



**INFORMACIJSKI POOBLAŠČENEC
REPUBLIKE SLOVENIJE**



'17

Letno poročilo

Informacijskega pooblaščenca

za leto 2017

Spoštovani,

med ključnimi temami, ki so zaznamovale delo Informacijskega pooblaščenca leta 2017, ni mogoče prezreti priprav na začetek uporabe nove evropske Splošne uredbe o varstvu podatkov. Te so zaznamovale delo Informacijskega pooblaščenca s posamezniki, podjetji in drugimi organizacijami – Informacijski pooblaščenec je izdal številna mnenja ter izvedel številna srečanja in izobraževanja – prav pripravam pa je bilo največ pozornosti namenjene tudi na mednarodnem področju v okviru delovne skupine evropskih nadzornih organov WP 29. Nova uredba je zaznamovala tudi velik del podajanja mnenj na predloge zakonov, med drugim na težko pričakovani predlog osnutka novega zakona o varstvu osebnih podatkov. Poleg tega je Informacijski pooblaščenec leta 2017 z željo po največjem možnem učinku na pravice posameznikov svoje sile usmerjal v hitro reševanje pritožbenih zadev na področju dostopa do informacij javnega značaja ter učinkovito ukrepanje proti kršitvam na področju varstva osebnih podatkov, izvajal pa je tudi izobraževanja na obeh pravnih področjih.



VIR: Jože Suhadolnik - Delo, d.d.

Na področju dostopa do informacij javnega značaja bi želela poudariti razveseljivo zmanjšanje števila pritožb, vloženih zoper ravnanje občin, kar po mojem mnenju izkazuje, da so občine leta 2017 na tem področju poslovale bolje, še posebej glede na podatke iz preteklih let, ki so kazali na slabšo odzivnost občin v postopkih po ZDIJZ. So pa prosilci vložili več pritožb zoper državne organe, vnovič pa se je tudi povečalo število prošenj za pojasnila in mnenja s strani zavezancev. Vse navedeno kaže, da so bili zavezanci leta 2017 bolj aktivni in odzivni kot leto poprej, saj so se na Informacijskega pooblaščenca večkrat obrnili tudi izven pritožbenega postopka.

Informacijski pooblaščenec je na področju dostopa do informacij javnega značaja leta 2017 skupaj prejel 522 pritožb, kar je več kot leto dni poprej, ko jih je prejel 514. Prizadevali smo si, da bi pritožbene zadeve reševali 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 znašal 37 dni; pritožbene zadeve so bile torej rešene precej hitreje kot v dvomesečnem roku, ki ga za reševanje tovrstnih zadev določa Zakon o splošnem upravnem postopku. Za primerjavo: leta 2016 je povprečen čas reševanja pritožbenih zadev znašal 47 dni.

Informacijski pooblaščenec je v pritožbenih postopkih obravnaval več vsebinsko pomembnih zadev. Z vidika izjem, na katere so se sklicevali zavezanci v postopkih, je bilo zaznati povečanje števila zadev, ki so se nanašale na t. i. zlorabo pravice. Ob tem velja opozoriti, da je institut zlorabe pravice skrajno sredstvo, na katerega se lahko zavezanci sklicujejo le v izjemnih primerih. Pravico dostopa do informacij javnega značaja kot temeljno človekovo pravico je namreč mogoče omejiti le zaradi varstva legitimnih interesov in pravic tretjih ter v najmanjši možni meri, ki še zagotavlja varstvo teh interesov.

Podatki kažejo, da se je leta 2017 delno spremenila struktura prosilcev, ki so se s pritožbo obrnili na Informacijskega pooblaščenca. Tudi v tem letu je bilo največ pritožnikov fizičnih oseb, manj pritožb je Informacijski pooblaščenec prejel s strani pravnih oseb zasebnega prava, število pritožb, ki so jih vložili novinarji, je ostalo na primerljivi ravni. Zanimiva pa je ugotovitev, da se je povečalo število pritožbenih primerov, v katerih so kot prosilci za informacije nastopale pravne osebe javnega prava, kar kaže na to, da je pravica dostopa do informacij javnega značaja institut, ki omogoča hitro in učinkovito pridobivanje informacij različnim kategorijam uporabnikov. Ob tem je zaradi vsakoletnega naraščanja števila pritožb mogoče zaključiti, da so prosilci s postopkom

dostopa do informacij dobro seznanjeni ter da je pritožbeni postopek zanje hiter, učinkovit in jim ne povzroča stroškov, kar pomeni, da zagotavlja učinkovito pravno varstvo.

Informacijski pooblaščenec je leta 2017 v okviru izvajanja inšpekcijskega nadzora na področju varstva osebnih podatkov obravnaval 655 inšpekcijskih zadev, od tega 226 na področju javnega in 429 na področju zasebnega sektorja ter 105 prekrškovnih zadev. Prejel je tudi 16 vlog za izdajo dovoljenja za povezovanje zbirk osebnih podatkov, štiri vloge za izdajo dovoljenja za izvajanje biometrijskih ukrepov, 29 vlog za izdajo dovoljenja za iznos osebnih podatkov ter 110 pritožb zaradi zavrnitve zahteve za seznanitev z lastnimi osebnimi podatki.

Največ prijav zaradi suma kršitev predpisov s področja varstva osebnih podatkov je bilo vloženih zaradi posredovanja osebnih podatkov nepooblaščenim uporabnikom, nezakonitega zbiranja oziroma posredovanja osebnih podatkov, 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), izvajanja videonadzora in nezakonite uporabe posnetkov (zlasti v delovnih prostorih), neustreznega zavarovanja osebnih podatkov, uporabe osebnih podatkov v nasprotju z namenom njihovega zbiranja ter zaradi nezakonitega vpogleda v osebne podatke. V zvezi z obravnavo prejetih prijav velja opozoriti na povečanje števila prijav in ugotovljenih kršitev zaradi neustreznega zavarovanja osebnih podatkov, ki se zbirajo ali so dostopni prek spletnih omrežij. Večje število bolnišnic in drugih zdravstvenih zavodov, ki omogoča elektronsko naročanje, namreč ni zagotavljalo varnih povezav v sistemih za elektronsko naročanje (npr. z uporabo protokola https oziroma ustreznega šifriranja), zaradi česar je Informacijski pooblaščenec v okviru systemskega nadzora vse zdravstvene zavode pozval k odpravi pomanjkljivosti. Informacijski pooblaščenec je v inšpekcijskih postopkih večkrat ugotovil, da tudi drugi zavezanci niso zagotovili zavarovanja osebnih podatkov na spletnih strežnikih, na katerih so bile shranjene zbirke (z omejitvijo dostopa s požarnim zidom, z uporabniškim imenom in geslom ali na drug podoben način).

Opozoriti je treba tudi na povečanje števila prijav zaradi nezakonitega zbiranja oziroma posredovanja osebnih podatkov kot posledica pomanjkljivega oziroma neustreznega informiranja posameznika, od katerega se osebni podatki pridobivajo. Nova evropska Splošna uredba o varstvu podatkov, ki se bo začela uporabljati 25. maja 2018, je glede zagotavljanja informacij, ki jih je treba zagotoviti posamezniku v primeru, ko se osebni podatki pridobivajo neposredno od njega, še zahtevnejša kot veljavni ZVOP-1, saj v drugem in tretjem odstavku 13. člena določa še precej širši nabor informacij, ki jih je treba zagotoviti posamezniku.

Informacijski pooblaščenec je poleg obravnave prejetih prijav tudi leta 2017 nadaljeval okrepljeno izvajanje t. i. planiranih ex offo inšpekcijskih nadzorov na področjih, na katerih glede na oceno tveganja obstaja večja verjetnost kršitve predpisov s področja varstva osebnih podatkov. Planirani inšpekcijski nadzor nad spoštovanjem določb ZVOP-1 se je leta 2017 izvajal na ministrstvih, v upravnih enotah, zdravstvenih zavodih, pri večjih pogodbenih obdelovalcih osebnih podatkov, turističnih agencijah, sindikatih in njihovih zvezah ter društvih in njihovih zvezah.

Poleg inšpekcijskih in prekrškovnih postopkov je Informacijski pooblaščenec leta 2017 s ciljem preventivnega delovanja posebno pozornost namenil nudenju podpore podjetjem; obravnaval je več kot 1289 zaprosil za pisna mnenja in pojasnila s področja varstva osebnih podatkov ter se s pojasnili odzval na 1998 telefonskih klicev. Na Informacijskega pooblaščenca se je obrnilo tudi več kot 115 upravljavcev in obdelovalcev iz javnega in zasebnega sektorja, ki so pripravljali zakonodajo, rešitve ali projekte ter so želeli pravočasno premisliti o tveganjih in se tako izogniti kršitvam zakonodaje. S ciljem pravočasnih priprav na novo uredbo ter v sklopu preventivnega delovanja je Informacijski pooblaščenec izvedel tudi 132 predavanj za različna podjetja in druge organizacije. Strokovnjaki Informacijskega pooblaščenca za dvig ozaveščenosti o pomenu zasebnosti in varstva osebnih podatkov so, kot vsako leto, nastopili na različnih konferencah, predavanjih, strokovnih dogodkih, posvetih ter okroglih mizah.

Izkušnje iz leta 2017 kažejo, da so se večji upravljavci že intenzivno začeli pripravljati na uporabo Splošne uredbe o varstvu podatkov, predvsem pri manjših upravljavcih, ki so bili po ZVOP-1 deležni določenih izjem (npr. glede priprave katalogov in prijave zbirk osebnih podatkov v register

Informacijskega pooblaščenca), pa se pokazalo, da nekateri zakonodajci o varstvu osebnih podatkov niso dobro poznali. Poseben izziv za določene upravljavce in obdelovalce osebnih podatkov predstavlja imenovanje pooblaščenih oseb za varstvo osebnih podatkov. Gre za institut, ki je bil v praksi doslej prisoten predvsem v bankah in zavarovalnicah, Splošna uredba pa določa precej širok krog zavezancev, ki bodo morali imenovati tako osebo, in sicer kadar obdelavo opravlja javni organ ali telo, razen sodišč, kadar delujejo kot sodni organi; kadar temeljne dejavnosti upravljavca ali obdelovalca zajemajo dejanja obdelave, pri katerih je treba zaradi njihove narave, obsega in/ali namenov posameznike, na katere se osebni podatki nanašajo, redno in sistematično obsežno spremljati; kadar temeljne dejavnosti upravljavca ali obdelovalca zajemajo obsežno obdelavo posebnih vrst podatkov v zvezi s kazenskimi obsodbami in prekrški.

V okviru mednarodnega delovanja je Informacijski pooblaščenec maja 2017 na Bledu organiziral tudi prvo, ustanovno zasedanje pobude Initiative 20i7, v okviru katere je gostil predstojnike nadzornih organov za varstvo osebnih podatkov iz Hrvaške, Srbije, Bosne in Hercegovine, Črne gore, Kosova in Makedonije. Pobuda Informacijskega pooblaščenca sledi zgledu nordijskih držav, ki si delijo podobne zgodovinske in pravne okvire in katerih nadzorni organi za varstvo osebnih podatkov tesno sodelujejo ter si izmenjujejo izkušnje. Prav v luči reforme varstva osebnih podatkov na ravni EU se je pobuda izkazala kot izredno učinkovit način izmenjave dobrih praks in izkušenj s pripravami na uporabo.

V letu 2018 nas čaka nemalo izzivov, ki bodo povezani predvsem z uporabo nove evropske Splošne uredbe o varstvu podatkov. Hkrati že opažamo, da pomeni nova evropska zakonodaja tudi nov veter v jedra varstva zasebnosti v Evropi in svetu. Zdi se, kot da se varstvo osebnih podatkov postavlja na novo. Informacijski pooblaščenec si bo na vseh področjih prizadeval, da bi ta novi veter čim boljše izkoristili tudi v Sloveniji. Kot član novega evropskega organa, Evropskega odbora za varstvo podatkov, bo Informacijski pooblaščenec aktivno sodeloval pri pripravi evropskih smernic in drugih preventivnih mehanizmov, ki jih bo odbor pripravljala, kot nadzorni organ pa bo sodeloval tudi v nacionalnih in mednarodnih inšpekcijah pod okriljem odbora. Dejstvo, da do 25. 5. 2018 Slovenija ni sprejela novega zakona o varstvu osebnih podatkov, namreč izzive in naloge v celoti prelaga na pleča podjetij, drugih organizacij in Informacijskega pooblaščenca. Delo Informacijskega pooblaščenca bo zahtevno, odsotnost systemskega zakona pa za pravno varnost ni dobra popotnica. Kljub temu sem prepričana, da bo Informacijski pooblaščenec tudi v prihodnje učinkovito varoval obe ustavni pravici. Naša glavna skrb namreč ostajajo preventivno delovanje, učinkovito reševanje pritožb ter odgovorna obravnava inšpekcij.

*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	15

2. DELO NA PODROČJU DOSTOPA DO INFORMACIJ JAVNEGA ZNAČAJA

2.1.	Pravna ureditev na področju dostopa do informacij javnega značaja v Republiki Sloveniji	19
2.2.	Število vloženih pritožb in število rešenih zadev	21
2.3.	Število vloženih tožb na Upravnem sodišču, število sodb Upravnega in Vrhovnega sodišča	22
2.4.	Statistika po posameznih področjih ZDIJZ	22
2.5.	Storjeni prekrški po ZDIJZ, ZInfP in ZMed	25
2.6.	Predstavitev najodmevnejših in precedenčnih primerov po področjih	25
2.6.1.	Ali gre za delovno področje organa, poslovna skrivnost	26
2.6.2.	Ali gre za zlorabo pravice?	26
2.6.3.	Avtorsko delo	27
2.6.4.	Dokument v izdelavi, tajni podatki, notranje delovanje	28
2.6.5.	Javno naročilo, poslovna skrivnost	29
2.6.6.	Osebni podatki, javni uslužbenci, funkcionarji	30
2.6.7.	Varstvo kazenskega postopka, osebni podatki	30
2.6.8.	Varstvo nadzornega postopka, notranje delovanje	31
2.6.9.	Okoljski podatki, poslovna skrivnost	32
2.6.10.	Stroški postopka	33
2.6.11.	Tajni podatki, dokument v izdelavi	33
2.6.12.	Ponovna uporaba	34
2.6.13.	Tajnost vira	35
2.6.14.	Varstvo upravnega postopka	36
2.7.	Splošna ocena in priporočila na področju dostopa do informacij javnega značaja	36

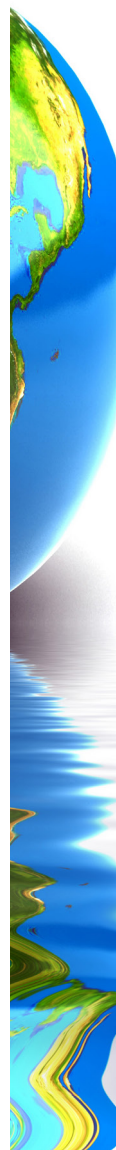
3. DELO NA PODROČJU VARSTVA OSEBNIH PODATKOV

3.1.	Koncept varstva osebnih podatkov v Republiki Sloveniji	40
3.2.	Dejavnost državnih nadzornikov za varstvo osebnih podatkov	41
3.2.1.	Pravice in dolžnosti državnega nadzornika	41
3.2.2.	Inšpekcijski nadzor	41
3.2.2.1.	Inšpekcijski nadzor v javnem sektorju	42
3.2.2.2.	Inšpekcijski nadzor v zasebnem sektorju	43
3.2.3.	Storjeni prekrški	44
3.3.	Dajanje mnenj in pojasnil	45
3.4.	Dopustnost izvajanja biometrijskih ukrepov	46
3.5.	Ugotavljanje ustrezne ravni varstva osebnih podatkov v tretjih državah	47
3.6.	Izdajanje dovoljenj za povezovanje javnih evidenc	49
3.7.	Pravica do seznanitve z lastnimi osebnimi podatki	51

3.8.	Zahteve za oceno ustavnosti	57
3.8.1.	Zahteva za oceno ustavnosti Zakona o Slovenski obveščevalno-varnostni agenciji	52
3.8.2.	Zahteva za oceno ustavnosti Zakona o nalogah in pooblastilih policije (ZNPPol-A)	55
3.9.	Izbrani primeri kršitev varstva osebnih podatkov	56
3.9.1.	Neustrezno zavarovanje dokumentacije, namenjene uničenju	56
3.9.2.	Zbiranje osebnih podatkov plačnikov	57
3.9.3.	Nezakonito razkritje osebnih podatkov učencev	58
3.9.4.	Nezakonita obdelava osebnih podatkov v evidencah policije	59
3.9.5.	Sporno posredovanje osebnih podatkov zaposlenega članom zveze	59
3.9.6.	Objava osebnih podatkov članov na spletni strani	60
3.9.7.	Objava dokumenta z osebnimi podatki prič v prekrškovnem postopku na spletnih straneh	61
3.9.8.	Neustrezno zavarovanje datotečne strukture v notarski pisarni	62
3.9.9.	Zbiranje podatkov o vzrokih za bolniško odsotnost	63
3.9.10.	Posredovanje videoposnetka tatvine in objava na Facebooku	64
3.11.	Splošna ocena stanja varstva osebnih podatkov in priporočila	65

4. DRUGE DEJAVNOSTI INFORMACIJSKEGA POOBLAŠČENCA

4.1.	Sodelovanje pri pripravi zakonov in drugih predpisov	71
4.2.	Sodelovanje z javnostmi	73
4.3.	Mednarodno sodelovanje	77
4.3.1.	Sodelovanje v mednarodnih delovnih telesih	77
4.3.2.	Ostale mednarodne dejavnosti	78
4.3.3.	Sodelovanje na mednarodnih srečanjih	79
4.3.4.	Projekti Informacijskega pooblaščenca	80
4.3.4.1.	Projekt CRISP	80



LETO 2017 V ŠTEVILKAH



32

ZAPOSLENIH ZA
NEDOLOČEN ČAS



1.459.747 EUR

PRORAČUN

V ARSTVO O SEBNIH P ODATKOV

655

INŠPEKCIJSKIH
POSTOPKOV



105

PREKRŠKOVNIH
POSTOPKOV



1289

PISNIH MNENJ



1998

USTNIH MNENJ



I NFORMACIJE J AVNEGA Z NAČAJA



522

VLOŽENIH PRITOŽB

316

IZDANIH ODLOČB



201

POZIV
ZARADI MOLKA



61

IN CAMERA OGLEDOV

324

PISNIH PROŠENJ
ZA POJASNILA

OSTALO

2

SMERNIC

100+

BREZPLAČNIH PREDAVANJ
ZAVEZANCEM



SODELOVANJE PRI PRIPRAVI **100+**
PREDPISOV



1

O INFORMACIJSKEM POOBLAŠČENCU

1.1. Nastanek Informacijskega pooblaščenca

Državni zbor Republike Slovenije je 30. 11. 2005 sprejel Zakon o Informacijskem pooblaščenju¹, s katerim je bil 31. 12. 2005 ustanovljen nov samostojen in neodvisen državni organ. Omenjeni zakon je združil dva organa, in sicer Pooblaščenca za dostop do informacij javnega značaja, ki je imel že prej status neodvisnega organa, in Inšpektorat za varstvo osebnih podatkov, ki je deloval kot organ v sestavi Ministrstva za pravosodje. Ob uveljavitvi ZInfP je Pooblaščenec za dostop do informacij javnega značaja nadaljeval delo kot Informacijski pooblaščenec, ki je prevzel inšpektorje in druge uslužbenke Inšpektorata za varstvo osebnih podatkov, pripadajočo opremo in sredstva. Hkrati je prevzel tudi vse nedokončane zadeve, arhive in evidence, ki jih je vodil Inšpektorat za varstvo osebnih podatkov. S tem so se pristojnosti organa, ki je skrbel za nemoteno izvajanje dostopa do informacij javnega značaja, močno spremenile in se razširile še na pravno področje varstva osebnih podatkov. Informacijski pooblaščenec je tako postal tudi državni nadzorni organ za varstvo osebnih podatkov. Delo je začel 1. 1. 2006.

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

Informacijski pooblaščenec je neodvisen državni organ. Njegova neodvisnost je zagotovljena na dva načina. Prvi je postopek imenovanja pooblaščenca kot funkcionarja, ki ga na predlog predsednika Republike Slovenije imenuje Državni zbor. 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 pristojen tudi 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 Informacijskemu pooblaščenju pristojnosti podeljuje tudi **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 razlog za pritožbo, o kateri odloča Informacijski pooblaščenec po določbah ZDIJZ.

Informacijski pooblaščenec je v primeru kršitev določb ZDIJZ in ZMed tudi prekrškovni organ.

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 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 ugotovi 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 (32. člen ZVOP-1);
7. izdaja odločbe o zagotavljanju ustreznih ravni varstva osebnih podatkov v tretjih državah (63. člen ZVOP-1);
8. vodi postopke ugotavljanja ustreznih 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 ustrežno raven varstva osebnih podatkov ali da te nimajo zagotovljene; če je ugotovljeno, da tretja država le delno zagotavlja ustrežno raven varstva osebnih podatkov, je v seznamu navedeno tudi, v katerem delu je ustrežna 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 povežalo, vsebuje občutljive osebnostne 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 osebnostne podatke;
15. daje in objavlja neobvezna mnenja o skladnosti kodeksov poklicne etike, splošnih pogojev 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 ali na drug primeren način objavlja predhodna mnenja o usklajenosti predlogov zakonov in drugih predpisov z zakonom in drugimi predpisi s področja varstva osebnih podatkov ter zahtev za oceno ustavnosti predpisov, 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 opravljenih 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 Evropa ter v skupini za nadzor Eurodac).

Informacijski pooblaščenec lahko v skladu s 6. alinejo prvega odstavka 23.a člena Zakona o ustavnem sodišču⁵ zahtevo začne postopek za oceno ustavnosti oziroma zakonitosti predpisa

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

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

ali splošnega akta, izdanega za izvrševanje javnih pooblastil, če nastane vprašanje ustavnosti ali zakonitosti v zvezi s postopkom, ki ga vodi.

Informacijski pooblaščenec ima pristojnosti še 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, **Zakonu o potrošniških kreditih**¹¹, **Uredbi o sistemih brezpilotnih zrakoplovov**¹² in **Uredbi o izvajanju Uredbe (EU) o državljski pobudi**¹³.

Na podlagi ZPacP Informacijski pooblaščenec deluje kot pritožbeni, inšpekcijski in prekrškovni organ.

V okviru pritožbenih postopkov Informacijski pooblaščenec:

- na podlagi desetega odstavka 41. člena ZPacP odloča o pritožbah pacientov in drugih upravičenih oseb ob kršitvi določbe, ki ureja način seznanitve z zdravstveno dokumentacijo;
- na podlagi petega odstavka 42. člena ZPacP odloča o pritožbi v zakonu opredeljenih oseb zoper delno ali v celoti zavrnjeno zahtevo za seznanitev z zdravstveno dokumentacijo po paciovni smrti;
- na podlagi sedmega odstavka 45. člena ZPacP odloča 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.

V skladu s četrtem odstavkom 85. člena ZPacP Informacijski pooblaščenec izvaja inšpekcijski nadzor in vodi prekrškovne postopke zaradi kršitev naslednjih določb ZPacP:

- 44. člena, ki opredeljuje pravico pacienta do zaupnosti osebnih podatkov ter pogoje za uporabo in drugo obdelavo osebnih podatkov za potrebe zdravljenja ali izven postopkov zdravstvene obravnave,
- 45. člena, ki določa dolžnost varovanja poklicne skrivnosti oziroma varovanja informacij o zdravstvenem stanju pacienta,
- 46. člena, ki izvajalcem zdravstvene dejavnosti nalaga izvedbo preiskave vsake zaznane nedovoljene obdelave osebnih podatkov o pacientu in obveščanje Informacijskega pooblaščenca o ugotovitvah,
- drugega odstavka 63. člena, ki določa način in rok hrambe dokumentacije, nastale v postopku z zahtevo za obravnavo kršitve pacientovih pravic,
- 68. člena, ki določa pogoje dostopa do zdravstvene dokumentacije pacienta s strani Komisije RS za varstvo pacientovih pravic.

Globe za kršitve 46., 63. in 68. člena so določene v 87. členu ZPacP, za druge prekrške se upoštevajo prekrškovne določbe v ZVOP-1.

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, pri čemer o prekršku odloča v skladu s 27. členom ZOIZk-1 in 34.b členom ZPLD-1.

ZEKom-1 določa pristojnosti Informacijskega pooblaščenca v 161. členu, in sicer:

- izvaja inšpekcijski nadzor 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 opravi inšpekcijski nadzor nad izvajanjem 153. in 153.a člena ZEKom-1, ki določata pogoje in postopke za posredovanje prometnih in lokacijskih podatkov v primerih varovanja življenja in telesa posameznika ter zavarovanje in hrambo teh podatkov in zagotovitev neizbrisne registracije;

⁶ Uradni list RS, št. 15/2008 in 55/2017; 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.

¹² Uradni list RS, št. 52/2016 in 81/2016.

¹³ Uradni list RS, št. 42/2012 in 17/2014.

- izvaja inšpekcijski nadzor 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;
- izvaja inšpekcijski nadzor 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;
- kot prekrškovni organ v skladu z zakonom, ki ureja prekrške, vodi postopke zaradi kršitev navedenih določb ZEKom-1; globe za kršitve so določene v 232. do 236. členu ZEKom-1.

ZCKR 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 bančništvu¹⁴ 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-1¹⁵. V skladu s 31. členom ZCKR Informacijski pooblaščenec z namenom preprečevanja in odvratanja ravnanj, ki pomenijo nezakonito obdelavo osebnih podatkov, javno objavi informacije v zvezi z ukrepi nadzora in sankcijami zaradi prekrška, ki jih je izrekel.

ZPotK-2 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. Globe, ki jih lahko Informacijski pooblaščenec izreče za kršitve členov, ki jih nadzira, so določene v 96. členu ZPotK-2.

Uredba o sistemih brezpilotnih zrakoplovov v drugem odstavku 21. člena določa, da Informacijski pooblaščenec izvaja nadzor nad izvajanjem petega odstavka 19. člena, ki določa, da mora operater pred izvajanjem letalskih dejavnosti izvesti oceno učinkov v zvezi z varstvom osebnih podatkov na obrazcu iz Priloge 6, ki je sestavni del te uredbe, ter da mora Informacijskemu pooblaščenca posredovati izpolnjeni obrazec iz Priloge 6 in kopijo izpolnjenega obrazca iz Priloge 2 k tej uredbi (obrazec izjave za opravljanje letalskih dejavnosti s sistemi brezpilotnih zrakoplovov). V primeru ugotovljene kršitve lahko Informacijski pooblaščenec kršitelju izreče sankcijo po 29. členu uredbe.

Na podlagi 3. člena Uredbe o izvajanju Uredbe (EU) o državljanski pobudi je Informacijski pooblaščenec pristojen za prekrške v primeru kršitve Uredbe (EU) št. 211/2011/EU Evropskega parlamenta in Sveta z dne 16. 2. 2011¹⁶ o državljanski pobudi s področja varstva osebnih podatkov.

Z vstopom Republike Slovenije v schengensko območje je Informacijski pooblaščenec prevzel nadzor nad izvajanjem 128. člena Konvencije o izvajanju Schengenskega sporazuma¹⁷. Na podlagi 114. člena te 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 pomeni kršenja pravic oseb, na katere se podatki nanašajo.

