževanje kopirnega stroja in klimatskih naprav ter zavarovanje), odmero nadomestila za uporabo stavbnega zemljišča, naročnino za IUS-INFO in prekrškovni portal, plačila sodb sodišč, kvote Javnemu jamstvenemu, preživninskemu in invalidskemu skladu, izdatke za strokovno izobraževanje zaposlenih. Na koncu leta je preostanek finančnih sredstev zaradi varčevalnih ukrepov, ki jih Informacijski pooblaščenec izvaja, znašal 4.946,85 EUR. Na začetku leta je Informacijski pooblaščenec finančna sredstva v višini 10.000,00 EUR s postavke materialni stroški prerazporedil na postavko plače.

Za **investicije** je bilo do konca leta porabljenih **5.047,33 EUR**. Sredstva so bila porabljena za nakup pisarniškega pohištva (ognjevarna omara za kadrovske spise), pisarniške opreme (stoli), strojne računalniške opreme (prenosni računalnik), opreme za tiskanje in razmnoževanje, opreme za varovanje, telekomunikacijske opreme, aktivne mreže in komunikacijske opreme (posodobitev licence) ter nakup nematerialnega premoženja (Amebis Besana licenca). Konec leta 2016 je na postavki investicije ostalo 0,60 EUR neporabljenih finančnih sredstev. Na začetku leta je Informacijski pooblaščenec finančna sredstva v višini 30.000,00 EUR s postavke investicije prerazporedil na postavko plače.

Za **plače zaposlenih** (plače in dodatki, regres za letni dopust, povračila in nadomestila, sredstva za delovno uspešnost zaradi povečanega obsega dela, drugi izdatki zaposlenim, prispevki delodajalcev za socialno varnost, prispevki za zdravstveno zavarovanje, prispevki za zaposlovanje in starševsko varstvo, premije kolektivnega dodatnega pokojninskega zavarovanja na podlagi Zakona o dodatnem pokojninskem zavarovanju javnih uslužbencev) je bilo porabljenih **1.204.845,68 EUR**. Za izplačilo manka na postavki plače zaposlenih zaradi napredovanj v plačne razrede in nazive ter zakonsko določenega povečanega zneska regresa za letni dopust je moral Informacijski pooblaščenec zagotoviti finančna sredstva v višini 40.000,00 EUR s prerazporeditvijo privarčevanih sredstev s postavke materialni stroški in investicije na začetku leta ter s prerazporeditvijo 5.100,00 EUR iz tekoče proračunske rezerve Ministrstva za finance.

Mednarodna spletna stran info-commissioners.org - iz leta 2016 je bilo preneseno 0,14 EUR. Leta 2016 na tej postavki ni bilo porabe, preostanek sredstev višini 0,14 EUR se je prenesel v leto 2017.

Namenska sredstva kupnine - v leto 2016 je bilo prenesenih 8.150,00 EUR finančnih sredstev kupnin. Leta 2016 je bilo porabljenih 832,08 EUR (stroški, povezani s službenimi vozili), ostanek finančnih sredstev v višini 7.317,92 EUR se je prenesel v leto 2017.

TAIEX projekt - iz leta 2015 je bilo leta 2016 na to postavko prenesenih 2.692,00 EUR. Porabljenih je bilo 2.689,01 EUR, predvsem za delo zaposlenih na projektu in za stroške reprezentance. Sredstva v višini 2,99 EUR so se prenesla v leto 2017.

Projekt IP-ARCADES – Informacijski pooblaščenec je kot partner sodeloval v projektu »ARCADES (Introducing dAta pRoteCtion AnD privacy issuEs atschoolS in the European Union)« v okviru Splošnega programa »Fundamental Rights and Justice«: Specific Programme »Fundamental Rights and Citizenship« (FRC), št. pogodbe: JUST/2013/FRAC/AG/6132. Projekt je bil financiran s strani Evropske komisije. Trajal je 18 mesecev in se je zaključil leta 2016. Projekt se je osredotočal na vnos vsebin na temo varstva osebnih podatkov in varstva zasebnosti v kurikulume osnovnih in srednjih šol. Zaposleni pri Informacijskem pooblaščencu so sodelovali pri pripravi posameznih gradiv, analiz, izvajanju raziskav in drugih aktivnostih projekta, udeleževali so se misij in sestankov v zvezi s projektom, kjer so izvajali posamezne naloge s področja varstva osebnih podatkov, ki jih je pokrival projekt. Med drugim so izvajali predstavitve, seminarje in delavnice za ciljne skupine projekta. Prvo nakazilo na poseben račun, odprt pri Upravi za javna plačila, je Informacijski pooblaščenec prejel dne 10. 12. 2014, in sicer v znesku 35.990,00 EUR, drugo, zaključno nakazilo pa 13.12. 2015, in sicer v znesku 8.245,46 EUR. Skupaj je v času trajanja projekta prejel 44.235,46 EUR. Leta 2015 so bile s sklepom Vlade RS povečane pravice porabe za 32.875,00 EUR, porabljenih je bilo 32.685,12 EUR. Sredstva so bila porabljena za stroške organizacije dvodnevnega seminarja v oktobru, delo zaposlenih in njihovo napotitev na sestanke ter za materialne stroške in investicije, ki jih je s projektom imel Informacijski pooblaščenec. Ostanek finančnih sredstev je konec leta 2015 znašal 189,88 EUR. Leta 2016 je veljavni proračun znašal 23.080,00 EUR, porabljenih je bilo 2.833,97 EUR, večina za pokrivanje stroškov zaposlenih. Projekt je bil leta 2016 uspešno zaključen. Zaključno poročilo je bilo oddano oktobra, zadnje končno nakazilo pa je Informacijski pooblaščenec prejel dne 13.12.2016, in sicer 8.245,46 EUR.

Projekt IP-CRISP – Informacijski pooblaščenec je leta 2014 začel sodelovati v projektu 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, in bo predvidoma trajal 36 mesecev. Osredotoča se na izboljšanje metodologije za certificiranje varnostnih izdelkov, med drugim upoštevajoč vidike varstva osebnih podatkov. Zaposleni pri Informacijskem pooblaščencu sodelujejo pri pripravi posameznih gradiv in analiz, izvajanju raziskav in drugih aktivnosti, napoteni so na misije in sestanke v zvezi s projektom, kjer izvajajo posamezne naloge s področja varstva osebnih podatkov, ki jih pokriva projekt, ter izvajajo predstavitve, seminarje in delavnice za ciljne skupine projekta. Za sodelovanje v projektu bo Informacijski pooblaščenec prejel namenska finančna sredstva v višini 149.230,00 EUR. V okviru rednih aktivnosti za izvajanje projekta v 36 mesecih njegovega trajanja bo Informacijski pooblaščenec iz integralnih proračunskih sredstev zagotovil 24.890,00 EUR. Iz teh sredstev bodo pokriti stroški dela zaposlenih, stroški njihove napotitve na sestanke in misije, sredstva bodo namenjena pokrivanju povečanega obsega dela zaposlenih, njihovih avtorskih honorarjev in drugih stroškov, povezanih s pripravo in izvedbo navedenih aktivnosti, ter pokrivanju materialnih stroškov, ki jih bo s tem imel Informacijski pooblaščenec. Leta 2014 je bilo s strani Evropske komisije na poseben račun, odprt pri Upravi za javna plačila, dne 3. 6. 2014 nakazanih 82.076,50 EUR. S sklepom Vlade so bile povečane pravice porabe za leto 2014 v znesku 9.549,00 EUR; porabljenih je bilo 9.236,60 EUR. Leta 2015 so bile s sklepom Vlade povečane pravice porabe na projektu za 22.101,00 EUR; porabljenih je bilo 22.099,25 EUR. Konec leta 2015 je preostanek sredstev znašal 1,75 EUR. Leta 2016 je bilo dne 20. 5. 2016 nakazanih 20.802,98 EUR. S sklepom Vlade so bile povečane pravice porabe za leto 2016 v znesku 12.300,00 EUR, in sicer s 50.720 EUR na 63,020,00 EUR. Za namen izvajanja projekta je bilo porabljenih 62.850,63 EUR, in sicer za delo zaposlenih na projektu in za stroške, povezane z omogočanjem nemotenega dela zaposlenih (stroški pisarniškega materiala, energije, vode, komunalnih storitev, izdatki za službena potovanja, nakup opreme in kotizacije za sestanke). Preostanek sredstev je konec leta 2016 znašal 169,37 EUR. Skladno z Zakonom o izvrševanju proračunov Republike Slovenije se namenska finančna sredstva EU ne prenašajo v naslednja leta.

2 DELO NA PODROČJU DOSTOPA DO INFORMACIJ JAVNEGA ZNAČAJA

2.1. Pravna ureditev na področju dostopa do informacij javnega značaja

Pravico dostopa do informacij javnega značaja je zakonodajalec zagotovil že z Ustavo Republike Slovenije[14]. Ta v drugem odstavku 39. člena določa, da ima vsakdo pravico dobiti informacijo javnega značaja, za katero ima v zakonu utemeljen pravni interes, razen v primerih, ki jih določa zakon. Čeprav je pravica dostopa do informacij javnega značaja ena od temeljnih človekovih pravic in kot taka tudi zaščitena na ustavni ravni, se je začela uveljavljati šele 11 let po sprejetju Ustave RS, in sicer s sprejetjem Zakona o dostopu do informacij javnega značaja[15]. Dotlej so se posamezne določbe o javnosti informacij pojavljale le v nekaterih zakonih, celostno pa jih je uredil šele ZDIJZ. Tega je Državni zbor RS sprejel konec februarja 2003, veljati pa je začel 22. 3. 2003.

ZDIJZ sledi usmeritvam mednarodnih aktov in Evropske unije. Njegov namen je zagotoviti javnost in odprtost delovanja javne uprave ter vsakomur omogočiti dostop do javnih informacij, torej tistih, ki so povezane z delovnimi področji organov javne uprave. Zakon ureja postopek, ki vsakomur omogoča prost dostop in ponovno uporabo informacij javnega značaja, s katerimi razpolagajo državni organi, organi lokalnih skupnosti, javne agencije, javni skladi in druge osebe javnega prava, nosilci javnih pooblastil in izvajalci javnih služb. S tem zakonom se v pravni red Republike Slovenije prenašajo direktive Evropske skupnosti: Direktiva 2003/4/ES Evropskega parlamenta in Sveta o javnem dostopu do okoljskih informacij in razveljavitvi Direktive 90/313/EGS, ki je začela veljati 28. 1. 2003, ter Direktiva 2003/98/ES Evropskega parlamenta in Sveta o ponovni uporabi informacij javnega sektorja, ki je začela veljati 17. 11. 2003.

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

Leta 2014 sta bili sprejeti dve noveli ZDIJZ (ZDIJZ-C[16] in ZDIJZ-D[17]). 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 (oziroma v večinski lasti) države, občin ali drugih oseb javnega prava ter da je AJPES 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 krepita tudi transparentnost in odgovorno ravnanje pri upravljanju s finančnimi sredstvi poslovnih subjektov pod prevladujočim vplivom oseb javnega prava. Nadzor javnosti, omejen zgolj na državne organe, občine in širši javni sektor, se je izkazal za nezadostnega. Finančna in gospodarska kriza preteklih let je namreč povečala občutljivost javnosti za korupcijo, zlorabo oblasti in slabo upravljanje. K večji transparentnosti bo prispevala tudi proaktivna objava informacij javnega značaja na spletnih straneh, ki jo zahteva novela ZDIJZ-C.

Dne 8. 5. 2016 se je začela uporabljati novela ZDIJZ-E[18], ki je bila sprejeta konec leta 2015. Novela je prinesla novosti na področju ponovne uporabe informacij javnega značaja (npr. ponovna uporaba informacij muzejev in knjižnic, ponovna uporaba arhivskega gradiva, zagotavljanje odprtih podatkov za ponovno uporabo). Novela določa, da organi na nacionalnem portalu odprtih podatkov javnega sektorja, ki ga vodi Ministrstvo za javno upravo, objavijo seznam vseh zbirk podatkov iz svoje pristojnosti z metapodatki ter zbirke odprtih podatkov ali povezave na spletne strani, kjer so zbirke odprtih podatkov objavljene. Podatke, objavljene na tem portalu, lahko kdor koli ponovno uporablja v pridobitne ali druge namene brezplačno, pod pogojem, da to poteka v skladu z ZVOP-1 in da se navede vir podatkov. Novela spreminja tudi področje zaračunavanja stroškov dostopa in ponovne uporabe informacij javnega značaja. Za dostop do informacij javnega značaja se lahko zaračunajo le materialni stroški, ne pa tudi urne postavke za stroške dela javnih uslužbencev, ki tovrstne zahteve obravnavajo. Na podlagi novele ZDIJZ-E je

14 Uradni list RS, št. 33/1991, 42/1997, 66/2000, 24/2003, 69/2004, 68/2006; v nadaljevanju Ustava RS.
15 Uradni list RS, št. 24/2003, s spremembami; v nadaljevanju ZDIJZ.
16 Uradni list RS, št. 23/2014.
17 Uradni list RS, št. 50/2014 in 19/2015.
18 Uradni list RS, št. 102/2015.

Vlada RS sprejela novo Uredbo o posredovanju in ponovni uporabi informacij javnega značaja[19], s katero je sprejela enotni stroškovnik za posredovanje informacij javnega značaja in s tem odpravila posebne stroškovnike organov, na podlagi katerih so ti zaračunavali stroške dela, ter določila vrste informacij javnega značaja, ki se posredujejo na splet.

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:

- 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 zavezancev je pojem »informacija javnega značaja« (torej informacija, ki jo morajo zavezanci praviloma posredovati prosilcu) drugače definiran; pri zavezancih iz druge skupine je ožji. Za organe na splošno lahko rečemo, da so vsi dokumenti, zadeve, dosjeji, registri, evidence ali dokumentarno gradivo, 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 pa velja ravno obraten miselni proces – informacije javnega značaja so le tisti dokumenti, zadeve, dosjeji, registri, evidence ali dokumentarno gradivo, ki jih kot take določa ZDIJZ (npr. informacije, povezane s sklenjenimi pravnimi posli, ter informacije o članih poslovodnega 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-odstotni 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 pridobitev informacije 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 da 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 (oziroma je v molku) ali če ni dobil informacije v obliki, v kateri 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 in 5.a členu ZDIJZ (tajni podatek, poslovna skrivnost, osebni podatek, davčna tajnost, sodni postopek, upravni postopek, statistična zaupnost, dokument v izdelavi, notranje delovanje organa, varovanje naravne oziroma kulturne vrednote,…). Kljub navedenim izjemam organ dostop do zahtevane informacije vedno dovoli, če gre za podatke o porabi javnih sredstev ali za podatke, povezane z opravljanjem javne funkcije ali z delovnim razmerjem javnega uslužbenca. Zavezanec pod prevladujočim vplivom prosilcu praviloma ne sme zavrniti 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

[19] Uradni list RS, št. 24/2016.

skladu z 21. členom Uredbe o posredovanju in ponovni uporabi informacij javnega značaja[20] varovane podatke prekriti in prosilcu omogočiti vpogled v preostanek dokumenta (ali 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 2016 je Informacijski pooblaščenec prejel 514 pritožb, od tega 316 zoper zavrnilne odločbe in 198 zoper molk prvostopenjskih organov.

V okviru pritožbenih postopkov zoper odločbe, s katerimi so zavezanci zavrnili zahteve po dostopu ali ponovni uporabi informacij javnega značaja, je Informacijski pooblaščenec vodil 22 postopkov zoper poslovne subjekte pod prevladujočim vplivom države, občin ali drugih oseb javnega prava. Izdal je 312 odločb, v dveh primerih pa je pritožbo s sklepom zavrgel. Pri reševanju pritožb je opravil 76 ogledov *in camera*, tj. ogledov brez prisotnosti strank, ki zahtevajo dostop do informacije javnega značaja, na katerih je ugotavljal dejansko stanje dokumentov pri organu.

Informacijski pooblaščenec je v pritožbenih postopkih zaradi molka zavezance najprej pozval, naj o zahtevi prosilca čim prej odločijo. V večini primerov so zavezanci po pozivu Informacijskega pooblaščenca o zahtevi prosilca odločili in prosilcem posredovali zahtevane informacije. Z odgovorom zavezanca je bil postopek zaradi molka zaključen, prosilci, ki so dobili zavrnilno odločbo, pa so imeli možnost pritožbe Informacijskemu pooblaščencu zaradi zavrnitve zahteve po dostopu do informacij javnega značaja. V 26 primerih je Informacijski pooblaščenec pritožbo s sklepom zavrgel, in sicer v 15 primerih zaradi preuranjenosti in v 11 primerih zaradi pomanjkljive vloge. Šest posameznikov je pritožbe umaknilo, ker so zahtevano dokumentacijo prejeli, v šestih primerih pa je Informacijski pooblaščenec prosilcem pojasnil, da za reševanje njihovih vlog ni pristojen, in je vloge odstopil v reševanje pristojnim organom.

Leta 2016 je Informacijski pooblaščenec prejel 308 prošenj za pomoč in različnih vprašanj posameznikov glede dostopa do informacij javnega značaja. Vsem je 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.

[20] Uradni list RS, št. 24/2016.

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 2016 je bilo zoper odločbe Informacijskega pooblaščenca na Upravnem sodišču vloženih 43 tožb, tj. zoper 12,9 % izdanih odločb. Delež je relativno majhen, kar kaže na uveljavitev transparentnosti in odprtosti javnega sektorja glede njegovega delovanja ter tudi na sprejemanje njegovih odločb s strani zavezancev in prosilcev.

Upravno sodišče je leta 2016 odločilo o 22 tožbah, ki so bile vložene zoper odločbe Informacijskega pooblaščenca, in:

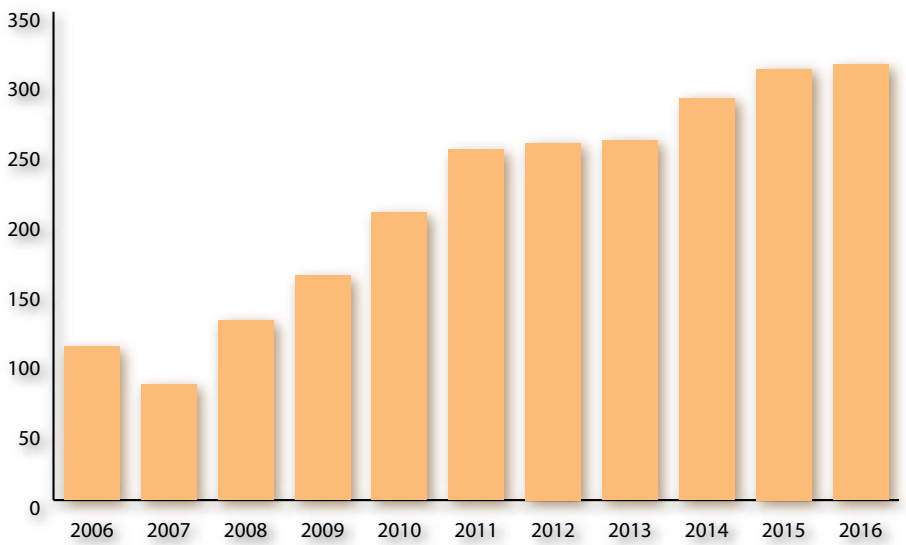
- tožbo zavrnilo – 8,
- tožbi ugodilo, izpodbijano odločbo oziroma del odločbe odpravilo in zadevo vrnilo Informacijskemu pooblaščencu v ponovno odločanje – 6,
- tožbo v enem delu zavrglo, v enem delu pa ji ugodilo, odločbo Informacijskega pooblaščenca delno odpravilo in mu jo vrnilo v ponoven postopek – 4,
- tožbo zavrglo – 2,
- tožbi ugodilo tako, da je odločbo Informacijskega pooblaščenca v enem delu odpravilo, v preostalem delu pa je tožbo zavrnilo – 1,
- tožbo v enem delu zavrnilo, v enem delu pa je postopek ustavilo – 1.

Leta 2016 Informacijski pooblaščenec ni vložil nobene revizije zoper sodbo Upravnega sodišča, je pa revizije vložilo pet zavezancev. Do konca leta 2016 Informacijski pooblaščenec ni prejel nobene odločitve Vrhovnega sodišča.

2.4. Statistika po posameznih področjih ZDIJZ

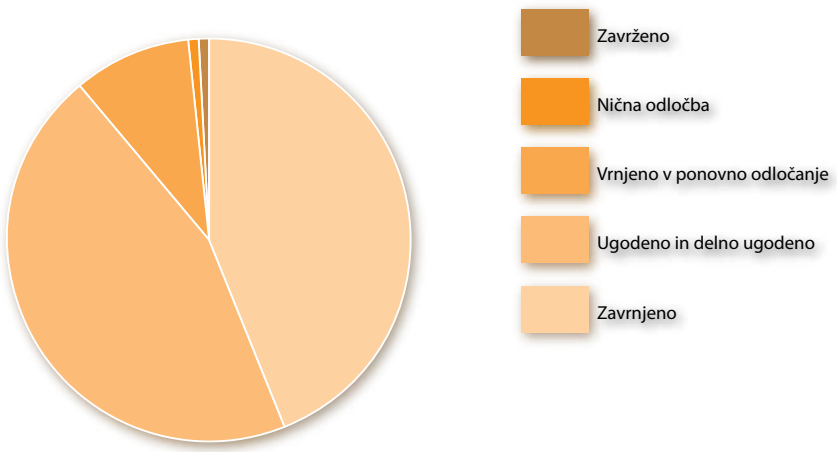
Število izdanih odločb na področju dostopa do informacij javnega značaja se je leta 2016 v primerjavi s preteklimi leti vnovič nekoliko povečalo: Informacijski pooblaščenec je izdal 312 odločb, kar je največ doslej.

Slika 3: Število izdanih odločb na področju dostopa do informacij javnega značaja med letoma 2006 in 2016.



Informacijski pooblaščenec je v izdanih odločbah:
- pritožbi delno ali v celoti ugodil oziroma rešil zadevo v korist prosilca – 141,
- pritožbo zavrnil – 137,
- pritožbi ugodil in zadevo vrnil v ponovno odločanje prvostopenjskemu organu – 29,
- odločbo prvostopenjskega organa razglasil za nično – 3,
- pritožbo zavrgel – 2.

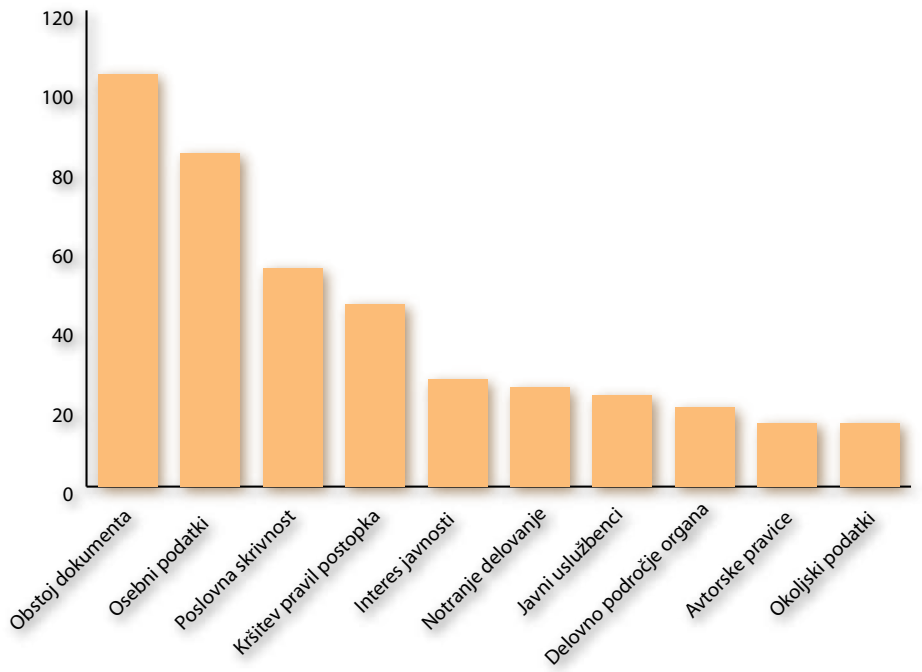
Slika 4: Odločitve Informacijskega pooblaščenca glede prejetih pritožb.



Informacijski pooblaščenec je v odločbah vsebinsko odločal oziroma presojal:
- ali zavezanec ima dokument oziroma informacijo javnega značaja, ki jo je prosilec zahteval – 104,
- ali zahtevani dokumenti vsebujejo osebne podatke, katerih razkritje bi pomenilo kršitev varstva osebnih podatkov v skladu z ZVOP-1 – 84,
- ali prosilci zahtevajo informacije oziroma podatke, ki so v skladu z zakonom, ki ureja gospodarske družbe, opredeljeni kot poslovna skrivnost – 55,
- ali gre za kršitev pravil postopka – 46,
- ali je interes javnosti glede razkritja močnejši od javnega interesa ali interesa drugih oseb za omejitev dostopa do zahtevane informacije – 27,
- ali so zahtevane informacije podatki iz dokumenta, ki je bil sestavljen v zvezi z notranjim delovanjem oziroma dejavnostjo organov, in bi njegovo razkritje povzročilo motnje v delovanju oziroma dejavnosti organa – 25,
- ali se zahtevane informacije nanašajo na delo in osebne podatke javnih uslužbencev in funkcionarjev – 23,
- ali gre za delovno področje organa – 20,
- ali je zahtevana informacija zavarovana skladno z zakonom, ki ureja avtorsko pravico – 16,
- ali gre za okoljske podatke – 16,
- odločba, izdana po sodbi Upravnega sodišča RS – 14,
- ali so zahtevane informacije podatki, ki so bili pridobljeni ali sestavljeni zaradi kazenskega pregona ali v zvezi z njim ali zaradi postopka o prekršku, in bi njihovo razkritje škodovalo njegovi izvedbi – 14,
- ali gre za zlorabo pravice po ZDIJZ – 13,
- ali so zahtevane informacije podatki, ki so na podlagi zakona, ki ureja tajne podatke, opredeljeni kot tajni – 13,
- ali zahtevani dokument izpolnjuje pogoje za obstoj informacije javnega značaja v skladu s prvim odstavkom 4. člena ZDIJZ – 13,
- izdaja odločbe v postopku, ko je prosilec zahteval dokument iz postopka javnega naročanja – 12;
- 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 – 8,
- 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

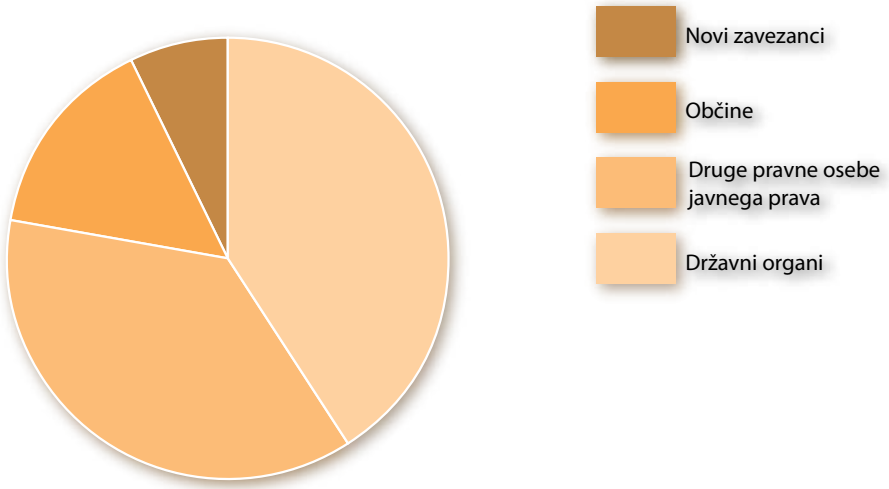
vsebine dokumentov – 7,
- ali so zahtevane informacije podatki, ki so bili pridobljeni ali sestavljeni zaradi upravnega postopka, in bi njihovo razkritje škodovalo njegovi izvedbi – 6,
- ali so zahtevane informacije podatki, ki so bili pridobljeni ali sestavljeni zaradi pravdnega, nepravdnega ali drugega sodnega postopka, in bi njihovo razkritje škodovalo njegovi izvedbi – 4,
- ali gre za kršitev materialnega prava – 4,
- izdaja odločbe v postopku, ko organ prosilcu ni izdal odločbe v zvezi z zahtevanimi dokumenti, ampak mu je posredoval informacije javnega značaja, ki jih prosilec sploh ni zahteval – 4,
- ali gre za podatek, glede katerega zakon določa varovanje tajnosti vira – 4,
- ali gre za ponovno uporabo informacije javnega značaja – 4,
- ali je organ pravilno zaračunal stroške posredovanja informacij javnega značaja – 4,
- ali so zahtevane informacije podatki, katerih razkritje bi pomenilo kršitev zaupnosti davčnega postopka ali davčne tajnosti skladno z zakonom, ki ureja davčni postopek – 3,
- ali gre za podatek, glede katerega je dostop v skladu z zakonom prepovedan ali omejen tudi strankam, udeležencem ali oškodovancem v sodnem, upravnem ali z zakonom določenem nadzornem postopku – 2,
- ali so podatki označeni s stopnjo tajnosti v nasprotju za zakonom, ki ureja tajne podatke – 2,
- ali je organ odstopil zahtevo organu, ki je glede na vsebino zahteve pristojen za njeno reševanje – 2,
- ali gre za proaktivno objavo informacij – 1,
- ali gre za podatek, katerega razkritje bi pomenilo kršitev zaupnosti individualnih podatkov o poročevalskih enotah skladno z zakonom, ki ureja dejavnost državne statistike – 1.

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



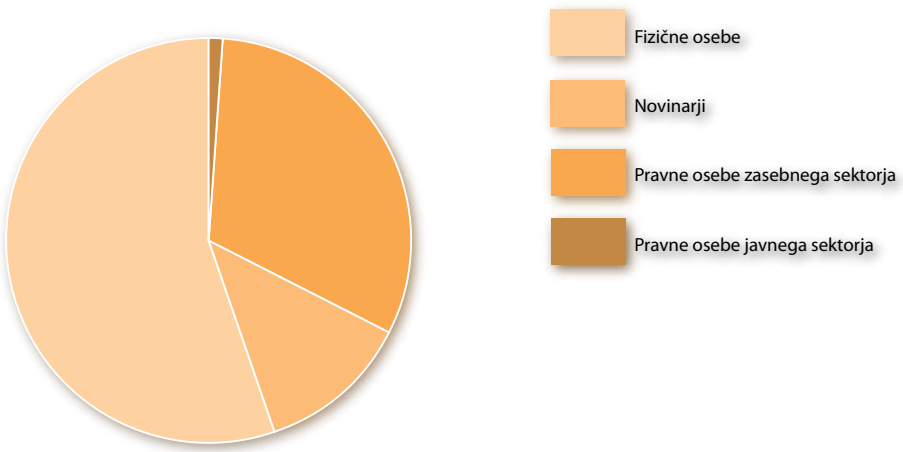
Pritožbe prosilcev zaradi zavrnitve dostopa do informacij javnega značaja, o katerih je Informacijski pooblaščenec odločil z odločbo, so zadevale naslednje skupine zavezancev:
- državni organi 128, od tega ministrstva in organi v sestavi ter upravne enote 106, sodišča, vrhovno državno tožilstvo, državno pravobranilstvo pa 22,
- javni skladi, zavodi, agencije, izvajalci javnih služb, nosilci javnih pooblastil in druge pravne osebe javnega prava 115,
- občine 47,
- poslovni subjekti pod prevladujočim vplivom države, občin ali drugih oseb javnega prava 22.

Slika 6: Pritožbe prosilcev glede na zavezanca.



V 172 primerih so bili prosilci fizične osebe, v 98 primerih so se pritožile pravne osebe zasebnega sektorja, novinarji so se pritožili 38-krat, pravne osebe javnega sektorja pa štirikrat.

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



2.5. Storjeni prekrški po ZDIJZ, ZInfP in ZMed

Leta 2016 je Informacijski pooblaščenec uvedel dva postopka o prekršku:

- zaradi prekrška po drugem odstavku 39. člena ZDIJZ, ker je organ uničil zahtevane informacije javnega značaja,
- zaradi prekrška po 15. členu ZInfP, ker organ kljub temu da mu je Informacijski pooblaščenec z odločbo naložil posredovanje informacij javnega značaja, tega ni storil.

V obeh primerih je bil kršiteljem izrečen opomin.

2.6. Predstavitev najodmevnejših in precedenčnih primerov po področjih

V nadaljevanju je predstavljenih nekaj najzahtevnejših in najzanimivejših odločb iz leta 2016. Razvrščene so po področjih.

2.6.1. Okoljski podatki, varstvo upravnega postopka

Z odločbo št. 090-38/2016/10 z dne 5. 5. 2016 je Informacijski pooblaščenec Ministrstvu za infrastrukturo (organ) naložil, da prosilcu posreduje osnutek Akcijskega načrta za obnovljive vire energije (ANOVE).

Organ je zahtevo prosilca v celoti zavrnil, pri čemer se je skliceval na 7. točko (varstvo upravnega postopka) in 9. točko (dokument v izdelavi) prvega odstavka 6. člena ZDIJZ. Organ je pojasnil, da je zahtevani dokument predmet upravnega postopka celovite presoje vplivov na okolje, ki ga vodi Ministrstvo za okolje in prostor. V tem postopku sodeluje več organov, obravnava pa se tudi večje število dokumentov. Posredovanje zahtevanega dokumenta prosilcu bi po mnenju organa privedlo do zastojev in motenj v upravnem postopku, predčasno razkritje dokumenta v fazi posvetovanja in usklajevanja pa naj bi povzročilo tudi napačno razumevanje njegove vsebine.

Informacijski pooblaščenec v pritožbenem postopku ni sledil obrazložitvi organa, saj je ocenil, da razkritje informacije izvedbi upravnega postopka ne bi škodovalo. Organ namreč ni z ničimer izkazal, da bi posredovanje dokumenta povzročilo zastoje in motnje v postopku, temveč je morebitne zastoje le predvideval. Možnost abstraktnega zastoja v postopku (ki po navedbah organa traja že od leta 2014, in to ne glede na to, da je prosilec zahtevo vložil šele leta 2016) ne predstavlja konkretno grozeče nevarnosti za izvedbo postopka.

Informacijski pooblaščenec tudi ni sledil organu, da gre za dokument, ki je še v postopku izdelave. Te izjeme namreč ni mogoče uporabiti v večfaznih postopkih, v katerih nastajajo različne verzije istega dokumenta. Zgolj dejstvo, da dokument predstavlja eno izmed zaključenih verzij dokumenta, ne pomeni, da gre za dokument, ki je še v postopku izdelave in posvetovanja. Vsaka zaključena različica predloga dokumenta namreč predstavlja samostojno informacijo javnega značaja.