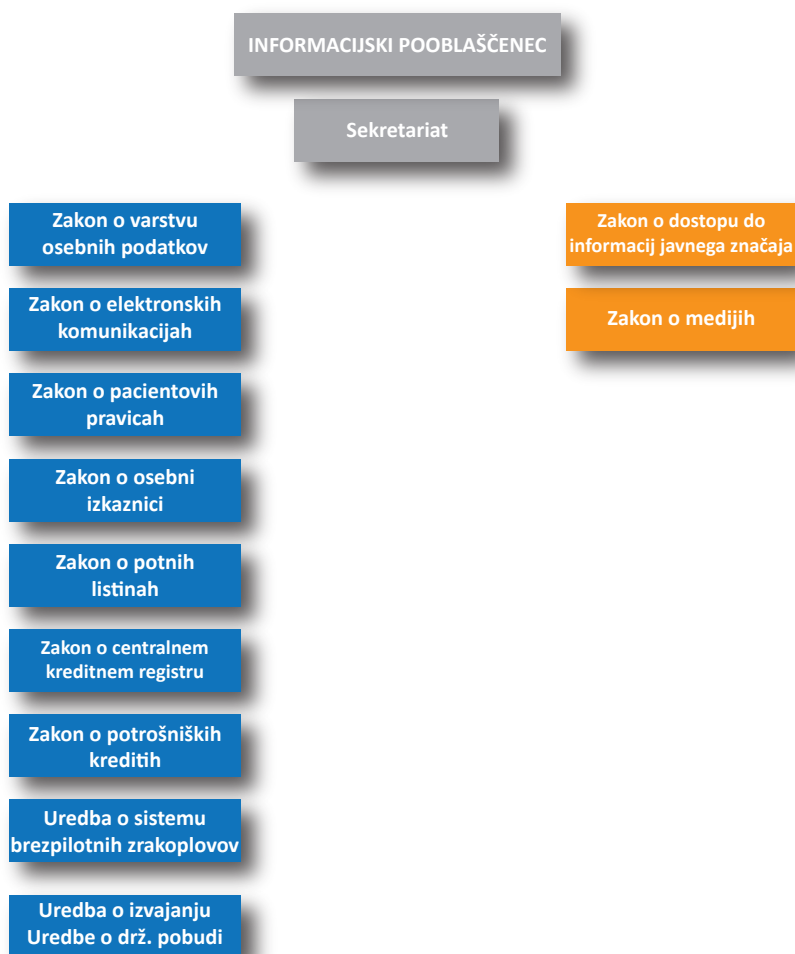
¹⁴ Uradni list RS, št. 25/2015, s spremembami; v nadaljevanju ZBan-2.

¹⁵ 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.

¹⁶ Uradni list EU, št. 65/1.

¹⁷ Uradni list Evropskih skupnosti, št. L239/19.

Slika 1: Pristojnosti Informacijskega pooblaščenca.



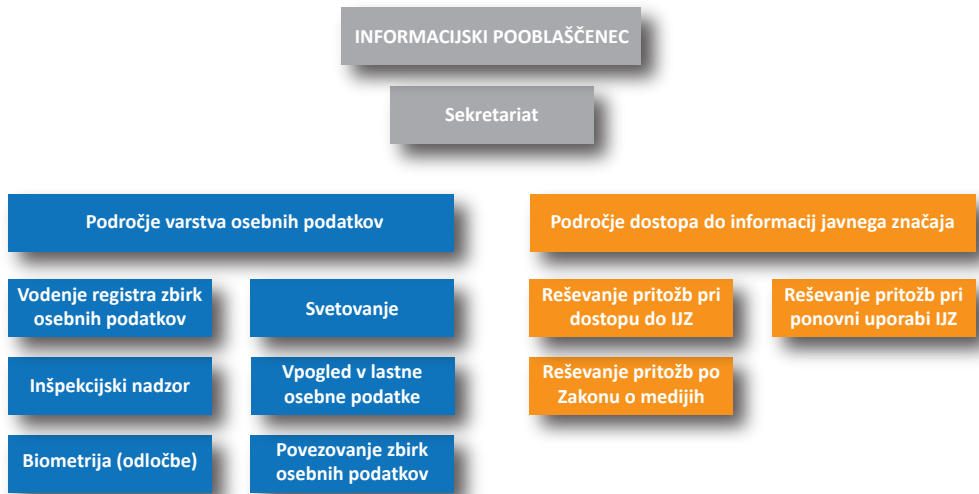
1.3. Organiziranost Informacijskega pooblaščenca

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

Informacijski pooblaščenec opravlja svoje naloge v naslednjih notranjih organizacijskih enotah:

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

Slika 2: Organigram Informacijskega pooblaščenca.



Na dan 31. 12. 2017 je imel Informacijski pooblaščenec 34 zaposlenih, od tega 32 za nedoločen in dva za določen čas (nadomeščanje zaradi daljše odsotnosti in pripravnik). V primerjavi z letom 2016 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,
- šest svetovalcev,
- štiri asistenti svetovalca,
- enajst državnih nadzornikov za varstvo osebnih podatkov,
- državni nadzornik za varstvo osebnih podatkov – informatik,
- dva raziskovalca,
- informatik – pripravnik,
- strokovna sodelavka za finančne in kadrovske zadeve,
- poslovna sekretarka,
- dokumentalistka.

Preglednica 1: Izobrazbena struktura zaposlenih pri Informacijskem pooblaščenču 31. 12. 2017.

	Višja strokovna šola	Visoka strokovna šola, univerzitetni program	Univerzitetna izobrazba	Magisterij	Doktorat	Skupaj
Pooblaščenka			1			1
Namestniki			3	1		4
Generalna sekretarka				1		1
Svetovalci			4	2		6
Asistenti svetovalca			4			4
Državni nadzorniki za varstvo osebnih podatkov			5	5	1	11

Državni nadzornik za varstvo osebnih podatkov – informatik				1		1
Raziskovalca		2				2
Informatik – pripravnik			1			1
Strokovna sodelavka za finančne in kadrovske zadeve	1					1
Poslovna sekretarka		1				1
Dokumentalistka	1					1
Skupaj	2	3	18	10	1	34

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. 2017 je bil **veljavni proračun Informacijskega pooblaščenca** na integralnih sredstvih **1.459.747,90 EUR** (leta 2014 1.247.110,10 EUR, leta 2015 1.243.661,35 EUR, leta 2016 1.335.457,02 EUR), od tega na postavki plače 1.306.000,00 EUR, na postavki materialni stroški 134.247,90 EUR in na postavki investicije 19.500,00 EUR. Evidentiranih odredb je bilo na dan 31. 12. 2017 1.454.573,77 EUR, od tega na postavki plače 1.303.250,66 EUR, na postavki materialni stroški 131.907,44 EUR in na postavki investicije 19.415,67 EUR.

Informacijski pooblaščenec je v letu 2017 razpolagal z namenskimi sredstvi v znesku 7.317,92 EUR in z donacijami za sodelovanje v projektih, ki jih je financirala Evropska unija, v višini 13.444,13 EUR (oziroma 8.212,61 EUR, kar je razlika zaradi dovoljene dejanske porabe na projektu Crisp). Poraba za namenska sredstva in donacije je znašala 8.126,28 EUR.

V proračun leta 2018 je Informacijski pooblaščenec prenesel skupno 7.321,05 EUR namenskih sredstev in sredstev donacij (7.317,92 EUR namenskih sredstev, 0,14 EUR donacije – mednarodna spletna stran in 2,99 EUR finančnih sredstev projekta Taiex). Na postavko Tekoča proračunska rezerva pri Ministrstvu za finance je bilo prenesenih 35.399,47 EUR z integralnih postavk.

Informacijski pooblaščenec je skrbno ter zelo restriktivno porabljal finančna sredstva na postavkah materialni stroški, investicije, znižal je stroške izdaje publikacij, študentskega dela in drugih storitev.

Preglednica 2: Proračun Informacijskega pooblaščenca 2017.

	Veljavni proračun v EUR	Evidentirane odredbe v EUR	Razpoložljiv proračun konec leta v EUR
Informacijski pooblaščenec	1.480.509,95	1.462.700,05	17.809,90
Podprogrami			
OPRAVLJANJE DEJAVNOSTI	1.459.747,90	1.454.573,77	5.174,13
Materialni stroški	134.247,90	131.907,44	2.340,46
Investicije	19.500,00	19.415,67	84,33
Plače	1.306.000,00	1.303.250,66	2.749,34

NAMENSKA SREDSTVA	7.317,92	0	7.317,92
Namenska sredstva – kupnine	7.317,92	0	7.317,92
DONACIJE	13.444,13	8.126,28	5.317,85
Mednarodna spletna stran	0,14	0	0,14
Projekt Taiex	2,99	0,00	2,99
Projekt Crisp	13.441,00	8.126,28	5.314,72

Za **materialne stroške** je bilo leta 2017 porabljenih **131.907,44 EUR**. Ti stroški vključujejo pisarniški material, 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 (namestitvev zaščitne mreže proti golobom, manjša popravila v poslovnih prostorih, vzdrževalna dela in zavarovanje), odmero nadomestila za uporabo stavbnega zemljišča, naročnino za IUS-INFO in prekrškovni portal, plačila sodb sodišč, kvote Javnemu jamstvenemu, preživninskemu in invalidskemu skladu. Na koncu leta je preostanek finančnih sredstev znašal 2.340,46 EUR. S postavke materialni stroški je Informacijski pooblaščenec v letu 2017 prerazporedil 12.144,47 EUR prostih pravic porabe v splošno proračunsko rezervacijo pri Ministrstvu za finance.

Za **investicije** je bilo do konca leta porabljenih **19.415,67 EUR**. Sredstva so bila porabljena za nakup strojne računalniške opreme (nadgradnja diskovnih pogonov, nakup računalnikov, monitorjev in skenerja ter telekomunikacijske opreme) in nakup nematerialnega premoženja (licenca Amebis Besana ter nadgradnja sistema CMS). Konec leta 2017 je na postavki investicije ostalo 84,33 EUR neporabljenih finančnih sredstev.

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 za pokojninsko in invalidsko zavarovanje, 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 **1.303.250,66 EUR**. Na koncu leta je ostanek finančnih sredstev znašal 2.749,34 EUR. S postavke plače je Informacijski pooblaščenec v letu 2017 prerazporedil 23.255,00 EUR prostih pravic porabe v splošno proračunsko rezervacijo pri Ministrstvu za finance.

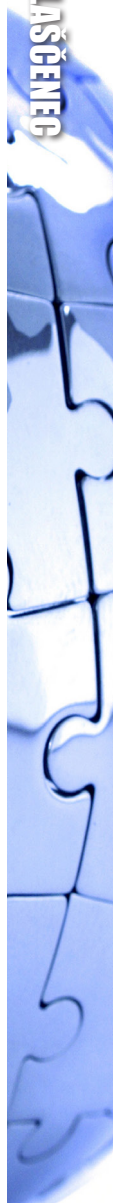
Namenska sredstva kupnine – v leto 2017 je bilo prenesenih **7.317,92 EUR** finančnih sredstev kupnin. V letu 2017 na postavki ni bilo niti prilivov niti porabe. Sredstva v višini 7.317,92 EUR so bila prenesena v leto 2018.

Mednarodna spletna stran info-commissioners.org – iz leta 2017 je bilo preneseno 0,14 EUR. Leta 2017 na tej postavki ni bilo porabe, sredstva višini 0,14 EUR so bila prenesena v leto 2018.

Projekt Taiex – iz leta 2016 je bilo v leto 2017 na to postavko preneseno 2,99 EUR. Leta 2017 na projektu ni bilo niti prilivov niti porabe, sredstva v višini 2,99 EUR so bila prenesena v leto 2018.

Projekt 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 financira Evropska komisija, 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 pooblaščenecu sodelujejo pri pripravi posameznih gradiv in analiz, izvajanju raziskav in drugih aktivnostih, napoteni so na sestanke, povezane 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 bo v 36 mesecih njegovega trajanja Informacijski pooblaščenec iz integralnih proračunskih sredstev zagotovil 24.890,00 EUR. Iz teh sredstev bodo pokriti stroški dela zaposlenih, stroški njihove napotitve na sestanke, 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. Dne 3. 6. 2014

je bilo s strani Evropske komisije na poseben račun, odprt pri Upravi za javna plačila, 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. Leta 2016 je bilo dne 20. 5. 2016 s strani Evropske komisije na poseben račun, odprt pri Upravi za javna plačila, 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, porabljenih je bilo 62.850,63 EUR. Leta 2017 je veljavni proračun znašal **13.441,00 EUR**, porabljenih je bilo 8.126,28 EUR (dovoljena je bila poraba samo 8.209,48 EUR, glede na prejeta sredstva v vseh letih). Sredstva so bila porabljena za pokrivanje stroškov zaposlenih ter za pokrivanje stroškov službene poti. Zaključno finančno poročilo je bilo oddano po koncu projekta, maja 2017, vendar je Evropska komisija od vseh sedmih partnerjev zahtevala dodatna pojasnila; Evropska komisija je finančno poročilo sprejela šele decembra 2017. Informacijski pooblaščenec je zadnje nakazilo sredstev v višini 29.520,86 prejel v začetku leta 2018.





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 Slovenije¹⁸. 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 značaja¹⁹. Dotlej so se posamezne določbe o javnosti informacij pojavljale le v nekaterih zakonih; celostno jih je uredil šele ZDIJZ. Tega je Državni zbor RS sprejel konec februarja 2003, veljati pa je začel 22. 3. 2003.

ZDIJZ sledi usmeritvam mednarodnih aktov in EU. Njegov namen je zagotoviti javnost in odprtost delovanja javne uprave ter vsakomur omogočiti dostop do javnih informacij, torej tistih, ki so povezane z delovnimi področji organov javne uprave. Zakon je uredil 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 sta se v pravni red Republike Slovenije prenesli dve direktivi 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 (ZDIJZ-A) narejen še korak naprej. Novela je namreč zožila možnost neupravičenega zapiranja dostopa do informacij in uvedla številne novosti, kot so ponovna uporaba informacij javnega značaja in pristojnosti upravne inšpekcije na področju izvajanja tega zakona. Najpomembnejša novost je bil zagotovo test javnega interesa. Z novelo je bila tudi poudarjena odprtost pri podatkih o porabi javnih sredstev in podatkih, povezanih z delovnim razmerjem ali opravljanjem javne funkcije. S tem se je Slovenija pridružila tistim demokratičnim državam, ki, kadar gre za javni interes, tudi izjeme obravnavajo s pridržkom.

Leta 2014 sta bili sprejeti dve noveli ZDIJZ (ZDIJZ-C²⁰ in ZDIJZ-D²¹). 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 AJPEŠ v šestih mesecih po uveljavitvi ZDIJZ-C vzpostavil spletni Register zavezancev za informacije javnega značaja, ki je javen, podatki v njem pa so dostopni brezplačno. Namen sprememb ZDIJZ je bil, da se poleg zagotavljanja javnosti in odprtosti delovanja javnega sektorja krepi 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 sta namreč povečali občutljivost javnosti za korupcijo, zlorabo oblasti in slabo upravljanje. K večji transparentnosti je prispevala tudi proaktivna objava informacij javnega značaja na spletnih straneh, ki jo zahteva novela ZDIJZ-C.

Dne 8. 5. 2016 je v uporabo stopila novela ZDIJZ-E²², 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 brezplačno uporablja v pridobitne ali druge namene, 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 Vlada RS sprejela novo Uredbo o posredovanju in ponovni uporabi informacij javnega značaja²³, s katero

¹⁸ Uradni list RS, št. 33/1991, s spremembami; v nadaljevanju Ustava RS.

¹⁹ Uradni list RS, št. 24/2003, s spremembami; v nadaljevanju ZDIJZ.

²⁰ Uradni list RS, št. 23/2014.

²¹ Uradni list RS, št. 50/2014 in 19/2015.

²² Uradni list RS, št. 102/2015.

²³ Uradni list RS, št. 24/2016.

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 jih je treba posredovati 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 posredovati prosilcu) drugače definiran; pri zavezancih iz druge skupine je ožji. Medtem ko za organe na splošno lahko rečemo, da so vsi dokumenti, zadeve, dosjeji, registri, evidence in dokumentarno gradivo, s katerim 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 poslovne subjekte pod prevladujočim vplivom oseb javnega prava velja ravno obraten miselni proces – informacije javnega značaja so le tisti dokumenti, zadeve, dosjeji, registri, evidence in 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 te 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 njihovo pridobitev ni treba izkazovati, dovolj sta radovednost ter želja po znanju in obveščeni. Vsak prosilec ima na zahtevo 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 za 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 informacije ni dobil 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 iz 5.a ali 6. člena ZDIJZ, to ni razlog, da bi zavezanec zavrnil dostop do celotnega dokumenta. Če je te informacije mogoče iz dokumenta izločiti, ne da bi to ogrozilo njihovo zaupnost, se jih prekrije, prosilcu pa se posreduje preostali del informacij javnega značaja. Zavezanec mora namreč v skladu z 19. členom Uredbe

o posredovanju in ponovni uporabi informacij javnega značaja²⁴ varovane podatke prekri in prisilcu 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 potrjeno ali elektronski podpis nista potrebna), zavezanec pa ga mora o zavrnitvi ali delni zavrnitvi 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 2017 je Informacijski pooblaščenec prejel 522 pritožb, od tega 314 zoper zavrnilne odločbe, 201 zoper molk prvostopenjskih organov in sedem zoper poslovne subjekte pod prevladujočim vplivom oseb javnega prava.

V okviru pritožbenih postopkov zoper odločbe, s katerimi so zavezanci zavrnili zahteve po dostopu ali ponovni uporabi informacij javnega značaja, je Informacijski pooblaščenec vodil sedem postopkov zoper poslovne subjekte pod prevladujočim vplivom države, občin ali drugih oseb javnega prava. Izdal je 316 odločb, v štirih primerih je pritožbo s sklepom zavrgel, dva prosilca pa sta svoji pritožbi umaknila. Pri reševanju pritožb je opravil 61 ogledov *in camera*, tj. ogledov brez prisotnosti stranke, ki zahteva dostop do informacije javnega značaja, na katerih je ugotavljal dejansko stanje dokumentov pri organu.

Informacijski pooblaščenec je v pritožbenih postopkih zaradi molka zavezanca 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 prejeli zavrnilno odločbo, pa so imeli možnost pritožbe Informacijskemu pooblaščenca. V 16 primerih je Informacijski pooblaščenec pritožbo s sklepom zavrgel, in sicer v 15 primerih zaradi preuranjenosti in v enem primeru zaradi pomanjkljive vloge. Osem posameznikov je pritožbe umaknilo, ker so zahtevano dokumentacijo prejeli, v dveh primerih je Informacijski pooblaščenec prosilcema pojasnil, da za reševanje njunih vlog ni pristojen, in jima svetoval, kako ravnati, v enem primeru je vlogo odstopil v reševanje pristojnemu organu, v enem primeru pa je podal tudi prijavo upravni inšpekciji zaradi kršitev določb ZDIJZ in ZUP.

Leta 2017 je Informacijski pooblaščenec prejel 324 pisnih prošenj za pomoč in različnih vprašanj posameznikov glede dostopa do informacij javnega značaja, v okviru dežurstev v času uradnih ur pa je prejel 729 klicev, ki so se nanašali na področje 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.

²⁴ Uradni list RS, št. 24/2016.

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

Pritožba zoper odločbo Informacijskega pooblaščenca ni dopustna, mogoče pa je sprožiti upravni spor. Leta 2017 je bilo zoper odločbe Informacijskega pooblaščenca na Upravnem sodišču vloženih 50 tožb, tj. zoper 15,8 % izdanih odločb. Delež je relativno majhen, kar kaže na uveljavitev transparentnosti in odprtosti javnega sektorja, pa tudi na sprejemanje odločb Informacijskega pooblaščenca s strani zavezancev in prosilcev.

Upravno sodišče je leta 2017 odločilo o 31 tožbah, ki so bile vložene zoper odločbe Informacijskega pooblaščenca, in:

- tožbo zavrnilo – 19,
- tožbi ugodilo, izpodbijano odločbo oziroma del odločbe odpravilo in zadevo vrnilo Informacijskemu pooblaščenca v ponovno odločanje – 10,
- tožbo v enem delu zavrglo, v enem delu pa ji ugodilo, odločbo Informacijskega pooblaščenca delno odpravilo in mu jo vrnilo v ponoven postopek – 1,
- postopek s sklepom ustavilo – 1.

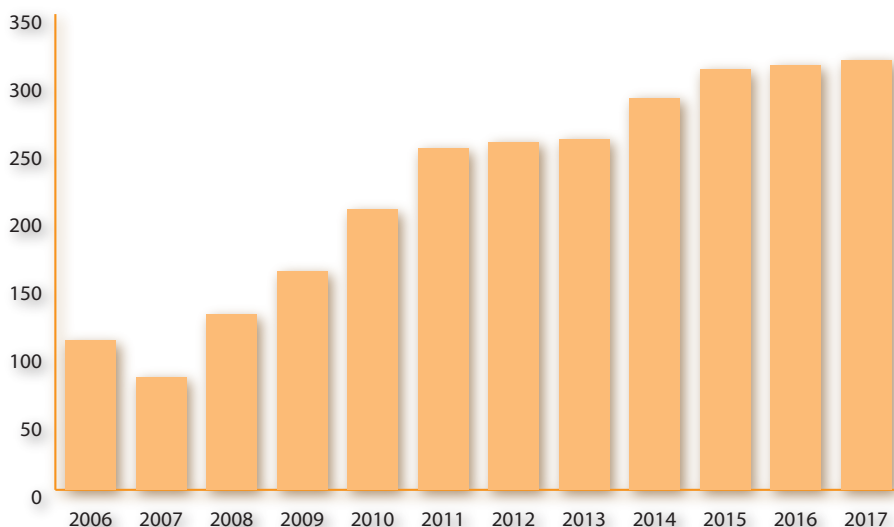
Leta 2017 Informacijski pooblaščenec ni vložil nobene revizije zoper sodbo Upravnega sodišča, je pa revizijo vložil en zavezanec. Do konca leta 2017 je Informacijski pooblaščenec prejel pet odločitev Vrhovnega sodišča v zvezi z revizijami zoper sodbe Upravnega sodišča. Vrhovno sodišče RS je:

- revizijo zavrnilo – 2,
- revizijo s sklepom zavrglo – 2,
- revizijski postopek do odločitve Sodišča Evropske unije o zastavljenem predhodnem vprašanju prekinilo – 1.

2.4. Statistika po posameznih področjih ZDIJZ

Število izdanih odločb na področju dostopa do informacij javnega značaja se je leta 2017 v primerjavi s preteklimi leti znova nekoliko povečalo: Informacijski pooblaščenec je izdal 316 odločb (leta 2016 jih je izdal 312), kar je največ doslej.

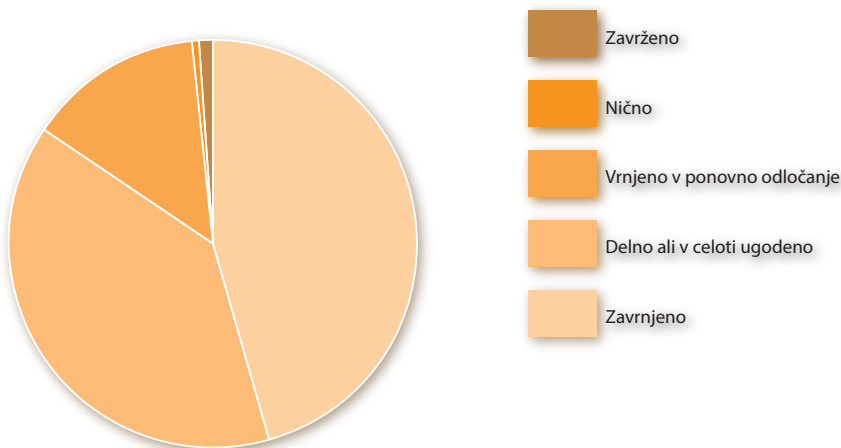
Slika 3: Število izdanih odločb na področju dostopa do informacij javnega značaja med letoma 2006 in 2017.



Informacijski pooblaščenec je v izdanih odločbah:

- pritožbo zavrnil – 144,
- pritožbi delno ali v celoti ugodil oziroma rešil zadevo v korist prosilca – 123,
- pritožbi ugodil in zadevo vrnil v ponovno odločanje prvostopenjskemu organu – 44,
- pritožbo zavrgel – 3,
- odločbo prvostopenjskega organa razglasil za nično – 2.

Slika 4: Odločitve Informacijskega pooblaščenca glede prejetih pritožb.

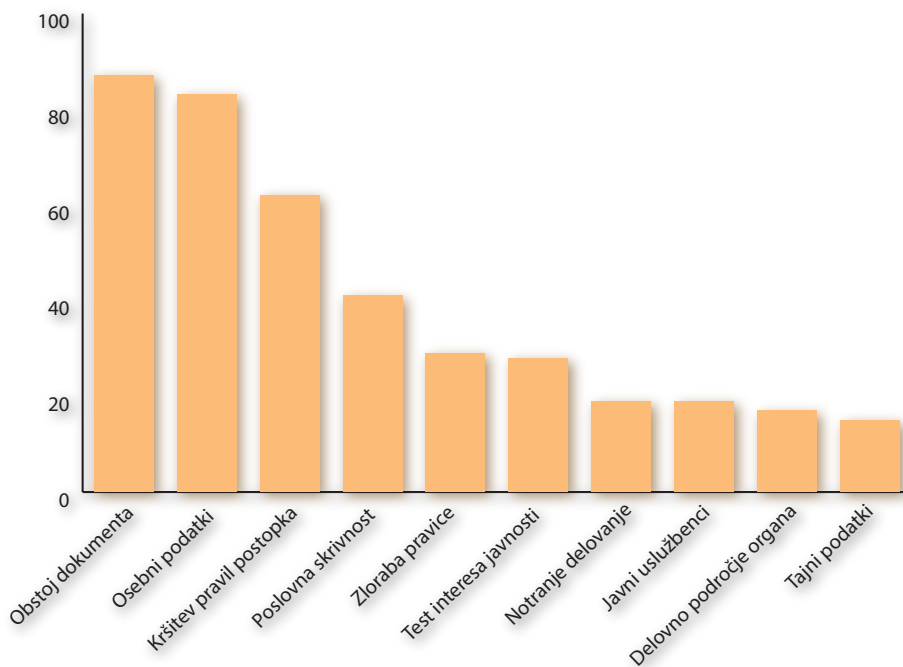


Informacijski pooblaščenec je v odločbah vsebinsko odločal oziroma presojal:

- ali zavezanec ima dokument oziroma informacijo javnega značaja, ki jo je zahteval prosilec – 87,
- ali zahtevani dokumenti vsebujejo osebne podatke, katerih razkritje bi pomenilo kršitev varstva osebnih podatkov v skladu z ZVOP-1 – 83,
- ali gre za kršitev pravil postopka – 62,
- ali prosilci zahtevajo informacije oziroma podatke, ki so v skladu z zakonom, ki ureja gospodarske družbe, opredeljeni kot poslovna skrivnost – 50,
- ali gre za zlorabo pravice po ZDIJZ – 29,
- ali je interes javnosti glede razkritja močnejši od javnega interesa ali interesa drugih oseb za omejitve dostopa do zahtevane informacije – 28,
- 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 – 19,
- ali se zahtevane informacije nanašajo na delo in osebne podatke javnih uslužbencev in funkcionarjev – 19,
- ali gre za delovno področje organa – 17,
- ali so zahtevane informacije podatki, ki so na podlagi zakona, ki ureja tajne podatke, opredeljeni kot tajni – 15,
- ali so zahtevane informacije podatki, katerih razkritje bi pomenilo kršitev zaupnosti davčnega postopka ali davčne tajnosti skladno z zakonom, ki ureja davčni postopek – 12,
- odločbe, izdane po sodbah Upravnega sodišča RS – 10,
- 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 – 9,
- ali zahtevani dokument izpolnjuje pogoje za obstoj informacije javnega značaja v skladu s prvim odstavkom 4. člena ZDIJZ – 9,
- ali gre za podatek, glede katerega zakon določa varovanje tajnosti vira – 9,
- 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 – 8,
- ali je zahtevana informacija zavarovana skladno z zakonom, ki ureja avtorsko pravico – 7,
- ali so zahtevani dokumenti iz postopkov javnega naročanja – 7,
- ali je organ pravilno zaračunal stroške posredovanja informacij javnega značaja – 6,
- ali gre za kršitev materialnega prava – 5,
- izdaja odločbe v postopku, ko je prosilec zahteval dokument, povezan s pravom EU – 5,

- ali so zahtevane informacije podatki, ki so bili pridobljeni ali sestavljeni zaradi pravnega, nepravdnega ali drugega sodnega postopka, in bi njihovo razkritje škodovalo njegovi izvedbi – 3,
- 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 – 3,
- ali gre za ponovno uporabo informacije javnega značaja – 3,
- ali so zahtevane informacije podatki, ki so bili pridobljeni ali sestavljeni zaradi nadzornega postopka, ki je v teku, ali zaključenega nadzornega postopka, če bi razkritje zahtevane informacije povzročilo škodo drugi osebi ali če bi to resno ogrozilo izvajanje drugih zakonskih nalog nadzorne institucije, ki je vodila postopek – 3,
- ali gre za okoljske podatke – 2,
- ali so zahtevane informacije podatki, ki so bili pridobljeni ali sestavljeni zaradi upravnega postopka, in bi njihovo razkritje škodovalo njegovi izvedbi – 2,
- ali sploh gre za pravico po ZDIJZ ali za pravico na kakšni drugi pravni podlagi – 2,
- ali gre za proaktivno objavo informacij – 1,
- ali so zahtevane informacije podatki, za katere drug zakon samostojno določa izjemo od prostega dostopa – 1,
- ali so podatki označeni s stopnjo tajnosti v nasprotju za zakonom, ki ureja tajne podatke – 1.

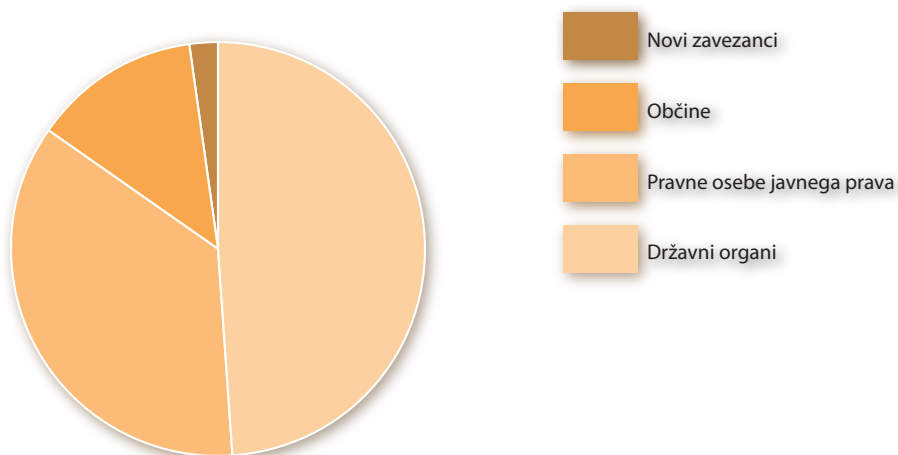
Slika 5: Odločbe na področju ZDIJZ glede na različne izjeme. (Opomba: ena odločba se lahko nanaša na več izjem.)



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

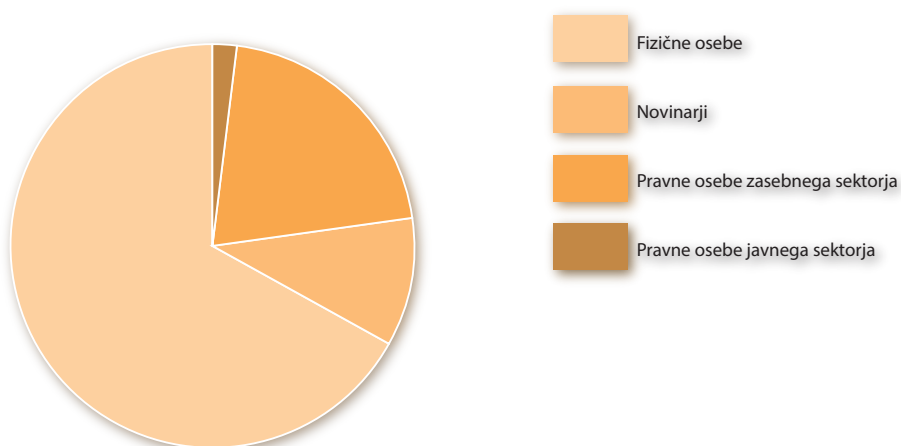
- državni organi – 155, od tega ministrstva in organi v sestavi ter upravne enote 114, sodišča, vrhovno državno tožilstvo, državno pravobranilstvo pa 30,
- javni skladi, zavodi, agencije, izvajalci javnih služb, nosilci javnih pooblastil in druge pravne osebe javnega prava – 113,
- občine – 41,
- poslovni subjekti pod prevladujočim vplivom države, občin ali drugih oseb javnega prava – 7.

Slika 6: Pritožbe prosilcev glede na zavezanca.



V 211 primerih so bili prosilci fizične osebe, v 65 primerih so se pritožile pravne osebe zasebnega sektorja, novinarji so se pritožili 33-krat, pravne osebe javnega sektorja pa sedemkrat.

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



2.5. Storjeni prekrški po ZDIJZ, ZInfP in ZMed

Leta 2017 je Informacijski pooblaščenec začel en postopek zaradi prekrška po drugem odstavku 39. člena ZDIJZ, ker je organ po prejemu zahteve za dostop do informacij javnega značaja trajno izbrisal zahtevane dokumente z namenom, da informacija ne bi bila dostopna javnosti. Postopek še ni zaključen.

2.6. Predstavitev najodmevnejših in precedenčnih primerov po področjih

V nadaljevanju je predstavljenih nekaj najzahtevnejših in najzanimivejših odločb iz leta 2017. Razvrščene so po področjih.



2.6.1 Ali gre za delovno področje organa, poslovna skrivnost

Z odločbo št. 090-153/2017/10 z dne 7. 9. 2017 je Informacijski pooblaščenec Javnemu podjetju Vodovod - Kanalizacija, d. o. o., (organ) naložil, da prosilcu omogoči vpogled v določene dele pogodb o poslovnem sodelovanju (zahtevane pogodbe), ki jih je organ sklenil s konkretnimi upravniki večstanovanjskih stavb (stranski udeleženci).

Organ je v izpodbijani odločbi zatrjeval, da predmetne pogodbe niso povezane z javnopravnim delovanjem in da so poslovna skrivnost. Informacijski pooblaščenec je v pritožbenem postopku ugotovil, da ima organ z etažnimi lastniki sklenjene dogovore o dobavi pitne vode, ki jo organ izvaja kot obvezno gospodarsko javno službo. Stranski udeleženci so, kot upravniki večstanovanjskih stavb, z organom sklenili zahtevane pogodbe, s katerimi je bilo dogovorjeno, da bodo račune za izvajanje storitev te javne službe organu v celoti poravnali stranski udeleženci, ki to obveznost prevzemajo kot poroki in plačniki. Z zahtevanimi pogodbami je bilo dogovorjeno tudi plačilo, ki za prevzem pogodbeno dogovorjenih obveznosti in rizika neplačevanja s strani etažnih lastnikov oziroma neizterjanega dolga pripada stranskim udeležencem. V skladu z ustaljeno sodno prakso so informacije javnega značaja vse informacije, ki so kakor koli povezane z izvajanjem dejavnosti javne službe oziroma kažejo na dejstvo oziroma okoliščino, ki vpliva ali bi lahko vplivala na izvrševanje javnih nalog. Organ z zahtevanimi pogodbami izvajanja javne službe sicer ni prenesel na tretjo osebo, je pa s temi pogodbami določene naloge v zvezi s plačilom za storitve javne službe prenesel na stranske udeležence, pri čemer je na podlagi z zahtevanimi pogodbami dogovorjenega načina plačila mogoče zaključiti, da so finančna sredstva, zaračunana končnim uporabnikom iz naslova izvajanja javne službe, razporejena drugače, kot bi bila, če zahtevane pogodbe ne bi bile sklenjene. Del sredstev namreč namesto na organ, tj. na dejanskega izvajalca javne službe, odpade na stranske udeležence v zameno za prevzem vseh pogodbeno dogovorjenih obveznosti. Zahtevane pogodbe imajo torej finančne posledice tudi na področju izvajanja javne službe organa, zaradi česar so povezane z izvajanjem javnopravnih nalog organa (tj. javne službe). Navedeno pomeni, da zahtevane pogodbe izvirajo iz delovnega področja organa in posledično predstavljajo informacije javnega značaja po prvem odstavku 4. člena ZDIJZ.

Informacijski pooblaščenec je v nadaljevanju presojal, ali zahtevane pogodbe vsebujejo podatke, ki so poslovna skrivnost (2. točka prvega odstavka 6. člena ZDIJZ). V zahtevanih pogodbah so bila kot plačilo za prevzem obveznosti dogovorjena (tudi) sredstva, ki bi jih organ pridobil za izvajanje gospodarske javne službe, ta sredstva pa nedvomno predstavljajo javna sredstva, kot so opredeljena v Zakonu o računskem sodišču.²⁵ Pojem javnih sredstev namreč ne zajema zgolj proračunskih sredstev, temveč tudi sredstva, ki jih izvajalec javne službe za izvajanje le-te pridobi iz drugih virov (npr. od končnih uporabnikov). Organ je torej v zvezi z izvajanjem obravnavane javne službe uporabnik javnih sredstev, posledično pa podatki o porabi teh sredstev (npr. plačilo stranskim udeležencem) predstavljajo podatke o porabi javnih sredstev. Ti podatki so javni na podlagi tretjega odstavka 6. člena ZDIJZ, ki javnosti omogoča seznanitev z načinom razpolaganja z javnimi sredstvi. Zato je v konkretnem primeru treba razkriti določbe zahtevanih pogodb, ki opredeljujejo predmet pogodbe ter obračun in plačilo storitev iz pogodbe, ter tudi podatke o pogodbenih strankah. Teh podatkov po naravi stvari ni mogoče določiti za poslovno skrivnost, ker gre za podatke, ki so javni že na podlagi zakona (tretji odstavek 39. člena Zakona o gospodarskih družbah)²⁶ in jih je organ zato dolžan posredovati prosilcu. V preostalem delu zahtevane pogodbe ne vsebujejo podatkov o porabi javnih sredstev in so varovane kot poslovna skrivnost, zato se v tem delu pritožba prosilca zavrne.

2.6.2. Ali gre za zlorabo pravice?

Informacijski pooblaščenec je z odločbo 090-175/2017 z dne 8. 11. 2017 potrdil odločbo, s katero je organ zavrnil zahtevo, ker so prosilci zlorabili pravico dostopa do informacij javnega značaja.

Prosilci so v elektronski obliki zahtevali dostop do tožb, odgovorov na tožbe, pripravljalnih vlog in ostalih vlog strank ter sklepov, sodb in ostalih odločb enega izmed oddelkov organa v zadevah za določeno preteklo obdobje in tudi v bodočih zadevah. Informacijski pooblaščenec je v pritožbenem postopku presojal, ali je organ ugotovil vsa dejstva, ki so potrebna pri presoji, ali bi bilo delo organa resno ohromljeno zaradi upravnega bremena, ki bi bilo posledica obravnave navedene zahteve. Organ je ugotovil, da se zahteva nanaša na 792 sodnih spisov, kar je pomenilo 10.407 strani. Nato

²⁵ Uradni list RS, št. 11/2001, s spremembami in dopolnitvami; v nadaljevanju ZRacS-1.

²⁶ Uradni list RS, št. 65/2009 – uradno prečiščeno besedilo, s spremembami; v nadaljevanju ZGD-1.

je preučil, kakšno delo bi bilo dejansko potrebno za zagotovitev dostopa do teh dokumentov. V konkretnem primeru je namreč problematična dolgotrajnost celotnega postopka identifikacije dokumentov, na katere se zahteva nanaša, in njihova obdelava v skladu z ZDIJZ (zlasti izvedba delnega dostopa, ker zahtevani dokumenti niso oblikovani kot tipski obrazci, na katerih bi bilo mogoče izvesti delni dostop po nekem ključu; ker gre za kompleksna, večinoma pravna, pisanja, katerih vsebina se razlikuje, zaradi česar je treba presojati vsebino vsakega dokumenta posebej; ker zaradi nepravilno izvedenega delnega dostopa lahko pride do neupravičenega razkrivanja podatkov, ki niso javni, kar lahko pripelje do posega v pravice tretjih oseb in do odškodninske odgovornosti organa). Organ je v preizkus zajel različne vrste dokumentov, pri čemer je ugotovil, da je v povprečju potrebna 1 minuta efektivnega dela za 1 stran zahtevane dokumentacije. Temu je treba dodati še čas, ki je težje vnaprej določljiv in se nanaša na ostale potrebne dejavnosti, ki v preizkusu, ki ga je izvedel organ, niso bile upoštevane (čas, potreben za prevoz na sedež organa, za razdelitev spisov med sodno osebje, za identifikacijo vlog in pregled že objavljenih sodnih odločb, ki niso predmet zahteve, za shranjevanje na CD, za vključitev stranskih udeležencev). Na podlagi pojasnil organa o tem, koliko oseb bi lahko sodelovalo pri pripravi zahtevane dokumentacije, je mogoče objektivno predvideti, da bi vsebinska obravnava zahteve prosilcev glede na naravo vsebovanih informacij, ki terja temeljitost, delo organa ovirala do te mere, da svojih nalog v sodnih postopkih ne bi mogel več izvajati tako, da bi ustrezno zavaroval pravice strank v teh postopkih. Grožnja, da bo delo organa resno ohromljeno zaradi upravnega bremena, ki bi bilo posledica obravnave zahteve po ZDIJZ, je torej v konkretnem primeru resnična.

Posredovanje informacij javnega značaja je ena izmed zakonsko določenih nalog organa, zato je organ dolžan zagotoviti ustrezna sredstva in kader, ki bo takšne zahteve reševal. Vendar pa ima tudi ta dolžnost meje. To izhaja iz določb Zakona o splošnem upravnem postopku²⁷, iz katerih med drugim izhaja, da morajo stranke pošteno uporabljati svoje pravice. Glede na količino dela, ki so jo prosilci v konkretnem primeru naložili organu, je mogoče njihovo zahtevo opisati kot ravnanje, ki ne predstavlja poštene uporabe pravic.

Iz ZUP in ZDIJZ izhaja dolžnost organa, da preden zahtevo zavrne zaradi zlorabe pravice, preuči tudi vse druge možnosti. V zvezi s tem je organ ugotovil, da težje upravnega bremena, ki jo prinaša obravnava zahteve v konkretnem primeru, ni mogoče zmanjšati niti s podaljšanjem roka za posredovanje zahtevane dokumentacije (24. člen ZDIJZ), niti z dodatnimi pojasnili prosilcem, niti z odločanjem z delnimi odločbami.

Informacijski pooblaščenec je na koncu presojal, ali je odvzem pravice iz drugega odstavka 39. člena Ustave RS v skladu z načelom sorazmernosti, in sicer na način, kot izhaja iz prakse Ustavnega sodišča RS. Zaradi uresničevanja pravice iz drugega odstavka 39. člena Ustave RS bi v konkretnem primeru prišlo do posega v pravico do sodnega varstva iz 23. člena Ustave RS, na podlagi katerega je organ dolžan zagotavljati sojenje v razumnem roku. Informacijski pooblaščenec je ocenil, da je v konkretnem primeru zavrnitev zahteve prosilcev iz razloga, da gre za zlorabo pravice, nujen in primeren ukrep za doseg ustavno varovanih ciljev. Poleg tega koristi, ki jih prinaša nemoten potek sodnih postopkov, ki tečejo pri organu in s katerimi se zagotavlja varstvo pravic strank v teh postopkih, odtehta težo posega v pravico prosilcev do dostopa do informacij javnega značaja. Odvzem pravice prosilcev v konkretnem primeru torej prestane vse tri vidike t. i. strogega testa sorazmernosti, kar pomeni, da je ustavno dopusten.

Informacijski pooblaščenec je zaključil, da so prosilci v konkretnem primeru prekoračili pravno mejo pravice dostopa do informacij javnega značaja, s čimer so izvršili ravnanje, ki predstavlja zlorabo pravice, zato je odločitev organa, da se zahteva zavrne na podlagi petega odstavka 5. člena ZDIJZ, pravilna.

2.6.3. Avtorsko delo

Z odločbo št. 090-131/2017 z dne 26. 7. 2017 je Informacijski pooblaščenec Slovenskemu inštitutu za standardizacijo (organ) naložil, da prosilcu v elektronski obliki posreduje angleški original in slovenski prevod standarda ISO 22716:2007 (zahtevana standarda).

Organ je v izpodbijani odločbi navedel, da zahtevana standarda ne sodita v delovno področje, kot je opredeljeno v 4. členu ZDIJZ. Informacijski pooblaščenec je v pritožbenem postopku pojasnil, da se delovno področje organa po ZDIJZ razteza na vsak podatek, ki je nastal v zvezi z izvajanjem

²⁷ Uradni list RS, št. 24/2006 – uradno prečiščeno besedilo, s spremembami; v nadaljevanju ZUP.

javnopravnih nalog oziroma v zvezi z dejavnostjo organa. Organ je slovenski nacionalni organ za standarde, ustanovljen za doseganje ciljev iz 3. člena Zakona o standardizaciji.²⁸ Naloge za doseg teh ciljev (med katere spada tudi izdajanje standardov) lahko opravlja izključno organ, pri čemer ima pravico v pečatu, stampilki ali na dokumentih uporabljati grb Republike Slovenije, njihovo izvajanje pa se financira iz državnega proračuna. Zahtevana standarda je organ prejel oziroma pripravil v okviru opravljanja svojih zakonsko določenih nalog po ZSt-1, zato sodita v delovno področja organa in sta posledično informacija javnega značaja.

Organ je zatrijeval, da zahtevana standarda predstavljata avtorsko delo, zaradi česar dostop ni mogoč. Informacijski pooblaščenec je poudaril, da se v primeru, če zahtevana informacija predstavlja avtorsko delo, lahko zavrne le določen način seznanitve z njo (elektronska kopija, fotokopija), ne pa tudi sam dostop do informacije (npr. vpogled). Zahtevana standarda sta avtorsko delo, kot ga določa Zakon o avtorski in sorodnih pravicah²⁹, vendar predstavljata uradno besedilo, ki ne uživa avtorskopravnega varstva (9. člen ZASP). Za takšno opredelitev je bistveno, da se na zahtevana standarda sklicuje Uredba (ES) št. 1223/2009 o kozmetičnih izdelkih³⁰, ki se neposredno uporablja v Republiki Sloveniji in ki od proizvajalcev kozmetičnih izdelkov, uvoznikov in distributerjev zahteva, da so vsi izdelki na trgu EU izdelani po načelu dobre proizvodne prakse. Neizvajanje teh obveznosti predstavlja prekršek po Uredbi o izvajanju Uredbe (ES) o kozmetičnih izdelkih³¹. Proizvodnja je skladna z dobro proizvodno prakso, kadar je skladna z ustreznimi usklajenimi standardi, katerih sklicevanja so objavljena v Uradnem listu Evropske unije. V Uradnem listu Evropske unije je bilo objavljeno Sporočilo Komisije v okviru izvajanja Uredbe št. 1223/2009³², v katerem sta bila navedena tudi naslov in sklic na angleški original standarda, ki ga zahteva prosilec. Iz ZASP izhaja, da se za uradno besedilo šteje le dokument, ki predstavlja zavezujoč predpis v smislu, da je njegova raba obvezna. Zadošča, da se organ z oblastvenimi upravičenji nanj sklicuje kot na merodajnega in tako vpliva na pravni položaj posameznika. V trenutku, ko dokument v veljavno zakonodajo vključi organ z oblastvenimi upravičenji, postane ta dokument uradno besedilo in njegovo reproduciranje ne sme biti omejeno. Bistvo takšne ureditve je čim večje razširjanje in objavljanje uradnih besedil, ki uravnavajo družbo, zaradi javnega interesa po seznanjenosti z njimi. V takem primeru se mora avtorjev interes umakniti javnemu, omejevanje uporabe predpisov z avtorskim pravom pa bi bilo v neposrednem nasprotju z njihovim poslanstvom in smislom. V konkretnem primeru je s prej navedenima uredbama določena obveznost skladnosti proizvodnje tudi z zahtevanima standardoma. Poznavanje teh standardov namreč vpliva na pravni položaj posameznika – proizvajalca, saj je proizvodnja izdelka, ki ni skladen z njima, nedopustna in pomeni prekršek. Na podlagi navedenega je Informacijski pooblaščenec zaključil, da zahtevana standarda predstavljata uradno besedilo in zato ne uživata avtorskopravnega varstva, kar pomeni, da ju je organ na podlagi ZDIJZ dolžan posredovati prosilcu v obliki elektronske kopije oziroma fotokopije.

2.6.4. Dokument v izdelavi, tajni podatki, notranje delovanje

Informacijski pooblaščenec je z odločbo št. 090-258/2017 z dne 13. 12. 2017 Kabinetu predsednika vlade RS (organ) naložil, da umakne stopnjo tajnosti z osnutka Zakona o spremembah in dopolnitvah Zakona o Slovenski obveščevalno-varnostni agenciji (zahtevani osnutek) in ta dokument v elektronski obliki posreduje prosilcu.

Organ se je v izpodbijani odločbi skliceval na izjeme iz 1. (tajni podatki), 9. (dokument v izdelavi) in 11. (notranje delovanje organa) točke prvega odstavka 6. člena ZDIJZ. Informacijski pooblaščenec je v pritožbenem postopku ugotovil, da zahtevani osnutek izpolnjuje formalni kriterij po Zakonu o tajnih podatkih³³, ne pa tudi materialnega. Za opredelitev materialnega kriterija je ključna vsebina dokumenta. Zahtevani osnutek predstavlja pripravo besedila zakona in se zato ne nanaša na interesna področja države, ki jih je ZTP v 5. členu opredelil kot posebej občutljiva oziroma takega pomena, da jih je ob izpolnjevanju nadaljnjih pogojev mogoče varovati s stopnjo tajnosti. Tudi originator tega osnutka v oceni škodljivih posledic ni jasno navedel, katerim konkretnim interesom države Republike Slovenije bi škodovalo razkritje informacij iz zahtevanega osnutka.

²⁸ Uradni list RS, št. 59/1999; v nadaljevanju ZSt-1.

²⁹ Uradni list RS, št. 16/2007 – uradno prečiščeno besedilo, s spremembami; v nadaljevanju ZASP.

³⁰ Uredba (ES) št. 1223/2009 Evropskega parlamenta in Sveta z dne 30. november 2009 o kozmetičnih izdelkih, UL L 342/59, 22. 12. 2009, v nadaljevanju Uredba št. 1223/2009.

³¹ Uradni list RS, št. 61/2013.

³² Sporočilo Komisije v okviru izvajanja Uredbe (ES) št. 1223/2009 Evropskega parlamenta in Sveta o kozmetičnih izdelkih (Objava naslovov in sklicev harmoniziranih standardov), 2011/C 123/04, 21. 4. 2011.

³³ Uradni list RS, št. 50/2006 – uradno prečiščeno besedilo, s spremembami; v nadaljevanju ZTP.

V oceni škodljivih posledic se je zgolj na splošno skliceval na zakonsko določbo, konkretno pa se ni opredelil niti do nastanka škode, ki naj bi z razkritjem nastala varnosti in interesom RS. Tako splošna in široka opredelitev dokumenta za tajnega po ZTP ne izpolnjuje pogojev, ki jih zahteva materialni kriterij tajnega podatka po ZTP. Ker morata biti za opredelitev tajnega podatka hkrati izpolnjena oba kriterija, je Informacijski pooblaščenec zaključil, da v konkretnem primeru ni podana izjema tajnih podatkov, in originatorju naložil, da z zahtevanega osnutka umakne stopnjo tajnosti »interno«.

Za obstoj izjeme notranjega delovanja organa morata biti kumulativno izpolnjena dva pogoja: podatek mora izhajati iz dokumenta, ki je bil sestavljen v zvezi z notranjim delovanjem oziroma dejavnostjo organa, razkritje takšnega podatka pa bi povzročilo motnje pri delovanju oziroma dejavnosti organa. Informacijski pooblaščenec je ugotovil, da gre v obravnavanem primeru za pripravo predpisa, ki vselej vpliva na življenje, pravice in obveznosti vseh državljanov. Priprava zakonskega besedila že po vsebini in namenu pomeni urejanje delovanja navzven in ne navznoter. Priprava predpisov predstavlja proces pravnega urejanja družbeno najpomembnejših vprašanj s strani organov javnih oblasti, zato je preglednost postopka in možnost sodelovanja stroke in civilne družbe demokratični standard, ki je v sodobnih demokratičnih državah nujen. Upoštevanje navedeno pri pripravi predpisa, ki nedvomno učinkuje navzven, ni mogoče govoriti, da gre za dokument v zvezi z notranjim delovanjem organa. Že prvi pogoj za obstoj izjeme notranjega delovanja organa torej ni izpolnjen, zaradi česar ta izjema ni podana.

Informacijski pooblaščenec je nadalje ugotavljal, ali gre za izjemo dokumenta v izdelavi, za opredelitev katere morajo biti kumulativno izpolnjeni trije pogoji: dokument mora biti še v postopku izdelave in predmet posvetovanja, razkritje dokumenta pa bi povzročilo napačno razumevanje njegove vsebine. Skladno z Uredbo se šteje, da je dokument v postopku izdelave, če ga še ni podpisala in odposlala ali kako drugače zaključila uradna oseba organa, ki je z veljavnimi predpisi pooblaščenca za odločanje. Zahtevani osnutek je nastal v postopku sprejemanja novele zakona, in sicer v začetni fazi postopka sprejemanja predloga zakona, saj gre za osnutek delovnega gradiva zakona. Med zakonodajnimi postopki že zaradi narave teh postopkov nastajajo dokumenti, ki sami po sebi ne predstavljajo končnega izdelka določene faze postopka (bodisi predpisa bodisi predloga predpisa), temveč zgolj verzije (različice) le-tega. Vendar pa to ne pomeni, da je konkretni dokument (tudi določena verzija delovnega gradiva zakona) še vedno v postopku izdelave. Informacijski pooblaščenec je ugotovil, da je zahtevani osnutek zaključen, saj ga je podpisala odgovorna oseba organa, obenem pa je bil dokument tudi posredovan izven organa na Ministrstvo za pravosodje. V konkretnem primeru tako nista izpolnjena ne prvi ne drugi pogoj za obstoj predmetne izjeme. Zahtevani osnutek pa ne bi prestal niti škodnega testa (tretjega pogoja), saj razkritje takšnega dokumenta ne more povzročiti napačnega razumevanja njegove vsebine. Povsem jasno je namreč, da gre za osnutek delovnega gradiva, ki ni pravno zavezujoč dokument. Nestrinjanja javnosti s predlagano rešitvijo ne moremo enačiti z napačnim razumevanjem same vsebine osnutka delovnega gradiva. Smisel transparentnosti postopka sprejemanja zakonov je namreč prav v tem, da se širša strokovna in nestrokovna javnost, torej vse zainteresirane skupine, vključi v postopek sprejemanja zakona ter izrazi svoje mnenje in stališče o predlaganem predpisu. Informacijski pooblaščenec je zaključil, da v konkretnem primeru ni podana izjema dokumenta v izdelavi, ker ni izpolnjen nobeden izmed treh predpisanih pogojev.

2.6.5. Javna naročila, poslovna skrivnost

Ministrstvo za notranje zadeve (organ) je prosilcu v celoti odobrilo dostop do ponudbenih predračunov, predloženih na povabilo k oddaji ponudbe glede dobave sanitarno-potrošnega materiala za potrebe organa (zahtevani predračuni). Informacijski pooblaščenec je na podlagi pritožbe stranskega udeleženca z odločbo št. 090-255/2017 z dne 21. 12. 2017 delno odpravil izpodbijano odločbo in organu naložil, da prosilcu v celoti posreduje ponudbeni predračun, ki je sestavni del pogodbe o dobavi blaga, pri pogodbenem predračunu, ki ni bil sestavni del pogodbe, pa je organ dolžan prekriti podatke o proizvajalcih.