Informacijski pooblaščenec je ugotovil tudi, da zahtevani dokument vsebuje okoljske podatke, ti podatki pa so na podlagi 2. alineje tretjega odstavka 6. člena ZDIJZ absolutno javni. Informacijski pooblaščenec je še pojasnil, da z zapiranjem in netransparentnostjo postopkov ni mogoče pričakovati zaupanja javnosti, ki je v tako pomembnih zadevah, kot je varstvo okolja, še kako pomembno. Le z zaupanjem države v kritično presojo javnosti je mogoče v javnosti ustvariti vtis, da je dejanjem države mogoče zaupati in da se postopki glede varstva okolja vodijo v javnem interesu.

2.6.2. Mediji, javni uslužbenci, delovno področje organa

Z odločbo št. 090-263/2015/7 z dne 7. 1. 2016 je Informacijski pooblaščenec Ekonomski fakulteti v Ljubljani (organ) naložil, da prosilki posreduje seznam 149 avtorskih in podjemnih pogodb, sklenjenih z Dušanom Mramorjem od 1. 1. 2005 do 17. 9. 2015, in avtorsko pogodbo za znanstveno monografijo.

Prosilka je kot novinarka zahtevala odgovore na vprašanja, organ pa je v zavrnilnem odgovoru navedel, da ji vsebine avtorskih in podjemnih pogodb ne more razkriti, saj bi s tem razkril varovane osebne podatke. Avtorske in podjemne pogodbe namreč niso povezane z opravljanjem javne funkcije ali delovnega razmerja javnega uslužbenca, posledično torej ne gre za porabo javnih sredstev. Na ogledu *in camera* je bilo ugotovljeno še, da ima organ sklenjene pogodbe le z Dušanom Mramorjem kot fizično osebo.

Informacijski pooblaščenec v pritožbenem postopku ni sledil obrazložitvi organa, saj je pri pregledu pogodb ugotovil, da se nanašajo na delovna področja, ki spadajo pod izvajanje javne službe organa, oziroma na dejavnosti, ki so opredeljene kot predavanja na izrednem študiju, seminarjih in tečajih, priprava učbenikov in študijskega gradiva, priprava študijskih programov,

predavanja in seminarji v okviru rednega študijskega programa, vaje, izpiti, mentorstvo, izvedba in pregled izpitov itd. Informacijski pooblaščenec je v obrazložitvi pojasnil, da navedene dejavnosti nedvomno sodijo v javno službo. Zgolj dejstvo, da določena dejavnost organa ni financirana neposredno iz proračuna, kar je zatrjeval organ, še ne pomeni, da ne gre za javno službo.

Informacijski pooblaščenec tudi ni sledil obrazložitvi organa, ki se je skliceval na izjemo varstva osebnih podatkov, ki jo določa 3. točka prvega odstavka 6. člena ZDIJZ. Navedeni podatki namreč izkazujejo porabo javnih sredstev, zato osebni podatki prejemnikov avtorskih honorarjev in izplačil po podjemnih pogodbah uživajo znatno zmanjšano stopnjo varovanja. Hkrati je Informacijski pooblaščenec ugotovil, da so se po avtorskih in podjemnih pogodbah opravljala dela, ki sodijo v okvir delovnih obveznosti iz rednega delovnega razmerja javnega uslužbenca. Na podlagi 1. alineje tretjega odstavka 6. člena pa se dostop do informacij ne glede na izjemo varstva osebnih podatkov dovoli, če gre za podatke o porabi javnih sredstev ali podatke, povezane z opravljanjem javne funkcije ali delovnega razmerja javnega uslužbenca.

Informacijski pooblaščenec je izvedel tudi test interesa javnosti in odločil, da je javni interes za razkritje imena in priimka prejemnika honorarja ter višine bruto honorarja močnejši od interesa posameznika, da se javnost ne seznani z navedenimi osebnimi podatki. V konkretnem primeru so zahtevane informacije namreč potrebne zaradi zagotavljanja večje odgovornosti pri odločanju o porabi javnih sredstev ter zaradi možnosti informiranega sodelovanja javnosti v javni razpravi o tej pomembni temi.

2.6.3. Dokument v izdelavi

Z odločbo št. 090-23/2016/5 z dne 23. 3. 2016 je Informacijski pooblaščenec družbi Nigrad, d. d., (organ) naložil, da prosilcu posreduje delovne osnutke gradiva za javno predstavitev projekta odvajanja komunalnih in padavinskih voda.

Organ je zahtevo prosilca v celoti zavrnil, pri čemer se je skliceval na 9. točko prvega odstavka 6. člena ZDIJZ (izjema dokument v izdelavi). Organ je pojasnil, da se zahteva prosilca nanaša na gradivo, ki je še v postopku izdelave, prav tako je še predmet posvetovanja skupnega sestanka predstavnikov javnih podjetij in vodij svetniških skupin mestnega sveta Mestne občine Maribor. Razkritje takšnih podatkov naj bi po mnenju organa povzročilo napačno razumevanje njegove vsebine.

Informacijski pooblaščenec je presojal, ali dokument izpolnjuje vse tri pogoje za navedeno izjemo, in odločil, da organ v odločbi ni izkazal, da bi in kako bi razkritje dokumenta povzročilo napačno razumevanje njegove vsebine. Povsem jasno je, da gre za delovno gradivo, ki ni zavezujoče, in da vsebuje pripombe, ki bodo še predmet razprave, zaradi česar je lahko vsakomur jasno, da je zadeva vsebinsko odprta in da lahko na vsaki točki pride do sprememb ali dopolnitev.

Informacijski pooblaščenec je ugotovil tudi, da je bilo gradivo tretjim osebam že razkrito, pri čemer organ ni dokazal, da bi mu zaradi razkritja nastala kakršna koli škoda oziroma da bi bilo razumevanje gradiva sedaj v čemer koli problematično.

2.6.4. Poslovni subjekt pod prevladujočim vplivom

Z odločbo št. 0902-14/2016/4 z dne 20. 7.2016 je Informacijski pooblaščenec odločil, da se pogodba, sklenjena med UPS, d. o. o., in Pošto Slovenija (organ), ne nanaša na izvajanje univerzalne poštne storitve niti ne izpolnjuje pogojev za informacijo javnega značaja po 4.a členu ZDIJZ, zato je pritožbo prosilca zavrnil. Informacijski pooblaščenec je odločanje o pogodbi, sklenjeni z GLS, d. o. o., in o pogodbi, sklenjeni z UPS Adria (s) Ekspres, vrnil v ponovno odločanje organu.

Organ je v odločbi navedel, da je zavezanec za posredovanje informacij javnega značaja zgolj v delu, kjer ima podeljeno dovoljenje za izvajanje univerzalne poštne storitve, v preostalem delu pa v okviru, kot zavezuje poslovne subjekte pod prevladujočim vplivom. Zahtevane informacije se deloma nanašajo na univerzalne poštne storitve, deloma na druge poštne storitve in deloma na komercialne storitve organa, zato v celoti ne predstavljajo informacij javnega značaja.

Informacijski pooblaščenec je sledil organu v delu, ki se nanaša na pogodbo, sklenjeno z družbo UPS, d. o. o. Storitve, ki se opravljajo na podlagi omenjene pogodbe, namreč ne sodijo

v univerzalno poštno storitev, prav tako pa po vsebini ne gre za pogodbe, ki bi se nanašale na pridobivanje, razpolaganje ali upravljanje s stvarnim premoženjem poslovnega subjekta ali na izdatke poslovnega subjekta za naročilo blaga, gradenj, agentskih, svetovalnih ali drugih storitev ter sponzorskih, donatorskih in avtorskih pogodb in drugih pravnih poslov, s katerimi se dosega enak učinek. Omenjena pogodba zato ne predstavlja informacije javnega značaja.

Informacijski pooblaščenec je v delu, ki se nanaša na pogodbi, sklenjeni z družbo GLS in UPS Adria (s) Ekspres, ugotovil, da organ v tem delu ni v celoti ugotovil dejanskega stanja, ki se nanaša na vprašanje univerzalne poštne storitve, v postopek pa tudi ni pritegnil stranskih udeležencev. Informacijski pooblaščenec je v tem delu odločbo organa odpravil in organu naložil, da se v ponovnem postopku jasno opredeli do tega, kateri deli pogodb se nanašajo na izvajanje univerzalne poštne storitve in posledično sodijo v delovno področje organa v smislu opravljanja javnopravnih nalog iz 4. člena ZDIJZ.

2.6.5. Poslovna skrivnost, poraba javnih sredstev

Informacijski pooblaščenec je z odločbo št. 090-148/2016/5 z dne 22. 7. 2016 odpravil zavrnilni odgovor Psihiatrične bolnišnice Begunje (organ) in ji naložil, da novinarki posreduje podatke o proizvajalcih zdravil in medicinskih pripomočkov, ki jih je leta 2015 in v prvem trimesečju leta 2016 dobavilo podjetje Sanolabor, d. d.

Organ je prosilki zahtevane podatke posredoval, vendar je prekril kataloške številke in podatke o proizvajalcih, saj naj bi ti podatki po stališču organa predstavljali poslovno skrivnost.

Informacijski pooblaščenec stališču organa ni sledil. Družba Sanolabor, d. d., je omenjene podatke v svojih notranjih aktih sicer označila kot poslovno skrivnost, vendar je v obravnavanem primeru treba upoštevati tudi določbo tretjega odstavka 39. člena Zakona o gospodarskih družbah[21], ki izrecno določa, da se za poslovno skrivnost ne morejo določiti podatki, ki so po zakonu javni, ali podatki o kršitvah zakona ali dobrih poslovnih običajev. Ker je šlo v konkretnem primeru za podatke o porabi javnih sredstev, je bilo treba na podlagi določbe 1. alineje tretjega odstavka 6. člena ZDIJZ dostop do zahtevanih informacij dovoliti.

2.6.6. Okoljski podatki

Z dopolnilno odločbo št. 090-120/2016/10 z dne 6. 9. 2016 je Informacijski pooblaščenec zavrnil pritožbo prosilke, ki se je nanašala na podatke o vodostaju reke Drave, in sicer zaradi neobstoja zahtevanega dokumenta.

Agencija RS za okolje (organ) je pri odločanju o zahtevi prosilke spregledala, da prosilko zanimajo tudi podatki o vodostaju, in ne le podatki o pretokih reke Drave na območju hidroelektrarn. Informacijski pooblaščenec je v pritožbenem postopku ugotovil, da organ ne razpolaga s podatki o vodostaju reke Drave. Teh podatkov namreč ne pridobiva niti od družbe DEM, d. o . o., ki v okviru gospodarske javne službe upravlja z vodami, niti iz drugega vira. Informacijski pooblaščenec je zato zaključil, da je bila odločitev organa pravilna, vendar napačno obrazložena, zato je pritožbo zavrnil na podlagi tretjega odstavka 248. člena ZUP[22].

2.6.7. Tajni podatki

Z odločbo št. 090-160/2016/3 z dne 27. 10. 2016 je Informacijski pooblaščenec Zavodu RS za blagovne rezerve (organ) naložil umik stopnje tajnosti INTERNO ter posredovanje naročilnic in prodajnih pogodb.

Organ je ocenil, da bi bili z razkritjem pogodb razkriti podatki o časovni dinamiki nabav varnostne žične ograje, s čimer bi bila ogrožena izvedba javnega naročila, delovanje in izvajanje s strani Vlade RS določenih nalog, ogrožena bi bila tudi varnost osebja dobavitelja ali njegovih sodelavcev. Posledično bi bilo ogroženo uresničevanje ciljev Vlade RS za učinkovito regulacijo migrantskih tokov na državni meji, ki pa je nujna za zavarovanje bistvenih varnostnih interesov Republike Slovenije, njenega prebivalstva ter njegovega premoženja.

---

21 Uradni list RS, št. 65/2009 – uradno prečiščeno besedilo 3, s spremembami; v nadaljevanju ZGD-1.

22 Uradni list RS, št. 24/2006 – uradno prečiščeno besedilo 2, s spremembami; v nadaljevanju ZUP.

Informacijski pooblaščenec obrazložitvi organa ni sledil. Čeprav so dokumenti izpolnjevali tako materialni kot formalni kriterij za tajne podatke, je Informacijski pooblaščenec ob tehtanju vseh argumentov sprejel zaključek, da je treba dostop do pogodb dovoliti. Prosilec je namreč zahteval le podatke iz pogodb, ki so bile v celoti izvršene in po katerih je izbrani ponudnik tudi že prejel plačila. Zneski, ki jih je prejel dobavitelj, so že bili javno znani, prav tako ni sporno dejstvo, da je bila žična ograja nabavljena in postavljena na državni meji.

Informacijski pooblaščenec je odločil, da je v javnem interesu, da se javnost celovito seznani s podatki o porabi javnih sredstev v zvezi z nabavo in postavitvijo mejne ograje. Škoda, ki bi s tem nastala organu, namreč ni večja od interesa javnosti, da se celovito seznani z zahtevanimi informacijami. V interesu javnosti je namreč, da v demokratični družbi razpolaga z nepristranskimi in objektivnimi informacijami, na podlagi katerih se lahko informirano odloča o javnopravnih zadevah in s tem tudi nadzoruje porabo javnih sredstev.

2.6.8. Tajnost vira

Prosilec je pri Inšpektoratu za okolje in prostor (organ) zahteval dostop do kopije anonimne prijave »črne gradnje«. Organ je zahtevo zavrnil s sklicevanjem na izjemo tajnosti vira prijave po 5.a členu ZDIJZ. Po stališču organa izjema tajnosti vira prijave varuje tako prijavitelja kot tudi vsebino prijave.

Informacijski pooblaščenec je z odločbo št. 090-1/2016 z dne 11. 2. 2016 odločil, da je organ preširoko tolmačil varovanje tajnosti vira, kot ga ureja Zakon o inšpekcijskem nadzoru[23] v povezavi s 5.a členom ZDIJZ, in odločil, da tajnost vira prijave varuje zgolj prijaviteljevo zasebnost, ne pa tudi vsebino prijave. Skladno s prvim odstavkom 16. člena ZIN so inšpektorji dolžni varovati vse vrste tajnosti, s katerimi se seznanijo pri svojem delu (npr. poslovne skrivnosti), drugi odstavek pa ureja tajnost vira prijave in drugih informacij. Informacijski pooblaščenec je zavzel stališče, da tajnost vira obsega zgolj varstvo prijaviteljeve zasebnosti, sama vsebina prijave pa je lahko varovana z drugo kategorijo varovanih informacij v skladu s prvim odstavkom 16. člena ZIN (npr. če je prijava poslovna skrivnost). Organ se je skliceval tudi na dve sodbi (na sodbi upravnega in vrhovnega sodišča, št. U 313/2004 in št. X Ips 775/2006), v katerih pa se ni odločalo o zadevah s področja dostopa do informacij javnega značaja, zato za konkretni primer nista bili relevantni. V skladu z zgoraj navedenim je Informacijski pooblaščenec pritožbi ugodil in omogočil dostop do anonimne prijave.

2.6.9. Mediji, varstvo kazenskega pregona

Novinarka je od Mestne občine Maribor (organ) zahtevala revizijsko poročilo o opravljeni izredni reviziji pravilnosti poslovanja v javnem zavodu Športni objekti Maribor za leto 2014. Organ je zahtevo zavrnil. Glede zahtevanega poročila je bilo pozvano tudi Okrožno državno tožilstvo v Mariboru (tožilstvo). Izkazalo se je, da je zahtevano poročilo del gradiva iz predkazenskega postopka, ki je bilo pomembno za izvedbo kazenskega pregona storilca. Organ je dostop posledično zavrnil na podlagi 6. točke prvega odstavka 6. člena ZDIJZ.

Informacijski pooblaščenec je v svoji odločbi št. 090-45/2016 z dne 23. 3. 2016 potrdil odločitev organa prve stopnje z utemeljitvijo, da izjema varstva kazenskega pregona po 6. točki prvega odstavka 6. člena ZDIJZ obsega tudi predkazenski postopek (vse ukrepe za odkrivanje kaznivih dejanj in njihovih storilcev). Po pojasnilu tožilstva je revizijsko poročilo sestavni del gradiva v predkazenskem postopku, ki ga ni dopustno razkriti niti v posameznih delih. Informacijski pooblaščenec je ocenil še, da je tožilstvo v zadostni meri argumentiralo škodljiv učinek razkritja zahtevanega revizijskega poročila. Z razkritjem le-tega bi namreč nastala škoda za izvedbo konkretnega (pred)kazenskega postopka, ki je večja od pravice javnosti, da se seznani z vsebino zahtevanega dokumenta. Ker sta bila kumulativno izpolnjena oba pogoja, ki ju za obstoj izjeme po 6. točki prvega odstavka 6. člena določa ZDIJZ, je Informacijski pooblaščenec pritožbo novinarke zavrnil kot neutemeljeno.

[23] Uradni list RS, št. 43/2007– uradno prečiščeno besedilo 1 in 40/2014; v nadaljevanju ZIN.

2.6.10. Ali je organ zavezanec?

Novinar Vala 202 je Nuklearno elektrarno Krško, d. o. o., (NEK) prosil za podatek o tem, koliko bi stale vse varnostne nadgradnje, ki so bile predvidene v nacionalnem akcijskem načrtu po nesreči v Fukušimi, koliko denarja je bilo za nadgradnje že porabljenega, koliko ga bo še treba vložiti in kdaj bodo nadgradnje predvideno realizirane. NEK je odgovorila, vendar se je prosilec zoper odgovor pritožil, saj ni prejel odgovora na vprašanje o predvidenih in realiziranih zneskih za nadgradnje.

Informacijski pooblaščenec je v pritožbenem postopku ugotovil, da družba NEK ni vpisana v register zavezancev. Pravni status NEK se je spremenil z ratifikacijo mednarodne pogodbe med Republiko Slovenijo in Republiko Hrvaško, ki je NEK preoblikovala v družbo z omejeno odgovornostjo. Po tej spremembi NEK ne sodi več med osebe javnega prava, glede na registrirano dejavnost družbe pa tudi ne izvaja javne službe in ni nosilec javnega pooblastila. Informacijski pooblaščenec je ugotovil, da NEK ne sodi niti med zavezance po prvem odstavku 1. člena ZDIJZ (t. i. organe) niti med zavezance po 1.a členu ZDIJZ kot subjekt pod prevladujočim vplivom oseb javnega prava. Iz statusne ureditve NEK namreč izhaja ureditev razmerij po paritetnem načelu, ki pomeni »usklajenost, sorazmerje« pogodbenih strank, zato v danem primeru ni mogoče zaključiti, da je NEK pod prevladujočim vplivom oseb javnega prava. Informacijski pooblaščenec je ugotovil, da Republika Slovenija nima v lasti več kot 50 % poslovnega deleža NEK, saj je z ratificirano mednarodno pogodbo izrecno dogovorjeno, da ima ELES GEN, d. o. o., Ljubljana točno 50-odstotni poslovni delež, kar ne predstavlja »večinskega deleža«. Republika Slovenija v NEK prav tako nima pravice nadzora večine niti ne imenuje več kot polovico članov poslovodnega ali nadzornega organa, saj so organi družbe sestavljeni paritetno, torej natančno na polovico po pogodbenih strankah. Navedeno pomeni, da Republika Slovenija prek ELES GEN, d. o. o., Ljubljana, ne more izvajati prevladujočega vpliva, kot ga predvideva ureditev po ZDIJZ. Informacijski pooblaščenec je zato zaključil, da NEK ni zavezanec za posredovanje informacij javnega značaja (odločba št. 0902-8/2016 z dne 9. 5. 2016).

2.6.11. Notranje delovanje organa, poslovna skrivnost

Novinar je od Mestne občine Maribor (organ) zahteval sporazum, sklenjen med organom in tujim potencialnim investitorjem, za nakup občinskih nepremičnin. Organ je zahtevo zavrnil z utemeljitvijo, da bi razkritje povzročilo motenje v njegovem delovanju, ki bi se kazale v izgubi zaupanja potencialnega investitorja, kar bi po mnenju organa vplivalo na uspeh prodaje. Ker je investitor v preteklosti že vlagal v projekte občine, je obstajala na strani organa tudi skrb, da bi to negativno vplivalo na dobre poslovne odnose (in torej prihodnje projekte), kar naj bi se kazalo tudi v izgubi poslovnih priložnosti in posledično v izgubi dobička.

Informacijski pooblaščenec je ugotovil (odločba št. 090-301/2015 z dne 13. 5. 2016), da izjema notranjega delovanja po 11. točki prvega odstavka 6. člena ZDIJZ, ki jo je zatrjeval organ, ni podana, ker ne gre za dokument v zvezi z notranjim delovanjem organa, ampak za izrazito zunanje delovanje. Dokument je bil sklenjen v tujini kot izkaz neposredne pripravljenosti za sodelovanje s potencialnimi investitorji. Razkritje tudi ne bi moglo vplivati na postopek prodaje občinskih nepremičnin. Postopek prodaje občinskega stvarnega premoženja je namreč strogo javnopravno reguliran in v skladu s področno ureditvijo tudi poudarjeno transparenten, zahtevani dokument pa ni akt, ki bi bil predviden s postopkom prodaje. Informacijski pooblaščenec je tudi ugotovil, da dokument izpolnjuje subjektivni kriterij za obstoj poslovne skrivnosti, saj 6. člen zahtevanega sporazuma ustreza kriterijem »pisnega sklepa« iz prvega odstavka 39. člena ZGD-1. Kljub temu pa je Informacijski pooblaščenec presodil, da nekatere informacije v sporazumu ne morejo biti določene za poslovno skrivnost, saj gre za podatke, ki so v povezavi s porabo javnih sredstev in delovnim razmerjem javnih uslužbencev oziroma z opravljanjem javne funkcije, ki so po zakonu javni. Informacijski pooblaščenec je odločil, da so bistvene sestavine sporazuma (namen sporazuma in dogovori strank) podatki v zvezi s porabo javnih sredstev. Šlo je namreč za namero o prodaji/nakupu občinskih nepremičnin, v kateri sta stranki izrazili interes in opredelili nepremičnine s parcelnimi številkami. Za zagotovitev gospodarnega razpolaganja z javnim nepremičnim premoženjem je namreč na tem področju še posebej poudarjena potreba po transparentnem upravljanju, ki omogoča javnosti, da nadzira delo oblasti.

2.6.12. Ponovna uporaba

Informacijski pooblaščenec je reševal pritožbo prosilca zoper odločbo Geodetske uprave Republike Slovenije (organ) o ponovni uporabi informacij javnega značaja in zoper račun, ki je bil izdan na podlagi te odločbe. V postopku je Informacijski pooblaščenec ugotovil, da je sporno, ali je prosilec sploh vložil zahtevo za ponovno uporabo in kaj je zahteval.

Prosilec je namreč pristopil k organu z zahtevo, vloženo na predpripravljenem obrazcu organa, ki omogoča dostop do »storitev spletnih servisov za namene ponovne uporabe informacij javnega značaja«. Na podlagi te vloge je bila dne 15. 12. 2015 sklenjena Pogodba o prenosu in uporabi elektronske storitve prevzemanja geodetskih podatkov (v nadaljevanju pogodba). Sklepanje pogodbe in ceno navedene storitve spletnih servisov ureja področni pravilnik[24]. Pozneje, dne 12. 4. 2016, je organ na podlagi ZDIJZ izdal odločbo o ponovni uporabi podatkov in račun za plačilo cene ponovne uporabe podatkov, ki ju je prosilec izpodbijal v pritožbenem postopku pred Informacijskim pooblaščencem.

Informacijski pooblaščenec je ugotovil, da za izdajo izpodbijane odločbe nikoli ni bila vložena pisna zahteva, zato je organ z izdajo odločbe brez zahteve storil bistveno kršitev pravil postopka. Niti zahteva, ki je po vsebini predstavljala naročilo storitev spletnega servisa, niti pogodba o zagotavljanju te storitve nista predstavljali vloge, iz katere bi bilo mogoče sklepati, da prosilec želi pred organom začeti upravni postopek za ponovno uporabo informacij javnega značaja. Glede izdanega računa pa je Informacijski pooblaščenec ugotovil, da je organ v ceno ponovne uporabe vračunal tudi stroške zagotavljanja spletnega servisa v skladu s prej omenjenim pravilnikom, ki pa jih ZDIJZ ne predvideva.

Posledično je Informacijski pooblaščenec zadevo vrnil v ponovno odločanje organu prve stopnje (odločba št. 090-105/2016 z dne 22. 6. 2016), pri čemer je slednjemu naložil, naj najprej razčisti vprašanje, kaj je prosilec zahteval (storitev spletnega servisa ali ponovno uporabo informacij javnega značaja). Ob tem je opozoril, da so pojasnila na spletni strani organa za dostop do storitev spletnih servisov za namene ponovne uporabe informacij javnega značaja zavajajoča, saj neuke stranke zlahka »pomešajo« namen in učinek obeh institutov. Informacijski pooblaščenec je v odločbi poudaril, da mora organ, ko zahtevo za ponovno uporabo vsebinsko obravnava, upoštevati ureditev na področju dostopa do informacij javnega značaja, zato v ceno ponovne uporabe ne sme vračunati tudi cene storitev spletnega servisa. Dodal je še, da o pravicah prosilca, ki jih določa ZDIJZ, organ ne sme sklepati obligacijsko-pravnih razmerij. Končno se je Informacijski pooblaščenec opredelil tudi do pomena načela prepovedi diskriminacije iz 36.a čelna ZDIJZ, pri čemer je izpostavil zlasti, da če organ uporablja informacije za dejavnost, ki ni del njegovih uradnih nalog, veljajo zanj enaka cena in drugi pogoji glede ponovne uporabe kot za druge osebe. Ponovna uporaba informacij mora biti po enaki ceni in pod enakimi pogoji dovoljena in omogočena vsem prosilcem oziroma uporabnikom, tudi če je tak uporabnik organ sam.

2.6.13. Tajni podatki, umik stopnje tajnosti

Prosilec je od Ministrstva za notranje zadeve (organ) zahteval poročilo Direktorata za policijo in druge varnostne naloge (v nadaljevanju DPDVN) glede primera informacijskih vdorov v računalniške sisteme, v katerega naj bi bila vpletena slovenska policija. Primer je v medijih sprožil

[24] Pravilnik o pogojih in načinu računalniškega dostopa do podatkov iz evidenc in zbirk geodetskih podatkov (Uradni list RS, št. 25/2008 in 10/2011), ki je sprejet na podlagi Zakona o infrastrukturi za prostorske informacije (Uradni list RS, št. 8/2010 in 84/2015).

širšo razpravo[25], obravnaval pa ga je tudi Državni zbor RS[26]. Zahtevano poročilo je bilo označeno s stopnjo tajnosti interno, zato je organ na podlagi izjeme varstva tajnih podatkov dostop zavrnil (1. točka prvega odstavka 6. člena ZDIJZ). Prosilec se je v pritožbi skliceval na prevladujoč interes javnosti za razkritje, saj naj bi iz dokumenta izhajali grobi posegi policije v komunikacijsko zasebnost posameznikov, zato naj bi bilo razkritje dokumenta (vsaj glede nepravilnosti pri delu policije) v prevladujočem interesu javnosti[27].

Informacijski pooblaščenec je potrdil ugotovitev organa, da gre za tajne podatke (izpolnjeni so vsi kriteriji za določitev podatkov za tajne). Hkrati pa je bil podan tudi prevladujoč interes javnosti za razkritje uvoda in zaključka zahtevanega poročila, iz katerega izhajajo sklepne ugotovitve in predvideni ukrepi iz opravljenega nadzora s strani DPDVN. Informacijski pooblaščenec je za utemeljitev prevladujočega interesa javnosti upošteval, da je policija organ z represivnimi pooblastili, ki je poudarjeno zavezana k varovanju javne varnosti in spoštovanju človekovih pravic ter temeljnih svoboščin. V velikem interesu javnosti je torej, da je seznanjena z relevantnimi informacijami glede dela policije, še zlasti, kadar te kažejo na domnevno kršenje človekovih pravic. Prav tako je upošteval, da se je okrog tematike odvijala širša javna razprava, in presodil, da bi lahko razkritje pomembno dodalo k seznanjenosti javnosti z relevantnimi informacijami. Informacijski pooblaščenec je navsezadnje upošteval tudi aktualen javni diskurz glede predvidenih sprememb na področju širitve policijskih pooblastil; razkritje zahtevane informacije bi lahko tvorno prispevalo k temu diskurzu. Upoštevaje navedeno je Informacijski pooblaščenec odločil, da mora organ umakniti stopnjo tajnosti interno iz uvoda in zaključka zahtevanega dokumenta in ga v tem delu posredovati prosilcu. Ostali deli dokumenta, ki vsebujejo podatke o osebah, taktiko ter metodiko dela policije z informatorji in viri, katerih razkritje bi ogrozilo varnost oseb in delo policije, pa po odločitvi Informacijskega pooblaščenca upravičeno sodijo med tajne podatke. V tem delu je Informacijski pooblaščenec torej presodil (odločba 090-213/2016 z dne 10. 11. 2016), da interes države za zavarovanje zaupnosti informacije prevlada nad interesom javnosti za razkritje.

2.6.14. Poslovna skrivnost, avtorsko delo

Prosilka je od komunalnega podjetja (organ) zahtevala dostop do študije »Pravilno ravnanje in izvajanje pogrebnih svečanosti glede na različne veroizpovedi, običaje in tradicije, in sicer za pripadnike judovske, pravoslavne in muslimanske veroizpovedi«, ki jo je organ pridobil po javnem naročilu. Organ je v času izdaje odločbe prve stopnje pogrebne storitve opravljal kot javno službo. Dostop do študije je organ zavrnil na podlagi izjeme poslovne skrivnosti (2. točka prvega odstavka 6. člena ZDIJZ). Organ je omenjeno študijo sam označil za svojo poslovno skrivnost. V utemeljitvi je navedel, da je študijo naročil zaradi zagotavljanja višje kakovosti storitev pogrebnih dejavnosti, ki bo po pričakovani spremembi področne zakonodaje postala tržna dejavnost. Organ je študijo tudi plačal iz sredstev, ki jih je pridobil z izvajanjem (dodatnih) tržnih dejavnosti.

Informacijski pooblaščenec je v postopku poudaril, da podatki, ki so v zvezi z izvajanjem javne službe, predstavljajo informacije, ki so javne po zakonu in zato ne morejo biti določene kot poslovne skrivnosti (tretji odstavek 39. člena ZGD-1). V skladu z ureditvijo dostopa do informacij

[25] Glej objave: »Policija: Ornigove izjave, da naj bi vodstvo vedelo za vdore, so zavajajoče« (rtvslo.si, 15. 6. 2016); »Vdor v elektronsko komunikacijo: Kako želi policija primer Ornig pomesti pod preprogo« (dnevnik.si, 3. 6. 2016); »Hekal po naročilu?« (vecer.si, 15. 6. 2016); »Odkril luknjo v policijskih frekvencah, sedaj v preiskavi« (zurnal24.si, 30. 4. 2016), »Izpoved Dejana Orniga, informatorja, ki je za policijo vdiral v zasebno komunikacijo posameznikov« (podcrto.si, 11. 6. 2016).

[26] Komisija za nadzor obveščevalnih in varnostnih služb, 21. nujna seja, dne 17. 3. 2016

[27] Dostop do zahtevane informacije se dovoli, ne glede na obstoj izjem, če je javni interes glede razkritja močnejši od javnega interesa ali interesa drugih oseb za omejitev dostopa do zahtevane informacije. Izjema velja za podatke, ki so v skladu z zakonom, ki ureja tajne podatke, označeni z najvišjima dvema stopnjama tajnosti (1. alineja drugega odstavka 6. člena ZDIJZ). V konkretnem primeru je bil zahtevani dokument označen s stopnjo tajnosti interno, kar ne sodi med najvišji dve kategoriji tajnosti podatkov, zato je bilo v konkretnem primeru dopustno uporabiti institut prevladujočega interesa javnosti za razkritje dokumenta.

javnega značaja namreč med absolutno javne podatke (ne glede na morebiten obstoj izjeme poslovne skrivnosti) sodijo tudi »informacije v zvezi z izvajanjem javne funkcije« (1. alineja tretjega odstavka 6. člena ZDIJZ). Izvajanje javne funkcije se v skladu s prakso Upravnega sodišča RS in Informacijskega pooblaščenca tolmači širše in zajema tudi izvajanje javne službe. Posledično je Informacijski pooblaščenec odločil (odločba št. 090-229/2016 z dne 10. 11. 2016), da zahtevana študija nedvomno predstavlja podatek v zvezi z izvajanjem javne službe (ki jo je organ kot javno službo izvajal še v času vložitve zahteve), zato študija ne more biti določena kot poslovna skrivnost. Na navedeno pa tudi ne more vplivati dejstvo, da je bila študija plačana iz sredstev tržne dejavnosti, saj vir plačila ne spreminja narave izvajanja pogrebne dejavnosti.

V konkretnem primeru se je odprlo tudi vprašanje avtorskopravnega varstva študije. Organ namreč ni razpolagal s pravico do reproduciranja avtorskega dela, zato je Informacijski pooblaščenec v skladu z ZDIJZ organu naložil, naj prosilki omogoči seznanitev s študijo v obliki vpogleda.

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

Informacijski pooblaščenec je na področju dostopa do informacij javnega značaja leta 2016 prejel 514 pritožb. Od tega je prejel 316 pritožb zoper zavrnilne odločbe ter 198 pritožb zoper molk organa. Prosilci in zavezanci so se na Informacijskega pooblaščenca v 308 primerih obrnili s prošnjo za mnenje oziroma pojasnilo. Obravnavanih je bilo torej 822 zadev.

Glede na podane številke Informacijski pooblaščenec pozdravlja dejstvo, da se je bistveno zmanjšalo število pritožb zaradi t. i. molka organa. Slednje je leta 2016 v primerjavi z letom poprej padlo za 37 %, povečalo pa se je število prošenj za mnenja in pojasnila. Navedeno kaže, da so bili zavezanci leta 2016 bolj aktivni in odzivni kot leta 2015 in da so se z vprašanji večkrat obrnili na Informacijskega pooblaščenca tudi izven pritožbenega postopka.

Število pritožb zoper izdane odločbe je leta 2016 ostalo na primerljivi ravni z letom pred tem, je pa Informacijski pooblaščenec v teh postopkih vnovič izdal več odločb kot v vseh letih svojega delovanja. Tudi leta 2016 se je Informacijski pooblaščenec trudil, da je pritožbene zadeve na tem področju reševal hitro in s kar najmanjšo zamudo za prosilce. Povprečen čas reševanja pritožbenih zadev zoper zavrnilne odločbe, v katerih je bil potreben poseben ugotovitveni postopek, je tako znašal 47 dni, kar je manj kot leta 2015, kot je za reševanje v povprečju potreboval 62 dni. Leta 2016 je Informacijski pooblaščenec zoper odločitve poslovnih subjektov pod prevladujočim vplivom obravnaval 22 pritožb, kar je nekaj več kot leta 2015, ko je bilo takih pritožb 15. Kljub temu velja poudariti, da gre za izjemno nizek odstotek vseh pritožbenih zadev (4 %), na podlagi česar je mogoče zaključiti, da se je stanje po uveljavitvi novele ZDIJZ-C v praksi glede novih zavezancev »stabiliziralo« in da iz podatkov o pritožbenih zadevah zoper poslovne subjekte pod prevladujočim vplivom ne izhaja, da bi bili ti z izvajanjem tega zakona prekomerno obremenjeni.

Kot izhaja iz statističnih podatkov, je bilo največ pritožb zoper zavrnilne odločbe vloženih zoper državne organe (med katere spadajo vsi državni organi, ministrstva in organi v sestavi, upravne enote, sodišča, vrhovno državno tožilstvo in državno pravobranilstvo), in sicer so se prosilci v teh primerih pritožili 128 (leta 2015 je bilo takih pritožb 156). Seveda pri tem velja opozoriti, da gre za najširšo skupino zavezancev, pri katerih je v praksi vloženih tudi največ zahtev za dostop do informacij javnega značaja.

Ob tem Informacijski pooblaščenec, podobno kot lani, znova ocenjuje, da je treba (še) več napora vložiti v aktivnejše usposabljanje vseh zavezancev za uporabo zakona v praksi. Informacijski pooblaščenec je bil aktiven tudi na tem področju: v okviru priprave na uporabo novele ZDIJZ-E, ki

se je začela uporabljati maja 2016, je sodeloval na več izobraževalnih delavnicah za zavezance, ki jih je organiziralo Ministrstvo za javno upravo.

Leta 2016 je Informacijski pooblaščenec v pritožbenih postopkih obravnaval več vsebinsko pomembnih zadev. Z vidika izjem, na katere so se sklicevali zavezanci v postopkih, velja opozoriti na zanimiv podatek: največ pritožbenih primerov se ni nanašalo na izjemo varstva osebnih podatkov (kot prej več let zapored), ampak na vprašanje, ali zahtevana informacija sploh obstaja. To je verjetno tudi posledica dejstva, da prosilci v času hitrega razvoja informacijske tehnologije od zavezancev pričakujejo, da bodo ti razpolagali z različnimi statističnimi podatki in z možnostjo iskanja po informacijah po različnih zahtevanih kriterijih, v praksi pa se pogosto izkaže, da zavezanec za potrebe svojih delovnih procesov informacij ne vodi v takšni vsebini, na način ali v obliki, kot to zahteva prosilec. Ker zavezanci za potrebe prosilca po ZDIJZ niso dolžni analizirati podatkov, pripravljati izvlečkov, povzetkov, pojasnil in odgovorov na vprašanja, se postopek zaključi z ugotovitvijo, da zahtevana informacija ne obstaja in posledično z izdajo zavrnilne odločbe. Informacijski pooblaščenec ob ugotovitvi, da zahtevana informacija ne obstaja, zavezanec pa je ni dolžan ustvariti, večino tovrstnih pritožb kot neutemeljene zavrne. Na to kaže tudi skupen delež zavrnjenih pritožb, ki je leta 2016 narastel (leta 2015 je bilo zavrnjenih pritožb 40 %, leta 2016 pa 44 %).

Podatki kažejo, da je struktura prosilcev, ki so vložili pritožbe, ostala bolj ali manj enaka kot leto pred tem. Največ pritožnikov je imelo status posameznikov – fizičnih oseb (172), sledili so prosilci – pravne osebe zasebnega prava (98) ter novinarji in medijske hiše (38). Zanimiv je podatek, da so kot prosilci v pritožbenih postopkih pred Informacijskim pooblaščencem nastopale tudi pravne osebe javnega prava (4).

Informacijski pooblaščenec je tudi v tem letu, kot že leto prej, zaznal porast pritožbenih zadev na področju dostopa do okoljskih informacij. Leta 2013 je obravnaval le eno zadevo s tega področja, leta 2014 štiri in leta 2015 osem zadev, letu 2016 pa je bilo teh zadev že 16. Informacijski pooblaščenec ob tem zavezance poziva, da pri odločanju o okoljskih informacijah postopajo v korist transparentnosti, v teh postopkih pa naj se odločajo še posebej skrbno. Okoljski podatki se namreč vedno nanašajo na širši krog ljudi, njihovo razkritje pa je v javnem interesu. Prav za okoljske podatke namreč naša zakonodaja določa najvišjo stopnjo transparentnosti in pri njih ne pride v poštev praktično nobena zakonska izjema.

Leto 2016 je pomembno zaznamovala tudi novela ZDIJZ-E, ki se uporablja od maja. Novela je prinesla predvsem novosti na področju ponovne uporabe informacij javnega značaja Med drugim se je krog zavezanih organov za ponovno uporabo razširil tudi na muzeje, knjižnice in arhive. V zvezi s ponovno uporabo je Informacijski pooblaščenec leta 2016 vodil štiri pritožbene postopke, kar je več kot leta 2015 (takrat je vodil le enega). Po oceni Informacijskega pooblaščenca so prosilci – potencialni ponovni uporabniki sicer dobro seznanjeni s pravnimi možnostmi, ki jih imajo v primeru, ko jim zavezanci vlogo za ponovno uporabo zavrnejo, vendar je sam pritožbeni postopek (ki je vezan na subsidiarno uporabo ZUP) zanje prekompleksen in predolgotrajen. Informacijski pooblaščenec zato pozdravlja rešitev, ki jo je prinesla novela ZDIJZ-E v 10.b členu: zakonodajalec je z njo zavezancem naložil, da s posredovanjem informacij v svetovni splet in na portal odprtih podatkov sami proaktivno zagotavljajo odprte podatke za ponovno uporabo, pri katerih ni nobene ovire za prosto ponovno uporabo in ki so z vidika potencialnih ponovnih uporabnikov tudi najbolj zanimivi.

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 pomemben predvsem drugi odstavek 38. člena Ustave RS, ki določa, 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 za uresničitev namena nujno potrebni.

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 registracija zbirk osebnih podatkov, pravice posameznika do seznanitve s podatki, ki se nanašajo nanj, ter vprašanja glede nadzora in pristojnosti nadzornega organa vedno predpisovali tudi v področnih zakonih. Namen sistemskega zakona torej ni podrobnejše predpisovanje načinov obdelave osebnih podatkov po posameznih področjih, temveč predvsem to, da se v njem enotno določijo splošne pravice, obveznosti, načela in ukrepi, s katerimi se preprečujejo neustavni, nezakoniti in neupravičeni posegi v zasebnost in dostojanstvo posameznika pri obdelavi osebnih podatkov. Področni zakoni morajo zato jasno določati, katere zbirke osebnih podatkov se bodo vzpostavile in vodile na posameznem področju, vrste osebnih podatkov, ki jih bodo posamezne zbirke vsebovale, način zbiranja osebnih podatkov, morebitne omejitve pravic posameznika, zlasti pa namen obdelave zbranih osebnih podatkov. Z vidika varstva posameznika je zelo priporočljivo, da se v področnem zakonu določi tudi rok hrambe osebnih podatkov.

Zakon o varstvu osebnih podatkov[28], ki ga je Državni zbor RS sprejel 15. 7. 2004, velja od 1. 1. 2005. Zakon je bilo treba sprejeti predvsem zaradi vstopa Republike Slovenije v 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[29]. Julija 2007 je bil sprejet Zakon o spremembah in dopolnitvah zakona o varstvu osebnih podatkov[30], ki 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 je predstavljalo administrativno in s tem tudi finančno razbremenitev upravljavcev osebnih podatkov. Uradno prečiščeno besedilo zakona je bilo izdano septembra 2007 v Uradnem listu RS, št. 94/2007.

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.

28 Uradni list RS, št. 86/2004; v nadaljevanju ZVOP-1.
29 Uradni list Evropskih skupnosti, št. L 281, 23. 11. 1995.
30 Uradni list RS, št. 67/2007.

3.2. Dejavnost državnih nadzornikov za varstvo osebnih podatkov

3.2.1. Pravice in dolžnosti državnega nadzornika

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

Splošna načela inšpekcijskega nadzora, pravice, dolžnosti in pooblastila državnih nadzornikov, postopek inšpekcijskega nadzora, inšpekcijski ukrepi in druga vprašanja, povezana z inšpekcijskim nadzorom, so določeni v Zakonu o inšpekcijskem nadzoru[31], specifične pristojnosti državnega nadzornika pa so določene v 53. členu ZVOP-1.

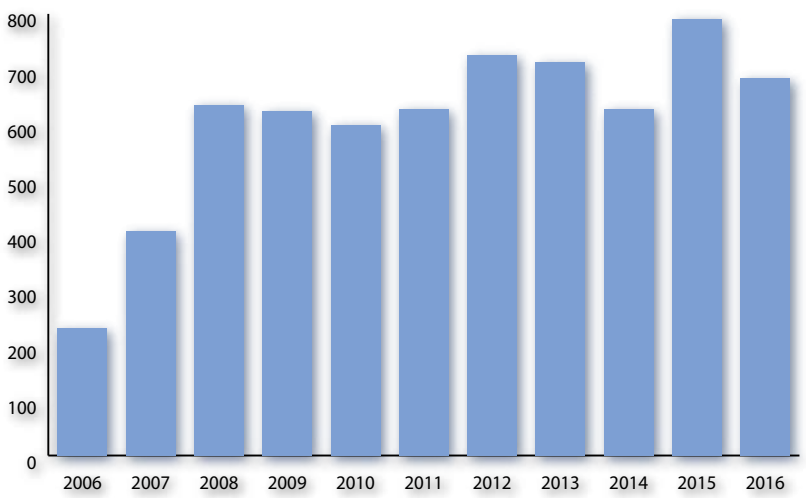
3.2.2. Inšpekcijski nadzor

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

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

Informacijski pooblaščenec je leta 2016 zaradi suma kršitev določb ZVOP-1 vodil 683 inšpekcijskih zadev, od tega 245 v javnem in 438 v zasebnem sektorju. Zoper pravne osebe javnega sektorja je na podlagi prijav uvedel 211 inšpekcijskih zadev, 34 postopkov pa je uvedel po uradni dolžnosti, v okviru načrtovanih ogledov ali npr. če je na podlagi objav v medijih zaznal sum kršitve varstva osebnih podatkov. Zoper zavezance v zasebnem sektorju je na podlagi prijav odprl 390 inšpekcijskih zadev, 48 postopkov je začel po uradni dolžnosti.

Slika 8: Število inšpekcijskih zadev med letoma 2006 in 2016.



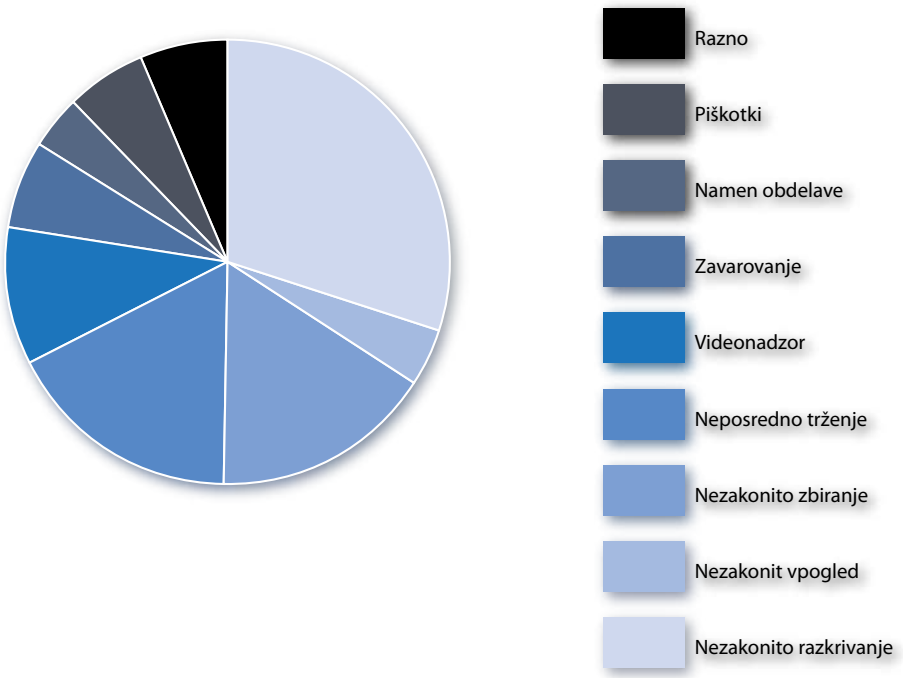
[31] Uradni list RS, št. 43/2007– uradno prečiščeno besedilo 1 in 40/2014; v nadaljevanju ZIN.

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

- nezakonito razkrivanje osebnih podatkov: posredovanje osebnih podatkov nepooblaščenim uporabnikom in nezakonita objava osebnih podatkov – 185,
- nezakonita obdelava osebnih podatkov pri izvajanju neposrednega trženja – 106,
- nezakonito zbiranje oziroma zahtevanje osebnih podatkov – 99,
- nezakonito izvajanje videonadzora – 61,
- neustrezno zavarovanje osebnih podatkov – 40,
- piškotki – 37,
- nezakonit vpogled v osebne podatke – 27,
- obdelava osebnih podatkov v nasprotju z namenom zbiranja – 23,
- razno: npr. obdelava osebnih podatkov po preteku roka hrambe, obdelava netočnih in neažurnih osebnih podatkov, zavrnitev posredovanja osebnih podatkov, zavrnitev izbrisa osebnih podatkov – 38.

Poleg zgoraj navedenih postopkov je Informacijski pooblaščenec uvedel 67 inšpekcijskih postopkov po uradni dolžnosti, v okviru katerih je preverjal izvajanje določb ZVOP-1 v celoti.

Slika 9: Sumi nezakonite obdelave osebnih podatkov leta 2016.



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 211 inšpekcijskih zadev, 34 jih je odprl po uradni dolžnosti, skupaj 245. V 88 primerih so državni nadzorniki prijaviteljem pisno pojasnili, zakaj uvedba postopka inšpekcijskega nadzora ne bi bila smiselna oziroma zakaj v prijavi opisano dejanje ne pomeni kršitve določb ZVOP-1. V štirih primerih Informacijski pooblaščenec ni uvedel postopka, ker prijavitelji niso posredovali svojih podatkov, zaradi česar jih ni mogel pozvati k posredovanju dodatnih podatkov, ki bi bili potrebni za uvedbo inšpekcijskega postopka. Na podlagi sedmih 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, tri prijave pa je Informacijski pooblaščenec odstopil v reševanje pristojnim organom.

Po preučitvi 211 prejetih prijav je bilo tako zaradi utemeljenega suma kršitev določb ZVOP-1 začetih 109 inšpekcijskih postopkov, 34 pa jih je uvedel še po uradni dolžnosti, skupaj torej 143. V okviru inšpekcijskih postopkov je bilo opravljenih 54 inšpekcijskih pregledov v prostorih zavezancev in 29 pregledov spletnih strani. Za odpravo ugotovljenih nepravilnosti je Informacijski pooblaščenec 55 zavezancem izrekel ukrepe v obliki opozorila na zapisnik, predodločbe[32], ureditvene odločbe ali ustnega poziva. Praktično vsi zavezanci so naložene ukrepe takoj izvršili.

Leta 2016 je bilo zaključenih 262 inšpekcijskih postopkov. Informacijski pooblaščenec v 49 inšpekcijskih postopkih ni zaznal kršitev določb ZVOP-1, 193 postopkov je ustavil, ker so zavezanci ugotovljene nepravilnosti odpravili, 20 postopkov pa je ustavil zato, ker je šlo za kršitve določb ZVOP-1, ki so predstavljale enkratna dejanja v preteklosti, ki jih z inšpekcijskimi ukrepi za nazaj ni bilo več mogoče odpraviti.

Informacijski pooblaščenec je prejel dve tožbi; ena je bila vložena zoper sklep o ustavitvi postopka, ena pa zoper odločbo, s katero je Informacijski pooblaščenec zavezancu odredil odpravo ugotovljenih nepravilnosti. Upravno sodišče RS do konca leta 2016 ni odločilo v nobenem izmed omenjenih primerov, je pa odločilo v dveh tožbah, ki sta bili vloženi leta 2015 zoper sklep o ustavitvi inšpekcijskega postopka. Sodišče je tožbam ugodilo na način, da je izpodbijani sklep odpravilo in zadevo vrnilo Informacijskemu pooblaščencu v ponovni postopek.

3.2.2.2. Inšpekcijski nadzor v zasebnem sektorju

Informacijski pooblaščenec je zoper zavezance v zasebnem sektorju na podlagi prijav odprl 390 zadev. V 163 primerih so bili prijavitelji obveščeni, da Informacijski pooblaščenec postopka inšpekcijskega nadzora ne bo uvedel, ker iz njihove prijave ne izhaja sum kršitev določb ZVOP-1 ali ker jih je napotil na pravico do vpogleda v lastne osebne podatke in pravico zahtevati prenehanje uporabe osebnih podatkov za namen neposrednega trženja. Slednjim (teh je bilo 10) je pojasnil, da mu v primeru zavrnitve zahteve lahko podajo pritožbo ali prijavo. V 11 primerih Informacijski pooblaščenec postopka inšpekcijskega nadzora ni mogel uvesti, ker prijavitelji tudi po pozivu k dopolnitvi prijave niso posredovali dovolj podatkov, nekaj prijav pa je bilo anonimnih, zaradi česar prijaviteljev ni mogel pozvati k dopolnitvi. Na podlagi devetih prijav je Informacijski pooblaščenec takoj uvedel postopek o prekršku, 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 mogoče preprečiti ali odpraviti, in ker je bilo prijavam priloženih dovolj dokazov o storitvi prekrškov. 18 prijav je Informacijski pooblaščenec posredoval v reševanje pristojnim institucijam in o tem obvestil prijavitelje.

Informacijski pooblaščenec je po preučitvi prejetih prijav začel 189 postopkov inšpekcijskega nadzora, 48 pa jih je uvedel po uradni dolžnosti, skupaj torej 237. Državni nadzorniki za varstvo osebnih podatkov so opravili 91 inšpekcijskih ogledov na terenu in 39 ogledov spletnih strani. Za odpravo ugotovljenih nepravilnosti so 89 zavezancem izrekli ukrepe v obliki opozorila na zapisnik, predodločbe, ureditvene odločbe ali ustnega poziva. Skoraj vsi zavezanci so naložene ukrepe v postavljenem roku izvršili. Informacijski pooblaščenec je prejel tri tožbe; dve sta bili vloženi zoper ureditveni odločbi, ena pa zoper sklep o zavrženju pritožbe.

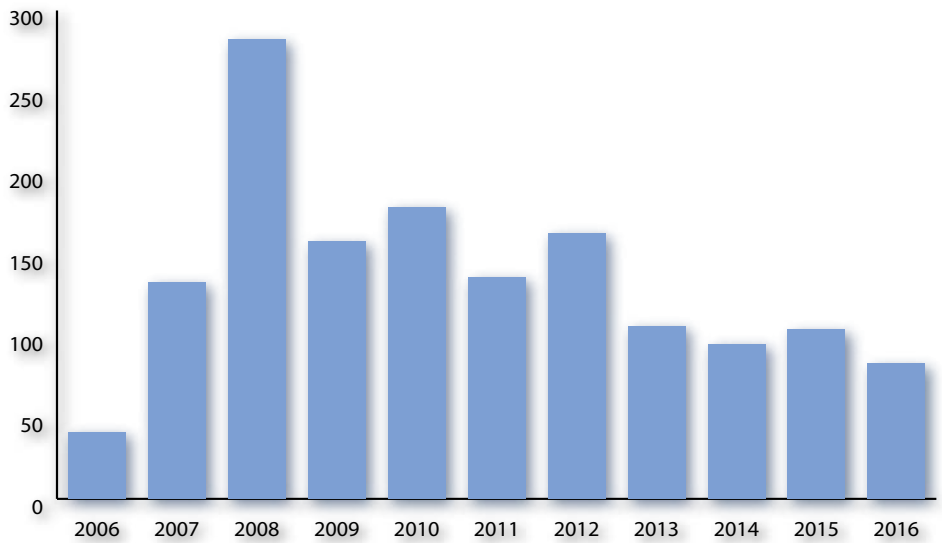
Leta 2016 je Informacijski pooblaščenec ustavil 190 postopkov; 80 postopkov je ustavil, ker ni ugotovil kršitev določb ZVOP-1, 72 postopkov je ustavil po tem, ko so zavezanci odpravili ugotovljene nepravilnosti, 38 postopkov pa je zaključil, ker v zvezi z ugotovljenimi prekrški ni bilo mogoče izreči inšpekcijskih ukrepov, ker je šlo za enkratna dejanja v preteklosti.

[32] Informacijski pooblaščenec mora v primeru, ko ugotovi nezakonito obdelavo osebnih podatkov, pred izdajo odločbe, s katero odredi prenehanje takšne obdelave, zavezanca skladno z načelom zaslišanja stranke (9. člen ZUP) predhodno seznaniti s tem, zakaj po njegovem mnenju za predmetno obdelavo osebnih podatkov nima pravne podlage, ter ga seznaniti z argumenti, ki njegovo mnenje potrjujejo. Zavezancu je namreč glede na sodno prakso treba pred izdajo ureditvene odločbe dati možnost, da se izjavi do stališča Informacijskega pooblaščenca (načelo kontradiktornosti strank), kar v praksi pomeni, da zavezanci po seznanitvi z argumenti Informacijskega pooblaščenca v večini primerov sami prenehajo z nezakonito obdelavo osebnih podatkov, zato izdaja ureditvene odločbe ni več potrebna.

3.2.3. Storjeni prekrški

Zaradi kršitev določb ZVOP-1 je bilo leta 2016 uvedenih 83 postopkov o prekršku, od tega 41 zoper pravne osebe zasebnega sektorja in njihove odgovorne osebe, 13 zoper pravne osebe javnega sektorja in njihove odgovorne osebe ter 29 postopkov zoper posameznike (v to število so vključeni tudi postopki zoper odgovorne osebe državnih organov in samoupravnih lokalnih skupnosti, saj v skladu z Zakonom o prekrških[33] Republika Slovenija in samoupravne lokalne skupnosti za prekrške ne odgovarjajo, odgovarjajo le njihove odgovorne osebe – teh je bilo 24). Za ugotovljeni prekršek lahko prekrškovni organ v skladu s 53. členom izreče opozorilo, če je storjeni prekršek neznaten in če pooblaščena uradna oseba oceni, da je glede na pomen dejanja opozorilo zadosten ukrep. Če je storjen hujši prekršek, prekrškovni organ izda odločbo o prekršku, s katero kršitelju izreče sankcijo. V skladu s 4. členom ZP-1 sta sankciji za prekršek globa in opomin, glede na 57. člen ZP-1 pa se lahko globa izreče tudi v obliki plačilnega naloga.

Slika 10: Število uvedenih postopkov o prekršku med letoma 2006 in 2016.



V prekrškovnih postopkih, vključno z odprtimi postopki iz preteklih let, je Informacijski pooblaščenec leta 2016 izdal:
- 7 opozoril,
- 80 odločb o prekršku (44 glob in 36 opominov).

Poleg opozoril, ki so bila izrečena v prekrškovnih postopkih, je Informacijski pooblaščenec v skladu z načelom ekonomičnosti izrekel tudi 62 opozoril po 53. členu ZP-1 v okviru postopkov inšpekcijskega nadzora, in sicer 14 v javnem in 48 v zasebnem sektorju.

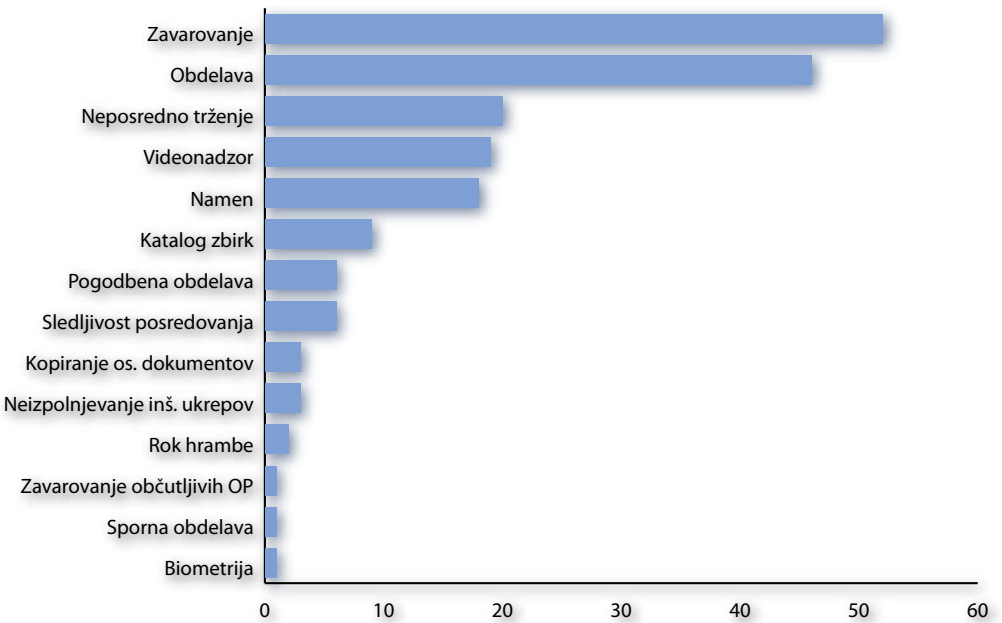
Kršitelji so zoper izdane odločbe o prekršku vložili deset zahtev za sodno varstvo (zoper 12,8 % odločb). Vse zahteve za sodno varstvo so bile vložene zoper odločbe, s katerimi je Informacijski pooblaščenec kršiteljem izrekel globe, saj so globe po ZVOP-1 visoke, zlasti če gre za stek prekrškov. Relativno majhen delež vloženih zahtev za sodno varstvo kaže na to, da storilci storjene prekrške priznavajo in se zavedajo svoje odgovornosti.

Kršitve (v okviru enega postopka je lahko več kršitev) so zadevale:
- neustrezno zavarovanje osebnih podatkov: 24. in 25. člen ZVOP-1 – 52,
- nezakonito obdelavo osebnih podatkov: 8. člen ZVOP-1 – 46,
- kršitev določb o neposrednem trženju: 72. in 73. člen ZVOP-1 – 20,
- nezakonito izvajanje videonadzora: 74., 75., 76. in 77. člen ZVOP-1 – 19,
- nezakonit namen zbiranja in nadaljnje obdelave osebnih podatkov: 16. člen ZVOP-1 – 18,

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

- nepravilnosti v zvezi z vzpostavitvijo katalogov zbirk osebnih podatkov in posredovanjem podatkov v register zbirk osebnih podatkov: 26. in 27. člen ZVOP-1 – 9,
- neustrezno pogodbeno obdelavo osebnih podatkov: 11. člen ZVOP-1 – 6,
- neustrezno sledljivost posredovanja osebnih podatkov: tretji odstavek 22. člena ZVOP-1 – 6,
- nezakonito kopiranje osebnih dokumentov: 4.a člen ZPLD in 4. člen ZOIzk – 3,
- neizpolnjevanje ukrepov, izrečenih v postopkih inšpekcijskega nadzora, kršitve določb ZIN – 3,
- neustrezen rok hrambe osebnih podatkov: 21. člen ZVOP-1 – 2,
- neustrezno zavarovanje občutljivih osebnih podatkov: 14. člen ZVOP-1 – 1,
- sporno dopolnitev, popravek, blokiranje ali izbris osebnih podatkov: 33. člen ZVOP-1 – 1,
- nezakonito izvajanje biometrijskih ukrepov: 79. člen – 1.

Slika 11: Najpogostejše kršitve določb ZVOP-1 leta 2016.



Leta 2016 je Informacijski pooblaščenec prejel pet sodb, s katerimi so okrajna sodišča odločila o zahtevah za sodno varstvo, ki so jih storilci vložili zoper odločbe o prekrških v letih 2015 in 2016:

- zahtevi za sodno varstvo je bilo ugodeno v delu, ki se nanaša na izrečeno sankcijo, tako da se je storilcem za prekršek spremenila sankcija ali višina globe, sicer je bila zahteva za sodno varstvo zavrnjena kot neutemeljena – 2,
- zahteva za sodno varstvo je bila zavrnjena kot neutemeljena, odločba Informacijskega pooblaščenca pa potrjena – 1,
- zahtevi za sodno varstvo je bilo ugodeno, odločba Informacijskega pooblaščenca je bila odpravljena, postopek o prekršku pa ustavljen – 1,
- zahtevi za sodno varstvo je bilo delno ugodeno tako, da je bil postopek v enem delu zaradi zastaranja prekrškov ustavljen in da pravni osebi zaradi izbrisa iz poslovnega registra globa ni bila izrečena, v preostalem delu pa je bila zahteva za sodno varstvo zavrnjena kot neutemeljena – 1.

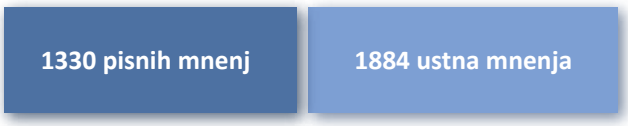
3.3. Dajanje mnenj in pojasnil

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 2016 izdal 1.330 pisnih mnenj in napotitev na mnenja. Če je posameznik zastavil vprašanje, na katerega je Informacijski pooblaščenec v preteklosti že odgovoril, ga je namreč le napotil na mnenje, objavljeno na spletni strani.

Na spletni strani Informacijskega pooblaščenca je objavljenih okrog 2.500 mnenj, v katerih lahko posamezniki najdejo odgovore na številna vprašanja. Informacijski pooblaščenec izdana mnenja razvršča na 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, pogodbena obdelava, policijski postopki, postopki na centrih za socialno delo, register zbirk osebnih podatkov, sindikati, sodni postopki, stanovanjsko in nepremičninsko pravo, statistika in raziskovanje, svetovni splet, šolstvo, telekomunikacije in pošta, trgovinska dejavnost, upravljanje gospodarskih družb, upravni postopki, verske skupnosti, video- in avdionadzor, vpogled v lastne osebne podatke, vrtci, zavarovalništvo, zavarovanje osebnih podatkov, zdravstveni osebni podatki). Mnenja so objavljena na spletni strani https://www.ip-rs.si/varstvo-osebnih-podatkov/iskalnik-po-odlocbah-in-mnenjih/odlocbe-in-mnenja-varstvo-osebnih-podatkov/.

Informacijski pooblaščenec spodbuja svetovanje oziroma posredovanje ustnih odgovorov na vprašanja. Zato je v uradu vsak dan na voljo dežurni državni nadzornik, ki na vprašanja odgovarja po telefonu. Leta 2016 so državni nadzorniki sprejeli 1.884 klicev, kar pomeni, da je Informacijski pooblaščenec skupno svetoval več kot 3.200 posameznikom.

Slika 12: Mnenja Informacijskega pooblaščenca leta 2015.

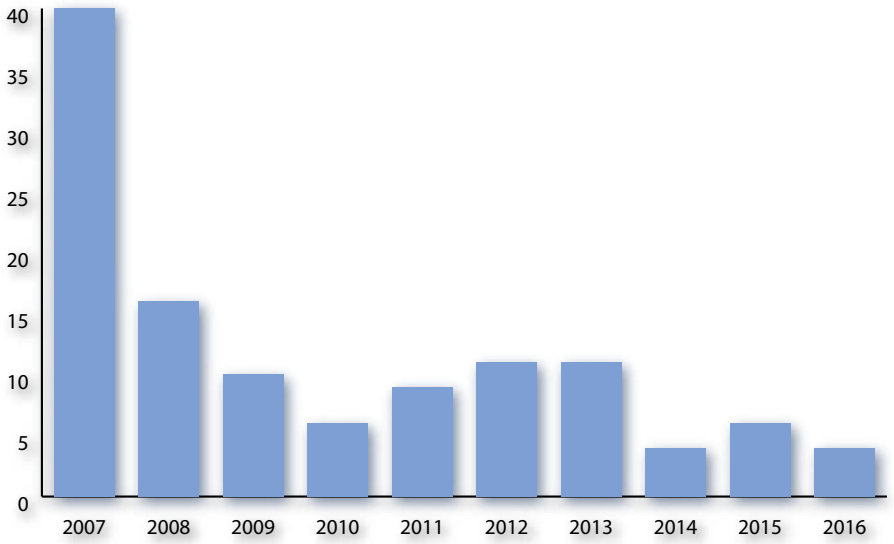


3.4. Dopustnost izvajanja biometrijskih ukrepov

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 varovanje tajnih podatkov ali poslovne skrivnosti. Z določitvijo teh pogojev je zakonodajalec sledil načelu sorazmernosti (3. člen ZVOP-1) ter s tem omejil možnosti prekomernih in neupravičenih posegov v zasebnost in dostojanstvo posameznika. Pri presoji, ali so biometrijski ukrepi nujno potrebni za dosego namena, Informacijski pooblaščenec zato ugotavlja, ali bi namen, ki ga zasleduje vlagatelj, lahko dosegel s postopki in ukrepi, ki manj posegajo v zasebnost zaposlenih oziroma ne vključujejo biometrijskih ukrepov. Pri uvajanju slednjih je namreč treba upoštevati, da predstavljajo velik poseg v informacijsko zasebnost posameznika, saj gre za obdelavo tistih značilnosti, ki so za vsakogar edinstvene in stalne in zloraba katerih bi za posameznika lahko imela hude, daljnosežne in nepopravljive posledice. Informacijski pooblaščenec presoja tudi tehnični vidik biometrijskih ukrepov (ali se bodo uporabljali za preverjanje identitete oziroma avtentikacijo ali za ugotavljanje identitete oziroma identifikacijo).

Slika 13: Število vlog za izdajo odločbe o dopustnosti izvajanja biometrijskih ukrepov med letoma 2007 in 2016.



Informacijski pooblaščenec je leta 2016 prejel štiri vloge za izdajo dovoljenja za uvedbo biometrijskih ukrepov. Izdal je šest odločb, dve v zadevah iz leta 2015: v dveh primerih je vlogi za izvajanje biometrijskih ukrepov ugodil, v enem delno ugodil, v treh primerih pa je vlogo zavrnil.