Sporno vprašanje v pritožbenem postopku je bilo, ali podatki o proizvajalcu artiklov v zahtevanih predračunih predstavljajo poslovno skrivnost stranskega udeleženca (2. točka prvega odstavka 6. člena ZDIJZ). Informacijski pooblaščenec je ugotovil, da ti podatki izpolnjujejo pogoje za opredelitev poslovne skrivnosti po subjektivnem kriteriju. Organ je javnost teh podatkov utemeljeval z določbami Zakona o javnem naročanju³⁴, vendar te v konkretnem primeru ne

³⁴ Uradni list RS, št. 91/2015; v nadaljevanju ZJN-3.

predstavljajo ustrezne pravne podlage. Zahtevana predračuna sta bila namreč pridobljena v postopku naročila male vrednosti, t. i. evidenčnega naročila, za katero se uporabljajo zgolj določene določbe ZJN-3, med katerimi ni člena, ki ureja javnost podatkov. Je pa v konkretnem primeru treba upoštevati, da sta bila zahtevana predračuna pridobljena z namenom sukcesivne dobave sanitarno-potrošnega materiala za potrebe organa, kar pomeni porabo javnih sredstev. Informacijski pooblaščenec je ugotovil, da je bila na podlagi enega izmed zahtevanih predračunov sklenjena pogodba, po kateri se izvaja dobava blaga s strani stranskega udeleženca in se torej porabljajo javna sredstva, pri čemer je predračun sestavni del te pogodbe. To pomeni, da navedeni ponudbeni predračun skupaj z drugimi podatki (količina, naziv artikla ...) izkazuje informacije o predmetu naročila, kar pomeni, da gre za podatke o porabi javnih sredstev. Gre za podatke, ki so bistveni za ugotavljanje ustreznosti oziroma kakovosti kupljenega izdelka. Šele s podatkom o »proizvajalcu« kupljenega blaga lahko javnost dejansko dobi informacijo o tem, kakšno blago in za kakšno ceno je organ kupil z javnimi sredstvi. Le če se javnost seznanj s to informacijo, lahko preverja, ali je organ javna sredstva porabil smotrno. Na ta način pride do izraza nadzorna funkcija pravice dostopa do informacij javnega značaja, ki preprečuje slabo upravljanje z javnimi sredstvi. Navedenega se mora zavedati tudi stranski udeleženec. Ob vstopu v poslovno razmerje s proračunskim uporabnikom je njegova svoboda pri določitvi podatkov za poslovno skrivnost omejena prav zaradi zahteve po transparentnem delovanju, zlasti pri porabi javnih sredstev, ko se troši denar davkoplačevalcev (1. alineja tretjega odstavka 6. člena ZDIJZ). To pomeni, da podatki o proizvajalcih na tem predračunu predstavljajo prosto dostopno informacijo javnega značaja, zaradi česar izjema poslovne skrivnosti ni podana, organ pa jih je dolžan posredovati prosilcu. Glede podatkov o proizvajalcih blaga v drugem ponudbenem predračunu, ki ni bil sestavni del nobene pogodbe, izjema poslovne skrivnosti ni presežena, zato se prosilcu v tem delu dostop zavrne.

2.6.6. Osební podatki, javni uslužbenci, funkcionarji

Z odločbo št. 090-117/2017 z dne 27. 6. 2017 je Informacijski pooblaščenec Ministrstvu za zunanje zadeve (organ) naložil, da prosilci posreduje skupne utemeljitve ocen, ki jih vsebujejo ocenjevalni listi za konkretne javne uslužbence (zahtevane skupne utemeljitve ocen).

Organ je v izpodbijani odločbi zatrjeval, da gre za izjemo po 3. točki prvega odstavka 6. člena ZDIJZ (varovani osebni podatki). Informacijski pooblaščenec je ob vpogledu v zahtevane skupne utemeljitve ocen sicer ugotovil, da vsebujejo osebne podatke, in sicer le na kratko povzete in zelo splošne podatke o opisu delovnih nalog javnih uslužbencev, ki so v večini primerov skoraj identične in ne vsebujejo podatkov, ki bi razkrivali kakršne koli osebne lastnosti katerega izmed navedenih javnih uslužbencev. V skladu s tretjim odstavkom 6. člena ZDIJZ pa je te podatke dopustno razkriti, saj gre za podatke, povezane z delom javnih uslužbencev. V predmetni zadevi dejansko stanje ni podobno ali enako dejanskemu stanju v primerih, ko so v preteklosti prosilci zahtevali dostop do ocen npr. dela sodniške službe. Utemeljitev ocene sodnikovega dela obsega več strani dolgo zelo konkretno in podrobno obrazložitev v skladu z zakonsko določenimi kriteriji, ki so v obrazložitvi vsebinsko izpolnjeni na način, ki nujno kaže tudi na osebne lastnosti, sposobnosti in značilnosti posameznega sodnika ter jih v skladu z načelom sorazmernosti ni mogoče šteti kot podatke, povezane z opravljanjem javne funkcije ali delovnega razmerja javnega uslužbenca. V predmetni zadevi pa temu ni tako, saj vsaka izmed presojanih utemeljitev ocene vsebuje od tri- do petvrstičen splošen opis delovnih nalog javnega uslužbenca, iz česar ni mogoče razbrati osebnih lastnosti posameznega javnega uslužbenca. Informacijski pooblaščenec je zato zaključil, da zatrjevana izjema ni podana.

2.6.7. Varstvo kazenskega postopka, osebni podatki

Informacijski pooblaščenec je v odločbi št. 090-236/2017 z dne 16. 11. 2017 potrdil odločitev Vrhovnega državnega tožilstva RS (organ) glede zavrnitve dostopa do kazenske ovadbe, pritožbi pa je ugodil v delu, ki se nanaša na prekrite opravilne številke zahtevanih dokumentov.

Prošilec je zahteval dostop do kazenske ovadbe v konkretni zadevi in dostop do z njo povezanih dokumentov. Organ je zahtevo za dostop do kazenske ovadbe zavrnil zaradi varstva kazenskega postopka (6. točka prvega odstavka 6. člena ZDIJZ). Za obstoj navedene izjeme morata biti kumulativno izpolnjena dva pogoja: postopek je še v teku in razkritje informacije bi škodovalo izvedbi postopka. Informacijski pooblaščenec je ugotovil, da je organ pravilno utemeljil obstoj obeh pogojev, in poudaril, da iz Uredbe o posredovanju in ponovni uporabi informacij javnega

značaja³⁵ izhaja, da je obvezna osnova za izvajanje škodnega testa mnenje organa, ki obravnava zadevo v fazi predkazenskega ali kazenskega postopka. Škodljiv učinek razkritja informacij na izvedbo (pred)kazenskega postopka lahko v prvi vrsti verodostojno oceni organ, ki ta postopek vodi. Kadar ta organ oceni, da bi razkritje podatkov škodovalo izvedbi postopka, imata tako prvostopenjski kot drugostopenjski organ, ki odločata o zahtevi za dostop do informacij javnega značaja, malo maneverskega prostora za drugačno odločitev.

V zvezi z ostalimi zahtevanimi dokumenti se je prosilec pritožil, da je organ na njih neupravičeno prekril opravilne številke, in sicer sklicujoč se na varstvo osebnih podatkov (3. točka prvega odstavka 6. člena ZDIJZ). Informacijski pooblaščenec je ocenil, da zatrjevana izjema ni podana, ker je sistem vodenja evidenc v zadevah iz pristojnosti organa zaprt, zato ni mogoče, da bi posamezniki opravilno številko dokumenta enostavno, brez velikih stroškov in velikega napora, povezali s konkretnim posameznikom. Poleg tega je na podlagi Zakona o sodiščih³⁶ podatek, ki ga zahteva prosilec, lahko javno objavljen s pritrditvijo na oglasno desko sodišča, zato ne gre za varovan osebni podatek skladno z ZVOP-1. Upošteva je navedeno je organ prosilcu dolžan posredovati dokumente na način, da bo iz njih razvidna tudi opravilna številka.

Organ je po mnenju prosilca neupravičeno prekril podatke, ki so ključni za razumevanje same vsebine izločitve oziroma predodelitve zadeve. Informacijski pooblaščenec je ugotovil, da gre za podatke o imenih in priimkih, nazivih in sorodstvenih in drugih razmerjih navedenih oseb z državno tožilko ter za podatke o nazivu obdolženca, očitanih kaznivih dejanjih in medijski naziv kazenske zadeve. Vsi ti podatki se nanašajo na posameznika ter že sami po sebi ali v kombinacijah omogočajo popolno določljivost posameznikov (obdolženca, oškodovancev ipd). V tem delu je podana izjema varstva osebnih podatkov, zato je pritožba v tem delu neutemeljena.

2.6.8. Varstvo nadzornega postopka, notranje delovanje organa

Z odločbo št. 090-5/2017 z dne 2. 3. 2017 je Informacijski pooblaščenec družbi DARS, d. d., (organ) naložil, da prosilcu posreduje dokumente, iz katerih izhaja postopek nakupa konkretne nepremičnine, mnenje nadzornega sveta organa glede tega odkupa in splošen opis postopka odkupov (zahtevani dokumenti). Pritožbo pa je zavrnil v delu, ki se nanaša na podatke o povprečnih cenah, uporabljenih za izračun višine pravične odškodnine na konkretnem območju.

Organ je zavrnil zahtevo, sklicujoč se na drugi odstavek 5.a člena ZDIJZ (varstvo nadzornega postopka), po katerem lahko organ dostop zavrne, če gre za dokumente v zvezi z nadzornim postopkom, ki je v teku, ali ko je postopek nadzora končan, če bi razkritje zahtevane informacije povzročilo škodo drugi osebi ali če bi to resno ogrozilo izvajanje drugih zakonskih nalog nadzorne institucije. Informacijski pooblaščenec je ugotovil, da iz pojasnila Računskega sodišča izhaja, da postopek nadzora, na katerega se je skliceval organ, ni v teku in da razkritje zahtevanih dokumentov tudi ne more vplivati na (morebitne) bodoče postopke. To pomeni, da v konkretnem primeru niso izpolnjeni pogoji za zavrnitev dostopa po drugem odstavku 5. a člena ZDIJZ.

Organ se je v izpodbijani odločbi skliceval tudi na izjemo po 2. točki prvega odstavka 6. člena ZDIJZ (poslovna skrivnost). Informacijski pooblaščenec je ugotovil, da gre v konkretnem primeru za podatke, ki so javni po zakonu in jih zato ni mogoče določiti kot poslovno skrivnost (tretji odstavek 39. člena ZGD-1). Zahtevani dokumenti namreč vsebujejo podatke v zvezi s porabo javnih sredstev in podatke v zvezi z opravljanjem javne funkcije, ti pa so javni na podlagi 1. alineje tretjega odstavka 6. člena ZDIJZ. Pojem javne funkcije je v skladu s sodno prakso treba tolmačiti široko in ne na način, da je vezan zgolj na funkcionarje v državnih organih in organih lokalnih skupnosti, temveč tudi na izvajanje javnopravnih nalog. Četudi prihaja pri izvajanju teh nalog do civilno pravnih poslov (npr. sklepanje kupoprodajnih in menjalnih pogodb itd.), že sam okvir izvajanja javnih nalog daje tem dejanjem javnopravno naravo, ki ne sovпада z namenom varstva (zasebnih) interesov, čemur je prvenstveno namenjen institut poslovne skrivnosti. Z drugimi besedami, institut poslovne skrivnosti prvenstveno ščiti interese poslovnih subjektov, ki delujejo na trgu in ki stremijo zlasti k maksimizaciji dobička. Pri izvajanju javnopravnih nalog pa organi ne sledijo takšnemu poslovnemu interesu, zato se tudi ne morejo sklicevati na institut poslovne skrivnosti. Informacijski pooblaščenec je na podlagi predpisov, ki urejajo naloge organa, ugotovil, da organ odkupe nepremičnin izvaja v okviru svojih temeljnih javnopravnih nalog, zato informacij v zvezi z izvajanjem odkupov ne more varovati kot poslovno skrivnost.

³⁵ Uradni list RS, št. 24/2016; v nadaljevanju Uredba.

³⁶ Uradni list RS, št. 94/2007 – uradno prečiščeno besedilo, s spremembami; v nadaljnjem besedilu ZS.

Informacijski pooblaščenec je ugotovil, da podatki o povprečnih cenah, uporabljenih za izračun višine pravične odškodnine na konkretnem območju, predstavljajo izjemo po 11. točki prvega odstavka 6. člena ZDIJZ (notranje delovanje organa), za obstoj katere morata biti kumulativno izpolnjena dva pogoja: podatek mora izhajati iz dokumenta, ki je bil sestavljen v zvezi z notranjim delovanjem oziroma dejavnostjo organa, razkritje takšnega podatka pa bi povzročilo motnje pri delovanju oziroma dejavnosti organa. V konkretnem primeru je prvi pogoj izpolnjen, ker gre za »razmišljanje« organa glede poteka konkretnega odkupa in prakse organa v zvezi z odkupovanjem zemljišč za izgradnjo avtocest. V zvezi z drugim pogojem obravnavane izjeme je organ uspel prepričljivo obrazložiti, da bi prišlo do motenj v njegovem delovanju, če bi se javnost seznanila s podatki o splošnih povprečnih cenah, ki se v dokumentih ne omenjajo v zvezi z individualno določenimi odkupi. Odkupovanje zemljišč za gradnjo avtoceste je namreč občutljiv proces, pri čemer je za njegovo uspešno izvedbo bistvena ravno pravočasnost izvedenih odkupov, kar pa je pretežno odvisno od sodelovanja lastnikov. Razkritje povprečnih cen (ki so bile uporabljene za izračun višine pravične odškodnine na določenem območju) bi lastnike zemljišč (že izvedenih in bodočih projektov) zagotovo spodbudilo k temu, da se med seboj primerjajo in zahtevajo zase ugodnejše ponudbe, kar bi nedvomno podaljšalo čas izvedbe odkupov. Posledično splošne (povprečne) cene, ki izhajajo iz zahtevanih dokumentov, predstavljajo informacije v zvezi z notranjim delovanjem organa, katerih razkritje bi povzročilo motnje v delovanju po 11. točki prvega odstavka 6. člena ZDIJZ. Povprečne cene so fiktivne in ne predstavljajo porabe javnih sredstev. Predmet presoje pa so tudi cene, ki so bile dejansko uporabljene v konkretnem primeru odkupa/menjave. Te cene so podatki o porabi javnih sredstev in v skladu s tretjim odstavkom 6. člena ZDIJZ predstavljajo absolutno javne informacije. V zvezi s preostalimi informacijami iz zahtevanih dokumentov pa ni izpolnjen drugi pogoj izjeme notranjega delovanja. Gre za informacije o poteku konkretnega odkupa/menjave in splošen opis postopka odkupov ter določanja cen, kar izhaja iz področne zakonodaje in strokovnih usmeritev. Navedbam organa, da bi razkritje teh informacij lahko ogrozilo ali motilo izvajanje postopkov bodočih odkupov, zato ni mogoče slediti. Tudi Računsko sodišče z vidika svojih nadzornih postopkov ni prepoznalo ovire za to, da se zahtevani dokumenti posredujejo javnosti.

2.6.9. Okoljski podatki, poslovna skrivnost

Z odločbo št. 090-210/2017 z dne 14. 11. 2017 je Informacijski pooblaščenec Agenciji RS za okolje (organ) naložil, da prosilcu posreduje stroške zbiranja in stroške obdelave odpadne električne in elektronske opreme (OEEO) po posameznih zbirno-predelovalnih skupinah ter stroške izvedenih aktivnosti – obveščanja javnosti iz revidiranih finančnih poročil določenih gospodarskih družb za 2016.

V pritožbenem postopku se je Informacijski pooblaščenec sicer strinjal z organom in stranskim udeležencem, da revidirana finančna poročila nosilcev skupnega načrta ravnanja z OEEO predstavljajo poslovno skrivnost po subjektivnem kriteriju (izjema po 2. točki prvega odstavka 6. člena ZDIJZ), vendar pa ti dokumenti vsebujejo tudi določene podatke, ki se jih ne more opredeliti kot poslovno skrivnost, ker so javni po zakonu (tretji odstavek 39. člena ZGD-1), in sicer so to podatki o stroških, povezanih z zbiranjem in obdelavo OEEO. To so informacije, nastale zaradi obveznosti, ki jih nalaga Uredba o odpadni električni in elektronski opremi³⁷, torej ne gre za informacije, ki bi nastale zaradi ozkih poslovnih interesov stranskih udeležencev. Ti podatki sodijo med okoljske podatke, ki so vselej javni (13. člen Zakona o varstvu okolja³⁸). Absolutno javnost okoljskih podatkov določa tudi druga alineja 3. odstavka 6. člena ZDIJZ. Iz opredelitev okoljskih podatkov v Aarhuški konvenciji in ZVO-1 izhaja, da med okoljske podatke sodijo vse informacije, ki kakor koli posegajo v okolje. V ZVO-1 so med okoljskimi podatki izrecno navedeni »odpadki«. Uredba OEEO izrecno ureja ravnanje z OEEO, kar pomeni, da tudi višina stroškov izvajanja skupnega načrta ravnanja z OEEO, ki se neposredno tiče odpadkov, brez dvoma sodi med okoljske podatke. Aarhuška konvencija je v svoj okvir izrecno zajela informacije »o analizah stroškov in koristi ter druge ekonomske analize in predpostavke, ki se uporabljajo pri okoljskem odločanju«, kar je predmet presoje v obravnavanem primeru. Slednje izhaja iz dejstva, da količina oziroma vrednost finančnih sredstev oziroma stroškov vselej sovpiva na okoljske odločitve, saj se pri subjektih, ki delujejo na trgu, vselej zastavlja vprašanje, ali ni zaradi želje po čim manjših stroških zanemarljiv tisti del ravnanja z odpadki, ki mora ustrezati okoljevarstvenim zahtevam.

Iz navedenega izhaja, da revidiranih finančnih poročil v delu, v katerem so zajeti stroški zbiranja

³⁷ Uradni list RS, št. 55/2015 in 47/2016; v nadaljevanju Uredba OEEO.

³⁸ Uradni list RS, št. 39/2006 – uradno prečiščeno besedilo, s spremembami; v nadaljevanju ZVO-1.

in obdelave OEE0 ter stroški obveščanja, ni mogoče obravnavati kot poslovno skrivnost, saj gre za okoljske podatke, ki so javni po zakonu. Pri ravnanju z odpadki OEE0 torej ni relevantna samo njihova količina, temveč tudi stroški, ki ob tem nastanejo in za katere bi lahko rekli, da so kazalnik resnosti in odgovornosti države do varstva okolja. Šele vsi ti podatki skupaj izkazujejo, kako, na kakšen način in s kakšnimi stroški se država prek nosilcev skupnega načrta loteva problematike varstva okolja pred škodljivimi vplivi OEE0, kar je izrednega pomena ne samo za ljudi, ki v določeni državi živijo, temveč globalno, za cel svet. Preostali podatki v revidiranih finančnih poročilih stranskih udeležencev, ki izkazujejo poslovanje družb in nimajo neposredne zveze s podatki o odpadkih, po oceni Informacijskega pooblaščenca niso javni po zakonu, zato jih je organ dolžan varovati kot poslovno skrivnost.

2.6.10. Stroški postopka

Informacijski pooblaščenec je z odločbo št. 090-268/2017 z dne 21. 11. 2017 odpravil sklep o stroških, ki ga je izdala Občina Podvelka (organ).

Presoja pritožbe zoper odločitev o stroških v postopku po ZDIJZ je dvostopenjska. Primarno je treba ugotoviti, ali je organ zadostil zahtevam glede objave stroškovnika ter ali je organ prosilca opozoril na plačilo stroškov. Šele ob navedenih predpostavkah, ki morajo biti izpolnjene kumulativno, se presoja utemeljenost višine stroškov.

Določba ZDIJZ, ki organu nalaga dolžnost, da prosilca opozori na plačilo stroškov, je bistvenega pomena za to, da si prosilec, še preden mu organ posreduje zahtevane informacije, lahko premisli, ko izve, da mu organ za posredovanje namerava zaračunati stroške. Prosilec ima tudi pravico zahtevati, da mu organ vnaprej sporoči višino stroškov, ki mu jih bo za posredovanje informacij zaračunal. Če prosilec ne ve, da mu organ namerava zaračunati stroške, niti nima razloga za to, da bi preveril, za kakšne stroške gre. Obveznost organa, da mora prosilca o tem, da bo zaračunal stroške, obvestiti vnaprej, posredno izhaja tudi iz Uredbe o posredovanju in ponovni uporabi informacij javnega značaja³⁹, na podlagi katere organ za plačilo stroškov posredovanja izda prosilcu sklep ob posredovanju zahtevanih informacij. Organ mora torej ob posredovanju informacij prosilcu že posredovati sklep o zaračunanih stroških, ne pa ga šele obvestiti o tem, da namerava stroške zaračunati.

V konkretnem primeru organ pred izdajo izpodbijanega sklepa prosilca ni opozoril na plačilo stroškov. Prosilec tako ni imel možnosti, da bi se še pred izdajo izpodbijane odločbe odločil, da bo informacije zahteval v manjšem obsegu, v drugi obliki (npr. vpogled) ali da jih sploh ne bo zahteval. Prav tako ni imel možnosti še pred prejemom izpodbijane odločbe pri organu poizvedeti o višini stroškov, ki jih namerava zaračunati organ. Informacijski pooblaščenec je zato ugotovil, da organ ni upravičen zaračunati stroškov posredovanja informacij javnega značaja na podlagi izpodbijanega sklepa, ker jih je prosilcu zaračunal v nasprotju z veljavnimi predpisi.

2.6.11. Tajni podatki, dokument v izdelavi

Na podlagi odločbe Informacijskega pooblaščenca št. 090-194/2017 z dne 1. 12. 2017 je moralo Ministrstvo za zunanje zadeve (organ) umakniti stopnjo tajnosti »interno« z določenih delov poročila o izrednem delnem nadzoru v konkretnem veleposlaništvu (zahtevano poročilo) in fotokopije teh delov posredovati prosilki. Informacijski pooblaščenec pa je potrdil odločitev organa o zavrnitvi dostopa do osnutka tega poročila in konkretne depeše.

Dostop do osnutka zahtevanega poročila je organ zavrnil zaradi izjeme po 9. točki prvega odstavka 6. člena ZDIJZ (dokument v izdelavi), ki ima tri pogoje, ki morajo biti izpolnjeni kumulativno: dokument mora biti še v postopku izdelave in predmet posvetovanja v organu, razkritje dokumenta pa bi povzročilo napačno razumevanje njegove vsebine. Skladno z Uredbo se šteje, da je dokument v postopku izdelave, če ga še ni podpisala in odposlala ali kako drugače zaključila uradna oseba organa, ki je z veljavnimi predpisi pooblaščenca za odločanje.

Informacijski pooblaščenec je ugotovil, da je postopek izdelave poročila zaključen, ko ga podpišeta glavni diplomatski nadzornik in minister. Ker navedeni uradni osebi organa osnutka zahtevanega poročila nista podpisali niti ta osnutek ni bil poslan izven organa, temveč zgolj notranjim

³⁹ Uradni list RS, št. 24/2016; v nadaljevanju Uredba.



organizacijskim enotam organa, gre za dokument, ki je pri organu v postopku izdelave. Podatki, ki so bili v osnutku zahtevanega poročila, so bili še predmet posvetovanja v organu oziroma vsebinsko še niso bili zaključeni, saj je bil osnutek posredovan veleposlaništvu oziroma relevantnim diplomatom oziroma osebju, da bi lahko nanj dali pripombe. Informacijski pooblaščenec se je strinjal z ugotovitvijo organa, da bi z razkritjem osnutka zahtevanega poročila lahko prišlo do napačnega razumevanja vsebine končnega poročila, predvsem obremenilnih ugotovitev nadzora glede javne uslužbenke, ki jih je bilo v osnutku v primerjavi s končno in podpisano verzijo poročila več. Podatki v osnutku so torej nepopolni oziroma neusklajeni z osebami, na katere se nanašajo, zato so (lahko) tudi napačni. Napačni podatki, ki se jih v javnosti predstavlja kot podatke iz uradnega dokumenta, ki ga je izdelal organ, pa brez dvoma lahko povzročijo napačno razumevanje, če se javnost nanje zanese. Zato je glede osnutka zahtevanega poročila obstoj zatrjevane izjeme utemeljen.

Dostop do določenih delov zahtevanega poročila je organ zavrnil s sklicevanjem na izjemo po 1. točki prvega odstavka 6. člena ZDIJZ (tajni podatki). Informacijski pooblaščenec je ugotovil, da je v konkretnem primeru izpolnjen formalni kriterij, kot ga opredeljuje Zakon o tajnih podatkih⁴⁰. Pri ugotavljanju obstoja materialnega kriterija pa je ugotovil, da se določeni deli zahtevanega poročila nanašajo na sisteme, naprave, projekte in načrte, pomembne za zunanje zadeve (5. točka 5. člena ZTP). Navedene informacije razkrivajo kronologijo ravnanja s konkretnim osnutkom in končnim poročilom o rednem nadzoru na veleposlaništvu, ki vsebujeta tajne podatke, ugotovitve nadzora v zvezi s tem ravnanjem, protokol ob prejemu pošte in ugotovitve nadzora glede vodenja predpisanih evidenc za tajne podatke. Gre za informacije, katerih razkritje bi pomenilo varnostno tveganje za organ in bi povzročilo nastanek možnosti, da bi kdo ogrozil varnost pri organu do mere, ko bi bil organ (natančneje veleposlaništvo) v svojem delovanju ohromljen. Razkritje teh informacij bi lahko ogrozilo zagotovitev varnosti osebja, opreme in dokumentov, ki se nanašajo na zunanje zadeve, kar posledično pomeni oteženo, ovirano ali celo onemogočeno izvajanje nalog organa, poleg tega pa bi razkritje teh podatkov lahko povzročilo škodljive posledice za varnost države ali ogrozilo njene politične ali gospodarske koristi. V zvezi s temi informacijami sta kumulativno izpolnjena oba kriterija, ki ju za obstoj izjeme tajnih podatkov določa ZTP, kar pomeni, da je v tem delu podana izjema tajnih podatkov. To pa ne velja za druge obravnavane dele zahtevanega poročila, ki se nanašajo na splošno navedbo vsebine prejete pošiljke in na zaposlovanje lokalnega osebja. Ugotovitev glede poslovanja in delovanja veleposlaništva le zaradi dejstva, da gre za »enoto« v tujini, in zato, ker spada pod organ, ki izvaja pristojnosti na področju zunanjih zadev, namreč ni mogoče kar avtomatično oziroma pavšalno uvrstiti v katero izmed področij iz 5. člena ZTP. Glede teh podatkov materialni kriterij za določitev tajnega podatka ni podan, zato ni zakonskega razloga, da bi ti deli zahtevanega poročila nosili stopnjo tajnosti. Informacijski pooblaščenec je organu naložil, da s teh delov umakne stopnjo tajnosti in jih posreduje prosilki.

Po vpogledu v zahtevano depešo je Informacijski pooblaščenec ugotovil, da ta vsebuje veliko koncentracijo podatkov, ki jih je treba opredeliti kot varovane osebne podatke (3. točka prvega odstavka 6. člena ZDIJZ). Zahtevana depeša vsebuje izrazito osebne izpovedi avtorice, ki vsebujejo njena osebna mnenja oziroma stališča glede ugotovitev nadzora, še zlasti v delu, ki se nanaša nanjo. Pri tem avtorica navaja predvsem vrednostne sodbe oziroma svoje osebno videnje določene problematike v zvezi z dogajanjem, ki je bilo predmet nadzora, in v zvezi z delovanjem organa. Vse navedeno izhaja izključno iz mnenja avtorice oziroma dogodkov, ki jih je avtorica doživela v zvezi z obravnavano problematiko. Za razkritje takšnih osebnih podatkov po ZDIJZ ne obstaja zakonska podlaga, zato predstavljajo varovane osebne podatke. Ker so v zahtevani depeši izražena predvsem osebna stališča avtorice, te vsebine ni mogoče subsumirati pod določilo tretjega odstavka 6. člena ZDIJZ, saj takšnih podatkov ni mogoče objektivno in neposredno povezati s podatki iz delovnega razmerja javnih uslužbencev ali s podatki v zvezi z opravljanjem javne funkcije.