Informacijski pooblaščenec je vlagatelju dovolil, da za namen varstva premoženja izvaja biometrijske ukrepe z uporabo čitalnikov prstnih odtisov nad zaposlenimi, ki imajo pooblastilo za vstop v predtrezorske in trezorske prostore v številnem centru. Gre za prostore, v katerih je veliko gotovine, saj se v njih izvaja dovoz in raztovarjanje gotovine, skladiščenje gotovine za določen čas, obdelava (štetje, izločanje, razvrščanje itd.) ter distribucija gotovine na posamezne lokacije. Informacijski pooblaščenec je presodil, da je premoženje, ki ga želi vlagatelj varovati z izvajanjem biometrijskih ukrepov, tako pomembno, da njegovo varovanje odtehta tudi poseg v informacijsko zasebnost zaposlenih. Pri tem je upošteval težo in obseg posledic odtujitve ali drugih posegov v varovano premoženje, do katerih bi lahko prišlo zaradi vstopa nepooblaščenih oseb v navedene prostore (neposredna škoda, ki bi nastala z odtujitvijo ali drugim posegom v gotovino, in sekundarne posledice, do katerih bi zaradi tega prišlo oziroma bi sledile v obliki motnje pri oskrbi države z gotovino, za katero je pristojen vlagatelj, pa tudi možnost izgube ugleda in negativen vpliv na finančni trg kot celoto), in dejstvo, da je izvajanje biometrijskih ukrepov v skladu z načelom sorazmernosti, saj se bodo izvajali le nad ozkim krogom zaposlenih pri vlagatelju, ki so v okviru opravljanja svojih del in nalog izrecno pooblaščeni za dostopanje do varovanih prostorov ter posebej usposobljeni za dela in naloge, ki se opravljajo v teh prostorih.

Informacijski pooblaščenec je dovolil vlagatelju, da za namen varovanja poslovne skrivnosti izvaja biometrijske ukrepe z uporabo čitalnikov prstnih odtisov nad člani uprave in njihovimi poslovnimi sekretarkami, ki imajo pooblastilo za vstop v pisarne teh članov uprave. Po preučitvi vlagateljevih navedb je Informacijski pooblaščenec zaključil, da je vlagatelj izkazal, da se v varovanih prostorih nahaja dokumentacija, ki vsebuje poslovne skrivnosti, katerih varovanje je eden od taksativno naštetih zakonitih namenov izvajanja biometrijskih ukrepov. V pisarnah članov uprave naj bi se obravnavali in hranili podatki ter ustvarjali dokumenti, ki predstavljajo različne vrste in stopnje zaupnosti (npr. podatki o strankah, ki so v skladu z Zakonom o bančništvu[34] zaupni; dokumentacija, ki v skladu z 39. členom Zakona o gospodarskih družbah[35] in Pravilnikom o poslovni skrivnosti vlagatelja predstavlja poslovne skrivnosti), zato bi bile posledice nepooblaščenega dostopa in prisvojitve podatkov, ki so vitalnega pomena za vlagateljevo poslovanje, nesorazmerno večje in težje od posega v informacijsko zasebnost zaposlenih z izvajanjem biometrijskih ukrepov. Nameravano izvajanje biometrijskih ukrepov je tudi v skladu z načelom sorazmernosti, saj se bodo ti ukrepi izvajali izključno nad ozkim krogom vodstvenih delavcev (člani uprave) in njihovih poslovnih sekretark.

[34] Uradni list RS, št. 25/2015 s spremembami.
[35] Uradni list RS, št. 65/2009 - uradno prečiščeno besedilo 3.

Informacijski pooblaščenec je delno ugodil zahtevi vlagatelja in mu za namen varstva premoženja dovolil izvajanje biometrijskih ukrepov z uporabo čitalnikov prstnih odtisov nad svojimi zaposlenimi, ki imajo pooblastilo za vstop v dva posebej varovana sistemska prostora (»bunkerja«), v katerih so strežniki s podatki, ki vsak zase, zlasti pa skupaj, predstavljajo premoženje večje vrednosti. Vlagatelj opravlja dejavnost kolokacije (gostovanje strežnikov), kar pomeni, da so uporabniki navedenih prostorov družbe (npr. telekomunikacijski operaterji, banke), ki pri vlagatelju najamejo strežniške omare, v katere namestijo svoje strežnike. Informacijski pooblaščenec je po preučitvi vseh dejstev in okoliščin, ki jih je navedel vlagatelj, presodil, da je vlagatelj upravičen in dolžan sprejeti in izvajati ukrepe, s katerimi bo premoženje v obliki opreme in podatkov svojih strank kar najučinkoviteje zavaroval. Prav zagotavljanje ustrezne stopnje zavarovanja opreme in podatkov je namreč eden bistvenih razlogov, zaradi katerega se stranke odločijo hrambo zaupati vlagatelju. Pri odločitvi je Informacijski pooblaščenec upošteval tudi premoženjske posledice, ki bi vlagatelju lahko nastale zaradi morebitnega nepooblaščenega dostopanja in razkrivanja podatkov strank (odškodninski zahtevki, izguba ugleda in zaupanja ter posledična izguba poslov), in sorazmernost izvajanja biometrijskih ukrepov, saj se bodo ti izvajali le nad dvema zaposlenima, ki sta tudi vlagateljeva zakonita zastopnika.

Vlagateljeva zahteva je bila zavrnjena v delu, ki se je nanašal na nameravano izvajanje biometrijskih ukrepov nad posamezniki, nad katerimi teh ukrepov že po samem zakonu ni dovoljeno izvajati, tj. posamezniki, ki niso zaposleni pri vlagatelju, ampak v družbah, ki pri njem najemajo strežniške omare za hrambo svojih podatkovnih baz. Informacijski pooblaščenec je pojasnil, da bi biometrijske ukrepe nad njimi lahko izvajala samo posamezna družba, ki uporablja storitve vlagatelja, kot njihov delodajalec, vendar šele po pridobitvi »svoje« odločbe, s katero bi ji Informacijski pooblaščenec dovolil izvajanje biometrijskih ukrepov. Posamezen uporabnik storitev vlagatelja pa bi po pridobitvi take odločbe izvajanje biometrijskih ukrepov lahko s pogodbo iz 11. člena ZVOP-1 prenesel na vlagatelja, ki bi nato te ukrepe tehnično izvajal na način, ki ga je predlagal v svoji vlogi, vendar ne kot upravljavec biometrijskih podatkov (razen za svoje zaposlene), ampak kot pogodbeni obdelovalec v imenu in za račun uporabnika.

Informacijski pooblaščenec je zavrnil zahtevo vlagatelja, ki je želel kontrolo pristopa na podlagi prstnega odtisa izvajati nad zaposlenimi in zunanjimi sodelavci za vstop v pisarno direktorja, finančno-računovodske službe in komerciale zaradi varovanja tajnih podatkov, poslovnih skrivnosti in premoženja. Po preučitvi vlagateljevih navedb je Informacijski pooblaščenec sicer ugotovil, da se v navedenih prostorih nahajajo poslovne skrivnosti in premoženje, ki ga je treba varovati, vendar pa je zaključil, da vlagatelj ni izkazal, da bi bilo za varstvo navedenih pravnih dobrin nujno potrebno izvajanje biometrijskih ukrepov. Vlagatelj lahko navedene pravne dobrine primerljivo učinkovito varuje z milejšimi sredstvi, tj. s postopki in ukrepi za zavarovanje, ki v informacijsko zasebnost zaposlenih sploh ne posegajo oziroma posegajo v znatno manjši meri, npr. z omejevanjem dostopa do navedenih prostorov (z brezkontaktnimi karticami ali osebnimi gesli ali s kombinacijo obojega) in z zavarovanjem samih nosilcev podatkov, na katerih so poslovne skrivnosti (npr. zaščita dostopov do računalnikov s tehnično in organizacijsko implementirano politiko gesel, hramba pogodb na papirju v posebnih sefih ali varovanih omarah). Informacijski pooblaščenec je poudaril, da se biometrijski ukrepi lahko uporabijo, ko je jasno izkazano, da učinkovitega varstva ni mogoče zagotavljati z drugimi varnostnimi ukrepi ali sistemom takih ukrepov, in ko je tudi konkretna varovana dobrina take vrednosti, vrste ali narave, da njeno varstvo odtehta poseg v zasebnost zaposlenih. Pri svoji odločitvi je Informacijski pooblaščenec upošteval tudi navedbo vlagatelja, da bi bilo v varovane prostore po uvedbi biometrijskih ukrepov mogoče vstopati tudi s ključi, saj ni mogoče trditi, da je izvajanje biometrijskih ukrepov nujno potrebno, hkrati pa omogočiti vstopanje tudi z milejšim ukrepom (ključem). Biometrijski ukrepi so namreč lahko učinkoviti le, če predstavljajo edini način vstopanja v zavarovane prostore.

Informacijski pooblaščenec je zavrnil zahtevo vlagatelja, ki je nameraval biometrijske ukrepe izvajati za namen opravljanja dejavnosti. Vlagatelj je navedel, da bi te ukrepe uvedel v okviru nadgradnje oziroma zamenjave sistema za registracijo delovnega časa, saj so zaposleni predlagali namestitev sistema s čitalcem prstnih odtisov, ker naj bi bila njegova uporaba preprostejša in hitrejša od prenašanja kartic. Čitalec prstnih odtisov bi uporabljali izključno tisti zaposleni, ki to želijo, ostali bi imeli registrsko brezkontaktno kartico.

Po proučitvi vlagateljevih navedb je Informacijski pooblaščenec zaključil, da vlagatelj ni izkazal, na kakšen način bi bilo lahko ogroženo opravljanje njegove dejavnosti, če za registracijo delovnega časa ne bi izvajal biometrijskih ukrepov, poleg tega je celo sam izrecno navedel, da uvedba biometrijskih ukrepov ni nujno potrebna, ampak jih želi uvesti in izvajati predvsem zaradi poenostavitve postopka registracije delovnega časa in na željo, torej s privolitvijo zaposlenih.

Informacijski pooblaščenec je pojasnil, da biometrijskih ukrepov ni mogoče uvesti zgolj zato, ker so bolj priročni ali ekonomični od ostalih sistemov registracije delovnega časa, saj gre za ukrepe, ki jih zakon dovoljuje izjemoma, za varstvo izrecno določenih pravnih dobrin in ob izpolnjevanju relativno strogih pogojev. Biometrijskih ukrepov tudi ni mogoče uvesti na podlagi privolitve zaposlenih, ker iz določbe 80. člena ZVOP-1 povsem jasno izhaja, da je privolitev zaposlenih za zakonitost izvajanja biometrijskih ukrepov povsem irelevantna, saj je zakonodajalec ne obravnava kot pogoj za dopustnost uvedbe biometrijskih ukrepov. To na eni strani pomeni, da morebitne privolitve zaposlenih ne morejo predstavljati alternativne pravne podlage za izvajanje biometrijskih ukrepov, na drugi strani pa to pomeni, da delodajalec lahko, če pridobi pozitivno odločbo Informacijskega pooblaščenca, biometrijske ukrepe nad svojimi zaposlenimi izvaja ne glede na njihovo privolitev, tj. tudi če temu nasprotujejo.

Informacijski pooblaščenec je zavrnil zahtevo vlagatelja, ki je navedel, da želi biometrijske ukrepe izvajati za evidentiranje prisotnosti na delovnem mestu, ker naj bi bilo to nujno za opravljanje njegove dejavnosti, tj. hotelirstva in gostinstva. Pojasnil je, da je pri sistemu evidentiranja delovnega časa prek računalniškega programa z identifikacijsko kodo ugotovil zlorabe, ki naj bi imele za posledico neverodostojne kvote opravljenih delovnih ur in posledično neupravičeno izplačevanje dodatkov. Zato je nameraval biometrijske ukrepe izvajati nad vsemi redno zaposlenimi, pogodbenimi delavci ter študenti, in sicer prek prstnega odtisa.

Pri svoji odločitvi je Informacijski pooblaščenec upošteval, da vlagatelj ni izkazal nujne potrebnosti uvedbe biometrijskih ukrepov, tj. da svoje dejavnosti ne bi mogel ustrezno opravljati, če delovnega časa zaposlenih ne bi evidentiral prav z biometrijskimi ukrepi, ampak na drug, informacijski zasebnosti prijaznejši način. Biometrijskih ukrepov, ki se uvajajo le zato, ker so bolj priročni ali ekonomični od ostalih sistemov registracije delovnega časa, namreč ni mogoče opredeliti kot nujno potrebnih za dosego namenov, opredeljenih v prvem odstavku 80. člena ZVOP-1. Zato je Informacijski pooblaščenec zaključil, da bi za namen evidence prisotnosti zadostovala uporaba brezkontaktnih kartic, drugih primerljivih sredstev ali njihove kombinacije, ki predstavljajo manjši poseg v zasebnost posameznika. Nasprotno bi namreč pomenilo, da verodostojnosti evidentiranja delovnega časa ni mogoče zagotoviti brez uporabe biometrijskih ukrepov, kar pa ne more držati, saj praktično vsa podjetja in inštitucije delovni čas evidentirajo brez uporabe biometrijskih ukrepov, goljufanje pri evidentiranju pa je mogoče zaznati tudi z drugimi, milejšimi ukrepi. To še toliko bolj velja za dejavnost, s katero se ukvarja vlagatelj, saj je narava dela hotelskega osebja taka, da je neupravičena odsotnost posameznika v delovnem procesu hitro zaznavna in da obstaja več drugih načinov poznejšega ugotavljanja morebitne neupravičene odsotnosti zaposlenega ter s tem povezanih goljufij pri evidentiranju delovnega časa. Ob tem je Informacijski pooblaščenec dodal, da tudi uporaba biometrijskih ukrepov delodajalcu ne zagotavlja, da je bil zaposleni v registriranem delovnem času res na delovnem mestu, še manj, da je tam ustrezno opravljal svoje delovne dolžnosti, ampak mu zagotavlja zgolj podatek, da je bil v kratkem trenutku registracije ob registracijski napravi. Informacijski pooblaščenec je pojasnil še, da ZVOP-1 poslovnemu subjektu dovoljuje izvajanje biometrijskih ukrepov zgolj nad njegovimi zaposlenimi, tj. nad osebami, ki so z njim v delovnem razmerju, ne pa tudi nad osebami, ki zanj opravljajo delo na podlagi kakšnega drugega pogodbenega razmerja (npr. študenti).

3.5. Ugotavljanje ustrezne ravni varstva osebnih podatkov v tretjih državah

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

- izdajo odločb o zagotavljanju ustrezne ravni varstva osebnih podatkov v tretjih državah (63. člen);
- vodenje postopkov ugotavljanja ustrezne ravni varstva osebnih podatkov v tretjih državah na podlagi ugotovitev inšpekcijskega nadzora in drugih informacij (64. člen);
- vodenje seznama tretjih držav, za katere je ugotovil, da imajo v celoti ali delno zagotovljeno ustrezno raven varstva osebnih podatkov ali da te nimajo zagotovljene; če je ugotovljeno, da tretja država ustrezno raven varstva osebnih podatkov zagotavlja le delno, je v seznamu navedeno tudi, v katerem delu je ustrezna raven zagotovljena (66. člen);
- vodenje upravnih postopkov za izdajo 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 izdaji posebnega dovoljenja za iznos osebnih podatkov v tretjo državo preveriti, ali upravljavec osebnih podatkov (izvoznik podatkov) zagotavlja ustrezne postopke in ukrepe zavarovanja osebnih podatkov ter 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 posebnega dovoljenja (odločbe) glede iznosa osebnih podatkov v tretje države opraviti tudi vsebinski preizkus, ali za posredovanje oziroma za razkrivanje, širjenje in dajanje določenih osebnih podatkov na razpolago drugi pravni osebi obstaja ustrezna pravna podlaga.

Informacijski pooblaščenec je leta 2016 prejel 53 vlog za iznos osebnih podatkov. Veliko število vlog je posledica odločitve Sodišča EU oktobra 2015 v zadevi Schrems ter posledične razveljavitve t. i. dogovora o Varnem pristanu, na podlagi katerega so upravljavci iznašali osebne podatke iz EU (tudi iz Slovenije) v ZDA. Ker je Informacijski pooblaščenec pri odločanju o ustrezni ravni varstva osebnih podatkov vezan na odločitve pristojnega organa EU, je odpravil odločbo, s katero je leta 2010 ugotovil, da ZDA zagotavljajo ustrezno raven varstva osebnih podatkov v delu, ko gre za iznos osebnih podatkov organizacijam, ki delujejo po načelih Varnega pristana. Upravljavci so morali zato za iznos osebnih podatkov v ZDA vložiti nove vloge. Marca 2017 je Informacijski pooblaščenec na podlagi odločitve Evropske komisije ZDA uvrstil na listo tretjih držav, za katere se šteje, da v delu, ko gre za iznos osebnih podatkov v okviru Ščita zasebnosti EU–ZDA, zagotavljajo ustrezno raven varstva osebnih podatkov. Tako upravljavci osebnih podatkov v Sloveniji, ki za obdelavo osebnih podatkov uporabljajo storitve pogodbenih partnerjev iz ZDA, za iznos osebnih podatkov ne potrebujejo več posebnega dovoljenja Informacijskega pooblaščenca, če je njihov pogodbeni partner ustrezno samocertificiran v okviru Ščita zasebnosti (Privacy Shield).

Informacijski pooblaščenec je izdal 52 odločb, vsem vlagateljem je dovolil iznos osebnih podatkov:

35 družbam je dovolil, da osebne podatke, katerih upravljavci so, iznašajo in posredujejo svojim pogodbenim obdelovalcem v tretjih državah. Poleg ZDA, kamor bo osebne podatke iznašalo kar 25 družb, je dovolil iznos tudi v Indijo, Avstralijo, Srbijo, Japonsko, Združene arabske emirate, Brazilijo, Singapur, Kostariko, Malezijo, Kanado, Mehiko, na Filipine, Kitajsko in Novo Zelandijo ter v Republiko Tatarstan Ruske federacije. Podatki, ki so bodo iznašali, se nanašajo na zaposlene in njihove družinske člane, posameznike, ki opravljajo delo na podlagi drugih civilnih pogodb, kandidate za zaposlitev, poslovne partnerje (npr. kupci, dobavitelji, distributerji, prodajalci, svetovalci), zdravstvene delavce, farmacevte in bolnike, ki sodelujejo v kliničnih raziskavah, udeležence nagradnih iger ter uporabnike različnih spletnih strani in aplikacij. Nameni iznosa osebnih podatkov, ki so jih navedle družbe, so npr. vodenje kadrovskih evidenc, zaposlitveno načrtovanje, upravljanje sistema varnosti in zdravja pri delu, zagotavljanje pomoči uporabnikom (*helpdesk*), zagotavljanje analitičnih storitev za potrebe marketinških aktivnosti, vzdrževanje serverjev, prenos podatkovnega centra in centralizacija upravljanja IT-storitev, obvladovanje incidentov in težav, izvajanje biomedicinskih raziskav, spremljanje farmakovigilance, izvajanje storitev v oblaku, centralizirano shranjevanje podatkov, delovanje mobilne aplikacije.

Pravno podlago za posredovanje osebnih podatkov v navedenih primerih predstavlja 11. člen ZVOP-1, ki določa, da lahko upravljavec osebnih podatkov posamezna opravila v zvezi z obdelavo osebnih podatkov s pogodbo zaupa pogodbenemu obdelovalcu, ki je registriran za opravljanje takšne dejavnosti in zagotavlja ustrezne postopke in ukrepe iz 24. člena ZVOP-1, tj. postopke in ukrepe za zavarovanje osebnih podatkov. 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 ZVOP-1. 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.

Informacijski pooblaščenec je 13 družbam dovolil, da drugim upravljavcem osebnih podatkov v tretjih državah (ZDA, Srbija, Bosna in Hercegovina, Črna gora, Singapur, Japonska, Gvatemala, Argentina) posredujejo osebne podatke zaposlenih (bivših in sedanjih) in njihovih sorodnikov, osebne podatke drugega osebja (pripravniki, študenti, prostovoljci), kandidatov za zaposlitev in osebne podatke strank oziroma poslovnih partnerjev za namene upravljanja s človeškimi viri oziroma centralizacije kadrovske politike in obdelave kadrovskih podatkov ter za namene izvajanja centralne poslovne in informacijsko-tehnične politike zaradi povečanja učinkovitosti in izboljšanja storitev.

Informacijski pooblaščenec je po pregledu vlog ugotovil, da izvoznik in uvoznik podatkov pripadata isti mednarodni skupini povezanih družb in da je namen iznosa osebnih podatkov predvsem združevanje oziroma centralizacija različnih sistemov ter s tem povečanje učinkovitosti in izboljšanje storitev. Pri preverjanju pravnih podlag je Informacijski pooblaščenec 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 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, za iznos osebnih podatkov poslovnih partnerjev pa drugi odstavek 10. člena ZVOP-1, saj je obdelava osebnih podatkov nujno potrebna med pogajanji ter za poslovanje in sklepanje pogodb. Informacijski pooblaščenec je opravil skrben pregled pogodb, ki so jih predložili izvozniki podatkov, in 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 pretoku takih podatkov.

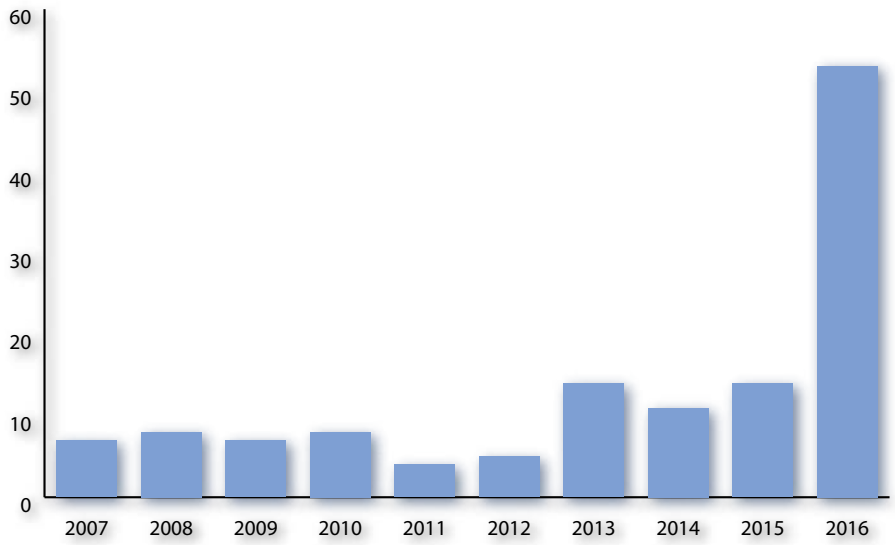
Trem družbam je dovolil, da pogodbenim obdelovalcem in upravljavcem osebnih podatkov v tretjih državah v okviru skupin, katerih članice so, iznašajo in posredujejo osebne podatke zaposlenih, delavcev, ki delo opravljajo na podlagi podjemnih, avtorskih in drugih pogodb, kandidatov za zaposlitev, prodajalcev in dobaviteljev, zdravstvenih delavcev in preizkušancev kliničnih raziskav ter uporabnikov spleta za namene zaposlovanja in upravljanja s kadri, internega imenika skupine, razvoja in upravljanja IT-sistema, promocije in ocene produktov in storitev, plačila storitev in povračila stroškov, izvajanja biomedicinskih raziskav oziroma kliničnih poskusov ter zagotavljanja uporabniku prilagojene izkušnje spletnih strani.

V zgoraj navedenih treh primerih je Informacijski pooblaščenec dovolil posredovanje osebnih podatkov na podlagi zavezujočih poslovnih pravil (BCR – *Binding Corporate Rules*). Po pregledu dokumentacije, ki so jo predložili izvozniki podatkov, je ugotovil, da so zavezani k spoštovanju zavezujočih poslovnih pravil, ki jih je sprejela mednarodna skupina, katere člani so. Zavezujoča poslovna pravila, sprejeta po ustreznem postopku, podrobneje predpisanim z dokumenti Delovne skupine iz 29. člena, ki zavezujejo vse članice mednarodne skupine, zagotavljajo, da skupina na področju prenosov podatkov v tretje države zagotavlja ustrezne ukrepe zavarovanja osebnih podatkov ter temeljnih pravic in svoboščin posameznikov ter navede možnosti njihovega uresničevanja ali varstva, skladno s 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, 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. Informacijski pooblaščenec je sodeloval v postopku vzajemnega priznavanja zavezujočih poslovnih pravil.

Informacijski pooblaščenec je prejel tudi predlog farmacevtske družbe za uvedbo postopka ugotavljanja ustrezne ravni varstva osebnih podatkov v Državi Izrael. Po proučitvi vloge je ugotovil, da Države Izrael ni na seznamu iz 66. člena ZVOP-1 in da je Komisija Evropskih skupnosti dne 31. 1. 2011 že izdala sklep Evropske Komisije št. 2011/61/EU o ustreznem varstvu osebnih podatkov, ki ga zagotavlja Država Izrael pri avtomatizirani obdelavi osebnih podatkov

v skladu z Direktivo Evropskega parlamenta in Sveta 95/46/ES. Kot navaja sklep v uvodni izjavi št. 9, pravni standardi varstva podatkov, ki se uporabljajo v Državi Izrael, zajemajo vsa temeljna načela, potrebna za ustrezno raven varstva za fizične osebe v zvezi z obdelavo osebnih podatkov v avtomatiziranih podatkovnih zbirkah. Ker je Informacijski pooblaščenec po določbi 67. člena ZVOP-1 pri svojem odločanju vezan na odločitve pristojnega organa EU, je v okviru prejete vloge in ob upoštevanju navedenega sklepa odločil, da Država Izrael zagotavlja ustrezno raven varstva osebnih podatkov v zvezi z avtomatiziranimi mednarodnimi prenosi osebnih podatkov iz EU ali neavtomatiziranimi prenosi, pri katerih se v Državi Izrael izvaja nadaljnja avtomatizirana obdelava.

Slika 14: Število vlog za izdajo odločbe glede iznosa osebnih podatkov med letoma 2007 in 2016.



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 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 oziroma obdelujejo le tiste vrste osebnih podatkov, ki jih določa veljavna zakonodaja. Povezovanje zbirk 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.); pri tem gre lahko zgolj za enosmeren tok prenosa podatkov.

Informacijski pooblaščenec je leta 2016 prejel štiri vloge za pridobitev dovoljenja za povezovanje zbirk osebnih podatkov. Izdal je tri odločbe, s katerimi je upravljavcem dovolil povezovanje zbirk osebnih podatkov, en postopek pa je s sklepom ustavil, ker je vlagatelj vlogo umaknil.

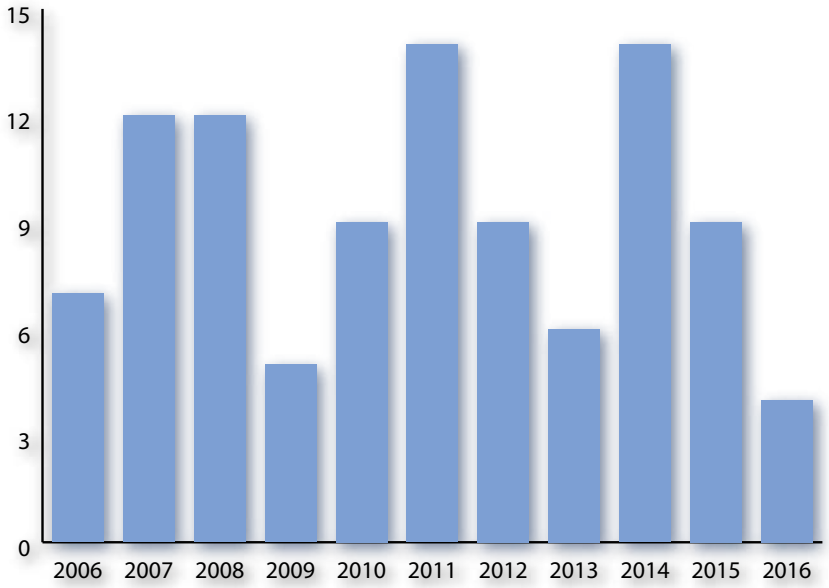
Informacijski pooblaščenec je dovolil povezovanje naslednjih zbirk osebnih podatkov:

1. Ministrstvu za delo, družino, socialne zadeve in enake možnosti je dovolil, da zbirke osebnih podatkov, vodene v okviru ISCSD (informacijski sistem centrov za socialno delo), neposredno računalniško poveže z Evidenco o davkih IDIS_REK, katere upravljavec je Ministrstvo za finance, Finančna uprava RS. Povezava med zbirkami se izvede na podlagi EMŠO.

2. Zavodu za zdravstveno zavarovanje Slovenije je dovolil, da Evidenco o zavarovanih osebah obveznega zdravstvenega zavarovanja poveže s Poslovnim registrom Slovenije, katerega upravljavec je Agencija RS za javnopravne evidence in storitve. Kot povezovalni znak se uporabi enotna matična številka občana (EMŠO) oziroma davčna številka.

3. Nacionalnemu inštitutu za javno zdravje je dovolil, da Centralni register podatkov o pacientih neposredno računalniško poveže s/z:
- Centralnim registrom prebivalstva in Matičnim registrom, katerega upravljavec je Ministrstvo za notranje zadeve;
- Evidenco o zavarovanih osebah obveznega zdravstvenega zavarovanja, katere upravljavec je Zavod za zdravstveno zavarovanje Slovenije;
- Zbirko osebnih podatkov o zavarovalcih in zavarovancih, katere upravljavec je Vzajemna zdravstvena zavarovalnica, d. v. z.;
- Zbirko podatkov o zavarovalcih, zavarovancih, plačnikih premije in upravičencih do izplačila zavarovalnine, katere upravljavec je Triglav, Zdravstvena zavarovalnica, d. d.;
- Zbirko podatkov o zavarovancih, katere upravljavec je Adriatic Slovenica, d. d.
- Neposredna računalniška povezava med zbirkami se lahko izvede z uporabo EMŠO oziroma številke obveznega zdravstvenega zavarovanja (ZZZS številka).

Slika 15: Število vlog za izdajo odločbe glede povezljivosti zbirk osebnih podatkov med letoma 2006 in 2016.



3.7. Pravica do seznanitve z lastnimi osebnimi podatki

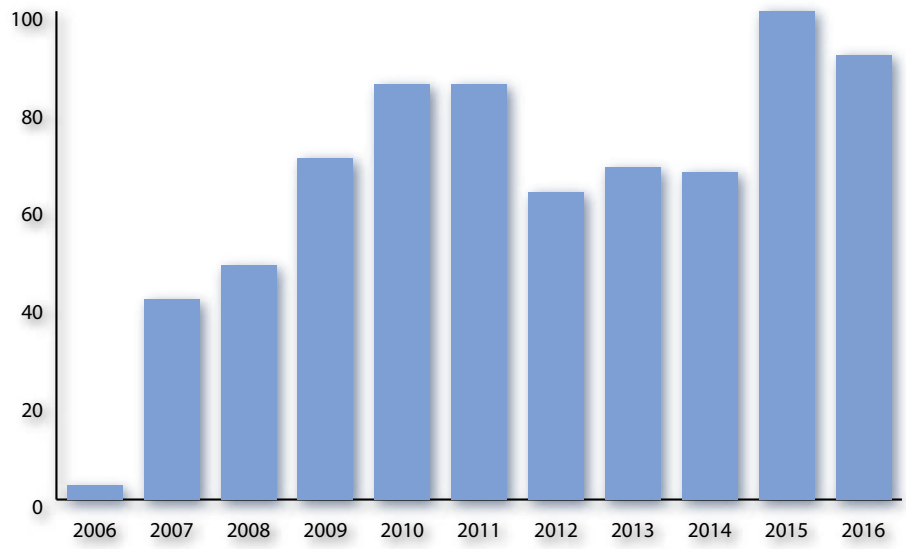
Pravica posameznika do seznanitve z lastnimi osebnimi podatki je ustavna pravica, določena v 38. členu Ustave RS, ki je konkretizirana v 30. (vsebina pravice) in 31. členu (postopek seznanitve) ZVOP-1. V skladu s prvim odstavkom 30. člena ZVOP-1 mora vsak upravljavec osebnih podatkov posamezniku na njegovo zahtevo npr. potrditi, ali se podatki v zvezi z njim obdelujejo ali ne, mu omogočiti vpogled v osebne podatke, ki so vsebovani v zbirki osebnih podatkov in se nanašajo nanj, ter mu omogočiti njihovo prepisovanje ali kopiranje; posredovati izpis osebnih

podatkov, ki so vsebovani v zbirki osebnih podatkov in se nanašajo nanj; posredovati seznam uporabnikov, katerim so bili osebni podatki posredovani, kdaj, na kakšni podlagi in za kakšen namen; dati informacijo o virih, na katerih temeljijo zapisi, ki jih o posamezniku vsebuje zbirka osebnih podatkov; dati informacije o namenu obdelave in vrsti osebnih podatkov, ki se obdelujejo. Glede na določbe 31. člena ZVOP-1 mora upravljavec osebnih podatkov posamezniku omogočiti seznanitev v 15 ali 30 dneh od prejema zahteve (odvisno od vsebine zahteve) ali pa ga v istem roku pisno obvestiti o razlogih, zaradi katerih mu seznanitve z lastnimi osebnimi podatki ne bo omogočil. Upravljavec osebnih podatkov mora posamezniku praviloma posredovati vse podatke, ki jih vodi v svojih zbirkah, saj je pravico posameznika do seznanitve z lastnimi osebnimi podatki, skladno s 36. členom ZVOP-1, mogoče izjemoma omejiti le z zakonom. Če upravljavec posamezniku ne odgovori ali njegovo zahtevo zavrne, lahko posameznik vloži pritožbo pri Informacijskem pooblaščencu.

Informacijski pooblaščenec je leta 2016 prejel 91 pritožb v zvezi s pravico do seznanitve z lastnimi osebnimi podatki. V okviru pritožbenih postopkov je Informacijski pooblaščenec reševal tudi pritožbe posameznikov, ki niso pridobili zdravstvene dokumentacije po ZPacP; teh je bilo 15.

Informacijski pooblaščenec je po preučitvi pritožb ugotovil, da je bil delež molka upravljavcev osebnih podatkov, ki na zahtevo posameznika po seznanitvi z lastnimi osebnimi podatki niso odgovorili, znašal 32 %, kar je skoraj isto kot leta 2015, ko je znašal 33 %. Leta 2014 je ta delež znašal 49 %, leta 2013 pa celo 52 %. Razlog za molk upravljavcev osebnih podatkov je bil v velikem številu primerov nepoznavanje pravice do seznanitve z lastnimi osebnimi podatki in dolžnosti upravljavcev v zvezi z njenim izvrševanjem.

Slika 16: Število pritožb v zvezi s pravico do seznanitve z lastnimi osebnimi podatki med letoma 2006 in 2016.



Vložene pritožbe so v 31 primerih zadevale državne organe (ministrstva in organe v njihovi sestavi, sodišča), v 15 primerih zdravstvene ustanove, v šestih primerih centre za socialno delo, v štirih primerih banke in v treh izobraževalne ustanove, preostale pritožbe pa so se nanašale na različne upravljavce osebnih podatkov (npr. društva, zavarovalnice, telekomunikacijske operaterje).

Informacijski pooblaščenec je po prejemu pritožbe upravljavca osebnih podatkov vedno najprej pozval, naj pojasni, zakaj posamezniku ni odgovoril ali zakaj mu ni omogočil seznanitve z lastnimi osebnimi podatki. V 27 primerih so upravljavci takoj po pozivu Informacijskega pooblaščenca posameznikom omogočili vpogled in pridobitev zahtevanih podatkov ali pa so jim posredovali pojasnilo, zakaj jim seznanitve ne bodo omogočili. Če upravljavec posamezniku seznanitve z lastnimi osebnimi podatki ni omogočil, je Informacijski pooblaščenec izdal odločbo in upravljavcu naložil, da mora posamezniku to omogočiti v določenem roku. Leta 2016 je izdal deset odločb, pri čemer je v petih odločbah pritožbam posameznikov v celoti ugodil, v petih pa delno. Devet upravljavcev je odločbe izvršilo, zoper eno odločbo pa je bila vložena tožba na Upravno sodišče

RS. Informacijski pooblaščenec je izdal tudi 11 odločb, s katerimi je pritožbe posameznikov zoper obvestila, ki so jim jih posredovali upravljavci osebnih podatkov, kot neutemeljene zavrnil, deset pritožb pa je zavrgel s sklepom (ker posameznik svoje vloge po pozivu ni dopolnil ali ker vloge ni vložila upravičena oseba).

V zvezi z vlogami, prejetimi leta 2016, je Informacijski pooblaščenec 23 posameznikom svetoval, kako naj postopajo, tri pritožbe je odstopil v reševanje pristojnim organom, dva posameznika pa sta pritožbi umaknila.

3.8. Pravica do dopolnitve, popravka, blokiranja, izbrisa in ugovora

Pravica do dopolnitve, popravka, blokiranja, izbrisa in ugovora je določena v 32. in 33. členu ZVOP-1. Prvi odstavek 32. člena ZVOP-1 določa, da mora upravljavec osebnih podatkov na zahtevo posameznika, na katerega se osebni podatki nanašajo, dopolniti, popraviti, blokirati ali izbrisati osebne podatke, za katere posameznik dokaže, da so nepopolni, netočni ali neažurni ali da so bili zbrani ali obdelani v nasprotju z zakonom. Dopolnitev, popravo, blokiranje ali izbris osebnih podatkov mora upravljavec osebnih podatkov v skladu z drugim odstavkom 33. člena ZVOP-1 opraviti v 15 dneh od dneva, ko je prejel zahtevo, in o tem obvestiti vlagatelja zahteve ali ga v istem roku obvestiti o razlogih, zaradi katerih tega ne bo storil. Če upravljavec zahtevi posameznika ne ugodi, varstva pravice do obdelave popolnih, točnih in ažurnih osebnih podatkov ta ne more zahtevati pri Informacijskem pooblaščencu, ampak skladno s 34. členom ZVOP-1 pred sodiščem.

Tretji odstavek 32. člena ZVOP-1 določa, da ima posameznik, katerega osebni podatki se obdelujejo v skladu s četrtim odstavkom 9. člena ali tretjim odstavkom 10. člena ZVOP-1, kadar koli z ugovorom pravico zahtevati prenehanje njihove obdelave. Upravljavec ugovoru ugodi, če posameznik dokaže, da niso izpolnjeni pogoji za obdelavo po navedenih členih. V tem primeru se njegovih osebnih podatkov ne sme več obdelovati. Če upravljavec ugovoru ne ugodi (tj. ne odloči v 15 dneh od njegovega prejema), lahko posameznik, ki je ugovor vložil, v skladu s četrtim odstavkom 32. člena ZVOP-1 zahteva, da o obdelavi osebnih podatkov odloči Državni nadzorni organ za varstvo osebnih podatkov, tj. Informacijski pooblaščenec. Vložena zahteva zadrži obdelavo tistih osebnih podatkov posameznika, glede katerih je vložil zahtevo.

Informacijski pooblaščenec je vodil tri postopke, v katerih je odločal o ugovorih treh vlagateljev, ki so zahtevali, da določenemu upravljavcu (upravniku večstanovanjske stavbe) in dvema posameznikoma prepove razkrivanje njihovih osebnih podatkov. Vlagatelji so navedli, da so skladno z drugim in tretjim odstavkom 32. člena ZVOP-1 od upravnika in posameznikov zahtevali, da takoj prenehajo protizakonito razkrivati njihove osebne podatke na način, da razpošiljajo odločbo Informacijskega pooblaščenca, na kateri niso zakrili vseh njihovih osebnih podatkov. Omenjeno odločbo je upravnik prejel od Informacijskega pooblaščenca in jo posredoval enemu izmed predstavnikov etažnih lastnikov določene soseske, jo je posredoval predsedniku nadzornega odbora, ta pa več stanovalcem določene večstanovanjske stavbe. Vlagatelji so od upravnika in posameznikov zahtevali tudi, da o prepovedi nadaljnjega razkrivanja osebnih podatkov obvestijo vse uporabnike, katerim so posredovali njihove osebne podatke, ter da jim to obvestilo pošljejo v vednost. Ker upravnik in posameznika na zahteve vlagateljev niso odgovorili v predvidenem roku 15 dni, se glede na tretji odstavek 33. člena ZVOP-1 šteje, da so njihove zahteve zavrnili.

Informacijski pooblaščenec je po pregledu odločbe ugotovil, da prikritje podatka o imenu ter naslovu prebivališča vlagateljev v konkretnem primeru ne more predstavljati anonimizacije v smislu 18. točke 6. člena ZVOP-1, ki določa, da je anonimiziranje takšna sprememba oblike osebnih podatkov, da jih ni več mogoče povezati s posameznikom ali pa je to mogoče le z nesorazmerno velikimi napori, stroški ali porabo časa. V konkretnem primeru gre namreč za specifično situacijo oziroma problematiko urejanja medsosedskih odnosov v zvezi z vzpostavitvijo vstopno-izstopnega sistema v določeni soseski, kjer je identiteta posameznikov, ki temu sistemu nasprotujejo, znana bolj ali manj širokemu krogu etažnih lastnikov in je relativno enostavno ugotovljiva. Zato je posredovanje odločbe Informacijskega pooblaščenca, čeprav v njej niso bila navedena celotna osebna imena in naslovi prebivališč vlagateljev, ampak le njihovi priimki in ulice prebivališč, predstavljalo obdelavo osebnih podatkov.

V postopku se Informacijski pooblaščenec ni posebej opredeljeval do vprašanja, ali je upravljavec

imel podlago za posredovanje osebnih podatkov v tretjem odstavku 10. člena ZVOP-1, saj je ugotovil, da že sam način obdelave osebnih podatkov v konkretnem primeru izključuje uveljavljanje pravice iz tretjega oziroma četrtega odstavka 32. člena ZVOP-1. Gramatikalna razlaga te zakonske določbe namreč kaže, da je predmet presoje lahko izključno dopustnost kontinuirane, še trajajoče obdelave osebnih podatkov, ki se izvršuje v enakih okoliščinah (na isti pravni in dejanski podlagi) in ki se bo po vsebini in naravi nadaljevala tudi v prihodnje. Tudi teleološka razlaga ne more voditi do drugačnega zaključka, saj je namen navedenih določb dati posamezniku pravico, da vsebinsko napade presojo upravljavca, ki meni, da ima za določeno obdelavo osebnih podatkov pravno podlago v tretjem odstavku 10. člena ZVOP-1, ki določa, da se osebni podatki lahko obdelujejo, če je to nujno zaradi uresničevanja zakonitih interesov zasebnega sektorja in ti interesi očitno prevladujejo nad interesi posameznika, na katerega se nanašajo osebni podatki. Posameznik, katerega osebni podatki se obdelujejo na podlagi tretjega odstavka 10. člena ZVOP-1, lahko najprej pri upravljavcu in nato še pri Informacijskem pooblaščencu uveljavlja argumente, zaradi katerih meni, da je upravljavec napačno opravil tehtanje zakonitih interesov zasebnega sektorja na eni strani in teže posega v informacijsko zasebnost posameznika na drugi. Cilj uveljavljanja teh argumentov je vedno prenehanje nadaljnje obdelave osebnih podatkov, ki še vedno poteka v okoliščinah, ki so predmet konkretne presoje.

Če je upravljavec osebnih podatkov podatke posredoval eni ali več osebam, lahko posameznik uveljavlja sodno varstvo po 34. členu ZVOP-1, v okviru katerega utemelji svoje stališče, da upravljavec za konkretno obdelavo (posredovanje) osebnih podatkov ni imel podlage niti v zakonu ali osebni privolitvi niti podlage ni mogla predstavljati določba tretjega odstavka 10. člena ZVOP-1. Posameznik na podlagi oziroma zaradi enkratnega posredovanja njegovih osebnih podatkov, ki se je z razkritjem le-teh tretji osebi že končalo, sklicujoč se na tretji oziroma četrti odstavek 32. člena ZVOP-1 ne more prepovedati vseh morebitnih prihodnjih posredovanj (ali drugih obdelav) njegovih osebnih podatkov, saj je zakonitost posamezne obdelave osebnih podatkov odvisna od okoliščin posameznega posredovanja, ki bo (npr. v primerih, kadar bo za posredovanje osebnih podatkov podana podlaga v zakonu) lahko tudi zakonito. Poleg tega vnaprejšnja prepoved »protizakonitega razkrivanja osebnih podatkov« zaradi nedoločnosti ni izvršljiva.

Presoja zakonitosti posameznega (vsakokratnega) posredovanja v preteklosti je tako mogoča v okviru prekrškovnega postopka, za vodenje katerega je pristojen Informacijski pooblaščenec, lahko pa je tudi predmet sodne presoje zahtevka, s katerim posameznik na podlagi 34. člena ZVOP-1 zahteva ugotovitev, da je kršitev obstajala, oziroma zahtevka za povračilo škode, ki je posamezniku nastala z (domnevno) nezakonitim posredovanjem njegovih osebnih podatkov nepooblaščenim osebam.

Informacijski pooblaščenec je zaradi posredovanja neanonimizirane odločbe vodil tudi postopek inšpekcijskega nadzora, v katerem je ugotovil, da upravnik in posameznika za posredovanje odločbe niso imeli ustrezne pravne podlage, pri čemer pa zaradi narave ugotovljene kršitve ni mogel odrediti prepovedi morebitne bodoče kršitve, pač pa je konkretno kršitev obravnaval po pravilih ZP-1. Vsakokratno morebitno ponovno posredovanje neanonimizirane odločbe, za katero ne bo podana pravna podlaga, bo predstavljalo nov prekršek, za katerega bo kršitelj odgovarjal skladno s pravili prekrškovnega prava.

Na podlagi navedenega je Informacijski pooblaščenec zaključil, da zahteve vlagateljev niso utemeljene, zaradi česar jih je z odločbami zavrnil.

3.9. Zahteve za oceno ustavnosti

Informacijski pooblaščenec lahko z zahtevo začne postopek za oceno ustavnosti oziroma zakonitosti predpisov na podlagi 23.a člena Zakona o Ustavnem sodišču[36], če se pojavi vprašanje ustavnosti ali zakonitosti v zvezi s postopkom, ki ga vodi. 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 2016 Informacijski pooblaščenec ni vložil nobene zahteve za oceno ustavnosti, je pa prejel v nadaljevanju povzeto odločitev Ustavnega sodišča.

[36] Uradni list RS, št. 64/2007 – uradno prečiščeno besedilo 1, s spremembami.

3.9.1. Odločitev Ustavnega sodišča RS v zvezi z zahtevo za presojo ustavnosti Zakona o davčnem postopku[37]

Informacijski pooblaščenec je prejel odločbo Ustavnega sodišča v zvezi z zahtevo iz aprila 2013, ko je vložil zahtevo za oceno ustavnosti določb prvega, sedmega in osmega odstavka 20. člena ZDavP-2, ki določajo javno objavo seznama neplačnikov davka na spletu, ker je ugotovil, da je z uporabo izpodbijanih zakonskih določb kršena pravica posameznikov do varstva osebnih podatkov, ki jo zagotavlja 38. člen Ustave RS. V postopku inšpekcijskega nadzora je namreč ugotovil, da so na spletnih straneh Davčne uprave RS in Carinske uprave RS objavljeni osebni podatki posameznikov (osebno ime, datum rojstva in »razred« višine zapadlih neplačanih davčnih obveznosti) in da so ti podatki objavljeni v skladu z zakonom, zaradi česar ni mogel naložiti njihovega umika. Informacijski pooblaščenec je v zahtevi navedel, da izpodbijane določbe ne prestanejo t. i. strogega testa sorazmernosti, po katerem mora biti ukrep, ki omejuje človekove pravice, primeren in nujen, da se dosežejo zasledovani legitimni cilji, škoda, ki bi posameznikom utegnila nastati zaradi ukrepa, pa mora odtehtati pozitivne učinke tega ukrepa. Informacijski pooblaščenec je poudaril, da ukrep javne objave osebnih podatkov ni nujen in tudi ne primeren za dosego cilja prostovoljnega poplačila davkov ali zvišanja stopnje splošne davčne kulture v državi, poleg tega je ureditev objave seznama dolžnikov neskladna tudi z 22. členom Ustave RS (enako varstvo pravic), in sicer zaradi odsotnosti ustreznih procesnih kavtel, ki bi posamezniku nudile primerno pravno varstvo v primeru neupravičene javne objave njegovih osebnih podatkov, saj svetovni splet praktično ne pozna pozabe. Pred objavo posameznik, katerega osebni podatki bodo objavljeni, namreč o tem ni posebej obveščen in nima možnosti, da bi se izjavil, ali je dolg dejansko pravilno ugotovljen in zakaj je nastal (mnogi posamezniki davka ne morejo plačati iz objektivnih razlogov).

Ustavno sodišče ni sledilo zahtevi za oceno ustavnosti Informacijskega pooblaščenca in je z odločbo U-I-122/13-13 z dne 10. 3. 2016 ugotovilo, da ZDavP-2 v izpodbijanem delu ni v neskladju z Ustavo in da je javna objava davčnih dolžnikov (fizičnih oseb) ustavno dopustna. Informacijski pooblaščenec bo odločitev Ustavnega sodišča seveda spoštoval, čeprav je prepričan, da predstavlja javna objava osebnih podatkov o dolžnikih na spletu določeno obliko stigmatizacije, četudi dolga ne morejo poplačati, in da gre glede na naravo spleta v resnici za nepovraten poseg v zasebnost posameznikov. Informacijski pooblaščenec bi si želel jasnejšo opredelitev Ustavnega sodišča do vprašanja, da gre vendarle za objavo podatkov iz nepravnomočnih davčnih odločb, na kar sta v odklonilnem ločenem mnenju opozorili tudi ustavni sodnici dr. Dunja Jadek Pensa in dr. Jadranka Sovdat.

Čeprav je Ustavno sodišče ocenilo, da predstavlja objava seznama dolžnikov primeren in sorazmeren ukrep za dosego cilja zvišanja davčne kulture, izboljšanja plačilne discipline ter spodbude k prostovoljnemu, pravilnemu in pravočasnemu plačevanju obveznosti, pa je po mnenju Informacijskega pooblaščenca zamudilo priložnost s tem, ko se ni opredelilo do vprašanja pravice do pravnega varstva posameznikov v luči presoje nujnosti in sorazmernosti posegov države v njihovo zasebnost. Poleg tega objava seznama dolžnikov ne doprinese k uresničitvi naštetih želenih ciljev, saj je vzpostavitev učinkovitega sistema plačevanja davkov dolžnost države in prevalitev kontrole na državljane ni ne ustrezna ne učinkovita.

Generalni finančni urad tako enkrat mesečno na svojih spletnih straneh objavi podatke o zavezancih za davek, ki so fizične osebe in ki dlje kot 90 dni dolgujejo več kot 5.000 evrov. Objavi dolžnikovo osebno ime in datum rojstva, podatki pa so razporejeni v razrede glede na višino zapadlih neplačanih davčnih obveznosti.

3.10. Izbrani primeri kršitev varstva osebnih podatkov

V nadaljevanju je predstavljenih osem odločitev Informacijskega pooblaščenca v postopkih, ki jih je vodil leta 2016.

[37] Uradni list RS, št. 13/2011– uradno prečičeno besedilo 4, s spremembami; v nadaljevanju ZDavP-2.

3.10.1. Izvajanje videonadzora nad dovozno potjo

Informacijski pooblaščenec je prejel prijavo, da je določen posameznik namestil kamero, s katero snema dovozno pot, ki jo uporablja več družin, s čimer nezakonito posega v njihovo zasebnost.

Po pregledu podatkov v zemljiški knjigi je Informacijski pooblaščenec ugotovil, da so vse ceste v okolici posameznikove hiše v zasebni lasti, torej tudi dovozna cesta, ki jo snema. Na podlagi tega je zaključil, da posameznik izvaja videonadzor za osebno uporabo, kar pomeni, da ga določbe ZVOP-1 ne zavezujejo. Prvi odstavek 7. člena ZVOP-1 namreč določa, da se ZVOP-1 ne uporablja za obdelavo osebnih podatkov (izvajanje videonadzora pomeni obdelavo osebnih podatkov), ki jo izvajajo posamezniki izključno za osebno uporabo, družinsko življenje ali za druge domače potrebe. Zato Informacijski pooblaščenec ni pristojen ukrepati. Ukrepal bi lahko, če bi posameznik snemal javno površino, saj je pri snemanju javnih površin treba upoštevati prakso Sodišča EU (sodba v zadevi C-212/13, František Ryneš proti Úřad pro ochranu osobních údajů), po kateri uporabe kamere, ki jo je fizična oseba namestila na družinsko hišo zaradi varovanja premoženja, zdravja in življenja lastnikov hiše, pri tem pa nadzira tudi javni prostor, ni več mogoče šteti izključno za osebno uporabo.

Informacijski pooblaščenec poudarja, da zgoraj navedeno ne pomeni, da posameznik, ki ga nekdo nepooblaščeno snema, nima pravnega varstva, če meni, da mu je bila kršena pravica do zasebnosti. Prizadeti posameznik lahko po 134. členu Obligacijskega zakonika[38] vloži tožbo na sodišče, ki lahko odredi prenehanje dejanja (videonadzora), s katerim se krši nedotakljivost človekove osebnosti, osebnega in družinskega življenja ali kakšna druga osebnostna pravica. Če nekdo brez dovoljenja in brez njihove vednosti snema druge ljudi na zemljišču izven meja svojih nepremičnin, je za svoja dejanja lahko tudi kazensko odgovoren. Neupravičeno slikovno snemanje pomeni po 138. členu Kazenskega zakonika[39] kaznivo dejanje, če storilec s svojim ravnanjem občutno poseže v zasebnost oziroma družinsko življenje drugega. Pregon se začne na predlog oškodovanca. Če je posamezniku s snemanjem njega, njegovih bližnjih ali njegovih prostorov ali s prikazovanjem posnetkov povzročena premoženjska ali nepremoženjska škoda, pa lahko od povzročitelja na podlagi 179. člena OZ zahteva odškodnino.

Ker Informacijski pooblaščenec vsako leto prejme večje število prijav, ki se nanašajo na izvajanje videonadzora nad zasebnimi zemljišči, poudarja, da videonadzor nad zasebnim zemljiščem, če ga ne izvaja poslovni subjekt, ne sodi v njegovo pristojnost, ne glede na to, da je na zemljišču vknjižena služnost. Zato v takih primerih ne more ukrepati. Vendar pa to, kot je pojasnjeno že zgoraj, ne pomeni, da snemani posamezniki nimajo pravnega varstva, saj lahko svoje pravice uveljavljajo pri drugih organih, npr. z vložitvijo tožbe na sodišče ali s podajo kazenske ovadbe policiji.

3.10.2. Zbiranje osebnih podatkov za namen izterjave parkirnin

Informacijski pooblaščenec je prejel več prijav zaradi suma neupravičenega pridobivanja osebnih podatkov za potrebe izterjav glob in neplačanih parkirnin v tujini, večinoma na Hrvaškem in v Srbiji. Iz prijav izhaja, da so slovenski državljani od tuje pravne osebe (v nadaljevanju TPO), ki naj bi njihove osebne podatke pridobila na nezakonit način, prejeli obvestila za plačilo terjatev oziroma pozive za plačilo globe zaradi napačnega parkiranja.

Na podlagi prijav je Informacijski pooblaščenec zoper odvetniško družbo uvedel inšpekcijski postopek, katerega predmet je bilo ugotavljanje zakonitosti obdelave (pridobivanja in posredovanja osebnih podatkov lastnikov oziroma uporabnikov motornih vozil iz centralne evidence registriranih motornih in priklopnih vozil) osebnih podatkov domnevnih dolžnikov terjatev, katerih plačilo TPO v imenu različnih pravnih oseb zahteva od posameznikov, ki so lastniki motornih vozil, registriranih v Republiki Sloveniji.

Informacijski pooblaščenec je ugotovil, da je odvetniška družba v zvezi z izterjavo domnevno neplačanih parkirnin za TPO nezakonito pridobivala osebne podatke lastnikov oziroma uporabnikov motornih vozil (imena, priimke, naslove prebivališča, EMŠO posameznikov ter maso motornega vozila), saj pogoji za pridobivanje osebnih podatkov na podlagi 10. člena Zakona o

[38] Uradni list RS, št. 97/2007 – uradno prečiščeno besedilo 1; v nadaljevanju OZ.
[39] Uradni list RS, št. 50/2012 – uradno prečiščeno besedilo 2, s spremembami in dopolnitvami; v nadaljevanju KZ-1.

odvetništvu[40] niso bili izpolnjeni. Odvetnik sme v skladu s tem členom pridobivati osebne podatke od zakonsko določenih upravljavcev (državni organi, organi samoupravnih lokalnih skupnosti ter nosilci javnih pooblastil) le takrat, ko te podatke potrebuje pri opravljanju odvetniškega poklica v posamični zadevi. Ne sme pa te pravice uporabiti na način, da za stranko izključno pridobiva osebne podatke na zalogo, ne da bi imel pri tem že v času pridobivanja podatkov namen (in naročilo) opraviti konkretno dejanje odvetniškega zastopanja, za katerega potrebuje podatke.

Odvetniška družba, kot je ugotovil Informacijski pooblaščenec, večine osebnih podatkov lastnikov motornih vozil, ki jih je na podlagi pooblastila TPO in seznama registrskih številk (pridobljenega od TPO) pridobivala od posameznih upravnih enot in jih nato posredovala TPO, ni potrebovala za opravljanje odvetniškega zastopanja, zato do njih ni bila upravičena. Naročnik oziroma TPO je namreč dejanja izterjave (pošiljanje opominov) opravljal sam in ne preko odvetniške družbe, slednja pa je trdila, da bo dejanja, usmerjena v izterjavo po potrebi eventualno opravila kasneje (na podlagi posebnih naknadnih naročil stranke). Ker je izpolnitev pogoja, da odvetnik te podatke potrebuje v posamičnem primeru, prestavljena v prihodnost in predstavlja bodoče negotovo dejstvo, ki se ne bo izpolnilo, če bo dolžnik na podlagi opomina upnika (ali njegovega pooblaščenca) svoj dolg poravnal, takšna praksa predstavlja pridobivanje osebnih podatkov v nasprotju z namenom 1. odstavka 10. člena ZOdv.

V postopku je bilo ugotovljeno, da je odvetniška družba od upravnih enot pridobila podatke približno 15.000 lastnikov motornih vozil in da je v manj kot 500 primerih izkazala, da osebne podatke potrebuje za izterjavo terjatev, ki jih dolžniki niso plačali na podlagi predhodnih opominov TPO. To pomeni, da je večino osebnih podatkov pridobila nezakonito, saj jih ni in jih ne bo potrebovala za opravljanje odvetniškega poklica, tj. za zastopanje svoje stranke. Zato je Informacijski pooblaščenec odvetniški družbi z odločbo odredil, da za TPO preneha pridobivati osebne podatke, če to počne zgolj z namenom posredovanja podatkov tej družbi, ter izbris vseh do trenutka izdaje odločbe nezakonito pridobljenih osebnih podatkov. Odločba še ni pravnomočna, ker je zavezanec zoper njo sprožil upravni spor.

Ker je bil omenjeni postopek medijsko odmeven, je Informacijski pooblaščenec, v izjavi za medije pojasnil, da v primerih, ko posamezniki so ali bodo prejeli pozive (opomine) na plačilo terjatev zaradi parkiranja v tujini od slovenske odvetniške družbe, najverjetneje ne gre za sum nezakonite obdelave osebnih podatkov, saj je odvetnik na podlagi pridobljenih podatkov opravil dejanje zastopanja – poslal opomin, to pa pomeni, da je osebne podatke pridobil skladno z 10. členom ZOdv. V primerih, ko posamezniki so ali bodo prejeli pozive (opomine) na plačilo terjatev iz naslova parkiranja v tujini izključno od katerekoli tuje pravne osebe, torej brez predhodnega opomina slovenskega odvetnika, pa gre zelo verjetno za primer nezakonite obdelave osebnih podatkov, kakršnega je Informacijski pooblaščenec obravnaval v tem postopku.

Informacijski pooblaščenec je poudaril, da posamezniki, kljub morebitnemu nezakonitemu pridobivanju njihovih osebnih podatkov, niso odvezani plačila dolga. Dejstvo namreč je, da upniki iz tujine (zakonito) razpolagajo s podatkom o registrski številki vozila, ki jim kadarkoli omogoča ugotavljanje identitete domnevnega dolžnika na zakonite načine. Če prejemniki opominov menijo, da dolga niso dolžni poravnati, bodo morali ugovor uveljavljati zoper upnika ali njegovega pooblaščenca, pri čemer pa jim Informacijski pooblaščenec ne more pomagati.

3.10.3. Uporaba telesnega skenerja na letališču

Informacijski pooblaščenec je prejel prijavo, iz katere je izhajalo, da naj bi zavezanec pri kontroli posameznikov, ki se opravi pred vstopom v potniške terminale, uporabljal telesni skener ter s tem nezakonito (ne da bi predhodno obvestil posameznike in pridobil njihove osebne privolitve) obdeloval oziroma zbiral osebne podatke.

V postopku inšpekcijskega nadzora je bilo ugotovljeno, da je zavezanec testiral varnostni skener, ki deluje na principu neionizirajočih milimetrskih valov. Zavezanec je pred uporabo skenerja pri Agenciji RS za civilno letalstvo podal vlogo za potrditev skladnosti skenerja z določili izvedbene uredbe Komisije (EU) št. 2015/1998 z dne 5. novembra 2015 o določitvi podrobnih ukrepov za izvajanje skupnih osnovnih standardov za varovanje letalstva. Agencija je ugotovila, da je skener skladen z uredbo in da je tudi ustrezno certificiran, certificirala ga je Evropska konferenca za civilno letalstvo (ECAC). Zato je agencija odobrila testno uporabo skenerja za obdobje od

[40] Uradni list RS, št. 18/1993 s spremembami; v nadaljevanju: ZOdv.

4. 4. 2016 do 30. 6. 2016, nadaljnja oziroma stalna uporaba pa bi bila dopustna, v kolikor bi jo zavezanec agenciji posebej priglasil.

Zavezanec je pojasnil, da pri skeniranju (posameznik se na za to označenem stojišču zavrti za 360 stopinj) sprejemne antene na podlagi odbitih valov sestavijo 3D-model posameznika, na katerem se označijo predeli, kjer bi lahko bili prepovedani materiali (npr. kovina, eksplozivo). Naprava 3D-model začasno shrani, vendar ga pregledovalcu ne pokaže neposredno, ampak v obliki dveh 2D-projekcij generične silhuete človeka (ene od spredaj in ene od zadaj), na katerih so s kvadratki označeni predeli, kjer je prišlo do neobičajnega odboja valov. Če naprava ne zazna neobičajnih odbojev, je pregled končan, v nasprotnem primeru se ponovi ali dopolni z ročnim pregledom. Potem se shranjena slika zavrže, kot to zahteva zgoraj omenjena uredba. To pomeni, da se niti izvorni 3D-modeli niti poenostavljeni 2D-modeli ne shranjujejo.

V postopku je bilo ugotovljeno še, da je zavezanec pri vhodu v napravo namestil pisno obvestilo, da se »pregled izvaja z varnostnim skenerjem, ki uporablja t. i. tehnologijo milimetrskih varnostnih valov«. Posameznik torej lahko rabo skenerja zavrne; v tem primeru je podvržen izključno ročnemu pregledu.

Na podlagi zgoraj navedenega je Informacijski pooblačenec zaključil, da zavezanec z uporabo varnostnega skenerja ne krši določb ZVOP-1, ker o potnikih ne zbira več osebnih podatkov, kot jih je zbiral pred začetkom uporabe skenerja, saj 3D- in 2D-modelov, ki se oblikujejo pri skeniranju, ne hrani. Zato je postopek inšpekcijskega nadzora ustavil.

3.10.4. Neustrezno zavarovanje osebnih podatkov uporabnikov storitev na strežnikih telekomunikacijskega operaterja

Informacijski pooblaščenec je prejel prijavo suma neustreznega zavarovanja osebnih podatkov uporabnikov storitev telekomunikacijskega operaterja (v nadaljevanju zavezanec), v kateri je bilo navedeno, da ima zavezanec nezavarovan dostop do osebnih podatkov uporabnikov storitev na dveh strežnikih, zaradi česar naj bi se na določenem spletnem naslovu nahajala odprta in prosto dostopna »Elasticsearch« podatkovna baza zavezanca, ki naj bi vsebovala dnevniške zapise zavezančevih e-poštnih strežnikov. Poleg tega naj bi se na določenem strežniku zavezanca nahajal prosto dostopen predpomnilnik »Memcached« povezane spletne aplikacije, ki naj bi razkrival e-poštne naslove prejemnikov in/ali pošiljateljev sporočil, časovne žige in IP-naslove.

24. in 25. člen ZVOP-1 določata, da mora upravljavec osebne podatke ustrezno zavarovati z uporabo organizacijskih, tehničnih in logično-tehničnih postopkov in ukrepov, s katerimi se prepreči slučajno ali namerno nepooblaščeno uničevanje osebnih podatkov, njihova sprememba ali izguba ter nepooblaščena obdelava tako, da se npr. varuje sistemsko programska in aplikativna programska oprema, s katero se obdelujejo osebni podatki, da se preprečuje nepooblaščen dostop do osebnih podatkov pri njihovem prenosu in da se zagotavlja sledljivost obdelave osebnih podatkov. Informacijski pooblaščenec je ugotovil, da zavezanec tega ni storil, saj so se na dveh poštnih strežnikih, s katerima je zavezanec upravljal, določeno obdobje nezavarovano hranili osebni podatki več kot 8.000 posameznikov (e-naslovi pošiljateljev sporočil in IP-naslovi, s katerih so sporočila pošiljali, e-naslovi prejemnikov sporočil, datumi in čas njihovega pošiljanja). Dostop do navedenih kategorij osebnih podatkov je bil mogoč z uporabo omrežnega protokola za oddaljeno povezovanje »Telnet«, s katerim je bilo v poštna strežnika zavezanca možno vstopiti prek določenih odprtih vrat iz razlogov, ker zavezanec ni zagotovil vključenosti požarne pregrade po nepredvidenem začasnem izklopu strežnika zaradi pregretja, varnostnih nastavitev pa zavezanec tudi ni redno preverjal in ker nikoli ni zagotovil omejitev dostopa do poštnih strežnikov z avtentikacijo (tj. najmanj z zahtevo po vnosu uporabniškega imena in gesla pooblaščenih zaposlenih) oziroma z drugimi ustreznimi metodami trajnega zavarovanja osebnih podatkov. Vsakdo, ki se je na zgoraj opisan način oddaljeno povezal na zavezančeva poštna strežnika, je nezavarovane osebne podatke lahko tudi kopiral, ker pa zavezanec ni imel zagotovljene ustrezne sledljivosti njihove obdelave, se osebne podatke nepooblaščeno, neizsledljivo in nenadzorovano še danes obdeluje.
Zaradi kršitve 24. in 25. člena ZVOP-1 je Informacijski pooblaščenec zoper zavezanca uvedel postopek o prekršku. Ko bo le-ta pravnomočno končan, bo Informacijski pooblaščenec zaključil tudi postopek inšpekcijskega nadzora, saj je zavezanec takoj po seznanitvi z varnostnimi pomanjkljivostmi sprejel ustrezne postopke in ukrepe za zavarovanje osebnih podatkov.

V postopku je bil podan sum, da je zavezanec poleg določb ZVOP-1 kršil tudi določbe Zakona o elektronskih komunikacijah[41], saj kot operater ni sprejel ustreznih tehničnih in organizacijskih ukrepov za obvladovanje tveganj za varnost omrežij in storitev, zaradi česar je Informacijski pooblaščenec prijavo, skupaj s svojimi ugotovitvami, v tem delu odstopil pristojnemu organu za nadzor nad izvajanjem ZEKom-1, to je Agenciji za komunikacijska omrežja in storitve. Ker so ugotovitve Informacijskega pooblaščenca nakazovale, da bi pri ukrepih nadzora obeh organov lahko prišlo do medsebojnega prekrivanja pristojnosti, je bilo med organoma vzpostavljeno strokovno sodelovanje.

3.10.5. Neustrezno zavarovanje osebnih podatkov pacientov in zaposlenih na spletni strani

Informacijski pooblaščenec je prejel prijavo, v kateri je bilo navedeno, da naj zavezanec ne bi ustrezno zavaroval osebnih in občutljivih osebnih podatkov na svoji spletni strani, saj naj bi zgolj vnos določene URL-povezave v spletni brskalnik omogočil dostop do občutljivih osebnih podatkov, med drugim tudi diagnoz posameznih pacientov.

Po ogledu zavezančeve spletne strani je Informacijski pooblaščenec ugotovil, da je vnos v prijavi navedene URL-povezave v spletni brskalnik omogočil nezaščiten dostop (tj. brez ustreznega uporabniškega imena in gesla) do večjega števila zdravstvene in druge dokumentacije, vključno z napotnicami, ki so vsebovale osebne in občutljive osebne podatke. Vnos povezave je omogočil tudi nezaščiten dostop do osebnih podatkov večjega števila zaposlenih pri zavezancu.

Zavezanec je še isti dan, ko je bil s strani Informacijskega pooblaščenca obveščen o varnostnem incidentu in pozvan, naj v čim krajšem času zavaruje dostop do podatkov na sporni spletni strani oziroma podstraneh na način, ki bo nepooblaščenim osebam onemogočal dostop do osebnih podatkov, po elektronski pošti poslal poročilo o razlogih, zaradi katerih je do incidenta prišlo, ter o ukrepih, ki jih je izvedel, da je varnostno luknjo odpravil. Pozneje je posredoval še dodatno pisno pojasnilo, v katerem je navedel, da je bil dostop do osebnih in občutljivih osebnih podatkov posledica varnostne luknje, ki jo je odkril anonimni napadalec. Zavezanec je poudaril, da javnost ni poznala spornega URL-naslova, ki je omogočal dostop do podatkov, iz dnevniškega zapisa, ki ga je zavezanec poslal skupaj s pojasnilom, pa je bilo razvidno, da je poleg Informacijskega pooblaščenca, ki je do spletne strani dostopal z namenom preverjanja navedb iz prijave, do podatkov dostopal zgolj napadalec. Zavezanec je navedel še, da je vzpostavil intervencijsko skupino strokovnjakov in da je o incidentu obvestil tudi SI-CERT.