2.6.12. Ponovna uporaba

Informacijski pooblaščenec je z odločbo št. 090-288/2016 z dne 21. 2. 2017 Agenciji RS za javnopravne evidence in storitve (organ) naložil, da mora prosilcu omogočiti ponovno uporabo podatkov o naslovih prebivališča fizičnih oseb – družbenikov, zastopnikov in članov organa nadzora (zahtevani podatki) –, prosilcu pa je postavil pogoje za ponovno uporabo, kot jih določata Zakon o Poslovnem registru Slovenije⁴¹ in Zakon o sodnem registru⁴².

⁴⁰ Uradni list RS, št. 50/2006 – uradno prečiščeno besedilo, s spremembami; v nadaljevanju ZTP.

⁴¹ Uradni list RS, št. 49/2006, s spremembami; v nadaljevanju ZPRS-1.

⁴² Uradni list RS, št. 54/2007 – uradno prečiščeno besedilo, s spremembami; v nadaljevanju ZSReg.

Organ je zavrnil zahtevo prosilca, ker naj bi bile glede zahtevanih podatkov podane izjeme od ponovne uporabe v skladu s šestim odstavkom 6. člena ZDIJZ. V skladu z določbo 1. točke šestega odstavka 6. člena ZDIJZ organ zavrne zahtevo za ponovno uporabo informacije javnega značaja, če se podatek nanaša na podatek iz prvega odstavka 6. člena ZDIJZ. Ker je prosilec zahteval ponovno uporabo osebnih podatkov – naslovov fizičnih oseb (zastopnikov, članov organa nadzora ter družbenikov) –, je Informacijski pooblaščenec ugotavljal, ali gre za varovane osebne podatke (3. točka prvega odstavka 6. člena ZDIJZ). Glede na veljavne določbe ZSReg in ZPRS-1 so podatki, ki jih zahteva prosilec, javno objavljeni v Poslovnem registru Slovenije in do njih lahko prosto dostopa vsakdo, bodisi posredno preko iskanja po poslovnih subjektih bodisi neposredno z iskanjem po fizičnih osebah, kadar razpolaga z določeno kombinacijo podatkov. Zakonodajalec je torej ocenil, da je takšno iskanje po fizičnih osebah v javnem interesu oziroma javni interes takšnega iskanja prevlada nad interesom teh fizičnih oseb po varstvu zasebnosti.

Prosilec je v zahtevi za ponovno uporabo navedel, da podatke potrebuje za dopolnitev že obstoječega registra poslovnih subjektov, in sicer kot dodatni kvalifikator postopka iskanja po osebah, saj želi slediti načinu iskanja in dobre prakse, kot je omogočen pri organu. Informacijski pooblaščenec je ugotovil, da je namen ponovne uporabe zahtevanih podatkov v konkretnem primeru v skladu z namenom omogočanja iskanja po fizičnih osebah, kot izhaja iz ZSReg in ZPRS-1. Ugoditev zahtevi prosilca tako ne bi bila v nasprotju z določbo 16. člena ZVOP-1, po kateri se osebni podatki lahko zbirajo le za določene in zakonite namene ter se ne smejo nadalje obdelovati tako, da bi bila njihova obdelava v neskladju s temi nameni, če zakon ne določa drugače.

Informacijski pooblaščenec je ugotovil, da ZPRS-1 in ZSReg ne vsebujeta določb v zvezi z omejitvami za vpogled v podatke oziroma posredovanje podatkov za namene ponovne uporabe. Omejitve, na katere se sklicuje organ v izpodbijani odločbi, veljajo le glede iskanja po Poslovnem registru Slovenije. Dejansko lahko kombinacijo podatkov o osebnem imenu in naslovu prebivališča fizične osebe pridobi kdor koli z vpogledom v podatke o določeni pravni osebi. Po oceni Informacijskega pooblaščenca zato določb ZPRS-1 in ZSReg ni mogoče razumeti na način, da osebe, ki razpolagajo s kombinacijo relevantnih podatkov, predstavljajo izključne upravičence za dostop do podatkov o fizičnih osebah, kot si to napačno razlaga organ. Takšna razlaga je nedvomno v nasprotju z namenom ZPRS-1 in ZSReg, ki določata, da se vsakomur omogoči brezplačen vpogled v objavljene podatke, tudi podatke o naslovih prebivališč v obeh zakonih opredeljenih fizičnih oseb. O izključnih upravičencih bi lahko govorili takrat, ko podatki, do katerih bi bili slednji upravičeni, ne bi bili prosto javno dostopni vsem, v danem primeru pa je takšna razlaga nelogična in v nasprotju z namenom zakona. Posledično tudi niso izpolnjeni pogoji iz 4. alineje šestega odstavka 6. člena ZDIJZ, ki je omejen na podatke, ki so dostopni samo upravičenim osebam, medtem ko v danem primeru govorimo o podatkih, ki morajo biti in tudi so na podlagi zakona dostopni vsem.

2.6.13. Tajnost vira

Z odločbo št. 090-190/2017 z dne 25. 9. 2017 je Informacijski pooblaščenec zavrnil pritožbo prosilke zoper odločbo, s katero je Ministrstvo za okolje in prostor (organ) zavrnilo njeno zahtevo za dostop do prijav, ki jih je vložila sama.

Organ je zavrnil zahtevo prosilke na podlagi tretjega odstavka 5.a člena ZDIJZ (varovanje tajnosti vira), na podlagi katerega organ prosilcu zavrne dostop do zahtevane informacije, če se zahteva nanaša na podatek, glede katerega zakon določa varovanje tajnosti vira. V konkretnem primeru so bile predmet presoje prijave v inšpekcijskem postopku, kjer varstvo vira prijave določa Zakon o inšpekcijskem nadzoru⁴³; skladno s slednjim je inšpektor dolžan varovati tajnost vira prijave in vira drugih informacij, na podlagi katerih opravlja inšpekcijski nadzor. Informacijski pooblaščenec je ugotovil, da je prosilka v konkretnem primeru zahtevala prijave, ki jih je sama vložila pri organu. Ker ZIN ne določa, da lahko prijavitelj z izjavo odveže inšpekcijski organ obveznosti varstva vira prijave, dolžnost varstva vira prijave skladno z ZIN obstaja ne glede na izjavo prosilke, da inšpekcijski organ odvezuje varovanja njenih prijav. Informacijski pooblaščenec je poudaril, da je zaradi narave postopka po ZDIJZ, kjer se ugotavlja prost dostop do dokumenta glede na fikcijo abstraktnega prosilca, treba ne glede na pravni interes oziroma status prosilca (načelo prostega dostopa po 5. členu ZDIJZ) o vsaki zahtevi odločiti enako, torej ne glede na to, kdo je zahtevo vložil. Ne glede na to, da je prosilka zahtevala prijave, ki jih je podala sama, je organ upravičeno v celoti zavrnil dostop na podlagi tretjega odstavka 5. a člena ZDIJZ, saj tudi delni dostop v konkretnem primeru ne bi bil mogoč brez razkritja varovanih informacij.

⁴³ Uradni list RS, št. 43/2007 – uradno prečiščeno besedilo in 40/14; v nadaljevanju ZIN.

2.6.14. Varstvo upravnega postopka

Z odločbo št. 090-76/2017 z dne 11. 4. 2017 je Informacijski pooblaščenec zavrnil pritožbo prosilke zoper odločbo, s katero je Inšpektorat RS za okolje in prostor (organ) zavrnil zahtevo za dostop do konkretnega dokumenta iz zadeve, ki jo vodi organ.

Organ se je v izpodbijani odločbi skliceval na izjemo po 7. točki prvega odstavka 6. člena ZDIJZ (varstvo upravnega postopka), za obstoj katere morata biti kumulativno izpolnjena dva pogoja: zahtevana informacija predstavlja podatek, ki je bil pridobljen ali sestavljen zaradi konkretnega upravnega postopka, razkritje zahtevanega podatka pa bi škodovalo izvedbi konkretnega postopka.

Informacijski pooblaščenec je ugotovil, da je dokument, ki je predmet zahteve prosilke, nastal v inšpekcijskem upravnem postopku. Izkazana je bila tudi škoda, ki bi nastala pri izvedbi tega postopka, če bi bil zahtevani dokument posredovan javnosti, še preden bi bil končan. Organ je namreč povsem utemeljeno navedel, da bi lahko prezgodnje razkritje dotlej pridobljenih podatkov ogrozilo izvedbo inšpekcijskega postopka, saj dejansko stanje še ni dokončno ugotovljeno in bi posredovani podatki lahko bili pomanjkljivi ali napačni. Da je pridobivanje dokazov in ugotavljanje dejanskega stanja še v teku, izhaja tudi iz popisa zadeve, saj v konkretni zadevi odločba še ni bila izdana. Razkritje dotlej zbranih dokumentov, v fazi, ko ugotovitveni postopek še poteka, bi lahko tudi po mnenju Informacijskega pooblaščenca ogrozilo nadaljnje zbiranje, izvedbo in obstoj dokazov. Zavezanci ali druge osebe, ki bi v teh postopkih lahko nudili koristne informacije, bi lahko prikrili ali uničili določene dokumente, pomembne za odločanje v predmetnih inšpekcijskih postopkih. Seznanjanje javnosti z informacijami iz posamezne faze inšpekcijskega postopka, dokler ta še teče, bi nedvomno negativno vplivalo na potek samega postopka (z informacijami bi se lahko seznanile priče, ki še niso bile zaslišane, ogrožena bi lahko bila izvedba posameznih procesnih dejanj ipd.), posledično pa bi to vplivalo na ugotovitev dejanskega stanja in na odločitev inšpektorja. Informacijski pooblaščenec se strinja z oceno organa, da gre za zahteven upravni postopek, v katerem mora inšpektor še ugotoviti resnično dejansko stanje ter presoditi o morebitnih nepravilnosti in upravnih ukrepih, zato bi lahko razkritje zahtevanih podatkov v tej fazi resno ogrozilo nadaljnje zbiranje, izvedbo ali celo obstoj dokazov, kar bi posledično lahko vplivalo na zakonitost in pravilnost inšpekcijske odločbe, ki (še) ni bila izdana. Na dan izdaje izpodbijane odločbe je torej zahtevani dokument izpolnjeval oba pogoja za obstoj zatrevane izjeme.

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

Informacijski pooblaščenec je na področju dostopa do informacij javnega značaja leta 2017 skupaj prejel 522 pritožb, kar je več kot leto prej, ko jih je prejel 514. Od tega je leta 2017 prejel 314 pritožb zoper zavrnilne odločbe (leto prej 316), 201 pritožbo zoper molk organa (leto prej 198) in sedem pritožb zoper poslovne subjekte pod prevladujočim vplivom oseb javnega prava. Prosilci in zavezanci so se na Informacijskega pooblaščenca v 324 primerih obrnili s pisno prošnjo za mnenje oziroma pojasnilo (leto prej je bilo takih prošenj 308). Skupaj je bilo tako na področju dostopa do informacij javnega značaja obravnavanih 853 zadev (leto prej 822 zadev).

V pritožbenih postopkih zoper zavrnilne odločbe je Informacijski pooblaščenec izdal 316 odločb, kar je več kot leto prej, ko jih je izdal 312. Tudi leta 2017 si je Informacijski pooblaščenec prizadeval, da bi pritožbene zadeve 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 znašal 37 dni – zadeve so bile torej rešene prej kot v dvomesečnem roku, ki ga za reševanje tovrstnih zadev določa Zakon o splošnem upravnem postopku. Leta 2016 je povprečen čas reševanja pritožbenih zadev znašal 47 dni, kar pomeni, da se je čas reševanja pritožb skrajšal za 22 %.

Informacijski pooblaščenec ugotavlja, da je bilo leta 2017 število pritožb zaradi t. i. molka organa primerljivo številu teh pritožb leta 2016, rahlo pa je naraslo število pritožb zoper zavrnilne odločbe. Glede na strukturo zavezancev, zoper odločitve katerih so prosilci vložili pritožbo, je leta 2017 bistveno naraslo število pritožb, vloženi zoper državne organe (leto 2016 je bilo teh pritožb 128, leta 2017 pa 156), zmanjšalo pa se je število pritožb, vloženi zoper ravnanje občin. Leta 2017 je namreč Informacijski pooblaščenec zoper občine prejel 41 pritožb, kar je 13 % manj kot leto prej. Po mnenju Informacijskega pooblaščenca slednje izkazuje, da so občine leta 2017 na področju dostopa do informacij javnega značaja poslovale bolje, še posebej glede na podatke iz preteklih

let, ki so kazali na slabšo odzivnost občin v postopkih po ZDIJZ. Znova pa se je povečalo število prošenj za pojasnila in mnenja, ki jih je Informacijski pooblaščenec prejel s strani zavezancev, kar kaže na to, da so bili zavezanci leta 2017 bolj aktivni in odzivni kot leto prej in da so se z vprašanji večkrat obrnili na Informacijskega pooblaščenca tudi izven pritožbenega postopka.

Leta 2017 je Informacijski pooblaščenec zoper odločitve poslovnih subjektov pod prevladujočim vplivom obravnaval sedem pritožb, precej manj kot leto prej, ko je bilo takih pritožb 22. Gre za izjemno nizek odstotek vseh pritožbenih zadev (1,3 %), 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. Podobno stanje je Informacijski pooblaščenec sicer ugotovil tudi leta 2016.

Leta 2017 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 povečanje števila zadev, ki so se nanašale na t. i. zlorabo pravice. Če je Informacijski pooblaščenec leta 2016 obravnaval 13 tovrstnih zadev, je bilo teh zadev leta 2017 kar 29. Le v enem od primerov je Informacijski pooblaščenec organu pritrnil in ugotovil, da gre za zlorabo, v vseh ostalih zadevah pa je ugotovil, da so se zavezanci na zlorabo pravice sklicevali neupravičeno. Ob tem Informacijski pooblaščenec opozarja, da je institut zlorabe pravice skrajno sredstvo, na katerega se lahko zavezanci sklicujejo le v izjemnih primerih. Pravico odstopa do informacij javnega značaja kot temeljno človekovo pravico je namreč mogoče omejiti le zaradi varstva legitimnih interesov in pravic tretjih oseb ter v najmanjši možni meri, ki še zagotavlja varstvo teh interesov. Organ mora ob tem v postopku konkretno izkazati, da je prosilec z eno ali več funkcionalno povezanimi zahtevami očitno zlorabil pravico dostopa do informacij javnega značaja oz. je očitno, da so zahteva ali zahteve šikanoznega značaja. Za zlorabo pravice (šikanozno zahtevo) gre le v primerih, ko prosilec prestopi meje pravno zavarovanega upravičenja tako, da s tem ogroža oz. posega v pravico drugega.

Podatki kažejo, da se je leta 2017 delno spremenila struktura prosilcev, ki so se s pritožbo obrnili na Informacijskega pooblaščenca. Tudi to leto je največ pritožnikov imelo status fizične osebe (211), kar je več kot leto prej (172). Manj pritožb je Informacijski pooblaščenec prejel s strani pravnih oseb zasebnega prava (65), število pritožb, ki so jih vložili novinarji (33) pa je ostalo na primerljivi ravni. Zanimiva pa je ugotovitev, da se je povečalo število pritožbenih primerov, v katerih so kot prosilci za informacije nastopale pravne osebe javnega prava (7), kar kaže na to, da je pravica dostopa do informacij javnega značaja institut, ki omogoča hitro in učinkovito pridobivanje informacij različnim kategorijam uporabnikov. Ob tem Informacijski pooblaščenec ugotavlja, da so prosilci s postopkom dostopa do informacij dobro seznanjeni, pritožbeni postopek pa je zanje hiter, učinkovit in jim ne povzroča stroškov.

V zvezi s ponovno uporabo je Informacijski pooblaščenec leta 2017 vodil tri pritožbene postopke, kar je primerljivo z letom 2016. 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 pritožb ne vlagajo pogosto. Na področju ponovne uporabe od uveljavitve novele ZDIJZ-E namreč primarno velja načelo t. i. proaktivnega zagotavljanja podatkov, ki se v praksi uresničuje prek zagotavljanja podatkov z objavo na portalu odprtih podatkov Ministrstva za javno upravo. Na ta način potencialni ponovni uporabniki odprte podatke, pri katerih ni nobene ovire za prosto ponovno uporabo, pridobijo hitro in brez posebnih postopkovnih zahtev, na katere je sicer vezan pritožbeni postopek po ZDIJZ in ZUP pred Informacijskim pooblaščenem.





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, katere 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 podatkov⁴⁴, ki ga je Državni zbor RS sprejel 15. 7. 2004, velja od 1. 1. 2005. Zakon je bilo treba sprejeti predvsem zaradi vstopa Republike Slovenije v Evropsko unijo in zaradi s tem povezane dolžnosti uskladitve varstva osebnih podatkov z določbami Direktive 95/46/ES Evropskega parlamenta in Sveta o zaščiti posameznikov pri obdelavi osebnih podatkov in o prostem pretoku takih podatkov⁴⁵. Julija 2007 je bil sprejet Zakon o spremembah in dopolnitvah zakona o varstvu osebnih podatkov⁴⁶, 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.

⁴⁴ Uradni list RS, št. 86/2004; v nadaljevanju ZVOP-1.

⁴⁵ Uradni list Evropskih skupnosti, št. L 281, 23. 11. 1995.

⁴⁶ 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 RS in zakonov.

Splošna načela inšpekcijskega nadzora, pravice, dolžnosti in pooblastila državnih nadzornikov, postopek inšpekcijskega nadzora, inšpekcijski ukrepi in druga vprašanja, povezana z inšpekcijskim nadzorom, so določeni v Zakonu o inšpekcijskem nadzoru,⁴⁷ **specifične pristojnosti državnega nadzornika pa so opredeljene v 53. členu ZVOP-1.**

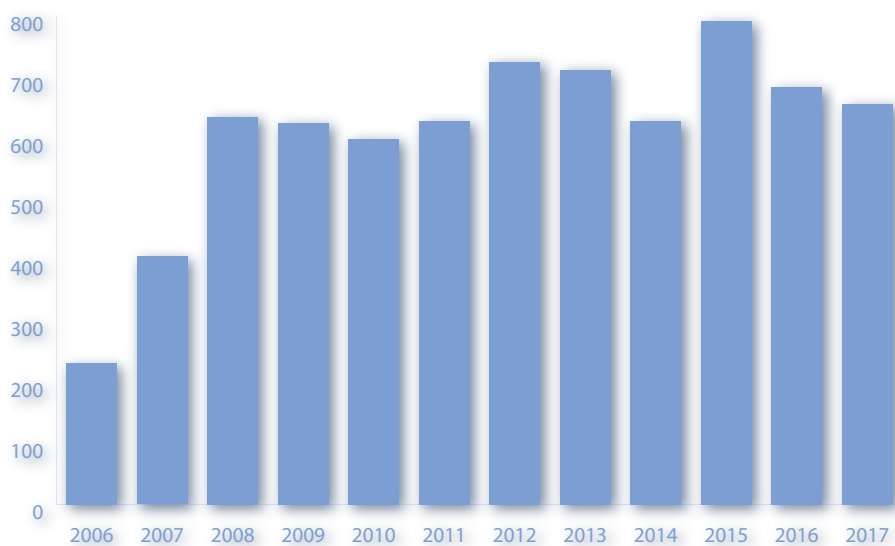
3.2.2. Inšpekcijski nadzor

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

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

Informacijski pooblaščenec je leta 2017 zaradi suma kršitev določb ZVOP-1 vodil 655 inšpekcijskih zadev, od tega 226 v javnem in 429 v zasebnem sektorju. Zoper pravne osebe javnega sektorja je na podlagi prijav uvedel 189 inšpekcijskih zadev, 37 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 zavezanca v zasebnem sektorju je na podlagi prijav odprl 370 inšpekcijskih zadev, 59 postopkov je začel po uradni dolžnosti.

Slika 8: Število inšpekcijskih zadev med letoma 2006 in 2017.



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

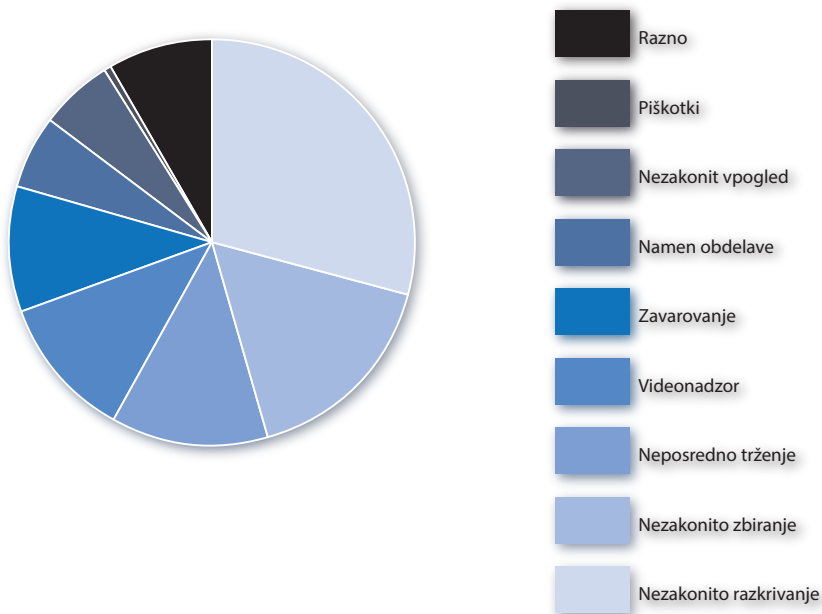
- nezakonito razkrivanje osebnih podatkov: posredovanje osebnih podatkov nepooblaščenim uporabnikom in nezakonita objava osebnih podatkov – 174,
- nezakonito zbiranje oziroma zahtevanje osebnih podatkov – 98,
- nezakonita obdelava osebnih podatkov pri izvajanju neposrednega trženja – 75,

⁴⁷ Uradni list RS, št. 43/2007 – uradno prečiščeno besedilo 1 in 40/2014; v nadaljevanju ZIN.

- nezakonito izvajanje videonadzora – 67,
- neustrezno zavarovanje osebnih podatkov – 59,
- obdelava osebnih podatkov v nasprotju z namenom zbiranja – 36,
- nezakonit vpogled v osebne podatke – 34,
- piškotki – 3,
- razno: npr. obdelava osebnih podatkov po preteku roka hrambe, zavrnitev posredovanja osebnih podatkov, zavrnitev izbrisa osebnih podatkov, iznos osebnih podatkov v tretje države, uporaba netočnih podatkov, neustrezna pogodbeno obdelava osebnih podatkov, kršitev pravice do seznanitve z lastnimi osebnimi podatki, sumi kršitev, ki ne sodijo v pristojnost Informacijskega pooblaščenca (npr. kršitev pravil v postopkih pri drugih organih, kazniva dejanja zoper čast in dobro ime) – 49.

Poleg zgoraj navedenih postopkov je Informacijski pooblaščenec uvedel 60 inšpekcijskih postopkov po uradni dolžnosti, v okviru katerih je preverjal izvajanje določb ZVOP-1 v celoti.

Slika 9: Sumi nezakonite obdelave osebnih podatkov leta 2017.



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 189 inšpekcijskih zadev, 37 jih je odprl po uradni dolžnosti, skupaj 226. V 72 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 šestih primerih Informacijski pooblaščenec ni uvedel postopka, ker prijavitelji niso posredovali svojih podatkov, zaradi česar jih ni mogel pozvati k posredovanju dodatnih podatkov, potrebnih za uvedbo inšpekcijskega postopka. Na podlagi petih 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, pet prijav je Informacijski pooblaščenec odstopil v reševanje pristojnim organom, od tega je v dveh primerih naznanil sum storitve kaznivega dejanja. Tri prijavitelje je Informacijski pooblaščenec napotil na pravico do seznanitve z lastnimi osebnimi podatki oziroma jim je svetoval, kako naj ravnajo.

Po preučitvi 189 prejetih prijav je bilo zaradi utemeljenega suma kršitev določb ZVOP-1 začeti 98 inšpekcijskih postopkov, 37 jih je bilo začeti po uradni dolžnosti, skupaj torej 135. V okviru inšpekcijskih postopkov je bilo opravljenih 28 inšpekcijskih pregledov v prostorih zavezancev in šest pregledov spletnih strani. Za odpravo ugotovljenih nepravilnosti je Informacijski pooblaščenec 50 zavezancem izrekel ukrepe v obliki ureditvene odločbe (3), opozorila na zapisnik

(12), predodločbe (13)⁴⁸ ali ustnega poziva (22). Vsi zavezanci, razen enega, ki je zoper odločbo vložil tožbo na Upravno sodišče RS, so naložene jim ukrepe takoj izvršili.

Leta 2017 je bilo zaključenih 140 inšpekcijskih postopkov. Informacijski pooblaščenec v 54 inšpekcijskih postopkih ni zaznal kršitev določb ZVOP-1, 58 postopkov je ustavil, ker so zavezanci ugotovljene nepravilnosti odpravili, 28 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 zavezancu odredil odpravo ugotovljenih nepravilnosti. Upravno sodišče RS je leta 2017 izdalo sodbo v zvezi s tožbo, vloženo leta 2016 zoper odločbo Informacijskega pooblaščenca, in sicer je tožbo zavrnilo. Zavezanec je zoper sodbo vložil revizijo na Vrhovno sodišče RS.

3.2.2.1. Inšpekcijski nadzor v zasebnem sektorju

Informacijski pooblaščenec je zoper zavezance v zasebnem sektorju na podlagi prijav odprl 370 zadev. V 149 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, pravico do popravka ali izbrisa osebnih podatkov ter pravico zahtevati prenehanje uporabe osebnih podatkov za namen neposrednega trženja. Slednjim (teh je bilo 15) je pojasnil, da mu v primeru zavrnitve zahteve lahko podajo pritožbo ali prijavo. 16 prijav je Informacijski pooblaščenec posredoval v reševanje pristojnim institucijam in o tem obvestil prijavitelje. Na podlagi sedmih prijav je Informacijski pooblaščenec takoj uvedel postopek o prekršku, ker je po preučitvi prijav zaključil, da uvedba inšpekcijskega postopka 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. V dveh primerih Informacijski pooblaščenec postopka inšpekcijskega nadzora ni mogel uvesti zaradi pomanjkanja podatkov.

Informacijski pooblaščenec je po preučitvi prejetih prijav začel 196 postopkov inšpekcijskega nadzora, 59 pa jih je uvedel po uradni dolžnosti, skupaj torej 255. Državni nadzorniki za varstvo osebnih podatkov so opravili 76 inšpekcijskih ogledov na terenu in 30 ogledov spletnih strani. Za odpravo ugotovljenih nepravilnosti so 91 zavezancem izrekli ukrepe v obliki opozorila na zapisnik (42), predodločbe (34), ustnega poziva (9) in ureditvene odločbe (6). En zavezanec je zoper odločbo Informacijskega pooblaščenca vložil tožbo, preostali so naložene jim ukrepe v postavljenem roku izvršili.

Leta 2017 je Informacijski pooblaščenec ustavil 197 postopkov; 79 postopkov je ustavil, ker ni ugotovil kršitev določb ZVOP-1, 74 postopkov je ustavil po tem, ko so zavezanci odpravili ugotovljene nepravilnosti, 44 postopkov pa je zaključil, ker v zvezi z ugotovljenimi prekrški ni bilo mogoče izreči inšpekcijskih ukrepov, saj je šlo za enkratna dejanja v preteklosti. Zoper en sklep o ustavitvi postopka je posameznik, ki bi lahko imel status stranskega udeleženca, vložil tožbo na Upravno sodišče RS.