Ker je zavezanec ugotovljene nepravilnosti odpravil, je Informacijski pooblaščenec postopek inšpekcijskega nadzora ustavil, zaradi neustreznega zavarovanja občutljivih osebnih podatkov pacientov in osebnih podatkov zaposlenih oziroma zaradi kršitve 24. in 25. člena ZVOP-1, ki določata postopke in ukrepe za zavarovanje osebnih podatkov, pa je zavezancu in njegovi odgovorni osebi izrekel globo.

3.10.6. Nezakonita pridobitev osebnih podatkov za namen neposrednega trženja

Informacijski pooblaščenec je prejel prijavo suma nezakonite pridobitve osebnih podatkov, iz katere je izhajalo, da direktor zavezanca za izvajanje neposrednega trženja uporablja bazo elektronskih naslovov družbe, pri kateri je pred ustanovitvijo svojega podjetja (zavezanca) opravljal delo prek študentskega servisa.

V postopku inšpekcijskega nadzora je bilo ugotovljeno, da je zavezanec v bazi podatkov, ki jo je uporabljal za namene neposrednega trženja, vodil osebne podatke fizičnih oseb, in sicer njihova imena, priimke in e-naslove. Zavezanec je imel dva meseca po začetku poslovanja v bazi za neposredno trženje skoraj 1.000 e-naslovov, od katerih naj bi jih 850 pridobil iz spletno dostopnih virov, preostale pa med lastnim poslovanjem, prek osebnih poznanstev in drugih virov. Informacijski pooblaščenec takšnim pojasnilom zavezanca ni mogel slediti, saj za večino e-naslovov, ki jih je naključno izbral iz baze, zavezanec ni uspel izkazati, da so dostopni na spletu. Po pregledu natisov spletnih strani, ki jih je predložil zavezanec, je Informacijski pooblaščenec ugotovil, da razen enega e-naslova kontekst objave ostalih ni v nikakršni zvezi z dejavnostjo, ki jo opravlja zavezanec. Zato je ocenil, da je najmanj neverjetno, da bi zavezanec v bazo za neposredno

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

trženje vnesel osebne podatke, ki so dostopni na spletu, ne da bi kontekst objave e-naslovov vsaj posredno nakazoval interese posameznikov, katerim je ponujal svoje storitve. Še toliko manj je bil navedeni način pridobivanja osebnih podatkov verjeten upoštevajoč ujemanje e-naslovov, ki jih je zavezanec uporabljal za neposredno trženje, z e-naslovi v bazi, ki jo je za neposredno trženje uporabljala družba, v kateri je direktor zavezanca delal. Ob primerjavi obeh baz je Informacijski pooblaščenec namreč ugotovil, da se kar 72 % e-naslovov ujema, zato je izključil tudi možnost, da bi si direktor zavezanca na podlagi izkušenj in poznanstev, ki si jih je pridobil v času opravljanja študentskega dela, uspel zapomniti takšno število strank ter pridobiti njihove kontaktne podatke (e-naslove) iz spletno dostopnih virov.

Na podlagi navedenega je Informacijski pooblaščenec zaključil, da direktor zavezanca e-naslovov, ki jih je uporabljal za neposredno trženje, ni pridobil na spletu, ampak je nezakonito skopiral bazo osebnih podatkov družbe, v kateri je prej delal. Poleg tega je zaključil, da bi zavezanec za hrambo in uporabo teh e-naslovov za neposredno trženje moral imeti ustrezno pravno podlago, ki bi jo glede na naravo stvari v konkretnem primeru lahko predstavljala izključno osebna privolitev posameznikov, na katere se e-naslovi nanašajo. Zavezanec je tekom postopka pridobil privolitve 98 posameznikov, da lahko njihove e-naslove uporablja za pošiljanje oglasnih sporočil, vse ostale e-naslove fizičnih oseb pa je iz svoje baze izbrisal. S tem je ugotovljene nepravilnosti odpravil, zaradi česar je Informacijski pooblaščenec inšpekcijski postopek ustavil, začel pa je postopek za prekške. Zavezanec oziroma njegov direktor je s svojim ravnanjem (obdelava osebnih podatkov brez podlage v zakonu ali v osebnih privolitvah posameznikov) kršil 8. člen ZVOP-1, za kar mu je Informacijski pooblaščenec izrekel globo.

3.10.7. Razkrivanje podatkov o osebnem stečaju na poštnih ovojnicah

Informacijski pooblaščenec je uvedel dva postopka inšpekcijskega nadzora zaradi suma nezakonitega razkrivanja podatkov o osebnem stečaju posameznikov na poštnih ovojnicah na način, da sta zavezanca na zunanjo stran pisemskih ovojnic, poleg imena in priimka naslovnika (posameznika, ki je bil v osebnem stečaju), zapisovala opombo »V OSEBNEM STEČAJU«, s čimer naj bi posegala v posameznikovo (informacijsko) zasebnost in kršila določbe ZVOP-1.

V prvem inšpekcijskem postopku je bilo ugotovljeno, da je zavezanec (dobavitelj komunalnih storitev) na vse pošiljke, ki jih je pošiljal neposredno insolventnim dolžnikom (tako posameznikom kot podjetnikom oziroma zasebnikom, ki so bili v postopku osebnega stečaja), pripisal opombo »V OSEBNEM STEČAJU«. Samo če je zavezanec pošiljke insolventnim dolžnikom pošiljal prek stečajnih upraviteljev, ta opomba ni bila vidna, saj ni bila izpisana na zunanji strani ovojnice, ampak na dokumentu, ki je bil vložen v pisemsko ovojnico. Zavezanec je v inšpekcijskem postopku navajal, da je navedeno opombo poleg imen in priimkov naslovnikov izpisoval na ovojnice oziroma dokumente zato, ker mu informacijska rešitev ni omogočala ločenega vodenja podatkovnih baz, da bi podatke o insolventnosti dolžnikov evidentiral ločeno.

Podatke o plačilni (ne)sposobnosti oziroma o osebnih stečajih naj bi posamezniki po pogodbi o dobavi komunalnih storitev bili dolžni zavezancu sporočati sami, zaradi njihove nedoslednosti pri izpolnjevanju te obveznosti iz pogodbenega razmerja pa jih je zavezanec bil primoran pridobivati iz javno dostopne evidence AJPES tudi sam. Pravno podlago za obdelavo (pridobitev in hrambo) osebnih podatkov uporabnikov komunalnih storitev, tudi podatkov o osebnih stečajih, je zavezancu tako predstavljal drugi odstavek 10. člena ZVOP-1, ki dopušča obdelavo osebnih podatkov posameznikov, ki so z zasebnim sektorjem sklenili pogodbo, če je obdelava potrebna in primerna za izpolnjevanje pogodbe. Vendar pa ta določba sama po sebi zavezancu ni zagotavljala ustrezne pravne podlage, da bi tako pridobljene podatke posameznikov razkrival naprej nepooblaščenim osebam ali celo javnosti.

Ker je zavezanec svoje ravnanje utemeljeval tudi s tem, da so podatki o osebnih stečajih vendar javno dostopni prek portala AJPES, mu je Informacijski pooblaščenec pojasnil, da iz Zakona o finančnem poslovanju, postopkih zaradi insolventnosti in prisilnem prenehanju[42] izhaja, da enostavno iskanje insolventnega posameznika zgolj po osebnem imenu ni dopustno in ga AJPES tudi ne omogoča. Vpogled v Vpisnik zadev v postopkih zaradi insolventnosti, ki je dostopen na spletnih straneh AJPES, je v skladu s tretjim odstavkom 122. člena ZFPPIPP za posameznika mogoč le pod posebnimi pogoji (npr. kombinacija EMŠO ter imena in priimka, kombinacija davčne številke ter imena in priimka, kombinacija imena, priimka, naslova stalnega prebivališča

[42] Uradni list RS, št. 13/2014 – uradno prečiščeno besedilo 1 s spremembami; v nadaljevanju ZFPPIPP.

in rojstnega datuma). ZFPPIPP je način iskanja podatkov o osebnem stečaju posameznika omejil prav zaradi varstva zasebnosti.

Informacijski pooblaščenec je zaključil, da podatki o osebnem stečaju posameznika niso javno dostopni, ampak gre za varovane osebne podatke, do katerih lahko pod posebnimi pogoji prek portala AJPES dostopajo le pooblaščeni uporabniki. Zato bi zavezanec v skladu s 24. in 25. členom ZVOP-1 moral poskrbeti za njihovo zavarovanje tudi v času prenosa pošiljke po pošti, bodisi z blokiranjem izpisa oznake »V OSEBNEM STEČAJU« na ovojnicah bodisi z njenim izbrisom pred pošiljanjem, česar pa ni storil. Zato je bil status plačilne (ne)sposobnosti posameznega uporabnika komunalnih storitev razviden iz ovojnice pošiljke ter tako dostopen oziroma nezakonito razkrit vsem, ki so rokovali s pošiljko (poštni delavci, sosedje, sostanovalci ipd.). Informacijski pooblaščenec je zaradi nezakonitega razkrivanja osebnih podatkov zoper zavezanca in njegovo odgovorno osebo uvedel postopek o prekršku, postopek inšpekcijskega nadzora pa je ustavil, saj je zavezanec izpisovanje opombe o osebnem stečaju na ovojnice in dokumente trajno preprečil ter o tem predložil ustrezna dokazila.

V drugem postopku inšpekcijskega nadzora je bilo ugotovljeno, da zavezanec (banka) osebne podatke komitentov, ki so v osebnem stečaju, obdeluje na podlagi sklenjene pogodbe za opravljanje posameznih bančnih in finančnih storitev, podatke o osebnem stečaju pa na podlagi obvestila stečajnega upravitelja oziroma sklepa stečajnega sodišča. Zavezanec je izjavil, da pri pošiljanju pisemskih pošiljk posameznikom, ki so v osebnem stečaju, poleg osebnega imena ne navaja opombe »V OS. STEČAJU«, ampak se dejstvo o uvedenem postopku osebnega stečaja komitenta zabeleži v posebno polje v bazo komitentov, saj iz tega statusa posameznika izhaja več pravnih obveznosti in odgovornosti zavezanca. V konkretnem primeru je kljub jasnim internim navodilom za zaposlene prišlo do napake pri vpisu podatkov v bazo, in sicer s strani delavke, ki je s soglasjem sodišča stečajni dolžnici posameznici odpirala nov transakcijski račun, pri čemer je v bazi podatkov v polju za naziv komitenta, namesto v polju insolvenčni postopki, evidentirala podatek o osebnem stečaju. Posledično so bile komitentki posredovane poštne pošiljke (opomini in obvestila o TRR) s spornim pripisom poleg imena in priimka. Ko je komitentka zavezanca na to opozorila, je ta iz polja za naziv komitentke takoj izbrisal sporen osebni podatek.

Informacijski pooblaščenec je zaključil, da zavezanec ni zagotovil ustreznega zavarovanja osebnih podatkov komitentke, saj se je podatek o osebnem stečaju, zaradi vnosa v napačno polje baze podatkov in zaradi nezagotovljenih kontrol odprave napak, izpisoval na ovojnicah poštnih pošiljk poleg njenega imena in priimka, zato se je z njim lahko nepooblaščeno seznanil vsak, ki mu je pošiljka prišla v roke. Zavezanec je s tem kršil določbe 3. točke prvega odstavka 24. člena in prvega odstavka 25. člena ZVOP-1, iz katerih izhaja, da je vsak upravljavec osebnih podatkov dolžan zagotoviti njihovo zavarovanje tudi pri njihovem prenosu (npr. pošiljanju po pošti). Informacijski pooblaščenec je zavezanki izrekel ukrep po ZP-1, postopek inšpekcijskega nadzora pa ustavil, ko mu je zavezanec izkazal, da je storjeno napako odpravil.

3.10.8. Nezakonito posredovanje osebnih podatkov v zvezi z zaračunavanjem stroškov kopiranja

Informacijski pooblaščenec je prejel prijavo, iz katere je izhajal sum, da je zavezanec osebne podatke dijakov nezakonito posredoval zasebnemu izvajalcu storitev fotokopiranja, ki svojo dejavnost opravlja v zavezančevih prostorih, in sicer za namen izstavitve predračuna za fotokopiranje neobveznih šolskih gradiv. Na podlagi prejete prijave je uvedel inšpekcijski postopek zoper zavezanca in izvajalca fotokopiranja.

V postopku inšpekcijskega nadzora je bilo ugotovljeno, da je zavezanec upravljavec osebnih podatkov dijakov in njihovih zakonitih zastopnikov, ki so ob vpisu dijakov v štiriletno izobraževanje podpisali izjavo, da sme zavezanec njihove osebne podatke v času šolanja obdelovati v zvezi z njihovim izobraževanjem in stroški, povezanimi z le-tem (prevozi za športni dan, prispevek za učbeniški sklad … ter prispevek za neobvezne fotokopije). Položnice za strošek fotokopiranja neobveznih gradiv v fotokopirnici je računovodstvo zavezanca dijakom izdajalo do šolskega leta 2015/2016, ko se je zavezanec zaradi vse večjih dolgov in zamud plačil odločil za spremembo zaračunavanja navedene storitve, v skladu s katero naj bi položnice v svojem imenu in za svoj račun izdajal izvajalec fotokopiranja. Zakoniti zastopniki dijakov so bili s spremembo načina plačevanja, ki jo je potrdil tudi Svet staršev oziroma šole, seznanjeni na različne načine (na roditeljskem sestanku, z objavo v šolski publikaciji, z elektronsko okrožnico ravnatelja) in ker spremembi niso izrecno nasprotovali, je zavezanec izvajalcu fotokopiranja za namen izstavitve

ponudb oziroma predračunov ocenjenega letnega stroška fotokopiranja po e-pošti poslal celotno preglednico z osebnimi podatki (ime, priimek, naslov bivališča) vseh 770 dijakov in 1.470 njihovih zakonitih zastopnikov, s čimer pa posamezniki, na katere so se osebni podatki nanašali, niso bili predhodno seznanjeni.

Informacijski pooblaščenec je zaključil, da zavezanec ni imel pravne podlage za posredovanje osebnih podatkov izvajalcu fotokopiranja. Glede na to, da obdelave osebnih podatkov dijakov in njihovih staršev za namen storitev fotokopiranja neobveznih gradiv (npr. neobveznih učnih listov in drugih, s strani šole priporočenih gradiv) ne ureja noben specialni zakon, je bilo treba pri presoji dopustnosti obdelave osebnih podatkov upoštevati drugi odstavek 9. člena ZVOP-1, v skladu s katerim bi zavezanec osebne podatke dijakov oziroma zakonitih zastopnikov, ki jih je pridobil za namen izvajanja obveznih vzgojno-izobraževalnih vsebin po programu javne šole, izvajalcu storitev fotokopiranja lahko posredoval le na podlagi predhodne osebne privolitve posameznikov (tj. vseh polnoletnih dijakov, zakonitih zastopnikov mladoletnih dijakov in ostalih zakonitih zastopnikov), v skladu z načelom sorazmernosti iz 3. člena ZVOP-1, pa še to le za enega posameznika na vsakega dijaka.

Tudi konkludentna privolitev dijakov in staršev, na katero se je skliceval zavezanec (ker starši spremembi plačila niso izrecno nasprotovali, je zavezanec to štel kot konkludentno privolitev k posredovanju podatkov), ni mogla predstavljati pravne podlage za obdelavo (posredovanje, razkrivanje, dejanje na razpolago) osebnih podatkov, saj so zavezančeva obvestila vsebovala zgolj informacijo o spremembi načina plačila neobveznih fotokopij in o novem prejemniku plačila, ne pa informacij, kaj ta sprememba pomeni za posameznike z vidika obdelave njihovih osebnih podatkov. Poleg tega zavezanec v postopku ni izkazal, da bi obvestila o spremembi plačila sploh dosegla vse posameznike, katerih osebne podatke je posredoval. Pravne podlage za posredovanje osebnih podatkov pa ni mogla predstavljati niti izjava zakonitih zastopnikov dijakov, ki so jo podpisali ob vpisu, da zavezanec lahko obdeluje njihove osebne podatke tudi za obračunavanje prispevka neobveznih fotokopij, saj iz nje ne izhaja, da lahko zavezanec za ta namen osebne podatke njih in njihovih dijakov razkriva in posreduje v uporabo tretjim osebam. Zato je Informacijski pooblaščenec zoper zavezanca in njegovo odgovorno osebo uvedel postopek o prekršku, inšpekcijski postopek pa je ustavil, ker je v obravnavanem primeru posredovanja zbirke osebnih podatkov šlo za enkratno dejanje v preteklosti, ki ga z inšpekcijskim ukrepom za nazaj ni bilo več možno preprečiti ali odpraviti.

V postopku zoper izvajalca fotokopiranja je Informacijski pooblaščenec ugotovil, da je osebne podatke dijakov, ki jih je pridobil od zavezanca, uporabil za izstavitev predračunov za ocenjeni strošek fotokopiranja v šolskem letu 2015/2016. Kot pravno podlago za takšno obdelavo osebnih podatkov je navedel 5. točko prvega odstavka 82. člena Zakona o davku na dodano vrednost[43], ki določa, da mora davčni zavezanec, ki izda račun, na računu navesti naslednje podatke: ime in naslov davčnega zavezanca in njegovega kupca ali naročnika.

Informacijski pooblaščenec je zaključil, da navedena določba ZDDV-1 ni bila ustrezna pravna podlaga za pridobivanje in nadaljnjo obdelavo osebnih podatkov vseh dijakov in njihovih zakonitih zastopnikov, saj izvajalec fotokopiranja ni izkazal, da je v času pridobivanja navedenih osebnih podatkov (že) obstajalo obligacijsko razmerje med njim in posameznim dijakom kot naročnikom ali kupcem storitev fotokopiranja gradiv. Takšno razmerje je v skladu z 28. členom Obligacijskega zakonika[44] nastalo šele s sprejemom ponudbe (tj. s plačilom predračuna, ki ga je izstavil izvajalec fotokopiranja), kar je predstavljalo zakonsko podlago za izstavitev računa v skladu z določbo 82. člena ZDDV-1. Izstavljeni predračun je izvajalcu plačalo 768 dijakov, katerim je izdal tudi račun. Dva dijaka izstavljenega predračuna nista plačala, kar pomeni, da nista sprejela ponudbe izvajalca, ki je zato njune osebne podatke v svoji zbirki osebnih podatkov vodil nezakonito. Glede na to, da so se vsi predračuni in računi glasili zgolj na dijake in ne na njihove zakonite zastopnike, je Informacijski pooblaščenec zaključil tudi, da je izvajalec fotokopiranja osebne podatke vseh 1.470 zakonitih zastopnikov obdeloval (pridobival in nadalje hranil) brez kakršne koli potrebe in upoštevanja načela sorazmernosti, poleg tega za njihovo obdelavo ni imel nobene od pravnih podlag iz 10. člena ZVOP-1, ki določa obdelavo osebnih podatkov v zasebnem sektorju. Informacijski pooblaščenec je zato izvajalca fotokopiranja pozval, da izbriše nezakonito pridobljene in hranjene osebne podatke dveh dijakov in vseh zakonitih zastopnikov. Izvajalec fotokopiranja je podatke v celoti in trajno izbrisal ter priložil dokazilo o tem, s čimer je ugotovljeno kršitev določb ZVOP-1 odpravil, zato je bil inšpekcijski postopek ustavljen.

[43] Uradni list RS, št. 13/2011 – uradno prečiščeno besedilo 3, s spremembami; v nadaljevanju ZDDV-1.
[44] Uradni list RS, št. 83/2001 s spremembami in dopolnitvami; v nadaljevanju OZ.

3.11. Splošna ocena stanja varstva osebnih podatkov in priporočila

Informacijski pooblaščenec je leta 2016 v okviru izvajanja inšpekcijskega nadzora na področju varstva osebnih podatkov obravnaval:

- 683 inšpekcijskih zadev, od tega 245 na področju javnega in 438 na področju zasebnega sektorja in
- 83 prekrškovnih zadev.

Poleg inšpekcijskih in prekrškovnih postopkov je Informacijski pooblaščenec leta 2016 prejel in obravnaval še:

- 1.330 zaprosil za pisna mnenja in pojasnila s področja varstva osebnih podatkov,
- štiri vloge za izdajo dovoljenja za povezovanje zbirk osebnih podatkov,
- štiri vloge za izdajo dovoljenja za izvajanje biometričnih ukrepov,
- 53 vlog za izdajo dovoljenja za iznos osebnih podatkov,
- 91 pritožb zaradi zavrnitve zahteve za seznanitev z lastnimi osebnimi podatki,
- tri pritožbe v zvezi z zavrnitvijo zahteve za prenehanje obdelave osebnih podatkov.

Od skupaj 683 inšpekcijskih zadev je bila 601 zadeva obravnavna zaradi prejetih prijav, 82 pa jih je bilo obravnavanih na lastno pobudo. Na področju javnega sektorja je bilo vloženih 211 prijav in pritožb, na področju zasebnega sektorja pa 390. Število prijav zaradi suma kršitev predpisov s področja varstva osebnih podatkov je bilo podobno kot v preteklih letih, prav tako so podobno prevladovale prijave zaradi posredovanja osebnih podatkov nepooblaščenim uporabnikom, zaradi uporabe osebnih podatkov za namene neposrednega trženja (zlasti zaradi suma nezakonitega pridobivanja osebnih podatkov za te namene ter neupoštevanja zahteve posameznika po prenehanju uporabe osebnih podatkov za te namene), zaradi preusmeritve in posledično branja elektronske pošte, ki prihaja na službeni elektronski naslov zaposlenih, zaradi izvajanja videonadzora (zlasti v delovnih prostorih), zaradi objave osebnih podatkov na spletnih straneh ter pomanjkljivega zavarovanja osebnih podatkov.

Podobno kot v preteklih letih je Informacijski pooblaščenec pri obravnavi prejetih prijav od skupaj 601 obravnavane prijave v 299 primerih že na podlagi preučitve navedb v sami prijavi in priložene dokumentacije presodil, da opisana ravnanja ne pomenijo takšne kršitve predpisov s področja varstva osebnih podatkov, ki sodi v njegovo pristojnost. Takšnih prijav je bilo torej kar 49 %. Glavni razlog za tako veliko število neutemeljenih prijav je, da prijavitelji pogosto premalo poznajo predpise s področja varstva osebnih podatkov in pristojnosti Informacijskega pooblaščenca, žal pa Informacijski pooblaščenec poleg takšnih prijav, ki so vložene »dobrohotno« in iz upravičenih razlogov, vse prepogosto dobiva tudi prijave, katerih namen ni varstvo javnega interesa ali vzpostavitev zakonitega stanja na področju varstva osebnih podatkov, temveč predvsem »nagajanje«, želja po maščevanju ter poizkus reševanja medsebojnih sporov in uveljavljanja takšnih zasebnih interesov, ki jih v postopku inšpekcijskega nadzora Informacijskega pooblaščenca sploh ni mogoče uveljavljati. Veliko število neupravičeno vloženih prijav ter nujnost njihove obravnave ovirata opravljanje t. i. preventivnega inšpekcijskega nadzora na področjih, kjer bi se ta moral več izvajati. Državni nadzornik, ki zadevo obravnava, vsem takšnim prijaviteljem pošlje pisno obvestilo, v katerem obrazloži razloge, zaradi katerih opisano ravnaje ne pomeni kršitve zakona oziroma zaradi katerih Informacijski pooblaščenec kot inšpekcijski oziroma prekrškovni organ ni pristojen ukrepati, pri čemer pa se prijavitelji na takšno obvestilo pogosto pritožijo in poskušajo izsiliti ukrepanje oziroma kaznovanje zavezanca.

Med prijavami, pritožbami in zadevami, ki so vložene zaradi nepoznavanja pristojnosti Informacijskega pooblaščenca, velja izpostaviti tiste, povezane z zbiranjem in uporabo osebnih podatkov v sodnih in upravnih postopkih. Informacijski pooblaščenec namreč vsako leto prejme precej prijav in zahtev, s katerimi stranke v sodnih in upravnih postopkih zatrjujejo, da sodnik ali uradna oseba, ki vodi postopek, za namene ugotavljanja dejanskega stanja nezakonito in nesorazmerno zbira osebne podatke, zaradi česar prijavitelji zahtevajo, da Informacijski pooblaščenec ukrepa zoper sodnika oziroma pooblaščeno uradno osebo ter ji naloži, da v sodnem ali upravnem spisu uniči dokumentacijo, ki vsebuje domnevno nezakonito pridobljene osebne podatke. Informacijski pooblaščenec v takšnih primerih prijaviteljem pošlje obvestilo o neuvedbi inšpekcijskega postopka, v katerem pojasni, da skladno s sklepom Ustavnega sodišča RS št. U-I-92/12-13 z dne 10. 10. 2013 inšpekcijskega nadzora nad izvajanjem ZVOP-1 ne sme izvajati tako, da pri izvrševanju svojih zakonsko določenih pooblastil poseže v posamične pravne postopke, ki jih vodijo za to pristojni državni organi, ter da v inšpekcijskem postopku ne sme preverjati, ali se v konkretnih pravnih postopkih ustavnoskladno in zakonito spoštuje varstvo osebnih podatkov. Kot

je v omenjenem sklepu zapisalo Ustavno sodišče, bi bila zakonska podlaga, ki bi to omogočala, v nasprotju z načelom samostojnosti pristojnega državnega organa pri odločanju (drugi odstavek 120. člena Ustave RS za upravne organe in 125. člen Ustave RS za sodišča) ter v nasprotju z rednim sistemom pravnih sredstev oziroma vzpostavljeno hierarhično strukturiranostjo državne oblasti (načelo večstopenjskega odločanja), s tem pa v nasprotju z načeli pravne države (2. člen Ustave RS). Ta načela zahtevajo, da o pravicah in obveznostih fizičnih in pravnih oseb odločajo pristojni organi v postopkih, ki so vnaprej zakonsko določeni, pri čemer se njihove odločitve lahko preverjajo le v vnaprej določenih postopkih s pravnimi sredstvi pred pristojnimi organi. Skladno s citiranim sklepom Ustavnega sodišča RS lahko posamezniki svoje pravice v zvezi z obdelavo osebnih podatkov, ki so bili pridobljeni in se uporabljajo za namene odločanja v sodnih in drugih pravnih postopkih, uveljavljajo pred organom, ki vodi postopek, in sicer z uporabo ugovorov, rednih ali izrednih pravnih sredstev, v skladu z zakoni, ki urejajo pravni postopek v konkretni zadevi, ne morejo pa tega uveljavljati s prijavo, pritožbo oziroma zahtevo, naslovljeno na Informacijskega pooblaščenca.

Informacijski pooblaščenec je leta 2016 okrepil izvajanje t. i. planiranih *ex offo* inšpekcijskih nadzorov, ki se vsako leto izvajajo skladno s sprejetim letnim načrtom. Planirani inšpekcijski nadzor nad spoštovanjem določb ZVOP-1 se je leta 2016 izvajal v policiji, zdravstvenih zavodih, bankah in hranilnicah, pri dajalcih potrošniških kreditov, v zavarovalnicah, organih lokalne samouprave, visokošolskih zavodih, srednjih šolah ter energetskih družbah.

Kot je bilo ugotovljeno že v poročilu za leto 2015, se je v zadnjih desetih letih delovanja Informacijskega pooblaščenca bistveno izboljšala ozaveščenost tako splošne kot strokovne javnosti glede zasebnosti in varstva osebnih podatkov. Osnovne težave glede poznavanja zakonodaje so bile presežene, še vedno pa pri upravljavcih osebnih podatkov in njihovih pogodbenih obdelovalcih na nekaterih področjih ostajajo pomanjkljivosti in se pojavljajo nepravilnosti. Pri tem je treba izpostaviti zlasti podatke o zdravstvenem stanju, ki sodijo med občutljive osebne podatke, zato morajo uživati najvišjo stopnjo varovanja; zlorabe teh podatkov imajo namreč lahko resne in dolgotrajne posledice za posameznika, vsaka nepooblaščena obdelava pa pomeni poseg v temeljne pravice pacientov. Informacijski pooblaščenec zato že ves čas veliko pozornosti namenja ustrezni ozaveščenosti in izvajanju nadzora v zdravstvenih institucijah, upoštevaje resurse, ki jih ima na voljo, ter dejstvo, da je pristojen za praktično celoten javni in zasebni sektor. Po uradni dolžnosti je tako v okviru planiranih vsakoletnih inšpekcijskih nadzorov opravil večje število nadzorov v bolnišnicah in pri drugih izvajalcih zdravstvenega varstva. Če je bila sledljivost dostopov do zdravstvenih podatkov pred desetimi leti redkost, so inšpekcijski postopki Informacijskega pooblaščenca in odrejeni ukrepi zdravstvenim zavodom možnost nezabeležnih dostopov precej zmanjšali. Čeprav se je stanje tudi na podlagi ugotovitev in ukrepov pristojnih nadzornih inštitucij popravilo, v zdravstvenem sektorju še vedno opažamo določene kršitve, med katerimi izpostavljamo zlasti:

- pošiljanje zdravstvenih podatkov po nezavarovanih (nešifriranih) povezavah (običajna e-pošta, nešifrirane spletne povezave);
- posojanje avtentikacijskih sredstev za dostop do podatkov, kot so gesla in kartice, ter njihovo neustrezno varovanje,
- curljanje in prodajanje podatkov iz zdravstvenih ustanov za namene neposrednega trženja,
- omejena preglednost in nadzor nad obdelavami podatkov s strani zunanjih izvajalcev,
- premalo zavedanja o neprimernosti širjenja informacij o pacientih,
- pomanjkljivo zavarovanje prostorov, v katerih se hranijo zdravstvene kartoteke.

Informacijski pooblaščenec je zato pozval vse upravljavce, ki obdelujejo zdravstvene osebne podatke, da preverijo obstoječe postopke in ukrepe za zavarovanje podatkov in jih prilagodijo, ter najavil, da bo nadaljeval in okrepil nadzor na področju zdravstvenih zavodov ter drugih upravljavcev občutljivih osebnih podatkov.

Poleg navedenega velja opozoriti še na druge pogosto ugotovljene nepravilnosti in pomanjkljivosti, ki jih Informacijski pooblaščenec ugotavlja na vseh področjih. Sem sodijo zlasti nepravilnosti in pomanjkljivosti v zvezi z vodenjem ažurnih katalogov zbirk osebnih podatkov ter s tem povezanim posredovanjem podatkov v register zbirk osebnih podatkov, nedefiniranimi ali pomanjkljivo definiranimi organizacijskimi, tehničnimi in logično-tehničnimi postopki ter ukrepi za zavarovanje osebnih podatkov v notranjih aktih upravljavcev, pomanjkljivem ali neustreznem zagotavljanju notranje in zunanje sledljivosti obdelave osebnih podatkov, neizdelanim seznamom oseb, ki so odgovorne za posamezne zbirke osebnih podatkov, in oseb, ki lahko zaradi narave njihovega dela obdelujejo določene osebne podatke, prekomernim in nesorazmernim izvajanjem videonadzora v delovnih prostorih ter uporabo posnetkov za namene nadzora nad zaposlenimi, neupoštevanje zahtev posameznikov po prenehanju uporabe osebnih podatkov za namene neposrednega trženja,

pomanjkljivimi pogodbami s pogodbenimi obdelovalci ter preusmeritvami in nepooblaščenim prebiranjem službene elektronske pošte.

Kar zadeva ugotovitve v zvezi z izvajanjem videonadzora v delovnih prostorih ter uporabo posnetkov za namene nadzora nad zaposlenimi je treba opozoriti na naraščanje uporabe cenovno dostopnih IP-kamer, ki vodilnim omogočajo, da prek interneta s pomočjo pametnih telefonov, tablic ali osebnih računalnikov kadar koli dostopajo do t. i. žive slike, ki jo prikazujejo posamezne kamere, in s tem nadzirajo delo zaposlenih v nadzorovanih prostorih. Takšen nadzor zaposlenih je z vidika sorazmernosti posega v zasebnost zaposlenih po mnenju Informacijskega pooblaščenca nedopusten. Videonadzor v delovnih prostorih je namreč dopustno zakonito izvajati le v izjemnih primerih, kadar je to nujno potrebno za varnost ljudi ali premoženja ali za varovanje tajnih podatkov in poslovne skrivnosti, tega namena pa ni mogoče doseči z milejšimi sredstvi. Ob upoštevanju navedenih strogih pogojev, ki jih za izvajanje videonadzora in uporabo posnetkov videonadzora znotraj delovnih prostorov določa zakon, je neposreden dostop in spremljanje žive slike kamer, ki so nameščene znotraj delovnih prostorov, dopustno omogočiti zgolj v primeru, ko je to zaradi varovanja ljudi in premoženja nujno potrebno. Spremljanje žive slike je v takih primerih dopustno omogočiti le osebam, ki so v okviru svojih delovnih nalog dolžne vseskozi spremljati dogajanje, ki ga pokrivajo kamere v varovanem prostoru. To so praviloma varnostniki oziroma osebe v nadzornem centru, nikakor pa ne tudi vodilni, ki se v sistem vključujejo, kadar imajo čas oziroma se jim zdi, da je treba preveriti, kaj se v delovnem prostoru dogaja. Če dopustimo, da do žive slike dostopajo tudi vodilni, to v praksi pomeni, da lahko vodja kadar koli vpogleda v živo sliko in preveri, kako zaposleni opravljajo svoje delo, kar pa pomeni nesorazmeren poseg v zasebnost zaposlenih ter uporabo videonadzornega sistema za nezakonite namene.

Glede uporabe IP-kamer, ki se internetno povezujejo in se do njih dostopa prek računalnika, tablice ali pametnega telefona, je treba še opozoriti, da uporabniki pogosto pozabijo na ustrezno zavarovanje dostopa do takih kamer, kar še dodatno povečuje tveganja za poseg v zasebnost. Informacijski pooblaščenec zato uporabnike tovrstnih naprav, ki se pogosto uporabljajo tudi za domačo uporabo in zasebne namene, vnovič poziva, da preverijo, ali so dostopi omejeni vsaj z ustreznimi gesli, ki morajo biti dovolj kompleksna in drugačna od tovarniško privzetih. V številnih primerih je namreč dostop do videonadzornih kamer, ki so povezane v internet, neustrezno zavarovan, kar zlonamernim in radovednim omogoča, da se nepooblaščeno in brez lastnikove vednosti seznanijo s tem, kar se dogaja v prostorih podjetja ali celo v prostorih posameznikovega domovanja.