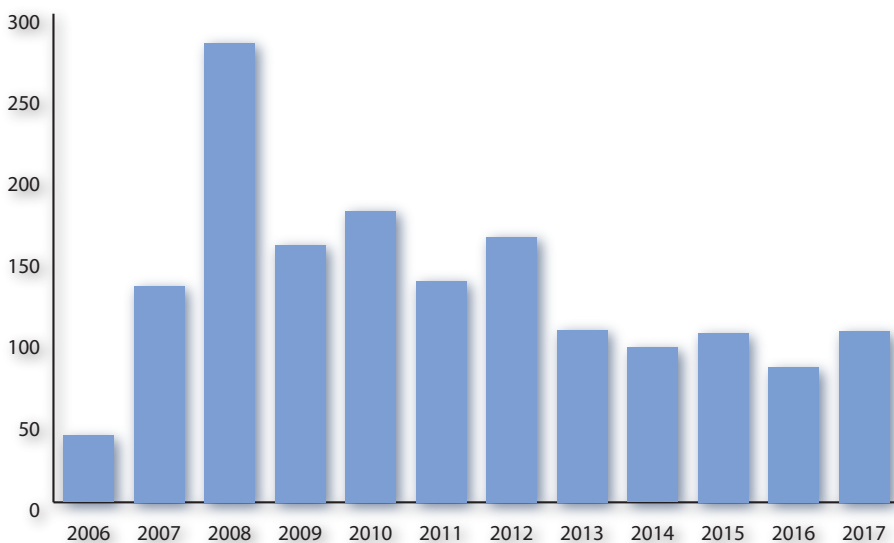
Informacijski pooblaščenec je leta 2017 prejel štiri sodbe Upravnega sodišča. V dveh primerih je sodišče tožbo zavezanca zoper odločbo Informacijskega pooblaščenca zavrnilo, v dveh primerih pa je tožbi ugodilo, sklepa Informacijskega pooblaščenca odpravilo (tožbi sta bili vloženi zoper sklep o zavrnitvi stranske udeležbe in zoper sklep o zavrnjenju pritožbe zoper obvestilo prijavitelju o neuvedbi postopka) in zadevo vrnilo v ponoven postopek.

⁴⁸ 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). To v praksi pomeni, da zavezanci po seznanitvi z argumenti Informacijskega pooblaščenca v večini primerov sami nehajo nezakonito obdelovati osebne podatke, zato izdaja ureditvene odločbe ni več potrebna.

3.2.3. Storjeni prekrški

Zaradi kršitev določb ZVOP-1 je bilo leta 2017 uvedenih 105 postopkov o prekršku, od tega 44 zoper pravne osebe zasebnega sektorja in njihove odgovorne osebe, 27 zoper pravne osebe javnega sektorja in njihove odgovorne osebe, 34 pa jih je bilo uvedenih zoper posameznike (v to število so vključeni tudi postopki zoper odgovorne osebe državnih organov in samoupravnih lokalnih skupnosti, saj v skladu z Zakonom o prekrških⁴⁹ Republika Slovenija in samoupravne lokalne skupnosti za prekrške ne odgovarjajo, odgovarjajo le njihove odgovorne osebe – teh je bilo 28). Za ugotovljeni prekršek lahko prekrškovni organ v skladu s 53. členom izreče opozorilo, če je storjeni prekršek neznaten in če pooblaščen uradna oseba oceni, da je glede na pomen dejanja opozorilo zadosten ukrep. Če je storjen hujši prekršek, prekrškovni organ izda odločbo o prekršku, s katero kršitelju izreče sankcijo. V skladu s 4. členom ZP-1 sta sankciji za prekršek globa in opomin, glede na 57. člen ZP-1 pa se lahko globa izreče tudi v obliki plačilnega naloga.

Slika 10: Število uvedenih postopkov o prekršku med letoma 2006 in 2017.



V prekrškovnih postopkih, vključno z odprtimi postopki iz preteklih let, je Informacijski pooblaščenec leta 2017 izdal:

- 10 opozoril ter
- 93 odločb o prekršku (49 glob in 44 opominov).

Poleg opozoril, ki so bila izrečena v prekrškovnih postopkih, je Informacijski pooblaščenec v skladu z načelom ekonomičnosti izrekel tudi 70 opozoril po 53. členu ZP-1 v okviru postopkov inšpekcijskega nadzora, in sicer 23 v javnem in 47 v zasebnem sektorju.

Kršitelji so zoper izdane odločbe o prekršku vložili deset zahtev za sodno varstvo (zoper 10,7 % odločb). Vse zahteve za sodno varstvo so bile vložene zoper odločbe, s katerimi je Informacijski pooblaščenec kršiteljem izrekel globe. Relativno majhen delež vloženih zahtev za sodno varstvo kaže na to, da storilci storjene prekrške priznavajo in se zavedajo svoje odgovornosti.

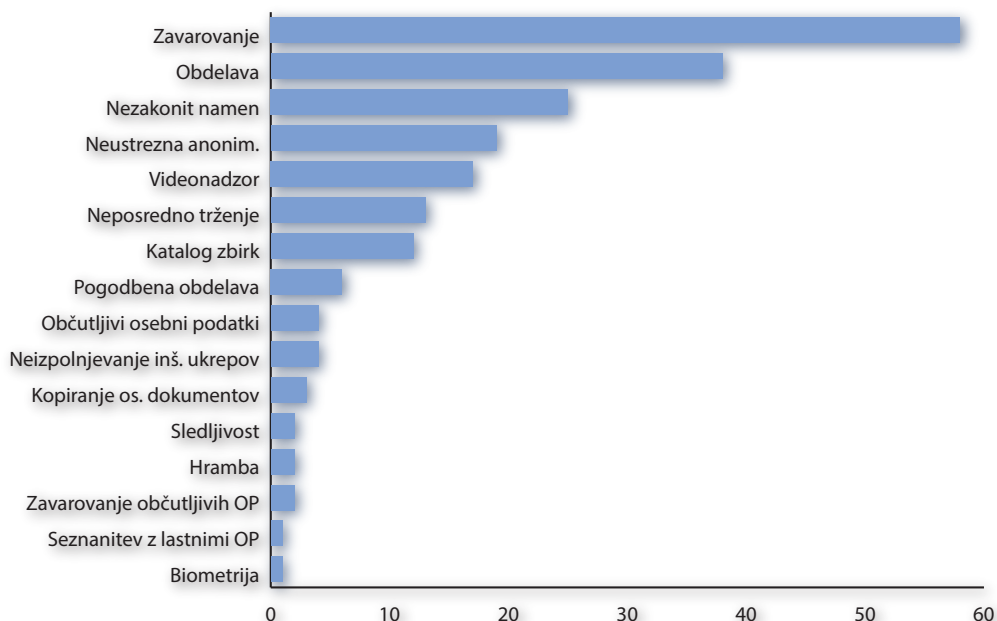
Kršitve (v okviru enega postopka je lahko več kršitev) so zadevale:

- neustrezno zavarovanje osebnih podatkov (24. in 25. člen ZVOP-1) – 58,
- nezakonito obdelavo osebnih podatkov (8. člen ZVOP-1) – 38,
- nezakonit namen zbiranja in nadaljnje obdelave osebnih podatkov (16. člen ZVOP-1) – 25,
- posredovanje neustrezno anonimiziranih podatkov za znanstveno-raziskovalne namene (17. člen ZVOP-1) – 19,
- kršitve določb v zvezi z izvajanjem videonadzora (74., 75., 76. in 77. člen ZVOP-1) – 17,
- kršitve določb o neposrednem trženju (72. in 73. člen ZVOP-1) – 13,
- nepravilnosti v zvezi z vzpostavitvijo katalogov zbirk osebnih podatkov in posredovanjem podatkov v register zbirk osebnih podatkov (26. in 27. člen ZVOP-1) – 12,
- neustrezno urejeno pogodbeno obdelavo osebnih podatkov (11. člen ZVOP-1) – 6,

⁴⁹ Uradni list RS, št. 29/2011 – uradno prečiščeno besedilo 8 s spremembami; v nadaljevanju ZP-1.

- nezakonito obdelavo občutljivih osebnih podatkov (13. člen ZVOP-1) – 4,
- neizpolnjevanje ukrepov, izrečenih v postopkih inšpekcijskega nadzora, kršitve določb ZIN – 4,
- nezakonito kopiranje osebnih dokumentov (4.a člen ZPLD in 4. člen ZOIzk) – 3,
- neustrezno sledljivost posredovanja osebnih podatkov (tretji odstavek 22. člena ZVOP-1) – 2,
- neustrezen rok hrambe osebnih podatkov (21. člen ZVOP-1) – 2,
- neustrezno zavarovanje občutljivih osebnih podatkov (14. člen ZVOP-1) – 2,
- neustrezno ravnanje v primeru prejema zahteve za seznanitev z lastnimi osebnimi podatki (31. člen ZVOP-1) – 1,
- nezakonito izvajanje biometrijskih ukrepov (80. člen ZVOP-1) – 1.

Slika 11: Najpogostejše kršitve določb ZVOP-1 leta 2017.



Leta 2017 je Informacijski pooblaščenec prejel 11 sodb, s katerimi so okrajna sodišča odločila o zahtevah za sodno varstvo, ki so jih storilci vložili zoper odločbe o prekrških v letih 2016 in 2017:

- zahteva za sodno varstvo je bila zavrtnjena kot neutemeljena, odločba Informacijskega pooblaščenca pa potrjena – 7,
- zahtevi za sodno varstvo je bilo ugodeno v delu, ki se nanaša na izrečeno sankcijo, tako da se je storilec za prekršek spremenila sankcija ali višina globe, sicer je bila zahteva za sodno varstvo zavrtnjena kot neutemeljena – 3,
- odločba Informacijskega pooblaščenca je bila spremenjena tako, da sta se dva prekrška združila v enega, sankcija (globa) pa je ostala ista – 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 2017 izdal 1.289 pisnih mnenj in napatitev na mnenja. Če je posameznik zastavil vprašanje, na katerega je Informacijski pooblaščenec v preteklosti že odgovoril, ga je Informacijski pooblaščenec namreč le napatil na mnenje, objavljeno na spletni strani.

Na spletni strani Informacijskega pooblaščenca je objavljenih okoli 2.500 mnenj in posamezniki lahko tam najdejo odgovore na številna vprašanja. Informacijski pooblaščenec izdane mnenja razvršča na 48 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/iskalniki-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 2017 so državni nadzorniki sprejeli 1.998 klicev; Informacijski pooblaščenec je skupno svetoval skoraj 3.300 posameznikom.

Slika 12: Mnenja Informacijskega pooblaščenca leta 2017.

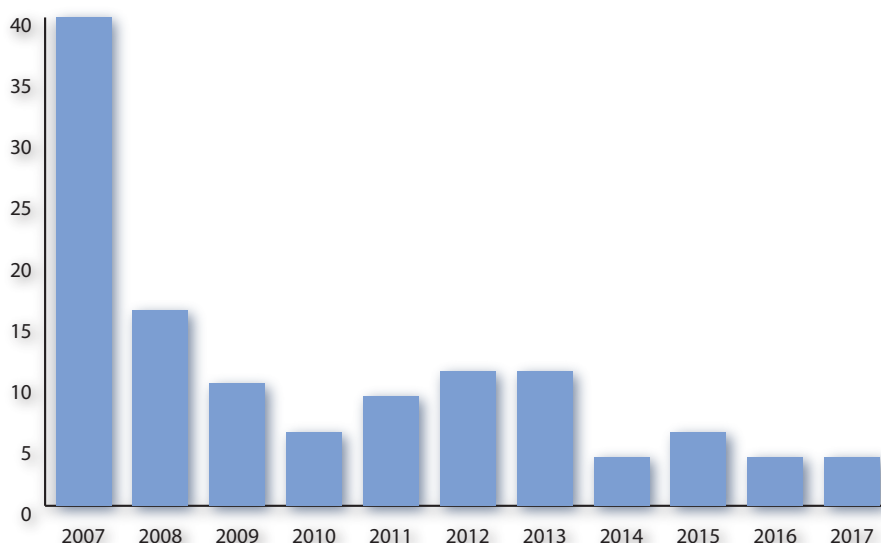


3.4. Dopustnost izvajanja biometrijskih ukrepov

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, ugotoviti predvsem, 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 ugotavlja, ali bi namen, ki ga zasleduje vlagatelj, ta lahko dosegel s postopki in ukrepi, ki manj posegajo v zasebnost zaposlenih oziroma ne vključujejo biometrijskih ukrepov. Slednji namreč 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 ti ukrepi 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 2017.



Informacijski pooblaščenec je leta 2017 prejel štiri vloge za izdajo dovoljenja za uvedbo biometrijskih ukrepov, izdal je eno odločbo.

Informacijski pooblaščenec je zahtevi vlagatelja delno ugodil in mu za namen varovanja ljudi dovolil izvajanje biometrijskih ukrepov z uporabo čitalnika prstnih odtisov, in sicer nad zaposlenimi, ki imajo pooblastilo za vstop v prostore radiografskega laboratorija. Po preučitvi vlagateljnih navedb je Informacijski pooblaščenec zaključil, da je varnost ljudi tako pomembna, da odtehta poseg v informacijsko zasebnost zaposlenih, ki ga predstavlja izvajanje biometrijskih ukrepov. Pri tem je upošteval predvsem obseg morebitnih negativnih posledic nepooblaščenega vstopa v laboratorij, saj bi iznos radioaktivnih snovi lahko imel zelo resne posledice tudi za širše okolje oziroma življenje in zdravje širšega kroga posameznikov. Radiografski laboratorij zato predstavlja posebno varovano območje, za varnost katerega je vlagatelj upravičen in dolžan sprejeti in izvajati ukrepe, s katerimi bo to območje kar najučinkoviteje zavaroval. Takšno varovanje nalagata tudi Zakon o varstvu pred ionizirajočimi sevanji in jedrski varnosti⁵⁰ ter Pravilnik o fizičnem varovanju jedrskih objektov, jedrskih in radioaktivnih snovi ter prevozov jedrskih snovi, ki vlagatelju sicer ne dajeta neposredne pravne podlage za izvajanje biometrijskih ukrepov, a ju je po mnenju Informacijskega pooblaščenca vsekakor treba upoštevati pri oceni občutljivosti območja radiografskega laboratorija in pri presoji ukrepov, potrebnih za njegovo zavarovanje. Med ukrepe, s katerimi se lahko v veliki meri poveča učinkovitost varstva takega posebej pomembnega in varnostno občutljivega območja, spadajo tudi biometrijski ukrepi.

Vlagatelj bo poleg nadzora dostopa do radiografskega laboratorija z biometrijskimi ukrepi zbiral tudi podatke o tem, koliko časa se je kateri od zaposlenih, ki so pooblaščen za vstop v laboratorij, nahajal v njem. Zaposleni so v laboratoriju izpostavljeni določeni stopnji radioaktivnega sevanja, zato je nujno zagotoviti, da se v teh prostorih nahajajo samo omejen čas, saj bi v nasprotnem primeru sevanje lahko škodljivo vplivalo na njihovo zdravje. Informacijski pooblaščenec je vlagatelja opozoril, da lahko v podatke o času vstopa v laboratorij in izstopa iz njega vpogleduje ali jih drugače nadalje obdeluje zgolj za namen, za katerega je bilo izvajanje biometrijskih ukrepov dovoljeno, tj. če je to potrebno za zagotavljanje varnosti konkretnega zaposlenega, ne pa za druge namene (npr. za nadzor nad delovnim časom posameznega zaposlenega, saj ne gre za evidentiranje prisotnosti zaposlenih na delovnem mestu v smislu registracije njihovega delovnega časa). Informacijski pooblaščenec je ocenil, da je nameravano izvajanje biometrijskih ukrepov v skladu z načelom sorazmernosti, saj se bodo ti ukrepi izvajali le nad ožjim krogom zaposlenih pri vlagatelju, ki so v okviru opravljanja svojih del in nalog pri vlagatelju izrecno pooblaščen za dostopanje do varovanega radiografskega laboratorija.

Vlagateljova zahteva je bila zavržena 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. Prvi odstavek 80. člena ZVOP-1 namreč izrecno določa, da je izvajanje teh ukrepov mogoče dopustiti zgolj nad zaposlenimi pri subjektu, ki bi te ukrepe želel izvajati, ne pa tudi nad drugimi posamezniki, ki s takim subjektom niso v delovnem razmerju. Taki posamezniki bodo zato v prostore vlagatelja lahko vstopali samo v spremstvu zaposlenih, ki so pooblaščen za dostop do teh prostorov.

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

⁵⁰ Uradni list RS, št. 60/2011.

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.

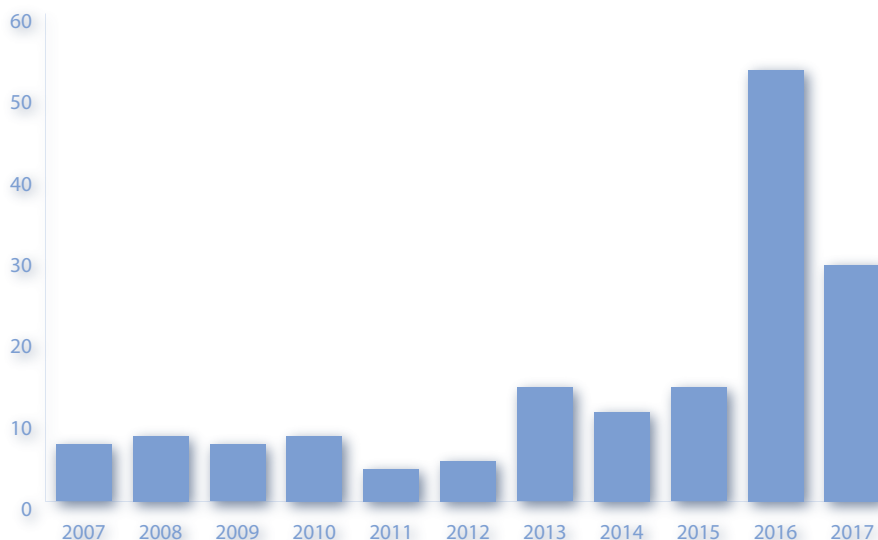
Informacijski pooblaščenec je leta 2017 prejel 29 vlog za iznos osebnih podatkov. En vlagatelj je vlogo umaknil, zato je Informacijski pooblaščenec postopek s sklepom ustavil, vsem ostalim je iznos osebnih podatkov dovolil. Izdal je 34 odločb, šest za vloge, vložene leta 2016:

- 25 družbam je dovolil, da osebne podatke iznašajo in posredujejo svojim pogodbenim obdelovalcem v tretjih državah, in sicer v ZDA, kamor bo osebne podatke iznašala večina družb, Indijo, Avstralijo, Srbijo, Združene arabske emirate, Turčijo, Maroko in na Filipine. Podatki, ki jih bodo iznašali, se nanašajo na zaposlene in njihove sorodnike, kandidate za zaposlitev, goste, kupce, dobavitelje, paciente in zdravstvene delavce, ki sodelujejo v kliničnih in drugih medicinskih raziskavah, uporabnike farmacevtskih proizvodov, ki poročajo o neželenih učinkih, in uporabnike kartic, ki opravljajo storitve na bankomatih. Nameni iznosa osebnih podatkov, ki so jih navedle družbe, so npr. uporaba storitev v oblaku, izvajanje kliničnih raziskav, spremljanje farmakovigilance, koriščenje platforme za merjenje izkušenj in zadovoljstva strank, gostovanje sistema in hramba podatkov, zagotavljanje pomoči uporabnikom, uporaba orodja za zagotavljanje stroškovne učinkovitosti, upravljanje in gostovanje aplikacij za razvoj človeških virov, IT-sistemov in spletnih strani, centralizirano izvajanje nadzora nad bankomati, analiza dostopov v različne IT-sisteme zaradi preprečevanja zunanjih napadov.
- Osmim družbam je dovolil, da drugim upravljavcem osebnih podatkov v ZDA posredujejo osebne podatke zaposlenih (sedanjih in nekdanjih) in kandidatov za zaposlitev, poslovnih partnerjev (zastopnikov, posrednikov, prodajalcev, dobaviteljev), kupcev, zdravnikov, farmacevtov in drugih zdravstvenih delavcev ter pacientov, ki sodelujejo v kliničnih raziskavah, za namene upravljanja s človeškimi viri oziroma kadri, priprave statističnih in drugih podatkov, upravljanja odnosov s strankami in izvajanja centralne poslovne in informacijsko-tehnične politike zaradi povečanja učinkovitosti in izboljšanja storitev.
- Eni družbi je dovolil, da po prejemu odločbe povezanim družbam znotraj mednarodne skupine družb, katere članica je, iznaša in posreduje osebne podatke subjektov kliničnih in drugih znanstvenih raziskav, pacientov, na katere se nanašajo poročila o neželenih učinkih, in posameznikov, ki poročajo o neželenih učinkih, osebne podatke raziskovalcev ter drugih znanstvenikov in osebja, zdravstvenih delavcev, strokovnjakov s področja industrije, bodočih, sedanjih in bivših zaposlenih in njihovih vzdrževanih članov, delavcev, ki delo opravljajo na podlagi podjemnih, avtorskih in drugih pogodb, ponudnikov storitev in poslovnih partnerjev, vlagateljev in delničarjev, dobaviteljev in prodajalcev, in sicer z namenom izvajanja raziskav in drugih proizvodnih namenov, zagotavljanja zdravstvenih storitev in rešitev, iz komercialnih namenov ter z namenom korporativne podpore.

Informacijski pooblaščenec pojasnjuje, da je tudi leta 2017 veliko število vlog (leta 2016 jih je bilo 53) za pridobitev dovoljenja za iznos osebnih podatkov 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 v ZDA. Ker je Informacijski pooblaščenec pri odločanju o ustrezni ravni varstva osebnih podatkov v skladu s 67. členom ZVOP-1 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 izdal odločbo, s katero je 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), kar lahko preverijo na seznamu, objavljenem na <https://www.privacyshield.gov/article?id=How-to-Verify-an-Organization-s-Privacy-Shield-Commitments>. Informacijski pooblaščenec je pri svoji odločitvi upošteval Izvedbeni sklep Evropske Komisije (EU) št. 2016/1250 na podlagi Direktive Evropskega parlamenta

in Sveta 95/46/ES o ustreznosti varstva, ki ga zagotavlja zasebnostni ščit EU–ZDA (notificirano pod dokumentarno številko C(2016) 4176) z dne 12. 7. 2016, po katerem se šteje, da ZDA zagotavljajo ustrezno raven varstva osebnih podatkov v delu, ko gre za iznos osebnih podatkov, ki se v okviru zasebnostnega ščita EU–ZDA prenašajo iz EU samocertificiranim organizacijam v ZDA.

Slika 14: Število vlog za izdajo odločbe glede iznosa osebnih podatkov med letoma 2007 in 2017.



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 ta 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. Zbirke 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 2017 prejel 16 vlog za pridobitev dovoljenja za povezovanje zbirk osebnih podatkov. Izdal je 12 odločb, 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 notranje zadeve je dovolil, da Evidenco imetnikov službene izkaznice nadzornika smučišča poveže s Centralnim registrom prebivalstva. Povezava med zbirkama se lahko izvede tako, da se kot povezovalni znak uporabita EMŠO in osebno ime.

2. Ministrstvu za finance, Uradu RS za preprečevanje pranja denarja, je dovolil, da Evidenco podatkov o osebah in transakcijah, Evidenco o prejetih pobudah, Evidenco obvestil in informacij ter Evidenco mednarodnih zaprosil, ki jih vodi na podlagi Zakona o preprečevanju pranja denarja

in financiranja terorizma, neposredno računalniško poveže:

- s Centralnim registrom prebivalstva, katerega upravljavec je Ministrstvo za notranje zadeve,
- z Registrom nepremičnin, Zemljiškim katastrom in Katastrom stavb, katerih upravljavec je Geodetska uprava RS.

Kot povezovalni znak se uporabi EMŠO ali davčna številka.

3. Ministrstvu za notranje zadeve je dovolil, da Evidenco nadomestil in služnosti v javno korist poveže s Centralnim registrom prebivalstva. Povezava med zbirkama se izvede na podlagi EMŠO.

4. Ministrstvu za infrastrukturo je dovolil, da:

a) Evidenco o vozniških dovoljenih poveže z Evidenco potnih listin, Evidenco osebnih izkaznic in Centralnim registrom prebivalstva, katerih upravljavec je Ministrstvo za notranje zadeve;

b) Evidenco registriranih vozil poveže s Centralnim registrom prebivalstva, katerega upravljavec je Ministrstvo za notranje zadeve.

Neposredna računalniška povezava med zbirkami se vzpostavi tako, da se kot povezovalni znak uporabi EMŠO.

5. Ministrstvu za infrastrukturo, Upravi RS za pomorstvo, je dovolil, da zbirki osebnih podatkov Evidenca o listinah o usposobljenosti za upravljanje s čolni ter Evidenca pooblastil, ki se ne izdajajo v skladu z mednarodnimi konvencijami, neposredno računalniško poveže

- s Centralnim registrom prebivalstva, katerega upravljavec je Ministrstvo za notranje zadeve, ter
- z Evidenco vozniških dovoljenj, katere upravljavec je Ministrstvo za infrastrukturo.

Povezava med zbirkami se izvede na podlagi EMŠO.

6. Vrhovnemu sodišču RS je dovolil, da Informacijski sistem PUND neposredno računalniško poveže

- s Centralnim registrom prebivalstva, katerega upravljavec je Ministrstvo za notranje zadeve, in
- z Davčnim registrom, katerega upravljavec je Finančna uprava RS.

Kot povezovalni znak se uporabi EMŠO ali davčna številka.

7. Ministrstvu za okolje in prostor je dovolil, da Evidenco izvajanja dimnikarskih storitev neposredno računalniško poveže s Centralnim registrom prebivalstva, katerega upravljavec je Ministrstvo za notranje zadeve. Neposredna računalniška povezava med zbirkama se vzpostavi tako, da se kot povezovalni znak uporabi EMŠO.

8. Ministrstvu za delo, družino, socialne zadeve in enake možnosti je dovolil, da Evidenco izdanih invalidskih kartic ugodnosti, Evidenco sofinanciranja tehničnih pripomočkov, Evidenco prilagoditve vozila in Evidenco pridobitve psa pomočnika neposredno računalniško poveže s Centralnim registrom prebivalstva, katerega upravljavec je Ministrstvo za notranje zadeve. Neposredna računalniška povezava med zbirkami se izvede na podlagi EMŠO.

9. Kapitalski družbi pokojninskega in invalidskega zavarovanja je dovolil, da zbirko osebnih podatkov Evidenca zavarovancev – članov neposredno računalniško poveže s Centralnim registrom prebivalstva, katerega upravljavec je Ministrstvo za notranje zadeve. Kot povezovalni znak se uporabi EMŠO.

10. Ministrstvu za infrastrukturo je dovolil, da Evidenco subvencij prevoza neposredno računalniško poveže s:

- Centralnim registrom prebivalstva, katerega upravljavec je Ministrstvo za notranje zadeve,
- Centralno evidenco udeležencev vzgoje in izobraževanja (CEUVIZ), katere upravljavec je Ministrstvo za izobraževanje, znanost in šport, in
- Evidenčnim in analitskim informacijskim sistemom visokega šolstva v Republiki Sloveniji (eVŠ), katerega upravljavec je Ministrstvo za izobraževanje, znanost in šport.

Neposredna računalniška povezava med zbirkami se vzpostavi na podlagi EMŠO.

11. Ministrstvu za izobraževanje, znanost in šport je dovolil, da zbirki osebnih podatkov Evidenčni in analitski sistem visokega šolstva Republike Slovenije – Evidenca študentov in diplomantov (eVŠ-EŠD) ter Centralna evidenca udeležencev vzgoje in izobraževanja (CEUVIZ) neposredno računalniško poveže

- s »Clani_msk«, katere upravljavec je Mladinski servis, pomurski študentski servis, d. o. o., in

- z Zbirko podatkov o študentih in dijakih, katere upravljavec je ŠS, d. o. o. Kot povezovalni znak se uporabi EMŠO.