Poudariti je treba, da zavezanci zgoraj opisane nepravilnosti in pomanjkljivosti praviloma prostovoljno odpravijo že na podlagi opozorila, ki ga jim v postopku izreče državni nadzornik za varstvo osebnih podatkov, zaradi česar izdaja inšpekcijske (ureditvene) odločbe praviloma ni potrebna. Zato in ker mora Informacijski pooblaščenec glede na sodno prakso v primeru, ko ugotovi nezakonito obdelavo osebnih podatkov, pred izdajo odločbe, s katero odredi prenehanje takšne obdelave in izbris nezakonito zbranih osebnih podatkov, zavezanca skladno z načelom zaslišanja stranke (9. člen ZUP) predhodno seznaniti s tem, zakaj po njegovem mnenju za predmetno obdelavo osebnih podatkov nima ustrezne pravne podlage ter ga seznaniti z argumenti, ki njegovo mnenje potrjujejo, je Informacijski pooblaščenec leta 2016 izdal le tri ureditvene odločbe, s katerimi je zavezancem prepovedal nezakonito obdelavo osebnih podatkov. Treba pa je še opozoriti, da prostovoljna odprava ugotovljenih nepravilnosti zavezanca ne odvezuje prekrškovne, kazenske in odškodninske odgovornosti ter da Informacijski pooblaščenec v primeru ugotovljenega suma kršitve zakona zoper zavezanca in njegovo odgovorno osebo vedno uvede postopek za prekrške oziroma izreče ukrep po zakonu, ki ureja prekrške.

Informacijski pooblaščenec je v zvezi z vodenjem postopkov za prekrške v preteklih obdobjih vseskozi opozarjal na problematiko izrekanja nesorazmerno visokih glob za prekrške v steku in predlagal, da se skupaj s strokovnjaki Ministrstva za pravosodje najde rešitev, ki bi Informacijskemu pooblaščencu omogočila, da v primeru steka istovrstnih prekrškov kršiteljem odmeri enotno globo, ki bo nižja od seštevka glob, ki se določijo za posamezen prekršek. Vrhovno sodišče RS je namreč v svoji sodbi št. IV Ips 51/2011 z dne 21. 6. 2011, ki se nanaša na stek prekrškov v primeru nezakonite obdelave osebnih podatkov, zapisalo, da je »pri tovrstnih prekrških toliko prekrškov, kolikor je oškodovancev«, in še, da »vsak poseg v posameznikovo pravico do informacijske zasebnosti predstavlja samostojen prekršek«. Takšno tolmačenje je v praksi ob odsotnosti pooblastil, ki bi Informacijskemu pooblaščencu v primeru steka (idealnega ali realnega) omogočala izrek enotne globe, ki je nižja od seštevka najnižje predpisane globe, v primerih velikega števila posameznikov, v katerih varstvo osebnih podatkov je kršitelj posegel, narekovala izrekanje nesorazmerno visokih glob. Tako izrečena enotna globa lahko za srednje velike in velike pravne

osebe znaša tudi milijon evrov, za odgovorne osebe pravnih oseb, samostojnih podjetnikov ter odgovorne osebe v državnih organih in v organih samoupravnih lokalnih skupnostih pa 20.000 evrov.

Ministrstvo za pravosodje je pobudo Informacijskega pooblaščenca upoštevalo pri pripravi novele Zakona o prekrških. Novela ZP-1J[45], ki je stopila v veljavo 6. 11. 2016, tako v 9. členu določa, da se na koncu drugega odstavka 27. člena doda nov drugi stavek, ki se glasi: »Če to opravičujejo okoliščine iz drugega, tretjega in petega odstavka prejšnjega člena, se za istovrstne prekrške v steku, za katere je izdana ena odločba o prekršku (56. člen), lahko storilcu izreče enotna sankcija, ki ne dosega seštevka določenih sankcij ali ne presega največje mere posamezne vrste sankcije po tem zakonu.« Informacijski pooblaščenec lahko tako po uveljavitvi navedene novele v primeru storitve istovrstnih prekrškov v steku kršitelju izreče enotno globo, ki je nižja od golega seštevka glob za posamezni prekršek, pri čemer pa to lahko stori le v primeru, če to opravičujejo okoliščine iz drugega, tretjega in petega odstavka 26. člena ZP-1, izpolnjevanje teh okoliščin pa mora pooblaščena uradna oseba Informacijskega pooblaščenca presojati za vsak primer posebej.

Velik problem pri opravljanju inšpekcijskega nadzora, ki ga opravlja Informacijski pooblaščenec, še vedno predstavljajo zavezanci, ki nimajo poslovnih prostorov, pač pa le poštni nabiralnik, ter zavezanci, ki imajo v Poslovni register kot pooblaščene osebe za zastopanje vpisane tuje državljane. V takih primerih gre večinoma za zavezance, ki se ukvarjajo s spletno prodajo ter osebne podatke zbirajo in uporabljajo za namene vsiljivega neposrednega trženja, trenutno stanje pa zavezancem omogoča nezakonito ravnanje ter izogibanje odgovornosti za storjene prekrške, kar Republiki Sloveniji in njenim prebivalcem povzroča konkretno gospodarsko škodo. Opisano problematiko je na pobudo Informacijskega pooblaščenca na seji, ki je bila 12. 10. 2016, obravnaval Inšpekcijski svet, ki je nato sprejel sklep, po katerem bodo člani Inšpekcijskega sveta posredovali predloge, kako izboljšati trenutno stanje glede težav pri vročanju zastopnikom gospodarskih družb, ki so tujci, odbor Inšpekcijskega sveta za pravno področje pa bo na podlagi prejetih odgovorov pripravil predlog in gradivo za Ministrstvo za gospodarski razvoj in tehnologijo ter za Ministrstvo za pravosodje.

Leta 2016 se je varstvo osebnih podatkov v evropskem prostoru znašlo pred pomembno prelomnico. Dne 4. 5. 2016 sta bila namreč v Uradnem listu Evropske unije objavljena ključna gradnika novega zakonodajnega svežnja EU o varstvu osebnih podatkov, in sicer:

- Uredba (EU) 2016/679 Evropskega parlamenta in Sveta z dne 27. aprila 2016 o varstvu posameznikov pri obdelavi osebnih podatkov in o prostem pretoku takih podatkov ter o razveljavitvi Direktive 95/46/ES (Splošna uredba o varstvu podatkov) in
- Direktiva (EU) 2016/680 Evropskega parlamenta in Sveta z dne 27. aprila 2016 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 ter o razveljavitvi Okvirnega sklepa Sveta 2008/977/PNZ.

Splošna uredba o varstvu podatkov (angl. *General Data Protection Regulation* – GDPR) je začela veljati 25. 5. 2016, njene določbe pa se bodo morale neposredno uporabljati v vseh državah članicah v dveh letih. Rok za prenos določb direktive v nacionalno zakonodajo je prav tako dve leti.

Na uporabo Splošne uredbe o varstvu podatkov so se večji upravljavci že začeli pripravljati, saj je potrebno določene prilagoditvene aktivnosti začeti dovolj zgodaj; prilagoditi bo treba procese, angažirati ustrezne kadre in podrobno preveriti obstoječe ravni varstva osebnih podatkov. Leto 2016 je tako minilo ob prvem spoznavanju novih določb, leta 2017 pa bo treba določbe že dobro poznati, država pa bo morala odločiti, kako uredbo implementirati v slovenski pravni red in kako urediti področja, kjer si lahko države članice privoščijo več svobode (npr. pravila glede zdravstvenih, biometrijskih in genetskih podatkov).
Z vidika ozaveščenosti in poznavanja pojma varstva osebnih podatkov ter določb zakonodaje Informacijski pooblaščenec ugotavlja, da je stanje dobro, seveda pa obstajajo določene razlike (glede na panogo, velikost upravljavca ipd.). Splošno zavedanje o pomenu varovanja zasebnosti in osebnih podatkov v javnosti je zmerno. Stalna in nikoli končana naloga Informacijskega pooblaščenca je, da se trudi pojasniti pomen pravice do samoodločitve, dolgoročnosti nekaterih ukrepov ter pravočasne celovite obravnave, ne zgolj pozitivnih vidikov novih tehnologij, pooblastil, predpisov in sistemov. Brez zasebnosti namreč ni mogoče govoriti o svobodni in demokratični

[45] Uradni list št. 32/2016.

družbi, zato je treba jasno opozoriti, kdaj jo hoče nekdo zlorabiti za skrivanje slabega. Ta naloga ni enostavna, saj razumevanje zasebnosti terja več kot razumevanje varnosti, ekonomičnosti in praktičnosti, ki se lahko enostavneje in populistično prikažejo javnosti.

Velik razmah se dogaja na področju **pametnih telefonov**, saj očitno postajajo enotna točka za identifikacijo posameznika, vstopno sredstvo do različnih sistemov in storitev ter nadomeščajo druge naprave. Pametni telefoni postajajo naše denarnice, hranijo kartice klubov zvestobe, prek njih dostopamo do e-pošte in profilov na družabnih omrežjih. Uporabljajo se kot naprave, ki omogočajo nagrajevanje voznikov glede na njihove profile vožnje, odklepanje električnih avtomobilov, odklepanje in zaklepanje hotelskih sob. Možnosti, ki jih nudi naprava, ki je redko nimamo ob sebi, so brezmejne, s tem pa se širi krog subjektov, ki o nas zbirajo podatke in jih lahko uporabijo za dobre ali slabe namene. Splošna uredba o varstvu osebnih podatkov v povezavi s pametnimi napravami priznava pomen različnih spletnih identifikatorjev, nevarnosti naraščajočega profiliranja in avtomatiziranega odločanja. Pred upravljavce bo postavila več zahtev po preventivnem delovanju, saj vsebuje mehanizme potrjevanja, pooblaščenih odgovornih oseb za varstvo osebnih podatkov, ocene učinkov, načela vgrajene in privzete zasebnosti ter odgovornosti (angl. *accountability*). Informacijski pooblaščenec ocenjuje, da je pristop, ki bolj poudarja preventivne in proaktivne pristope k varovanju zasebnosti, pravi, bo pa za nekatere upravljavce to novost, ki jo bodo morali sprejeti. Ocene učinkov na varstvo osebnih podatkov in pooblaščene odgovorne osebe so zaenkrat domena zgolj največjih upravljavcev, kot so banke, zavarovalnice in farmacevtska podjetja, prednost preventivnih ukrepov pa bodo morali spoznati in priznati tudi drugi upravljavci.

Nadaljujejo se **trendi**, ki jih je Informacijski pooblaščenec identificiral že v predhodnih poročilih: pospešena digitalizacija na vseh področjih življenja, t. i. *big data*, **profiliranje** in razvoj **umetne inteligence** ter internet stvari. Posamezniki so profilirani na vseh področjih in odločitve o njih pospešeno prevzemajo algoritmi in umetna inteligenca. Te odločitve so lahko manj škodljive oziroma koristne (kateri oglas jim bo prikazan), njihov učinek pa je lahko tudi zelo pomemben (ali bodo dobili štipendijo, pod kakšnimi pogoji lahko dobijo kredit), če ne celo kritičen (ali so primerni za zdravljenje z določnim dragim zdravilom). Ob koristih, ki jih obljubljajo trendi *big data* in umetne inteligence, se premalo pozornosti namenja nevarnostim, na primer samoučečim strojem, ki sprejemajo odločitve o posameznikih, ki jih nihče več ne zna razložiti niti se jim ne upa oporekati. Morda to zveni kot znanstvena fantastika, a čez deset let to branje ne bo tako futuristično.

Podobno pomembni sta področji **genetskih** in **biometrijskih** podatkov, kjer bo državam članicam Splošna uredba o varstvu podatkov prepustila več možnosti za ohranitev ali določitev pravil. **Internet stvari** prinaša predvsem izzive z varnostnega vidika, saj mnogim razvijalcem ni najpomembnejše, kako zavarovati nove povezane točke, temveč v internet povezujejo čedalje več stvari, ne glede na to, ali tja sodijo ali ne (pametne žarnice, hladilnike, športne ure in v zadnjem času pospešeno avtomobile). Tako kot velja na drugih področjih informacijsko-komunikacijskih tehnologij, je tudi tu treba razumeti, da varnost ni enkratno dejanje; varnostne mehanizme je treba ustrezno zasnovati, jih preverjati, posodabljati in nadgrajevati. Več povezanih naprav zahteva tudi več truda. Po nekaterih ocenah naj bi bilo leta 2020 v internet stvari povezanih celo do 30 milijard naprav, dnevno pa je mogoče brati, da se pojavljajo ogromne težave že z obstoječimi napravami; tudi največji upravljavci imajo namreč ranljive sisteme, beležijo vdore v strežnike in se soočajo z izgubo podatkov.

Ne glede na to, za kašen trend gre, se je treba zavedati, da so spremembe na področju zasebnosti hitre, gradualne in težko zaznavne. Se spomnite, kdaj smo dobili kartice zvestobe? Kaj pa digitalno televizijo? Področij, kjer nihče ne zbira podatkov o nas, je vse manj, pa tega niti ne opazimo. Podatki pa predstavljajo moč, in ta se pospešeno seli k drugim – k našim trgovcem, operaterjem, državi, obveščevalnim agencijam, organom pregona. O nas vedno več ljudi ve vse več, s tem pa je naša moč odločanja manjša. Smo šele na začetku res masovnega zbiranja podatkov o posameznikih; kolikšna je vrednost in moč teh podatkov pa lepo kažejo podatki o vrednosti tehnoloških velikanov, o uporabi podatkov za manipulacije z volivci ter usmerjanje naših nakupovalnih in drugih odločitev. Če prej ne, bomo vrednost zasebnosti spoznali takrat, ko jo bomo dokončno izgubili.

Posebno pozornost je Informacijski poolaščenec tudi leta 2016 posvetil preventivnim vidikom delovanja. S ciljem **izobraževanja** upravljavcev in drugih zavezancev so zaposleni pri Informacijskem pooblaščencu izvedli 96 brezplačnih predavanj domačim slušateljem, upoštevajoč tudi predavanja gostom iz tujine pa je bilo brezplačnih predavanj več kot 100. Prav tako je

Informacijski pooblaščenec v stalnem stiku z upravljavci, obdelovalci in predlagatelji predpisov z namenom pravočasnega naslavljanja različnih dilem glede novih načinov zbiranja in obdelave osebnih podatkov ter iskanja zasebnosti prijaznih zakonskih rešitev ob uvajanju novih tehnologij ter povečevanju učinkovitosti. Med drugim je zato **na vseh ministrstvih izvedel predavanja za strokovnjake, ki pripravljajo zakonske in podzakonske predpise**, ki se dotikajo področja varstva osebnih podatkov, podal pa je tudi več kot **120 mnenj na predloge zakonov** in drugih predpisov, ki se nanašajo na različne vidike urejanja, zbiranja in obdelave osebnih podatkov.

Informacijski pooblaščenec omogoča tudi neformalno izvedbo **ocen učinkov na varstvo osebnih podatkov** kot enega temeljnih preventivnih orodij za pravočasni pristop k varstvu osebnih podatkov. Tudi leta 2016 se je nanj obrnilo več kot 100 upravljavcev in obdelovalcev iz javnega in zasebnega sektorja, ki so pripravljali zakonodajo, rešitve ali projekte in so želeli pravočasno spoznati tveganja ter se tako izogniti kršitvam zakonodaje. Ocene učinkov na varstvo osebnih podatkov imajo močan preventivni učinek, saj je zaradi njih potrebnih manj inšpekcijskih ukrepov, manj je ugotovljenih kršitev, upravljavci podatkov pa se tako izognejo stroškom zaradi izrečenih sankcij ter izgube ugleda in zaupanja strank. Številni upravljavci so dizajn svojih rešitev, obseg in način zbiranja osebnih podatkov, varovalne mehanizme ter ukrepe za varnost vnaprej prilagodili ter se s tem izognili negativnim posledicam napačnih odločitev.

Informacijski pooblaščenec je izdal tudi štiri nove **smernice** ter napotke za upravljavce brezpilotnih letalnikov glede izvedbe ocen učinkov na varstvo osebnih podatkov:

- *Smernice o uporabi zasebnih naprav v službene namene* (BYOD) naslavljajo tveganja, ki izvirajo iz čedalje pogostejše uporabe zasebnih mobilnikov, tablic in prenosnikov tudi za službene namene. To odpira številna vprašanja in tveganja za izgube, nepooblaščene dostope in druge zlorabe tako osebnih podatkov zaposlenega kot podatkov njegovih oseb (npr. otrok in partnerjev), na zasebnih mobilnih napravah pa se lahko znajdejo tudi neustrezno zavarovani poslovni podatki, saj imajo zaposleni prek svojih zasebnih naprav pogosto dostop do službene e-pošte, aplikacij in drugih poslovnih sistemov. Podjetjem in inštitucijam, ki želijo uvesti takšne sisteme, Informacijski pooblaščenec priporoča, da temeljito premislijo, kaj želijo s tem doseči in česa ne, ter podaja priporočila, kako varno in zakonito uvesti sisteme za upravljanje mobilnih naprav.
- *Smernice o obdelavi osebnih podatkov iz centralnega registra prebivalstva* opisujejo, pod kakšnimi pogoji je zbiranje in obdelovanje podatkov o posameznikih dopustno, kdaj, kdo in za kakšen namen lahko pridobi osebne podatke iz centralnega registra prebivalstva (detektivi, zavarovalnice, policija, banke, občine, odvetniki, stečajni upravitelji …), kako jih lahko naprej obdeluje ter kako so urejeni načini dostopanja do podatkov. V njih so podani tudi odgovori na pogosta vprašanja in opisani konkretni primeri.
- *Smernice za upravnike večstanovanjskih stavb* obravnavajo številna vprašanja, s katerimi se soočajo etažni lastniki in upravniki večstanovanjskih stavb, kot npr. kdaj lahko upravnik od lastnikov in/ali najemnikov zahteva osebne podatke, katere osebne podatke drugih lastnikov in/ali najemnikov so upravičeni pridobiti etažni lastniki/najemniki, katere osebne podatke drugih lastnikov in/ali najemnikov lahko upravnik posreduje tretjim osebam ali organizacijam, kako je z dopustnostjo videonadzora v blokih, na parkiriščih in pred vhodi v posamezna stanovanja.
- *Smernice za varstvo osebnih podatkov v delovnih razmerjih* predstavljajo nujno posodobitev že obstoječih gradiv Informacijskega pooblaščenca na področju, kjer se še vedno sooča z največ dilemami tako delodajalcev kot zaposlenih in sindikatov. Smernice pojasnjujejo pravne podlage za zbiranje, obdelavo, objavo osebnih podatkov zaposlenih, pokrivajo področje varnosti in zdravja pri delu (npr. nadzor alkoholiziranosti, bolniškega staleža) in obdelavo osebnih podatkov v okviru sindikalne dejavnosti. Posebno poglavje je posvečeno vprašanjem nadzora nad delovnimi sredstvi (e-pošta, internet, telefoni, računalniki), kjer se v praksi zaznavajo neustrezna ravnanja, ko se ti podatki uporabljajo nenamensko.

Informacijski pooblaščenec je leta 2016 okrepil **sodelovanje z deležniki**, s čimer dosega sinergijske in multiplikativne učinke. Ob že obstoječemu delovanju na področju ozaveščanja o varni rabi spleta s sodelovanjem v projektu Safe-si, s sodelovanjem z Inštitutom za korporativne varnostne študije (ICS) ter Agencijo za komunikacijska omrežja in storitve, je leta 2016 podpisal dogovor s SI-CERT, nacionalnim odzivnim centrom za obravnavo incidentov s področja varnosti elektronskih omrežij in informacij ter pristopil k dogovorom z Združenjem bank Slovenije in Zvezo potrošnikov Slovenije. Tesno sodeluje tudi z Javno agencijo za civilno letalstvo, kjer je pomagal pri izobraževanjih operaterjev brezpilotnih letalnikov ter jih ozaveščal o varovanju zasebnosti in osebnih podatkov. S partnerji izvaja skupne aktivnosti, kot so nastopi na konferencah, strokovni prispevki v publikacijah, izobraževanja, s tem pa učinkoviteje dosega upravljavce osebnih podatkov

in posameznike. V prihodnjem letu bo Informacijski pooblaščenec še okrepil sodelovanje z deležniki na drugih področjih.

Informacijski pooblaščenec veliko pozornosti posveča tudi dostopnosti informacij prek **spletne strani**, ki je bila leta 2016 prenovljena. Register zbirk osebnih podatkov je javnosti na voljo v odprtem formatu, za listanje po zbirkah odločb in mnenj je na voljo iskalnik, ki ga bo še izboljšal. Z željo po izboljšanju uporabnosti in prijaznosti spletne strani je Informacijski pooblaščenec izvedel zunanje testiranje uporabniške izkušnje; rezultati bodo znani v prihodnjem letu.

Preventivno delovanje Informacijskega pooblaščenca se kaže tudi ob **strokovnem sodelovanju v medresorskih delovnih skupinah**. Poleg udeležbe v Inšpekcijskem svetu velja izpostaviti sodelovanje v Medresorski delovni skupini za uredbo eIDAS o elektronski identifikaciji, sodelovanje pri pripravi predpisov, sodelovanje z Ministrstvom za javno upravo pri različnih projektih digitalizacije ter sodelovanje v Svetu za razvoj informatike.

Strokovnjaki Informacijskega pooblaščenca za dvig ozaveščenosti o pomenu zasebnosti in varstva osebnih podatkov nastopajo na različnih **konferencah, strokovnih dogodkih, posvetih ter okroglih mizah**. Leta 2016 so med drugim nastopili na konferencah INFOSEK 2016, Cryptoparty 2016 in CSA CEE Cloud Security Summit ter na Mednarodni konferenci o varstvu podatkov (Moskva), 24. mednarodni konferenci o revidiranju, 7. mednarodni konferenci Dnevi korporativne varnosti, na konferenci Varnost mobilnih telefonov, na XV. dnevih delovnega prava in socialne varnosti, sodelovali so na okrogli mizi z naslovom *Pravica do zasebnosti in nove tehnologije*, na Dnevih kazenskega prava, udeležili so se posveta *Priložnost digitalne preobrazbe za Slovenijo* ter nastopili na Festivalu odprtih podatkov.

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.

Leta 2016 je Informacijski pooblaščenec izdal več kot 100 mnenj na predloge sprememb zakonov ter na predloge novih zakonov in drugih predpisov. Pri tem ugotavlja skrb vzbujajoč trend, da se število predpisov, ki prinašajo posege v zasebnost posameznikov z vidika obdelave osebnih podatkov, že več let ne zmanjšuje, sprejemajo pa se po hitrem postopku, brez ustreznih analiz in ocen njihovih posledic za zagotavljanje ustavno zagotovljenega varstva zasebnosti in osebnih podatkov posameznikov.

Leta 2016 je Informacijski pooblaščenec podal mnenje, pripombe oziroma je sodeloval pri pripravi naslednjih predpisov (v zvezi z nekaterimi je podal več mnenj):

- Predlog uredbe Evropskega parlamenta in Sveta o sodelovanju med nacionalnimi organi, odgovornimi za izvrševanje zakonodaje o varstvu potrošnikov (dve mnenji),
- Predlog Zakona o nevladnih organizacijah,
- Predlog Zakona o spremembah in dopolnitvah Stanovanjskega zakona (tri mnenja),
- Osnutek Pravilnika o zapisniku o ogledu kraja nesreče na smučišču in potrdilu o prevzemu predmetov,
- Predlog uredbe Evropskega parlamenta in Sveta o vzpostavitvi evropskega sistema za potovalne informacije in odobritve (ETIAS) ter spremembe uredb (EU) št. 515/2014, (EU) št. 2016/399, (EU) št. 2016/794 in (EU) št. 2016/1624,
- Predlog Pravilnika o naročanju in načinu vodenja čakalnih seznamov in najdaljših čakalnih dobah v mreži javne zdravstvene službe,
- Predlog novele Zakona o pacientovih pravicah (dve mnenji),
- Predlog Zakona o spremembah in dopolnitvah Zakona o kmetijstvu (tri mnenja),
- Predlog Zakona o spremembah in dopolnitvah Zakona o integriteti in preprečevanju korupcije (dve mnenji),
- Predlog Strategije Republike Slovenije na področju medijev za obdobje 2017–2025,
- Predlog Družinskega zakonika,
- Predlog Zakona o stvarnem premoženju države in samoupravnih lokalnih skupnosti (tri mnenja),
- Predlog Odloka o odvajanju in čiščenju komunalne in padavinske vode na območju Občine Slovenska Bistrica,
- Predlog Zakona o športu (dve mnenji),
- Predlog plurilateralnega sporazuma o trgovini s storitvami – TiSA,
- Predlog Pravilnika o vsebinah vlog za izdajo dovoljenj dimnikarskim družbam in licenc dimnikarjem,
- Predlog Načrta razvoja namakanja in rabe vode za namakanje v kmetijstvu do leta 2020 in Programa ukrepov za izvedbo načrta razvoja namakanja in rabe vode za namakanje v kmetijstvu do leta 2020 ter Okoljskega poročila za načrt in program,
- Predlog Letnega programa statističnih raziskovanj za leto 2017 (dve mnenji),
- Predlog Uredbe o spremembah Uredbe o izvajanju podukrepa Pomoč za zagon dejavnosti za mlade kmete iz Programa razvoja podeželja Republike Slovenije za obdobje 2014–2020 (dve mnenji),
- Predlog Zakona o spremembah in dopolnitvah Zakona o organu in skladu za reševanje bank,
- Predlog Pravilnika o opredelitvi glede darovanja delov človeškega telesa,
- Predlog Zakona o spremembah in dopolnitvah Zakona o urejanju trga dela (tri mnenja),
- Zakon o spremembah in dopolnitvah Zakona o tujcih (dve mnenji),
- Predlog Pravilnika o izdajanju certifikatov z evropsko ravnjo znanja tujega jezika,
- Predlog Zakona o revidiranju in ocenjevanju vrednosti (dve mnenji),
- Predlog Zakona o množičnem vrednotenju nepremičnin,
- Predlog sprememb Zakona o motornih vozilih,
- Predlog Zakona o spremembah in dopolnitvah Zakona o kazenskem postopku (dve mnenji),
- Zakon o spremembah in dopolnitvah Zakona o kmetijstvu (tri mnenja),
- Predlog direktive Evropskega parlamenta in Sveta o spremembi Direktive (EU) 2015/849 o preprečevanju uporabe finančnega sistema za pranje denarja in financiranje terorizma ter Direktive 2009/101/ES,
- Predlog Uredbe o upravnem poslovanju,

- Predlog Zakona za vzpostavitev javnosti, preglednosti in odgovornosti v pravosodju,
- Predlog Zakona o voznikih,
- Predlog Zakona o spremembah in dopolnitvah Zakona o davčnem postopku,
- Predlog Zakona o spremembah in dopolnitvah Zakona o nalogah in pooblastilih policije (šest mnenj),
- Predlog Zakona o spremembah in dopolnitvah Zakona o trgu finančnih instrumentov (dve mnenji),
- Osnutek predloga Zakona o spremembah in dopolnitvah Zakona o elektronskih komunikacijah,
- Predlog Zakona o lekarniški dejavnosti (dve mnenji),
- Predlog Zakona o spremembah in dopolnitvah Zakona o občinskem redarstvu (dve mnenji),
- Predlog Zakona o centralnem kreditnem registru (dve mnenji),
- Predlog sprememb Zakona o tajnih podatkih,
- Predlog Zakona o spremembah in dopolnitvah Zakona o nematerializiranih vrednostnih papirjih,
- Osnutek predloga Priporočila Sveta OECD v zvezi z upravljanjem z zdravstvenimi podatki,
- Predlog Zakona o spremembah in dopolnitvah Zakona o zdravstveni dejavnosti,
- Osnutek besedila členov 161 do 165 iz delovnega osnutka Zakona o državnem pravobranilstvu,
- Predlog Pravilnika o evidenci ribiških plovil in evidenci plovil, ki se uporabljajo v marikulturi,
- Predlog Zakona o čezmejnem izvajanju storitev,
- Predlog Pravilnika o spremembah in dopolnitvah Pravilnika o vpisih v kataster stavb in Predlog Uredbe o spremembah in dopolnitvah Uredbe o podatkih o lastnostih nepremičnin v registru nepremičnin,
- Zakon o spremembah in dopolnitvah Zakona o preprečevanju nasilja v družini,
- Predlog Pravilnika o postopkih (so)financiranja, ocenjevanja in spremljanju izvajanja raziskovalne dejavnosti,
- Predlog Uredbe o izvajanju Uredbe (EU, EURATOM) št. 1141/2014 Evropskega parlamenta in Sveta z dne 22. oktobra 2014 o statutu in financiranju evropskih političnih strank in evropskih političnih fundacij,
- Paket uredb Pametne meje,
- Zakon o preprečevanju pranja denarja in financiranja terorizma (dve mnenji),
- Zakon o dopolnitvah Zakona o nadzoru državne meje,
- Predlog Uredbe o sistemih brezpilotnih zrakoplovov (dve mnenji),
- Predlog uredbe Evropskega parlamenta in sveta o zagotavljanju čezmejne prenosljivosti storitev spletnih vsebin na notranjem trgu,
- Zakon o investicijskih skladih in družbah za upravljanje,
- Uredba o ukrepih kmetijske zemljiške politike, ki se sofinancirajo s sredstvi, zbranimi iz naslova odškodnine zaradi spremembe namembnosti kmetijskega zemljišča,
- Osnutek Programa ravnanja z odpadki in Programa preprečevanja odpadkov,
- Predlog Zakona o dimnikarskih storitvah (dve mnenji),
- Predlog novele Uredbe o odlagališčih odpadkov,
- Predlog Zakona o javnih uslužbencih (dve mnenji),
- Predlog Pravilnika o pooblastilih za obdelavo osebnih podatkov v Centralnem registru podatkov o pacientih,
- Predlog Zakona o varstvu pred diskriminacijo,
- Predlog Zakona o reševanju in prisilnem prenehanju bank,
- Predlog sprememb Zakona o organizaciji in financiranju vzgoje in izobraževanja,
- Predlog sprememb Zakona o visokem šolstvu glede dopolnitev, vezanih na informacijski sistem eVŠ,
- Predlog Pravilnika o spremembah in dopolnitvah Pravilnika za izvajanje Zakona o orožju,
- Predlog Uredbe o izvajanju Uredbe (EU) o izboljšanju ureditve poravnav vrednostnih papirjev v Evropski uniji in o centralnih depotnih družbah,
- Predlog Zakona o spremembah in dopolnitvah Zakona o opravljanju plačilnih storitev za proračunske uporabnike,
- Predlog pridobivanja podatkov o prometu v zvezi z nekaterimi prekrški oziroma uvedbe enotne evidence prekrškov,
- Predlog Zakona o spremembah in dopolnitvah Zakona o plačilnih storitvah in sistemih,
- Predlog Zakona o potrošniških kreditih (dve mnenji),
- Osnutek Uredbe o informacijski varnosti,
- Predlog Zakona o sistemu jamstva za vloge,
- Zakon o mednarodni zaščiti,
- Predlog Zakona o spremembah in dopolnitvah Zakona o državni upravi (dve mnenji),
- Predlog Zakona o spremembah in dopolnitvah Zakona o socialnem varstvu (tri mnenja),
- Predlog Zakona o kolektivnem upravljanju avtorske in sorodnih pravic (dve mnenji),

- Predlog Uredbe o izvedbi ukrepov kmetijske politike za leto 2016,
- Predlog Pravilnika o izvrševanju pooblastil in nalog pravosodnih policistov,
- Predlog Zakona o spremembah in dopolnitvah Pomorskega zakonika,
- Predlog Pravilnika o izvrševanju kazni zapora,
- Predlog Pravilnika o plačilu za delo obsojencev.

4.2. Sodelovanje z javnostmi

Informacijski pooblaščenec je leta 2016 skrbel za javnost svojega dela ter za osveščanje pravnih in fizičnih oseb z rednimi in doslednimi odnosi z mediji (sporočila za javnost, izjave, komentarji, intervjuji pooblaščenke, novinarske konference) ter prek svoje spletne strani.

V začetku leta 2016 je Informacijski pooblaščenec prenovil svojo **spletno stran www.ip-rs.si**, ki vsebuje:

- predstavitev zgodovine Informacijskega pooblaščenca in zaposlenih,
- predstavitev obeh področij delovanja, to je varstva osebnih podatkov (npr. pravice posameznika, inšpekcijski nadzor, obveznosti upravljavcev, informacijske tehnologije in osebni podatki) in dostopa do informacij javnega značaja (npr. informacije javnega značaja pri organih in pri subjektih pod prevladujočim vplivom, dostop do informacij za medije, ponovna uporaba informacij javnega značaja) ter pristojnosti na obeh področjih,
- predstavitev domače in tuje zakonodaje za obe področji,
- odgovore na najpogosteje zastavljena vprašanja z obeh področij,
- mnenja s področja varstva osebnih podatkov,
- vse odločbe, s katerimi je Informacijski pooblaščenec odločil o pritožbah v zvezi z informacijami javnega značaja,
- zahteve za oceno ustavnosti, ki jih je vložil na Ustavno sodišče RS,
- sodbe Upravnega sodišča RS in Vrhovnega sodišča RS v zadevah, ki jih je vodil Informacijski pooblaščenec in zoper katere so bile vložene tožbe,
- pripombe na predloge predpisov,
- predstavitev mednarodnega delovanja Informacijskega pooblaščenca,
- predstavitev projektov, pri katerih sodeluje Informacijski pooblaščenec,
- uporabne povezave (npr. na spletne strani sorodnih organov v EU in drugod po svetu),
- izdane publikacije (priročniki in smernice, letna poročila),
- domače in tuje članke z obeh področij,
- vzorce oziroma obrazce, namenjene fizičnim osebam za uveljavljanje njihovih pravic (npr. zahteva za dostop do informacij javnega značaja, zahteva za ponovno uporabo informacij javnega značaja, pritožba zoper molk zavezanca po ZDIJZ, pritožba zoper zavrnilno odločbo ali obvestilo zavezanca po ZDIJZ, prijava zlorabe osebnih podatkov, zahteva za seznanitev z lastnimi osebnimi podatki, pritožba zaradi kršitve pravice do seznanitve z lastnimi osebnimi podatki, zahteva za prenehanje uporabe osebnih podatkov za namen neposrednega trženja, zahteva za seznanitev z osebnimi podatki v Schengenskem informacijskem sistemu v Sloveniji, pritožba v zadevi seznanitve z lastno zdravstveno dokumentacijo ali z zdravstveno dokumentacijo umrlega pacienta) in upravljavcem zbirk osebnih podatkov za lažje delo pri vlaganju različnih zahtev in zagotovitvi ustreznega varovanja osebnih podatkov (npr. vloga za povezovanje zbirk osebnih podatkov, obvestilo o povezovanju zbirk osebnih podatkov, obvestilo o prenehanju vodenja zbirke osebnih podatkov, prijava biometrijskih ukrepov, vloga za iznos osebnih podatkov v tretje države, vzorec kataloga zbirk osebnih podatkov, vzorec pravilnika o zavarovanju osebnih podatkov in vzorec pogodbe za potrebe pogodbene obdelave osebnih podatkov po 11. členu ZVOP-1, vzorec evidence uporabe videonadzornega sistema),
- register zbirk osebnih podatkov in katalog informacij javnega značaja Informacijskega pooblaščenca,
- e-novice, na katere se lahko prijavijo posamezniki, ki želijo biti seznanjeni z dogajanjem na obeh področjih v Sloveniji in tujini.

Informacijski pooblaščenec je bil leta 2016 prisoten tudi na spletnem družabnem omrežju **Facebook**, kjer prek svojega profila skrbi za dvig ozaveščenosti glede pomena varstva osebnih podatkov.

V okviru **preventivnega dela** je Informacijski pooblaščenec veliko pozornosti namenil nadaljnji širitvi orodij in pripomočkov za dvig ozaveščenosti, in sicer s pripravo različnih publikacij. Leta 2016 je izdal:

- Smernice o uporabi zasebnih naprav v službene namene (BYOD),
- Smernice o obdelavi osebnih podatkov iz centralnega registra prebivalstva,
- Smernice za upravnike večstanovanjskih stavb,
- Smernice za varstvo osebnih podatkov v delovnih razmerjih,
- Letno poročilo Informacijskega pooblaščenca za leto 2015.

S pomočjo smernic naj bi upravljavci dobili priporočila, kako naj v praksi zadostijo zahtevam ZVOP-1. Namen smernic je namreč podati skupne praktične napotke za upravljavce zbirk osebnih podatkov na jasen, razumljiv in uporaben način ter s tem odgovoriti na najpogosteje zastavljena vprašanja s področja varstva osebnih podatkov, s katerimi se srečujejo posamezni upravljavci. Pravno podlago za izdajo smernic Informacijskemu pooblaščencu daje 49. člen ZVOP-1, ki med drugim določa, da Informacijski pooblaščenec daje neobvezna mnenja, pojasnila in stališča o vprašanjih s področja varstva osebnih podatkov 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 varčevalnih ukrepov Informacijski pooblaščenec nobene izmed naštetih publikacij ni natisnil, ampak jih je objavil zgolj v elektronski obliki. Vse publikacije so dostopne na spletni strani https://www.ip-rs.si/publikacije/prirocniki-in-smernice/.

Informacijski pooblaščenec je skrbel za **stalno izobraževanje zavezancev**. S tem namenom je tudi sodeloval na različnih izobraževalnih konferencah, delavnicah in okroglih mizah. Leta 2016 so zaposleni pri Informacijskem pooblaščencu izvedli kar **98 *pro bono* predavanj** za različne strokovne javnosti in zavezance na obeh področjih delovanja, tj. za upravljavce osebnih podatkov in zavezance za posredovanje informacij javnega značaja.

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

Informacijski pooblaščenec je **28. januarja ob dnevu varstva osebnih podatkov**, ki se obeležuje po celi Evropi, organiziral okroglo mizo z naslovom *Kakšno varstvo zasebnosti potrebujemo v svetu novih dimenzij nadzora?*. Dogodek je bil posvečen izzivom, ki jih predvsem varuhom in zagovornikom zasebnosti prinašajo brezpilotni letalniki – droni in z njimi povezane oblike nadzora. Uporaba dronov namreč poleg številnih prednosti prinaša tudi določena tveganja glede varnosti in upoštevanja temeljnih človekovih pravic. Informacijska pooblaščenka Mojca Prelesnik je z gosti, dr. Denisom Čaleto z Inštituta za korporativne varnostne študije, mag. Tatjano Bobnar, namestnico generalnega direktorja policije, Boštjanom Vidmarjem z Inštituta za razvoj brezpilotnih sistemov, dr. Alešem Završnikom z Inštituta za kriminologijo pri Pravni fakulteti v Ljubljani, in novinarjem Lenartom J. Kučičem razpravljala o prednostih in slabostih dronov, vplivih, ki jih nove tehnologije prinašajo za pravico do zasebnosti, ter ustreznih regulativnih rešitvah, s katerimi lahko zagotovimo njihovo varno uporabo. Udeleženci okrogle mize so odprli številna vprašanja in zaključili, da je normativna ureditev brezpilotnikov nujna, vsako odlašanje pa nevarno. Neurejenost povečuje varnostna tveganja ter tveganja za storitev kaznivih dejanj in za posege v temeljne človekove pravice, hkrati pa ovira razvoj novih storitev in delovnih mest.

V času dogodka si je bilo mogoče v živo ogledati različne vrste brezpilotnih letalnikov, strokovnjaki z Inštituta za razvoj brezpilotnih sistemov pa so odgovarjali na vprašanja o njihovem delovanju ter o njihovih prednostih in slabostih.

Že tradicionalno je Informacijski pooblaščenec podelil **priznanja za dobro prakso** na področju varstva osebnih podatkov. *Priznanje ambasador zasebnosti* je prejel Inštitut za razvoj brezpilotnih sistemov iz Ljubljane, ki izvaja številne aktivnosti, namenjene ozaveščanju uporabnikov, javnosti in strokovnjakov o različnih vidikih uporabe brezpilotnikov ter si aktivno prizadeva za njihovo premišljeno regulacijo. S tem namenom povezuje deležnike na tem področju in prispeva svoje obsežno znanje, pri tem pa ves čas opozarja na pravočasno upoštevanje zasebnosti in na nujnost vzpostavitve določenih varoval. Inštitut je s svojim delom aktivno pripomogel k uveljavljanju koncepta vgrajene zasebnosti, kjer ima zasebnost že v sami zasnovi tehnoloških, zakonodajnih ali upravljavskih rešitev svoje mesto.

Nagrado za dobro prakso na področju varovanja osebnih podatkov je prejel Adria Mobil, d. o. o., pri katerem je Informacijski pooblaščenec po uradni dolžnosti opravil podroben inšpekcijski nadzor nad izvrševanjem določb ZVOP-1. Ugotovljeno je bilo, da ima družba zagotovljen domišljen sistem postopkov in ukrepov za zavarovanje osebnih podatkov ter da ima ustrezne interne akte, ki opredeljujejo obdelavo in zavarovanje osebnih podatkov. Podjetje odlikuje visoka stopnja zavedanja o pomenu varstva osebnih podatkov, ki je vpeto v vse ravni sistema dela, tehnične rešitve pa zagotavljajo vnaprejšnje preprečevanje nevarnosti morebitnih zlorab.

Posebna priznanja je Informacijski pooblaščenec podelil tudi družbam, ki so leta 2015 pridobile *certifikat po standardu za varovanje informacij ISO/IEC 27001* in s tem izkazale visoko raven varovanja osebnih podatkov: Metra Inženiring, d. o. o., ŽALE Javno podjetje, d. o. o., in ZZI, d. o. o.

Svetovni dan pravice vedeti zaznamujemo vsako leto 28. septembra, vse odkar so se leta 2002 različne organizacije civilne družbe iz številnih držav povezale v organizacijo Freedom of Information Advocates Network (FOIAnet). Ob svetovnem dnevu pravice vedeti organizacije javnega in nevladnega sektorja, ki se ukvarjajo s tem področjem, opozarjajo na pomembnost transparentnosti delovanja javnega sektorja ter zagotavljanja pogojev za učinkovitejšo participacijo državljanov pri odločanju o skupnih zadevah.

Leta 2016 je Informacijski pooblaščenec ta dan posvetil izzivom, ki jih institucijam s področja kulture (knjižnicam, muzejem in arhivom) prinaša Direktiva EU o ponovni uporabi podatkov javnega sektorja in nacionalna zakonodaja (ZDIJZ-E). V sodelovanju z Ministrstvom za javno upravo in Ministrstvom za kulturo je organiziral posvet z naslovom *Odprti podatki – odprta in bogata družba*, s katerim je želel opozoriti na pomen uporabe podatkov kulturnih institucij za razvoj odprte in bogate družbe. Pravica vedeti je tesno povezana s transparentnostjo javne uprave in je osnovno vodilo njenega delovanja. Informacije, ki nastajajo pri delu javne uprave, niso last teh organov, ampak skupno dobro. Danes si namreč težko predstavljamo življenje brez navigacijskih naprav, pametnih aplikacij, spletnih enciklopedij in podobnega. Mnoge digitalne storitve in produkti pa ne bi nastali, če ne bi bilo podatkov javnega sektorja. Takšni izdelki in storitve, ki v celoti ali delno temeljijo na informacijah javnega sektorja, vodijo k ustanavljanju novih podjetij in nastajanju novih delovnih mest, potrošnikom pa dajejo več možnosti izbire. Organi javnega sektorja bi morali prisluhniti ponovnim uporabnikom in jim v postopkih pomagati po svojih najboljših močeh, zasebni sektor pa je treba spodbujati k ponovni uporabi, še toliko bolj, ker so lahko postopki prezapleteni in dolgotrajni, kar zainteresirane lahko odvrača od polne uveljavitve pravice do ponovne uporabe.

Na posvetu so udeležence nagovorili minister za javno upravo Boris Koprivnikar, minister za kulturo Tone Peršak in informacijska pooblaščenka Mojca Prelesnik. Svoje praktične izkušnje na področju ponovne uporabe zbirk podatkov so predstavili tudi številni strokovnjaki z različnih področij: mag. Mitja Sadek iz Zgodovinskega arhiva Ljubljana in dr. Andrej Pančur z Inštituta za novejšo zgodovino sta prikazala zgodovinski okvir in pomen popisovanja prebivalstva ter začetek projekta objave popisnic prebivalstva na spletnih straneh SIstory in projekt digitalizacije popisnic prebivalstva; dr. Dalibor Radovan z Geodetskega inštituta je predstavil spremembe paradigem, ki so se zgodile na področju galerij, knjižnic, arhivov in muzejev (GLAM) ter pomen odpiranja podatkov in primere geoinformacijskih storitev za GLAM; mag. Zoran Krstulović je predstavil tipe podatkov, ki jih ponuja Digitalna knjižnica Slovenije, ter možnosti dostopa za ponovno uporabo metapodatkov in digitalnih objektov; dr. Jože Škofljanec in Gregor Završnik iz Arhiva RS sta se osredotočila na primer (ponovne) uporabe podatkov, ki so izvirno nastali v digitalni obliki, in predstavila primer »združevanja« podatkov GURS in DVK; dr. Maja Bogataj Jančič z Inštituta za intelektualno lastnino pa se je posvetila izzivom, ki jih za kulturne inštitucije predstavljata nova direktiva in nacionalna zakonodaja, ter vprašanju, kako se z njimi soočiti. Strokovni del posveta se je zaključil s predavanjem nizozemskega gosta, dr. Marca de Vriesa, ki je predstavil dobre prakse in izkušnje Nizozemske na področju odpiranja podatkov.

Informacijski pooblaščenec je podelil tudi priznanje *ambasador transparentnosti* za dobro prakso na področju dostopa do informacij javnega značaja. Ker je bilo eno od vodil dogodka povezovanje med organi javnega sektorja in zasebnim sektorjem, je nagrado podelil Zavodu za ustvarjanje kakovostnega novinarstva Pod črto. Ta je bil v zadnjih letih zelo dejaven v postopkih z zahtevami po informacijah javnega značaja, svoje ugotovitve skupaj z informacijami in prejetimi zbirkami dokumentov pa objavlja na portalu. Tako informacijam ustvarja dodano vrednost in prispeva k njihovi večji uporabni vrednosti za širši krog ljudi.

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 za varstvo osebnih podatkov EU in Sveta Evrope. Sodelovanje na mednarodni ravni in sodelovanje pri zakonodajnih postopkih EU mu narekuje tudi Direktiva 95/46/ES. Informacijski pooblaščenec je leta 2016 na ravni EU sodeloval na plenarnih sestankih ter pri delu štirih izmed številnih podskupin Delovne skupine za varstvo podatkov iz 29. člena Direktive 95/46/ES (Article 29 Data Protection Working Party – WP29), poleg tega pa je sodeloval še v šestih delovnih telesih EU, ki se ukvarjajo z nadzorom nad izvajanjem varstva osebnih podatkov v okviru velikih informacijskih sistemov EU, in sicer:

- v WP29 ter štirih njenih podskupinah (v podskupini Future of Privacy, v Tehnološki podskupini, v podskupini za iznos podatkov in v 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.

WP29, ki Evropski komisiji daje strokovna mnenja s področja varstva osebnih podatkov, se je leta 2016 osredotočila predvsem na začetek priprav na uporabo nove Splošne uredbe o varstvu podatkov ter aktivnosti, povezane z uveljavitvijo odločitve Sodišča EU (SEU) glede iznosa osebnih podatkov v ZDA na podlagi razveljavljenega dogovora Varni pristan in pozneje na pripravo gradiv za izvajanje novega dogovora o Ščitu zasebnosti. SEU je namreč oktobra 2015 razveljavilo dogovor Varni pristan, ki je omogočal enostaven prenos osebnih podatkov iz EU certificiranim organizacijam v ZDA. Evropska komisija in ameriška vlada sta 2. februarja 2016 dosegli politični dogovor o novem okviru za čezatlantsko izmenjavo osebnih podatkov za komercialne namene – Ščitu zasebnosti EU-ZDA. WP29 je podala mnenje na osnutek gradiv dogovora. Potem ko je Evropska komisija julija 2016 sprejela sklep o ustreznosti varstva osebnih podatkov pri iznosu v ZDA na podlagi dogovora o Ščitu zasebnosti, se je WP29 aktivno vključila v pripravo praktičnih vidikov njegovega izvajanja z vidika svojih pristojnosti.

WP29 je leta 2016 sprejela naslednja pomembna mnenja:

- Izjavo o akcijskem načrtu 2016 za izvedbo Splošne uredbe o varstvu podatkov (GDPR) (WP 236),
- Delovni dokument 01/2016 o upravičenosti posegov v temeljne pravice do zasebnosti in varstva podatkov med prenosom osebnih podatkov v tretje države za namen varnostnoobveščevalnih služb (Bistvene evropske garancije) (WP 237),
- Mnenje 01/2016 o osnutku sklepa o ustreznosti Zasebnostnega ščita EU–ZDA (WP 238),
- Mnenje 02/2016 o objavi osebnih podatkov s strani javnega sektorja za namene transparentnosti (WP 239),
- Mnenje 03/2016 o oceni in pregledu Direktive o zasebnosti v elektronskih komunikacijah (t. i. ePrivacy direktiva) (WP 240).

V okviru WP29 je Informacijski pooblaščenec aktivno sodeloval tudi v štirih njenih podskupinah, in sicer v:
(1) podskupini Future of Privacy (glede novega pravnega okvira za varstvo osebnih podatkov),
(2) podskupini za internet in informacijske tehnologije, t. i. Tehnološki podskupini,
(3) podskupini za iznos podatkov v tretje države ter
(4) podskupini BTLE (za varstvo osebnih podatkov na področju nadzora mej, transporta in organov pregona).

Podskupina Future of Privacy je leta 2016 nadaljevala razprave in pripravo mnenj za WP29 glede reformnih predlogov za varstvo osebnih podatkov s poudarkom na predlogih glede ustanovitve, upravljanja in delovanja t. i. European Data Protection Board (EDPB). Podskupina Future of

Privacy je v skladu s sprejetim akcijskim načrtom usmerjala delo drugih podskupin in z njimi sodelovala na področju priprav na izvajanje Splošne uredbe o varstvu podatkov. Med drugim se bile organizirane delavnice na temo mehanizma skladnosti, medsebojne pomoči in skupnega ukrepanja ter administrativnih kazni. V primeru neenotnih mnenj je skrbela za enotno odločanje pred uradnim sprejemom dokumentov na plenarnih zasedanjih.

Tehnološka podskupina se je leta 2016 ukvarjala z Mnenjem o evalvaciji in prenovi Direktive o zasebnosti v elektronskih komunikacijah in s Smernicami o pravici do prenosljivosti osebnih podatkov. Poleg tega je obravnavala primere upravljavcev, kot so Yahoo, ki je utrpel veliko izgubo osebnih podatkov, WhatsApp, ki je baze podatkov želel povezovati s podatki uporabnikov Facebooka, ter primer Microsoftovega operacijskega sistema Windows 10. Podskupina je obravnavala mnoge teme, ki se tičejo nove Splošne uredbe o varstvu podatkov in njene implementacije, kot npr. certificiranje, ocene vplivov na varstvo osebnih podatkov itd.

Podskupina za iznos podatkov v tretje države je sodelovala pri pripravi mnenja o ustreznosti varstva osebnih podatkov, ki ga zagotavlja Zasebnostni ščit EU–ZDA, pripravila je delovni dokument o utemeljenih posegih v temeljne pravice posameznikov med prenosom osebnih podatkov v tretje države za namen varnostnoobveščevalnih služb ter delovni dokument z odgovori na pogosta vprašanja glede zavezujočih poslovnih pravil. Pripravljeni so bili tudi odgovori na pogosta vprašanja glede iznosa osebnih podatkov v okviru Zasebnostnega ščita za državljane v EU in podjetja v EU.

Leta 2016 je bila znova aktivirana podskupina za nadzor (Enforcement Subgroup), na ravni katere naj bi v prihodnosti potekala koordinacija čezmejnih primerov kršitev varstva podatkov.

Podskupina BTLE je leta 2016 osrednji del svojega dela posvetila implikacijam novega Zasebnostnega ščita EU–ZDA ter pogajanjem glede krovnega sporazuma o varstvu podatkov med EU in ZDA. Delovala je na področju implementacije novih dveh direktiv v nacionalno pravo držav članic EU: 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, ter t. i. Direktive PNR. Še naprej se je ukvarjala s predlogom Evropske komisije o t. i. paketu uredb Pametne meje.

Informacijski pooblaščenec je tudi leta 2016 aktivno deloval v Mednarodni delovni skupini za varstvo osebnih podatkov v telekomunikacijah (IWGDPT – *International Working Group on Data Protection in Telecommunications*), v okviru katere se srečujejo predstavniki informacijskih pooblaščencev in organov za varstvo osebnih podatkov in zasebnosti s celega sveta. Delovna skupina, ki šteje že skoraj 60 članov iz različnih držav, je na zasedanjih v Oslu in Berlinu sprejela dva nova delovna dokumenta. Na pobudo Informacijskega pooblaščenca so se delovni skupini pridružili tudi nadzorni organi nekaterih držav bivše Jugoslavije. Delovni dokument o vprašanjih zasebnosti in varnosti na področju internetne telefonije[46] (VoIP) posodablja delovni dokument skupine iz leta 2006, saj je v medtem prišlo do razmaha internetne telefonije in različnih t. i. *over-the-top* storitev, ki so terjale posodobitev priporočil. Drugi delovni dokument se posveča uporabi biometrijskih ukrepov pri spletni avtentikaciji[47]. Informacijski pooblaščenec je pomembno prispeval k vsebini dokumenta, ki opisuje prednosti in slabosti biometrijskih ukrepov, razvoj tehnologije in standardizacije na tem področju ter podaja priporočila zakonodajalcem, nadzornim organom ter ponudnikom in uporabnikom tovrstnih rešitev. IWGDPT je leta 2016 začela pripravljati mnenja za področji e-izobraževanja ter obdelave podatkov o vozilih in voznikih (*connected cars*).

V okviru Sveta Evrope je predstavnik Informacijskega pooblaščenca tudi leta 2016 sodeloval v Posvetovalnem odboru (T-PD) po Konvenciji Sveta Evrope o varstvu posameznikov glede na avtomatsko obdelavo osebnih podatkov (Konvencija št. 108). Odbor T-PD je na plenarnem zasedanju junija obravnaval predloge sprememb v t. i. procesu posodabljanja Konvencije št. 108, ki poteka od začetka leta 2011, ter procesna vprašanja k sprejemu prenovljene Konvencije št. 108. Kot vsako leto je Odbor obravnaval poročila o mednarodnem in globalnem sodelovanju Sveta Evrope v zvezi z varstvom osebnih podatkov in poročila nadzornih organov za varstvo osebnih podatkov iz držav članic Sveta Evrope o novostih in dosežkih na tem področju ter še posebej informacije o obeležitvi dneva varstva osebnih podatkov. Na ravni Odbora so bile sprejete Smernice o velikem podatkovju (*Guidelines on Big Data*) ter Mnenje o varstvu osebnih podatkov v okviru PNR sistema.

[46] https://datenschutz-berlin.de/attachments/1237/675.52.10_WP_Update_VoIP_2016.pdf?1470059412.

[47] https://datenschutz-berlin.de/attachments/1288/Use_of_Biometrics_in_Online_Authentication_-_IWGDPT_Working.pdf?1488969672.

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 2016 Informacijski pooblaščenec ni prejel nobene pritožbe zaradi nezakonite obdelave osebnih podatkov iz SISII kot tudi ne zaradi izvajanja pravice do seznanitve z lastnimi osebnimi podatki iz SIS II.

Informacijski pooblaščenec je leta 2016 gostil predstavnike sorodnih institucij iz Albanije, Ukrajine, Srbije in Moldavije ter jim predstavil svoje delovanje in dobre prakse s področij, za katera je pristojen.

Informacijski pooblaščenec je leta 2016 pripravil odgovore na 95 vprašanj in vprašalnikov tujih organov za varstvo osebnih podatkov, mednarodnih organizacij, akademskih in raziskovalnih inštitucij ter tujih nevladnih organizacij.

4.3.3. Sodelovanje na mednarodnih srečanjih

Leta 2016 so se zaposleni pri Informacijskem pooblaščencu poleg sestankov v okviru mednarodnih dejavnosti (delovne skupine EU, projekti) udeležili tudi naslednjih mednarodnih konferenc:

- 19. april, Bruselj, Belgija: Meeting with National Authorities on the Review of the ePrivacy Directive,
- 11.-12. maj , Sarajevo, Bosna in Hercegovina: 18th Meeting of Central and Eastern European Data Protection Authorities,
- 25.-27. maj, Budimpešta, Madžarska: European Data Protection Conference,
- 1. junij, Amsterdam, Nizozemska: Transparecy Camp Europe,
- 7. september, Zagreb, Hrvaška: 2nd Annual SEE Cloud Computing Forum,
- 7.-8. september, Frankfurt, Nemčija: Annual Privacy Forum 2016 - Bringing research&policy together,
- 14.-16. september, Wroclaw, Poljska: EELF konferenca 2016,
- 16.-21. oktober, Marakeš, Maroko: 38th International Data Protection and Privacy Commissioners Conference,
- 8. november, Moskva, Rusija: 7th International Conference »Protection of Personal Data«.

Glavne teme evropske konference nadzornih organov za varstvo osebnih podatkov v Budimpešti so bile sodelovanje med nadzornimi organi in priprava na izzive, ki jih prinaša nova Uredba o varstvu podatkov, posodobitev Konvencije Sveta Evrope št. 108 ter vprašanja zasebnosti na področju obveščevalnih agencij.

Namestnik informacijske pooblaščenke je v Moskvi na mednarodni konferenci o varstvu osebnih podatkov predstavil področje certificiranja varstva osebnih podatkov ter potekajoči projekt CRISP.

4.3.4. Projekti Informacijskega pooblaščenca

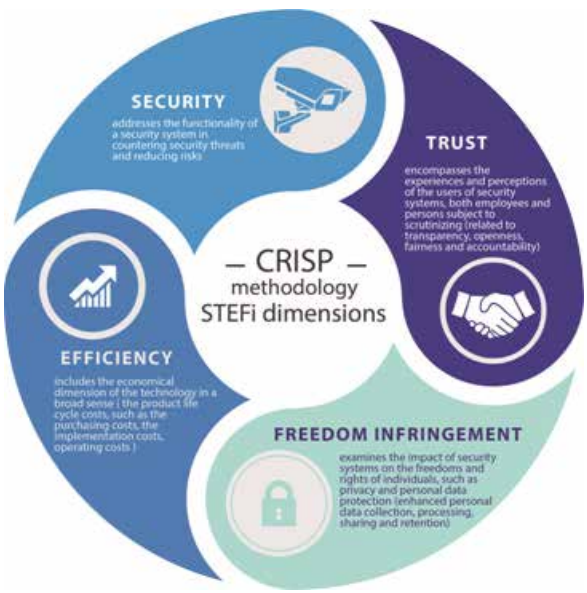
Informacijski pooblaščenec je leta 2016 kot partner aktivno sodeloval v dveh mednarodnih projektih:

- CRISP (Evaluation and Certification Schemes for Security Products) in
- ARCADES (Introducing dAta pRoteCtion AnD privacy issuEs at schoolS in the European Union).

4.3.4.1. Projekt CRISP

Informacijski pooblaščenec sodeluje v konzorciju EU FP7 projekta CRISP, katerega namen je postaviti temelje za razvoj sheme za evalvacijo in certificiranje varnostnih sistemov, kot so (pametni) videonadzorni sistemi, varnostne informacijske rešitve, biometrijske rešitve, telesni skenerji itd. V okviru projekta je bila razvita inovativna metodologija za evalvacijo varnostnih sistemov, kjer sta poleg varnosti sistema ocenjeni tudi dimenziji zaupanja in učinkovitosti ter je pri oceni upoštevan vpliv sistema na morebitne kršitve človekovih pravic s posebnim poudarkom na varstvu osebnih podatkov in prispevanju k skladnosti z novo uredbo o varstvu osebnih podatkov (STEFi dimenzije). Za testno področje je bil izbran (pametni) videonadzor.

Slika 17: Shematski prikaz dimenzij STEFi za evalvacijo varnostnih sistemov



V konzorciju projekta so: koordinator Netherlands Standardization Institute (Nizozemska), Trilateral Research & Consulting (Velika Britanija), Technische Universität Berlin (Nemčija), Vienna Centre for Societal Security (Avstrija), Vrije Universiteit Brussel (Belgija), University Jaume I of Castellón (Španija) in Informacijski pooblaščenec. Projekt je sofinanciran s strani Sedmega okvirnega programa Evropske skupnosti za raziskave, tehnološki razvoj in predstavitvene dejavnosti (številka dogovora 607941). Projekt traja tri leta, od aprila 2014 do aprila 2017. Vse informacije o projektu so dostopne na spletni strani http://crispproject.eu/.

Leta 2016 so sodelujoči v projektu med drugim:

- razvili inovativno metodologijo za evalvacijo varnostnih produktov glede na dimenzije varnosti, zaupanja, učinkovitosti in varstva pravic posameznikov – STEFi (http://data.trilateralresearch.com/wp-content/ uploads/2015/12/CRISP_D5.1_Validated-CRISP-Methodology.pdf in http://data.trilateralresearch.com/wp-content/uploads/2016/03/CRISP_DEL5.2.compressed.pdf);
- pripravili navodila za postopek evalvacije in certificiranja (http://crispproject.eu/wp-content/uploads/ 2016/09/CRISP_D6.2_Final-certification-manual.pdf);
- izdelali praktični načrt implementacije CRISP sheme za nadaljnjih 20 let (http://crispproject.eu/wp-content/uploads/2016/09/CRISP_DEL_6.1_Final-Roadmap-and-Implementation-Plan.pdf). Vsa raziskovalna poročila in dokumenti so na voljo na povezavi http://crispproject.eu/research-reports/

Od junija 2016 do konca leta (in do marca 2017) je dejavnosti celotnega konzorcija vodil Informacijski pooblaščenec kot vodja Delovnega paketa 7. V desetih mesecih je:

- izvajal aktivnosti za dvigovanje zaupanja v predlagano rešitev za evalvacijo, in sicer z informacijskim gradivom, organizacijo dogodkov, sestankov in predstavitev projekta za različne deležnike (proizvajalce in uporabnike varnostnih sistemov, potrošniške organizacije, regulatorje na ravni držav članic EU in na EU-ravni ter nadzorne organe za varstvo osebnih podatkov);
- pred evropskim standardizacijskim telesom CEN začel postopek standardizacije pristopa evalvacije na podlagi STEFi dimenzij v obliki CEN Workshop Agreement dokumenta (v postopek se lahko vključi vsak zainteresirani na EU-ravni, sprejete smernice prestavljajo dokument dobre prakse, ki velja tri leta in ga je mogoče podaljšati, odobrijo pa ga organizacije, ki se formalno registrirajo v postopek sprejema).

Vse aktivnosti so bile izpeljane uspešno in učinkovito. Informacijski pooblaščenec je vse dejavnosti v delovnem paketu 7 predstavil v podrobnem poročilu za Evropsko komisijo, ki je dostopno na povezavi http://crisppproject.eu/wp-content/uploads/2017/05/CRISP_D7.1_Consolidated-WP7-report.pdf. Sprejet in potrjen CEN Workshop Agreement dokument pa je na voljo na: http://crisppproject.eu/wp-content/uploads/2017/05/ CRISP_D7.2_CEN-Workshop-Agreement.pdf.

Med največje uspehe vodenja konzorcija v letu 2016 Informacijski pooblaščenec šteje izjemno uspešno delavnico o certificiranju in varstvu osebnih podatkov za nadzorne organe za varstvo osebnih podatkov, ki jo je s pomočjo University Jaume I of Castellón in španskega nadzornega organa za varstvo osebnih podatkov organiziral v Madridu 30. 9. 2016. Delavnice so se udeležili predstavniki iz desetih držav članic EU in širše, predstavniki Evropskega nadzornika za varstvo osebnih podatkov ter strokovnjaki iz različnih zasebnih združenj in svetovalnega sektorja. V okviru delavnice so potekala predavanja na temo določb o certificiranju in kodeksih ravnanja iz nove uredbe o varstvu osebnih podatkov, predstavitev certifikacijskih shem, ki so že implementirane, in izkušenj tistih organov, ki že delujejo na področju certificiranja. Predstavljen je bil CRISP pristop, udeleženci pa so sodelovali tudi pri oblikovanju rešitev za prihodnost. Delavnica je bila odlična priložnost, da so nadzorni organi soočili mnenja in izkušnje o tem, kako bo po uveljavitvi uredbe potekalo certificiranje skladnosti s pravili varstva osebnih podatkov. Več o delavnici je na voljo na spletni strani http://crisppproject.eu/crisp-workshops/, agenda pa je dostopna na naslovu http://data.trilateralresearch.com/wp-content/uploads/2016/09/DPA-agenda-2.pdf.

4.3.4.2. Projekt ARCADES

Informacijski pooblaščenec verjame, da je izobraževanje ključ za dvig zavesti o pomenu varovanja zasebnosti, zato vsako leto sodeluje v številnih aktivnostih za ozaveščanje otrok in mladih. Prav s tem namenom je sodeloval tudi v evropskem projektu ARCADES, ki je namenjen spodbujanju poučevanja o varstvu osebnih podatkov in zasebnosti v osnovnih in srednjih šolah. V okviru projekta so bila na ravni EU pripravljena enotna gradiva in orodja za poučevanje o varstvu zasebnosti in osebnih podatkov, ki jih bodo učitelji in svetovalni delavci v osnovnih in srednjih šolah lahko uporabili. Projekt je bil sofinanciran s strani Programa za temeljne pravice in državljanstvo Evropske skupnosti (številka dogovora JUST/2013/FRAC/AG/6132), zaključil se je maja 2016.

V konzorciju projekta so bili: Inspector General for Personal Data Protection (Poljska), Informacijski pooblaščenec (Slovenija), National Authority for Data Protection and Freedom of Information (Madžarska) in Vrije Universiteit Brussel (Belgija).

V okviru projekta je bil leta 2016 razglašen zmagovalec natečaja za najboljšo uro na temo varovanja zasebnosti in osebnih podatkov. Zmagali so učenci in učenke Osnovne šole Ivana Skvarče Zagorje ob Savi, Podružnične šole Podkum z učiteljico Nino Jelen. Izziv so odlično opravili: njihova učna ura o varovanju spletne identitete je prepričala z izvirnostjo in domiselnostjo. Pesem o škraticah in možičkih za grički ter Zlata pravila fac in faconov, ki so jih pripravili, bodo zagotovo v pomoč tudi drugim otrokom pri varnejšem raziskovanju spleta. Razglasitev je potekala na posebnem dogodku 19. januarja 2016 v City Teatru v Ljubljani, kjer so učenci in učenke zmagovalne šole učno uro tudi izpeljali.

Slika 18: Učenci in učenke Osnovne šole Ivana Skvarče Zagorje ob Savi, Podružnične šole Podkum, v City Teatru.

4. marca 2016 je v Barceloni v Španiji potekala zaključna konferenca projekta ARCADES ob boku s konferenco Delovne skupine za digitalno opismenjevanje. Na zaključnem dogodku so zmagovalci natečaja za najboljšo učno uro iz Slovenije, Madžarke in Poljske predstavili nagrajene učne ure, primere dobre prakse pri poučevanju o zasebnosti pa so predstavili govorci z različnih področij.

Projekt se je zaključil z julija 2016 izdanim *Evropskim priročnikom za poučevanje o zasebnosti in varstvu osebnih podatkov v osnovnih in srednjih šolah*. Namenjen je učiteljem in strokovnim delavcem v izobraževanju. Obravnava varstvo zasebnosti in osebnih podatkov, varnost na spletu, digitalno identiteto, vedenjsko oglaševanje, spletno nadlegovanje ter nadzor staršev. Priročnik vsebuje izčrpno razlago teh tem, konkretne ideje za pogovor učitelja z učenci vseh starostnih skupin, praktične vaje ter primere celotnih učnih ur. Priročnik je izšel v štirih jezikih (v angleščini, poljščini, madžarščini in slovenščini) in vsebuje vse nagrajene učne ure o zasebnosti, tudi slovensko, ki je na mednarodni predstavitvi v Barceloni doživela izjemen uspeh ter je tako voljo vsem učiteljem, ki bi radi podobno učno uro pripravili za svoje učence. Tiskane verzije priročnika je Informacijski pooblaščenec posredoval slovenskim šolam in organizacijam, ki izobražujejo o varni rabi interneta in sodobnih tehnologij, ter knjižnicam, elektronske verzije pa so prosto dostopne na spletu. Priročnik je na voljo na povezavi http://arcades-project.eu/images/pdf/arcades_teaching_handbook_final_SI.pdf.

Slika 19: Evropski priročnik za poučevanje zasebnosti in varstva osebnih podatkov v šolah

Odgovorna urednica:

Mojca Prelesnik, informacijska pooblaščenka

Avtorji besedil:

dr. Monika Benkovič Krašovec, državna nadzornica za varstvo osebnih podatkov
Jože Bogataj, namestnik informacijske pooblaščenke, vodja državnih nadzornikov za varstvo osebnih podatkov
Jelena Burnik, MSc (Velika Britanija), državna nadzornica za varstvo osebnih podatkov
Alenka Jerše, namestnica informacijske pooblaščenke
mag. Eva Kalan, državna nadzornica za varstvo osebnih podatkov
mag. Kristina Kotnik Šumah, namestnica informacijske pooblaščenke
Anže Novak, asistent svetovalca
mag. Andrej Tomšič, namestnik informacijske pooblaščenke
mag. Vanja Zrimšek, svetovalka

Oblikovanje:

mag. Matjaž Drev

Lektorirala:

Katja Klopčič Lavrenčič

Informacijski pooblaščenec Republike Slovenije
Zaloška cesta 59
1000 Ljubljana

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

Ljubljana, maj 2017

ISSN 1854-9500