12. Agenciji RS za javnopravne evidence in storitve je dovolil, da Register dejanskih lastnikov neposredno računalniško poveže

- s Centralnim registrom prebivalstva, katerega upravljavec je Ministrstvo za notranje zadeve, in
- z Davčnim registrom, katerega upravljavec je Finančna uprava RS.

Povezava med zbirkami se vzpostavi na podlagi EMŠO.

Slika 15: Število vlog za izdajo odločbe glede povezljivosti zbirk osebnih podatkov med letoma 2006 in 2017.



3.7. Pravica do seznanitve z lastnimi osebnimi podatki

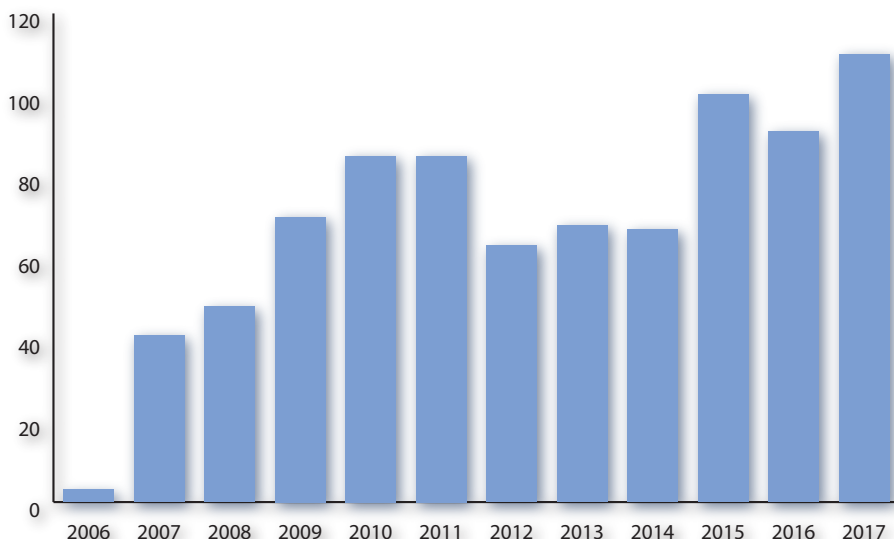
Pravica posameznika do seznanitve z lastnimi osebnimi podatki je ustavna pravica, določena v 38. členu Ustave RS in konkretizirana v 30. (vsebina pravice) in 31. členu (postopek seznanitve) ZVOP-1. V skladu s prvim odstavkom 30. člena ZVOP-1 mora vsak upravljavec osebnih podatkov posamezniku na njegovo 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 vložiti pritožbo pri Informacijskem pooblaščenca.

Informacijski pooblaščenec je leta 2017 prejel 110 pritožb v zvezi s pravico do seznanitve z lastnimi osebnimi podatki. V okviru teh pritožbenih postopkov je reševal tudi pritožbe posameznikov zaradi kršitve Zakona o pacientovih pravicah⁵¹, in sicer pritožbe pacientov in drugih upravičenih oseb v zvezi s seznanitvijo z lastno zdravstveno dokumentacijo (41. člen ZPacP) ter pritožbe uporabnikov v zvezi s seznanitvijo z zdravstveno dokumentacijo po pacientovi smrti (42. člen ZPacP).

⁵¹ Uradni list RS, št. 15/2008, s spremembami; v nadaljevanju ZPacP.

Vložene pritožbe so v 40 primerih zadevale državne organe (ministrstva in organe v njihovi sestavi, sodišča), v 21 primerih zdravstvene ustanove, v 11 primerih vzgojno-izobraževalne ustanove, v desetih primerih centre za socialno delo, preostale pritožbe pa so se nanašale na različne upravljavce osebnih podatkov, predvsem iz zasebnega sektorja.

Slika 16: Število pritožb v zvezi s pravico do seznanitve z lastnimi osebnimi podatki med letoma 2006 in 2017.



Informacijski pooblaščenec je poleg več zadev iz leta 2016 rešil 78 zadev, prejetih v letu 2017. Pri tem je izdal 11 odločb, pri čemer je v dveh pritožbam posameznikov v celoti ugodil, v petih pa delno. Vsi upravljavci so odločbe izvršili in posameznikom posredovali zahtevane dokumente oziroma podatke. S štirimi odločbami je pritožbe posameznikov zoper obvestila, ki so jim jih posredovali upravljavci osebnih podatkov, kot neutemeljene zavrnil, zoper eno zavrnilno odločbo je posameznik vložil tožbo na Upravno sodišče RS. Ostale pritožbe so bile večinoma rešene na način izdaje nezavezujočih predlogov za ravnanje, pojasnil (predhodnih mnenj, obvestil) in zavezujočih pozivov ter zaključene z uradnimi zaznamki. Tri pritožbe je Informacijski pooblaščenec zavrgel s sklepom (zaradi postopkovnih pomanjkljivosti), pet pa jih je odstopil v reševanje pristojnim organom.

3.8. 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 sodišču⁵², 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.

3.8.1. Zahteva za oceno ustavnosti Zakona o Slovenski obveščevalno-varnostni agenciji⁵³

Informacijski pooblaščenec je vložil zahtevo za oceno ustavnosti prvega in tretjega odstavka 21. člena ZSOVA zaradi neskladja z 2., 15., 37. in 38. členom Ustave RS. Prvi odstavek določa, da spremljanje mednarodnih sistemov zvez ter tajni nakup dokumentov in predmetov dovoljuje direktor agencije s pisno odredbo, tretji odstavek pa določa, da se spremljanje mednarodnih sistemov zvez ne sme nanašati na določljiv priključek telekomunikacijskega sredstva ali na določenega uporabnika tega priključka na območju Republike Slovenije.

⁵² Uradni list RS, št. 64/2007 – uradno prečiščeno besedilo 1, s spremembami; v nadaljevanju ZUstS.

⁵³ Uradni list RS, št. 81/2006 – uradno prečiščeno besedilo 2; v nadaljevanju ZSOVA.

Informacijski pooblaščenec je zoper Slovensko obveščevalno-varnostno agencijo (SOVA) v letu 2013 po uradni dolžnosti uvedel postopek inšpekcijskega nadzora z namenom preveriti, ali obdelava osebnih podatkov pri spremljanju sistemov mednarodnih zvez, ki jo urejajo določbe 21. člena ZSOVA, poteka skladno z določbami ZVOP-1. Informacijski pooblaščenec je v okviru inšpekcijskega nadzora ugotovil, da zaradi domnevne neustavnosti dela ZSOVA do njegove ustrezne spremembe inšpekcijskega postopka ne more učinkovito zaključiti. Podrobnosti postopka zaradi tajnosti obravnavanih podatkov ne more razkriti.

Problematika nadzora oziroma spremljanja komunikacij v mednarodnem elektronskem komunikacijskem omrežju je aktualna že vrsto let. Kljub večkratnim pozivom Informacijskega pooblaščenca do sprememb ZSOVA še ni prišlo. Obenem pa tudi iz neuradno javno objavljenega osnutka sprememb zakona ni razbrati, da bodo (po mnenju Informacijskega pooblaščenca neustavni vidiki pooblastil SOVA glede zbiranja in obdelave osebnih podatkov) v bližnji prihodnosti zakonsko ustrezno urejeni. Zato je Informacijski pooblaščenec Ustavnemu sodišču, upoštevajoč zahteve 8. člena Evropske konvencije o človekovih pravicah (EKČP), znova predlagal, da razveljavi prvi in tretji odstavek 21. člena ZSOVA.

Določba prvega odstavka 21. člena ZSOVA je po oceni Informacijskega pooblaščenca v neskladju z drugim odstavkom 37. člena Ustave RS, ker:

1. za poseg v pravico do informacijske in komunikacijske zasebnosti (določljivih in nedoločljivih posameznikov – državljanov RS ali tujcev, če se oseba nahaja izven območja Republike Slovenije oziroma tam uporablja priključek) s strani državnega organa z ukrepom spremljanja mednarodnih sistemov zvez ni zahtevana predhodna sodna odločba, pač pa zadostuje že pisna odredba direktorja SOVA;
2. ni navedenih razlogov, ki bi sploh omogočali nujen preizkus, ali je bil poseg dopusten, ker naj bi bil nujen, potreben in primeren za varnost države.

Določba tretjega odstavka 21. člena ZSOVA pa je po oceni Informacijskega pooblaščenca v neskladju z 2., 15., 37. in 38. členom Ustave, ker:

1. poseg v pravico do informacijske in komunikacijske zasebnosti z ukrepom spremljanja mednarodnih sistemov zvez v zakonu ni določen tako, da bi omogočal jasne in preverljive pogoje, okoliščine in razloge, pod katerimi je ta poseg (in s tem tudi obdelava osebnih podatkov) dopusten in zakonit;
2. ni nedvoumno in jasno določeno, v kakšnih razmerah in na kakšen način se ta poseg lahko opravi;
3. ni določenih časovnih omejitev posega, ki bi se lahko razlikoval glede na različnost okoliščin;
4. ni določena omejitev roka hrambe tako pridobljenih prometnih podatkov in zapisov komunikacij.

Po ustaljeni ustavnosodni presoji pomeni vsako zbiranje in obdelovanje osebnih podatkov poseg v pravico do varstva zasebnosti oziroma v pravico posameznika, da obdrži informacije o sebi, ker noče, da bi bili z njimi seznanjeni drugi. Temeljna vrednostna podstat te pravice je spoznanje, da ima posameznik pravico zadržati informacije o sebi zase in da je v izhodišču on tisti, ki odloča, koliko informacij o sebi bo razkril in komu. Vendar pravica do informacijske zasebnosti ni neomejena, ni absolutna. Zato mora posameznik sprejeti omejitve informacijske zasebnosti oziroma dopustiti posege vanjo v prevladujočem splošnem interesu in ob izpolnjevanju ustavno določenih pogojev. Poseg je dopusten pod pogoji iz tretjega odstavka 15. člena in 2. člena Ustave. Ustava zakonodajalcu izrecno nalaga, da mora vsako materijo posega v zasebnost ne le zakonsko urediti, ampak da mora to urediti določno in nedvoumno, izključena mora biti vsaka možnost arbitrarnega odločanja državnega organa.

Po mnenju Informacijskega pooblaščenca ZSOVA v delu, ki določa zakonsko pooblastilo SOVA za spremljanje mednarodnih sistemov zvez, tem načelom ne zadosti. Pojem »spremljanje mednarodnih sistemov zvez« je namreč nedefiniran in ne določa, kje se nadzor izvaja oziroma kje je mesto telekomunikacijskega priključka in mesto priklopa. Prav tako ne pojasni, ali je zakonsko dopustno nadzorovati vse mednarodne zveze, do katerih ima lahko dostop SOVA, ali je npr. zakonsko dopustno prestrezati vse komunikacije na komunikacijskih vodih, ki potekajo čez Slovenijo, dokler gre za komunikacije tujih državljanov. Posledično je stopnja spoštovanja ene

od temeljnih pravic odvisna zgolj od proste presoje SOVA in njene izvedbe predpisa, kar z vidika predvidljivosti posegov v ustavno varovane pravice in 2. člena Ustave RS ni sprejemljivo.

Varstvo t. i. prometnih podatkov o komunikaciji (npr. podatkov o osebnem imenu, telefonski številki in času komunikacije) in vsebine zapisa pogovora je dejansko dvojno. Dvojno varstvo v tem primeru pomeni, da so na ta način zbrani podatki varovani ne le na podlagi 38. člena Ustave RS, temveč tudi na podlagi 37. člena Ustave RS. Do zbiranja osebnih podatkov namreč v tem primeru dejansko ne more priti brez posega v komunikacijsko zasebnost. Če naj se torej zagotovi zakonito zbiranje osebnih podatkov, mora biti zakonit in ustavno skladen najprej poseg v komunikacijo zasebnost, ki je omogočil samo zbiranje osebnih podatkov. To pa pomeni, da mora biti v skladu s pogoji iz drugega odstavka 37. člena Ustave RS, ki določa, da lahko samo zakon predpiše, da se na podlagi odločbe sodišča za določen čas ne upošteva varstvo tajnosti pisem in drugih občil ter nedotakljivost človekove zasebnosti, če je to nujno za uvedbo ali potek kazenskega postopka ali za varnost države, pri čemer morajo biti izpolnjeni navedeni štirje osnovni pogoji za omejitev te pravice. Namen tega varstva je preprečiti, da bi se kdor koli seznanil z vsebino posredovanega poročila. Prav tako pa ta pravica zagotavlja svobodo komuniciranja, ki se izraža kot svobodna odločitev posameznika o tem, komu in kako bo določeno sporočilo posredovano, iz česar izhajajo prepovedi nesorazmernih poseganj v posameznikovo odločitev, kako, kdaj in s kom bo komuniciral.

Evropsko sodišče za človekove pravice (ESČP) je v sodbi Zakharov proti Rusiji z dne 4. 12. 2015 glede varstva pri posegih v informacijsko in komunikacijsko zasebnost s strani države odločilo, da že sam obstoj zakonodaje, ki omogoča poseg v zasebnost s prikritim prestrezanjem komunikacij, a ne omogoča učinkovitega pravnega sredstva osebi, ki sumi, da se poseg zoper njo izvaja, predstavlja poseg v pravico do zasebnosti po 8. členu EKČP. ESČP se je pri oceni, ali postopki dopuščanja tajnega nadzora niso odredeni samovoljno, nezakonito ali brez ustrezne in primerne obravnave, osredotočilo predvsem na vprašanja, kateri organ je pristojen za odreditev nadzora, kakšen je obseg nadzora teh postopkov in vsebine pooblastil za prestrezanje komunikacij.

Vse to pa je relevantno tudi v primeru pooblastil za spremljanje mednarodnih sistemov zvez na podlagi 21. člena ZSOVA. Pri tem je ESČP postavilo rigorozne standarde za dopustnost množičnega nadzora telekomunikacij za obveščevalske namene. Zahteve ESČP bi lahko strnili v naslednje točke:

- Zakonodaja države mora zamejiti prisluškovalne aktivnosti tako, da ne bo mogoč »strateški nadzor« komunikacij (vseh relevantnih telefonskih števil oziroma priključkov v neki zadevi), ampak da se bo ciljalo na individualizirane osebe oziroma telefonske priključke.
- Prisluškovanje se lahko začne šele po zunanji odobritvi, ki mora biti vsebinska in ne zgolj formalna, in mora temeljiti vsaj na navedbi razlogov, zakaj je prisluškovanje določeni osebi oziroma številki v posamični zadevi pomembno in primerno. »Interne« odobritve s strani direktorja varnostno-obveščevalne agencije, pravosodnega ministra, notranjega ministra idr. ne zadostujejo, ker so vse del izvršne veje oblasti in s tem nezdržljivo povezane z obveščevalnimi agencijami.
- Neposredni nadzor telekomunikacijskih vodov s strani obveščevalcev mora zagotavljati ustrezne in učinkovite varovalke zoper zlorabe.
- Zakonodaja mora jasno in predvidljivo določati pogoje, kdaj je tajni nadzor s strani države dopusten.

Na ustavno sporno zakonsko ureditev v ZSOVA sta z vložnima zahtevama za presojo ustavnosti v preteklosti že opozorila tako Informacijski pooblaščenec kot tudi predsednik Vrhovnega sodišča RS, a žal ni prišlo do vsebinske odločitve, saj je Ustavno sodišče obe zahtevi zavrglo. Na to, da mora redno ocenjevanje delovanja in legitimnosti okvirov, s katerimi se ureja dejavnost obveščevalnih služb, postati sestavni del sistema nadzora, pa v svojem poročilu o analizi »Nadzora, ki ga izvajajo obveščevalne službe: zaščitni ukrepi in pravna sredstva v zvezi s temeljnimi pravicami v Evropski uniji« opozarja tudi Agencija Evropske unije za temeljne pravice.

3.8.2. Zahteva za oceno ustavnosti Zakona o nalogah in pooblastilih policije (ZNPPol-A)

Informacijski pooblaščenec je ugotovil, da novela Zakona o nalogah in pooblastilih policije (ZNPPol-A), kot jo je Državni zbor RS sprejel dne 17. 2. 2017, kljub mnogim opozorilom v številnih vidikih ni usklajena z Ustavo RS in ZVOP-1, na kar je poleg Informacijskega pooblaščenca opozarjal tudi Varuh človekovih pravic (Varuh).

Ključne vsebine, ki so po mnenju Informacijskega pooblaščenca z vidika 35. in 38. člena Ustave RS sporne predvsem zato, ker predstavljajo uzakonitev nesorazmernega poseganja v zasebnost vseh posameznikov s strani organov pregona, so:

- splošna dopustnost zbiranja biometrijskih podatkov – 39. člen ZNPPol-A (dopolnitev 112. člena ZNPPol),
- zbiranje podatkov o vseh letalskih potnikih – 40. člen ZNPPol-A (nov 112.a člen ZNPPol),
- optična prepoznavna registrskih tablic – 41., 46. in 49. člen ZNPPol-A (dopolnitve 113., 125. in 128. člena ZNPPol),
- uporaba brezpilotnih letalnikov – 42. člen ZNPPol-A (nov 114.a člen ZNPPol).

Informacijski pooblaščenec je še zlasti zaskrbljen, ker:

- se nova pooblastila policije uvajajo brez učinkovitih zakonskih varovalk za njihovo uporabo;
- navedena nova pooblastila nediskriminatorno nesorazmerno posegajo v ustavne pravice vseh posameznikov;
- nobena demokratična družba ne bi smela uzakoniti uporabe policijskih pooblastil, ki omogočajo množični nadzor, na način, da je njihova sorazmerna in zakonita uporaba prepuščena prosti presoji posameznega policista; vedno je treba z zakonom določiti jasne pogoje, ki ne omogočajo širokih interpretacij dopustnosti uporabe takšnih pooblastil;
- posegi v zasebnost, ki jih izpostavlja pooblastila omogočajo, zahtevajo ustrezne učinkovite zakonske varovalke za preprečevanje morebitnih zlorab, saj za to zgolj splošen nadzor policije ne zadošča.

Ker Informacijski pooblaščenec ni izpolnil pogojev za podajo zahteve za začetek postopka za oceno ustavnosti po 23.a členu ZUstS (vprašanje ustavnosti ali zakonitosti se ni pojavilo v zvezi s postopkom, ki ga vodi) in ker lahko Varuh v skladu z istim členom poda zahtevo v trenutku, ko meni, da predpis ali splošni akt, izdan za izvrševanje javnih pooblastil, nedopustno posega v človekove pravice ali temeljne svoboščine, je Informacijski pooblaščenec Varuhu predlagal, naj vložijo zahtevo za oceno ustavnosti ZNPPol-A. S takojšnjo zahtevo za oceno ustavnosti in predlogom za začasno zadržanje izvrševanja ZNPPol-A s strani Varuha bi namreč lahko hitreje in predvsem takoj preprečili morebitne težko popravljive škodljive posledice za posameznike.

Varuh je vložil zahtevo za oceno ustavnosti ZNPPol-A, pri čemer je podrobno preučil ureditev, ki se je uveljavila z navedenim zakonom, in pri tem predvsem upošteval stališča Evropskega sodišča za človekove pravice, da je povečana pozornost pri varovanju zasebnega življenja nujna pri spoprijemanju z novimi komunikacijskimi tehnologijami, ki omogočajo hranjenje in reproduciranje osebnih podatkov, ter da mora razvoj metod nadzora z najnovejšimi tehnologijami spremljati simultani razvoj pravnih varovalk. Varuha je pri pripravi zahteve za oceno ustavnosti vodila tudi dosedanja praksa Ustavnega sodišča RS, v kateri izpostavlja, da mora zakonodajalec, ko gre za obdelavo osebnih podatkov za namene policijskega dela, še posebej skrbno pretehtati težo ukrepa, s katerim brez privolitve posameznika posega v občutljivo območje njegove zasebnosti.

Med bistvenimi spornimi dopolnitvami, ki jih v svoji zahtevi izpodbija Varuh, in na katere je ves čas opozarjal tudi Informacijski pooblaščenec, je uzakonitev pooblastila, ki policiji dopušča avtomatično preverjanje registrskih tablic s sistemom optične prepoznave. To pomeni, da lahko policija na ta način ne glede na kakršen koli sum nepravilnosti preverja vse, ki se na določen dan peljejo po določeni cesti mimo na policijskem vozilu nameščenih kamer. Gre za povsem drugačen ukrep, kot je rutinska kontrola določenega manjšega vzorca voznikov (brez suma), saj bo tako ob zadostnem številu kamer brez kakršnega koli razloga dejansko preverjeno izredno veliko število vozil. Enako velja za prekomerno preverjanje podatkov vseh prihajajočih letalskih potnikov, ki z letalom prihajajo v Slovenijo (PNR), skrb vzbujajoča pa je tudi uzakonitev široke uporabe brezpilotnih letalnikov brez ustrezne ocene učinkov na varstvo osebnih podatkov.

Informacijski pooblaščenec je v svojih opozorilih izpostavil še sporno znižanje pogojev za razpis ukrepa prikrite in namenske kontrole za posameznika v Schengenskem informacijskem sistemu, kar bi lahko povzročilo, da bodo na seznam vpisane tudi nedolžne osebe. Te bodo posledično ob vsakem potovanju znotraj EU deležne poostrelega policijskega nadzora brez kakršnega koli

pojasnila, zakaj je to potrebno. Prav tako ni sprejemljiva ureditev, ki daje splošno podlago za zbiranje biometrijskih podatkov (fotografiranje, odvzem prstnih odtisov, brisov idr.) vsakogar.

Informacijski pooblaščenec upa, da bo Ustavno sodišče pri obravnavi zahteve Varuha sledilo v Evropi in Sloveniji uveljavljenim visokim standardom glede zahtevanih varovalk ustavno varovane pravice do zasebnosti, ko gre za poseganje države in posebej organov pregona v to pravico.

3.9. Izbrani primeri kršitev varstva osebnih podatkov

V nadaljevanju je predstavljenih 10 odločitev Informacijskega pooblaščenca v postopkih, ki jih je vodil leta 2017.

3.9.1. Neustrezno zavarovanje dokumentacije, namenjene uničenju

Informacijski pooblaščenec je na podlagi obvestila, da je bilo v okolici določenega skladišča najdenih več zdravniških receptov, zaradi suma neustreznega zavarovanja osebnih podatkov uvedel postopek inšpekcijskega nadzora zoper lastnika skladišča (zavezanec). V skladu s 24. členom ZVOP-1 zavarovanje osebnih podatkov namreč obsega organizacijske, tehnične in logično-tehnične postopke in ukrepe, s katerimi se varujejo osebni podatki, preprečuje naključno ali namerno nepooblaščenno uničevanje podatkov, njihova sprememba ali izguba ter nepooblaščen obdelava teh podatkov tako, da se med drugim zagotavlja tudi učinkovit način njihovega uničenja.

Državni nadzornik za varstvo osebnih podatkov je opravil ogled zavezančevih prostorov ter se seznanil s postopkom prevzema in uničenja odpadnega papirja, v dokazne namene pa je zasegel več najdenih receptov. Zavezanec je pojasnil, da postopek uničenja zaupne dokumentacije predvideva takojšnje baliranje v skladišču, kjer je stiskalnica, alternativno pa hrambo v skladišču v zaprtem kontejnerju s ključavnico in pod videonadzorom do odvoza na uničenje v mlin. Bale stisnjene papirja so povezane z žico, kar avtomatsko naredi stroj, do prevoza na uničenje v Ljubljano, običajno še isti dan, pa so shranjene na določenem mestu v skladišču. Uničenje dokumentacije je bilo v konkretnem primeru sicer izvedeno skladno z zavezančevimi pravili, vendar je zaradi tehnične napake (počena žica na bali) veter raznesel nekaj dokumentacije po javni cesti ob skladišču in po dvorišču skladišča. V izogib morebitnim podobnim težavam je zavezanec takoj spremenil postopek uničenja zaupne dokumentacije tako, da je opustil stiskanje in baliranje; v dokaz je predložil spremenjen »Protokol za prevzem odpadnega papirja in zaupne papirne dokumentacije«, s katerim je seznanil vse zaposlene v skladišču, ki so bili seznanjeni tudi z internim aktom o zavarovanju osebnih podatkov.

Ker je bil zavezanec pogodbeni obdelovalec osebnih podatkov, je Informacijski pooblaščenec uvedel postopek inšpekcijskega nadzora tudi zoper lekarno kot upravljavca osebnih podatkov, ki so bili predani v uničenje. V skladu s 7. točko 6. člena ZVOP-1 je pogodbeni obdelovalec fizična ali pravna oseba, ki obdeluje osebne podatke v imenu in na račun upravljavca osebnih podatkov. Pogodbena obdelava osebnih podatkov ureja 11. člen ZVOP-1, ki med drugim določa, da lahko upravljavec osebnih podatkov posamezna opravila v zvezi z obdelavo osebnih podatkov (v skladu s 3. točko 19. člena ZVOP-1 tudi uničenje osebnih podatkov pomeni njihovo obdelavo) s pogodbo zaupa pogodbenemu obdelovalcu, ki je registriran za opravljanje takšne dejavnosti ter zagotavlja ustrezne postopke in ukrepe iz 24. člena tega zakona, 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, katerih izvajanje mora upravljavec osebnih podatkov nadzorovati.

Ugotovljeno je bilo, da je lekarna zunanjemu izvajalcu pisno odredila, da na podlagi izdane naročilnice zavezancu odda v uničenje recepte in drugo dokumentacijo iz arhiva, ki ji je pretekel rok hrambe, pri čemer pa z zavezancem kot pogodbenim obdelovalcem ni sklenila pisne pogodbe v skladu z 11. členom ZVOP-1. Pogodba, ki jo je lekarna sklenila z zunanjim izvajalcem za izvedbo storitev vzdrževanja arhiva receptov ter oddaje in prevzema materiala, ni vsebovala določb oziroma dogovora o postopkih in ukrepih iz 24. člena ZVOP-1, kot je predpisano v drugem odstavku 11. člena ZVOP-1, je pa zunanji izvajalec podpisal posebno izjavo o varovanju osebnih podatkov. Zunanji izvajalec je dokumentacijo v skladišče odpeljal v zapakiranih kartonskih škatlah, ki jih je pripravila lekarna, postopek oddaje in baliranja papirja pa je ves čas spremljal.

Informacijski pooblaščenec zaradi ugotovljenih nepravilnosti oziroma kršitev ZVOP-1 ni odredil inšpekcijskih ukrepov (npr. sklenitev ustreznih pogodb o obdelavi osebnih podatkov), ker je zavezanec

samoiniciativno zagotovil ustrezne postopke in ukrepe za zavarovanje osebnih podatkov pri uničevanju zaupne dokumentacije in ker je lekarna zaradi obravnavanega primera prekinila nadaljnje poslovno sodelovanje z njim, prenehalo pa je tudi pogodbeno razmerje z zunanjim izvajalcem, ker je zaradi upokojitve zaprl firmo. Zaradi ugotovljenih kršitev ZVOP-1 je Informacijski pooblaščenec zoper zavezanca in lekarno uvedel postopka o prekrških, v katerih je zavezancu in njegovi odgovorni osebi izrekel globo za prekršek po prvem in drugem odstavku 93. člena ZVOP-1 (ker pri predaji in prevzemu receptov v uničenje ni zagotovil ustreznega zavarovanja osebnih podatkov, zaradi česar so se z njimi lahko seznanile nepooblaščen osebe), lekarni in njeni odgovorni osebi pa opomin za prekršek po 2. točki prvega odstavka in po drugem odstavku 91. člena ZVOP-1 (ker s pogodbenim obdelovalcem za uničenje dokumentacije z osebnimi podatki ni sklenila pogodbe, ki bi vsebovala tudi dogovor o postopkih in ukrepih za zavarovanje osebnih podatkov).

3.9.2. Zbiranje osebnih podatkov plačnikov

Informacijski pooblaščenec je prejel več obvestil in prijav o tem, da Pošta Slovenije, d. o. o., (zavezanec) pri storitvi plačila položnice in dostavi paketov s plačilom po povzetju z zneskom pod 1.000 EUR brez pravne podlage zbira osebne podatke plačnikov položnic oziroma prejemnikov paketov.

V postopku inšpekcijskega nadzora je bilo ugotovljeno, da se je dne 26. 6. 2017 v Republiki Sloveniji začela uporabljati Uredba (EU) št. 2015/847 Evropskega parlamenta in Sveta o informacijah, ki spremljajo prenose sredstev, in razveljavitvi Uredbe (ES) št. 1781/2006. Uredba št. 2015/847 določa pravila o informacijah o plačnikih in prejemnikih plačil (razen v primerih dopustnih odstopanj), ki jih morajo ponudniki plačilnih storitev ne glede na valuto priložiti k informacijam o prenosu sredstev za namen preprečevanja, odkrivanja in preiskovanja pranja denarja in financiranja terorizma, kadar ima vsaj eden od ponudnikov plačilnih storitev, udeležen v prenosu sredstev, sedež v Evropski uniji.

Zavezanec se po določitih Uredbe 2015/847 ne šteje med ponudnike plačilnih storitev, ampak se mednje šteje Nova KBM, d. d., kot pravna naslednica Poštne banke Slovenije, d. d. Zavezanec je pogodbeni izvajalec plačilnih storitev prek svojih poštних okenc, in sicer po navodilih Nove KBM, d. d., v njenem imenu in za njen račun, kar pomeni, da je njen pogodbeni obdelovalec osebnih podatkov. Nova KBM, d. d., in zavezanec sta sklenila pogodbo v skladu z 11. členom ZVOP-1, ki ureja pogodbeno obdelavo osebnih podatkov.

V zvezi z zbiranjem osebnih podatkov je bilo ugotovljeno, da identifikacija plačnika oziroma zbiranje osebnih podatkov ni potrebno, kadar se plačilo izvede z univerzalnim plačilnim nalogom, ki ima QR-kodo z vsemi podatki ali OCR-vrstico in znesek do vključno 1.000 EUR, ne glede na to, ali je plačnik za plačilo predložil gotovino ali drug plačilni instrument. Za obe navedeni vrsti plačilnega naloga do vključno 1.000 EUR velja izjema po Uredbi 2015/847, saj lahko ponudnik plačilnih storitev z enolično identifikacijsko oznako transakcije (OCR- ali QR-koda) izsledi prenos sredstev oziroma plačnika. Ustreznost OCR- ali QR-kode (ki bo v prihodnje nadomestila OCR-kodo) preveri zaposleni pri zavezancu, ko plačilni nalog (položnico) spusti skozi čitalec, računalniški program pa odčita podatke na plačilnem nalogu. Če je OCR- ali QR-koda pravilna, računalniški program ne zahteva dodatnih osebnih podatkov in plačniku ni treba predložiti osebnega dokumenta. V primerih plačilnih nalogov brez ene ali druge omenjene kode oziroma v primerih, kadar koda ni pravilna, pa računalniški program nepravilnost zazna in »odpre« novo okno, v katero mora zaposleni vnesti določene osebne podatke, da lahko opravi plačilno transakcijo: ime in priimek ter naslov plačnika (če je drugačen od zapsanega na plačilnem nalogu), državo, vrsto in številko osebnega dokumenta ter kraj in datum rojstva. Za takšno obdelavo osebnih podatkov plačnikov ima zavezanec ustrezno pravno podlago v prvem odstavku 4. člena Uredbe 2015/847, ki določa, da ponudnik plačilnih storitev zagotovi, da prenose sredstev spremljajo naslednje informacije o plačniku: ime plačnika, številka plačilnega računa plačnika, naslov plačnika, številka uradnega osebnega dokumenta, identifikacijska številka stranke ali datum in kraj rojstva.

V primeru dostave paketa in plačila po povzetju poštar na terenu ne more preveriti ustreznosti plačilnega naloga oziroma OCR- ali QR-kode, zato od plačnika zbere naslednje osebne podatke,

ki jih zapiše na hrbtno stran plačilnega naloga, v poslovalnici pa jih ob knjiženju vplačil vnesejo v računalnik:

1. če sta plačnik in prejemnik ista oseba: vrsto in številko osebnega dokumenta, datum in kraj rojstva plačnika;
2. če sta plačnik in prejemnik različni osebi: ime in priimek, naslov, vrsto in številko osebnega dokumenta, datum in kraj rojstva prejemnika.

Poštar zbira osebne podatke na podlagi osebne privolitve posameznika, torej plačnika oziroma prejemnika, kar je v zasebnem sektorju, kamor spada zavezanec oziroma Nova KBM, d. d., dopustno na podlagi prvega odstavka 10. člena ZVOP-1, ki določa, da se osebni podatki v zasebnem sektorju lahko obdelujejo, če obdelavo osebnih podatkov in osebne podatke, ki se obdelujejo, določa zakon ali če je za obdelavo določenih osebnih podatkov podana osebna privolitve posameznika. Plačnik oziroma prejemnik ima možnost plačilo odkloniti in paket prevzeti na poštnem okencu, kjer ima zaposleni možnost preveriti OCR- ali QR-kodo na plačilnem nalogu za odkupnino za dostavljeni paket. Na to možnost mora poštar na terenu plačnika oziroma prejemnika posebej opozoriti.

Zavezanec identifikacije plačnikov ne izvaja tudi v primeru plačil na račune proračunskih uporabnikov, ki imajo v registru oznako P (namen plačila je poravnava davkov, kazni ali drugih dajatev javnim organom), do vključno 1.000 EUR, ter pri pologu gotovine za pravne osebe v dnevno-nočni trezor.

Informacijski pooblaščenec je zaključil, da zavezanec v obravnavanem primeru zbiranja osebnih podatkov ni kršil določb ZVOP-1, zato je postopek inšpekcijskega nadzora ustavil.

3.9.3. Nezakonito razkrivanje osebnih podatkov učencev

Informacijski pooblaščenec je zoper osnovno šolo (zavezanec) po uradni dolžnosti uvedel postopek inšpekcijskega nadzora nad izvajanjem in spoštovanjem določb ZVOP-1 ter drugih predpisov, ki urejajo varstvo osebnih podatkov, po prejeti prijavi, da so bili staršem učencev s posredovanjem seznama učencev določenega razreda, ki ga je vodila učiteljica zaradi plačila likovnega materiala, nezakonito razkriti osebni podatki. Na spornem seznamu so bili v tabeli navedeni naslednji osebni podatki učencev: ime in priimek, datum rojstva, državljanstvo, kraj rojstva, EMŠO, naslov prebivališča, številka matičnega lista ter navedba o plačilu.

Zavezanec je kot razlog vodenja seznama učencev navedel pobiranje sredstev za nakup materiala za likovni pouk. Učiteljica je seznam prejela od šolske svetovalne delavke, ki na podlagi Zakona o osnovni šoli⁵⁴ hrani podatke v uradni Zbirki osebnih podatkov o učencih, vpisanih v osnovno šolo, in njihovih starših za namene obveznega izobraževanja in za izvajanje z zakonom določenih nalog, uporabniki te zbirke pa so pooblaščen delavci šole. Učiteljica je seznam po elektronski pošti poslala ravnatelju, ker jo je prosil za pojasnilo o poteku pobiranja sredstev, saj so to želeli starši učencev oziroma je to od njega zahtevala predstavnica v Svetu staršev, ki je način zbiranja sredstev tudi potrdil. Ravnatelj je slednji po elektronski pošti posredoval prejeto sporočilo učiteljice, skupaj s pripetim seznamom v obliki dokumenta v Wordu, predstavnica staršev pa ga je še istega dne posredovala vsem staršem učencev določenega razreda. Informacijski pooblaščenec je zavezanca pozval k uničenju oziroma izbrisu spornega seznama, ker je vseboval prekomeren nabor osebnih podatkov in je bil sestavljen z nezakonito uporabo osebnih podatkov učencev iz uradne evidence, poleg tega je bil namen sicer zakonite uporabe potrebnih osebnih podatkov učencev (ime in priimek) za evidentiranje plačil že dosežen. Ravnatelj in učiteljica sta sporni seznam uničila oziroma izbrisala, poleg tega je ravnatelj v skladu s pozivom Informacijskega pooblaščenca po elektronski pošti starše osebno pozval, da izbrišejo prejeto e-pošto s spornim seznamom.

Informacijski pooblaščenec je zaključil, da je zavezanec z opisanim ravnanjem osebne podatke učencev iz uradne zbirke, ki jo je dolžan voditi v skladu s predpisi s področja osnovnošolskega izobraževanja, uporabil v nasprotju z zakonitimi nameni ter jih brez podlage v zakonu ali osebni privolitvi posameznikov (staršev ali skrbnikov učencev, ker je šlo za mladoletne osebe) razkril nepooblaščenim osebam, s čimer je kršil določbe 8. člena ZVOP-1. Zato je zoper odgovorne osebe uvedel prekrškovne postopke ter jim za storjene prekrške izrekel ustrezne sankcije po drugem odstavku 91. člena ZVOP-1 v povezavi s 1. točko prvega odstavka 91. člena ZVOP-1: ravnatelju

⁵⁴ Uradni list RS, št. 81/2006 – uradno prečiščeno besedilo 3, s spremembami; v nadaljevanju ZOsn.

globo, ker je seznam učencev po elektronski pošti poslal predstavnici staršev, učiteljici likovne umetnosti opomin, ker je osebne podatke učencev iz uradne zbirke uporabila na način, da je iz njih sestavila seznam, ki ga je uporabljala za vodenje evidence plačil za nakup likovnega materiala tako, da ga je dala v podpis učencem, ki so že prispevali denar za nakup likovnega materiala, s čimer jim je nezakonito razkrila osebne podatke na seznamu, ter šolski svetovalni delavki prav tako opomin, ker je vsem učiteljem na šoli poslala elektronsko sporočilo s priloženo datoteko, ki je vsebovala osebne podatke vseh učencev šole (priimke in imena, datume, države in kraje rojstva, EMŠO, naslove prebivališč in številke matičnih listov).

3.9.4. Nezakonita obdelava osebnih podatkov v evidencah Policije

Informacijski pooblaščenec je s strani Policije prejel več predlogov za uvedbo postopka o prekršku, ker je v postopku internega nadzora ugotovila, da so določeni zaposleni, ki imajo dostop do zbirk osebnih podatkov zaradi opravljanja del in nalog, osebne podatke obdelovali v nasprotju z nameni, za katere so bili zbrani. Policija je predložila tudi ustrezne dokaze, tj. izpise vpogledov v evidence in izjave zaposlenih glede namena obdelave osebnih podatkov.

Informacijski pooblaščenec je vsem kršiteljem izrekel globo za prekrške po tretjem odstavku 91. člena ZVOP-1 v povezavi s 5. točko prvega odstavka 91. člena ZVOP-1, ker so s svojim ravnanjem kršili 16. člen ZVOP-1, ki določa, da se osebni podatki lahko zbirajo le za določene in zakonite namene ter se ne smejo nadalje obdelovati tako, da bi bila njihova obdelava v neskladju s temi nameni, če zakon ne določa drugače. Kršitelji so prekrške storili na način, da so z uporabo osebnih gesel v glavnem računalniku Policije vpogledali v poročilo o opravljenem delu določene policijske postaje in v tem dokumentu v konkreten dogodek, ki je vseboval osebne podatke, pri čemer pa za takšen vpogled v osebne podatke niso imeli podlage v zakonu, saj so osebne podatke, ki so bili zakonito zbrani za namene izvajanja nalog Policije in drugih zakonsko določenih nalog, nadalje obdelovali za osebne namene. Kršitelji posameznikov, v katerih osebne podatke so vpogledali, namreč niso obravnavali v nobenem uradnem postopku, ki bi ga v okviru opravljanja oziroma izvajanja svojih del in nalog vodili ali v njem kakor koli sodelovali.

Informacijski pooblaščenec poudarja, da za prekrške, kakršni so opisani zgoraj, kršiteljem vedno izreče globo, saj gre za zlorabo osebnih podatkov iz uradnih evidenc za zasebne namene (največkrat gre za radovednost) in za uporabo podatkov, do katerih so kršitelji pridobili dostop izključno zaradi opravljanja svojega dela. Posamezniki, ki imajo dostop do zbirk osebnih podatkov, se namreč morajo zavedati, da lahko te podatke uporabljajo izključno za opravljanje svojega dela (kar morajo tudi izkazati) in da so v skladu s četrtrim odstavkom 24. člena ZVOP-1 dolžni varovati tajnost osebnih podatkov, s katerimi se seznanijo pri opravljanju svojih del in nalog. Dolžnost varovanja tajnosti osebnih podatkov jih obvezuje tudi po prenehanju funkcije ali zaposlitve.

3.9.5. Sporno posredovanje osebnih podatkov zaposlenega članom zveze

Informacijski pooblaščenec je prejel prijavo, v kateri je bilo navedeno, da je moral določen zaposleni po navodilu predsednika zveze po elektronski pošti vsem članom zveze (društvom), članom izvršnega odbora in nadzornega odbora zveze poslati dopis z več prilogami (nepodpisani potni nalogi, nalogi za izplačilo, nepodpisana odločba za letni dopust in plačilna lista), ki vsebujejo osebne podatke zaposlenih pri zvezi. Ker je iz prijave izhajal sum nezakonitega razkrivanja osebnih podatkov, je Informacijski pooblaščenec uvedel postopek inšpekcijskega nadzora zoper zvezo (zavezanec).

Na podlagi preučitve navedb v prijavi, navedb zavezanca in priložene dokumentacije je Informacijski pooblaščenec ugotovil, da je določen zaposleni po naročilu predsednika zavezanca po elektronski pošti na 154 naslovov poslal obvestilo o nepravilnostih pri delu zaposlene, kateremu je priložil kopije potnih nalogov, kopijo odločbe o letnem dopustu in kopijo plačilne liste zaposlene z naslednjimi osebnimi podatki: ime in priimek, naslov, davčna številka, podatek o delovni dobi in številka transakcijskega računa. Zavezanec je pojasnil, da je bila plačilna lista v priponki poslana pomotoma in da je bilo sporočilo poslano nadzornim organom in članom, ki s prispevki v obliki članarin prispevajo k njegovemu delovanju, torej tudi za plače zaposlenih, zato so bili

upravičeni do seznanitve z nepravilnostmi pri delovanju zveze, pri čemer je naslov zaposlene tisti podatek, ki kaže na hujše kršitve delovnih obveznosti in domnevno goljufijo zaposlene, ki naj bi z neupravičeno obračunanimi potnimi stroški in stroški prevoza na delo in z dela oškodovala zavezanca.

Informacijski pooblaščenec je zaključil, da je imel zavezanec pravno podlago za posredovanje nepodpisanih potnih nalogov in plačilnega naloga s ponarejenim podpisom, na katerem je naveden naslov zaposlene, v 48. členu Zakona o delovnih razmerjih⁵⁵ (na podlagi katerega se osebni podatki delavcev lahko zbirajo, obdelujejo, uporabljajo in posredujejo tretjim osebam samo, če je to določeno s tem ali drugim zakonom ali če je to potrebno zaradi uresničevanja pravic in obveznosti iz delovnega razmerja ali v zvezi z delovnim razmerjem) v povezavi z določbami statuta zavezanca (na podlagi katerega imajo člani pravico, da so obveščeni o delu organov zavezanca, in na podlagi katerega je ena izmed pristojnosti izvršnega odbora nadzor dela strokovne službe, naloga nadzornega odbora pa poročanje Skupščini o izvrševanju sklepov izvršilnega odbora in o finančnem poslovanju zavezanca). Za posredovanje plačilne liste pa ni imel nobene od pravnih podlag iz 10. člena ZVOP-1, ki določa pravne podlage za obdelavo osebnih podatkov v zasebnem sektorju, kamor se šteje zavezanec (zakon, osebna privolitve posameznika, sklenitev in izpolnjevanje pogodbe, uresničevanje zakonitih interesov zasebnega sektorja).

Ker je šlo pri ugotovljeni nepravilnosti oziroma kršitvi za enkratno dejanje v preteklosti (nezakonito posredovanje plačilne liste in razkrivanje osebnih podatkov, ki jih vsebuje), ki ga s postopki in ukrepi, ki jih ima Informacijski pooblaščenec na voljo v postopku inšpekcijskega nadzora, ni več mogoče odpraviti, je bilo treba inšpekcijski postopek zoper zavezanca ustaviti. Informacijski pooblaščenec je zoper zavezanca in njegovo odgovorno osebo zaradi kršitve prvega odstavka 8. člena ZVOP-1 (obdelava osebnih podatkov brez podlage v zakonu ali osebni privolitvi posameznika) uvedel postopek o prekršku in kršitelju izrekel globo.

3.9.6. Objava osebnih podatkov članov na spletni strani

Informacijski pooblaščenec je prejel prijavo, v kateri je bilo navedeno, da zveza društev (zavezanec) ni ustrezno zavarovala osebnih in občutljivih osebnih podatkov na svoji spletni strani, saj naj bi zgolj vnos določenih URL-povezav v spletni brskalnik omogočil nezavarovan oziroma prost dostop do večjega števila osebnih podatkov posameznikov.

V postopku inšpekcijskega nadzora je bil opravljen ogled zavezančeve spletne strani, pri čemer je bilo ugotovljeno, da vnos v prijavi navedenih URL-povezav v spletni brskalnik res omogoča nezavarovan dostop do večjega števila osebnih podatkov članov društev, ki so včlanjena v zvezo. Tabele z objavljenimi podatki so med drugim vsebovale imena in priimke članov društva, njihove elektronske naslove in naslove prebivališča, datume rojstva, GSM-številke in telefonske številke ter številke izkaznic društev. Zaradi čim hitreje odprave kršitve 24. člena ZVOP-1, tj. nezavarovanega dostopa do osebnih podatkov prek spletne strani zavezanca, je državni nadzornik po telefonu poklical zavezanca in ga pozval, naj nemudoma umakne prosto dostopne osebne podatke s spletne strani oziroma zavaruje dostop do teh podatkov, kar je zavezanec tudi storil.

Zavezanec je posredoval poročilo o razlogih, zaradi katerih je prišlo do incidenta, ter o ukrepih, ki jih je izvedel, da je odpravil varnostno luknjo. Pojasnil je, da je bil dostop do spletnega naslova nekaj časa nezavarovan zaradi obsežnega testiranja prenosa podatkov o članarinah iz enega informacijskega sistema v drugega in da je sedaj dostop do spletne strani zavaroval s SSL-protokolom, kar pomeni, da je povezava med spletnim strežnikom in odjemalcem šifrirana, obenem pa je do osebnih podatkov mogoče dostopati le z vnosom ustreznega gesla.

Ker je zavezanec ugotovljeno nepravilnost odpravil, je Informacijski pooblaščenec postopek inšpekcijskega nadzora ustavil, ugotovljeno kršitev v zvezi z neustreznim zavarovanjem osebnih podatkov pa je obravnaval v okviru postopka za prekrške, ki ga je uvedel zoper zavezanca in zunanjega izvajalca oziroma pogodbenega obdelovalca osebnih podatkov. Prvi odstavek 25. člena ZVOP-1 namreč določa, da so tako upravljavci osebnih podatkov kot tudi pogodbeni obdelovalci dolžni zagotoviti zavarovanje osebnih podatkov na način iz 24. člena ZVOP-1, tj. sprejeti organizacijske, tehnične in logično-tehnične postopke in ukrepe, s katerimi se varujejo osebni podatki, preprečuje slučajno ali namerno nepooblaščen uničenje podatkov, njihova sprememba ali izguba ter nepooblaščen obdelava. Informacijski pooblaščenec je zaradi kršitve prvega in

⁵⁵ Uradni list RS, št. 21/2013, s spremembami; v nadaljevanju ZDR-1.

drugega odstavka 24. ter prvega odstavka 25. člena ZVOP-1 zavezancu in njegovi odgovorni osebi izrekel opomin, zunanjemu izvajalcu pa globo, ker ni zagotovil ukrepov za zavarovanje osebnih podatkov na zavezančevem spletnem strežniku, na katerem so bile shranjene tabele z osebnimi podatki večjega števila posameznikov (okrog 500), na način, da bi dostop do osebnih podatkov omejil s požarnim zidom, z uporabniškim imenom in geslom ali na drug podoben način ter tako preprečil nepooblaščenno obdelavo osebnih podatkov, ki so bili prosto dostopni vsem uporabnikom svetovnega spleta z vnosom določenih URL-povezav v spletni brskalnik.

3.9.7. Objava dokumentov z osebnimi podatki prič v prekrškovnem postopku na spletnih straneh

Na podlagi prejete prijave, v kateri je bilo navedeno, da so v članku, objavljenem na določeni spletni strani, fotografije originalnih dokumentov z osebnimi podatki prič v konkretnem prekrškovnem postopku, je Informacijski pooblaščenec uvedel postopek inšpekcijskega nadzora zoper upravljavca spletne strani (zavezanec).

V postopku inšpekcijskega nadzora je bil opravljen ogled zavezančevih spletnih strani, pri čemer je bilo ugotovljeno, da se na določenem spletnem naslovu kot del članka v obliki fotografij uradnih dokumentov (obdolžilni predlog, vabilo obdolžencu) nahajajo naslednji nezavarovani osebni podatki:

- osebni podatki posameznika, zoper katerega je bil podan predmetni obdolžilni predlog, in sicer ime in priimek, EMŠO, spol, kraj rojstva, državljanstvo, stalno prebivališče, upravna enota, država, začasno prebivališče, država, podatki o prekršku;
- osebni podatki šestih posameznikov, ki so bili v postopku zaslišani kot priče: imena, priimki in naslovi prebivališč ter podatki o tem, kaj so priče izpovedale.

Navedeni podatki so del zbirke osebnih podatkov, vsi podatki pa tudi uživajo varstvo po ZVOP-1, saj nihče od posameznikov ni (ne relativno ne absolutno) javna oseba, zato bi zavezanec za objavo osebnih podatkov moral imeti ustrezno pravno podlago. Splošne pravne podlage za obdelavo osebnih podatkov določa 8. člen ZVOP-1, pravne podlage za obdelavo osebnih podatkov v zasebnem sektorju, kamor se šteje zavezanec, pa 10. člen ZVOP-1. Prva odstavka obeh členov določata, da se lahko osebni podatki obdelujejo, če obdelavo osebnih podatkov in osebne podatke, ki se obdelujejo, določa zakon ali če je za obdelavo določenih osebnih podatkov podana osebna privolitve posameznika.

V postopku inšpekcijskega nadzora je bilo ugotovljeno, da je zavezanec razpolagal zgolj z osebno privolitvijo enega posameznika, in sicer s pisno privolitvijo posameznika, zoper katerega je bil vložen obdolžilni predlog in ki je zavezancu objavljene dokumente tudi posredoval. Zavezanec je pojasnil, da je bil namen objave informirati javnost o prekrškovnem postopku ter da je pri objavi osebnih podatkov prič šlo za napako in ne za namerno kršenje predpisov, saj pred objavo dokumenta ni bilo dovolj temeljito preverjeno, ali so v dokumentu poleg podatkov posameznika, ki je posredoval dokumente, še osebni podatki drugih oseb. Zavezanec je te osebne podatke takoj po seznanitvi z ugotovljenimi nepravilnostmi oziroma spoznanju storjene napake umaknil s spleta.

Informacijski pooblaščenec je zaključil, da bi moral zavezanec glede na odsotnost pravne podlage za obdelavo osebnih podatkov in glede na dolžnost zavarovanja osebnih podatkov iz 24. in 25. člena ZVOP-1 osebne podatke prič pred slikovnim zajemom dokumenta in njegovo javno objavo na spletu ustrezno zavarovati z organizacijskimi, tehničnimi in logično-tehničnimi postopki in ukrepi, s katerimi bi zagotovil učinkovit način blokiranja, uničenja, izbrisa ali anonimiziranja osebnih podatkov vseh šestih prič na način, da bi podatke izbrisal oziroma prekril. Objava osebnih podatkov na svetovnem spletu pomeni po mnenju Informacijskega pooblaščenca eno najhujših oblik kršitve pravice do varstva osebnih podatkov in s tem povezanega posega v zasebnost posameznika, saj se dostop do osebnih podatkov omogoči najširšemu krogu uporabnikov, tj. vsem uporabnikom svetovnega spleta, ki lahko pridobljene podatke nekontrolirano uporabljajo za najrazličnejše namene. Zato je zoper zavezanca in njegovo odgovorno osebo začel postopek o prekršku in jima zaradi neustreznega zavarovanja osebnih podatkov (kršitev 4. točke prvega odstavka 24. člena ZVOP-1 in prvega odstavka 25. člena ZVOP-1), katerega posledica je bila nezakonita objava osebnih podatkov, izrekel globo. Postopek o prekršku še ni zaključen, ker sta kršitelja zoper odločbo o prekršku vložila zahtevo za sodno varstvo, ki jo je Informacijski pooblaščenec posredoval pristojnemu okrajnemu sodišču.

3.9.8. Neustrezno zavarovanje datotečne strukture notarske pisarne

Informacijski pooblaščenec je na podlagi prejete prijave kršitve varstva osebnih podatkov uvedel postopek inšpekcijskega nadzora zoper notarsko pisarno (zavezanec), v katerem je preverjal, ali ima zavezanec ustrezno zavarovan dostop do osebnih podatkov, ki so se nahajali v elektronskih dokumentih, shranjenih na datotečnem strežniku. Do dokumentov naj bi bilo možno priti zgolj z vnosom določenega URL-naslova v vnosno vrstico brskalnika, brez kakršne koli avtentikacije ali zahteve po vnosu uporabniškega naslova ali gesla.

V postopku inšpekcijskega nadzora je Informacijski pooblaščenec najprej izvedel ogled dostopa do osebnih podatkov v dokumentih zavezanca na določenem spletnem mestu in pri tem ugotovil, da je do osebnih podatkov res možno dostopati na način, naveden v prijavi. Na spletnem mestu se je prosto dostopno nahajala celotna datotečna struktura zavezanca, v kateri so bile mape s shranjenimi dokumenti, ki prav tako niso bili posebej zaščiteni, zaradi česar je bilo možno obdelovati vse osebne podatke, ki so se v njih nahajali: imena, priimke, datume rojstva, naslove prebivališč, EMŠO, podatke iz osebnih dokumentov, številke bančnih računov, podatke o lastništvu in vrednosti nepremičnin, sorodstvene vezi in druge okoliščine iz družinskega življenja posameznikov. Informacijski pooblaščenec je sestavil zapisnik o ogledu spletne strani v pisarni in shranil pridobljene dokaze. Z namenom čim hitreje vzpostavitve ustreznega zavarovanja osebnih podatkov je Informacijski pooblaščenec zavezanca takoj telefonsko pozval, da v najkrajšem možnem času odpravi ugotovljene nepravilnosti. Zavezanec je še isti dan poskrbel za zavarovanje dostopa do datotečnega strežnika in s tem do osebnih podatkov.

Zavezanec je pojasnil, da informacijsko infrastrukturo redno vzdržuje zunanji izvajalec ter v dokaz predložil pogodbo. Ker je iz pogodbe o vzdrževanju opreme in informacijskega sistema izhajalo, da je bil za ustrezno zaščito podatkov in protivirusno zaščito zadolžen zunanji izvajalec oziroma zavezančev pogodbeni obdelovalec osebnih podatkov, je Informacijski pooblaščenec uvedel inšpekcijski postopek tudi zoper njega. Pogodbeni obdelovalec je pojasnil, da je bila zaradi povišanja nivoja varnosti informacijskega sistema vgrajena nova arhivska enota, stara arhivska enota pa je ostala priklopljena izključno z namenom preverjanja uspešnosti kopiranja podatkov na novo napravo. Dostop do stare arhivske enote je bil zaščiten z domenskim uporabniškim imenom in geslom, znanim zgolj zavezancu in pogodbenemu obdelovalcu, ter tako omogočen izključno v interni mreži kot mapa v skupni rabi. Po navedbah pogodbenega obdelovalca je bila odprtost stare arhivske enote navzven, za javni dostop prek spleta, posledica vdora v sistem s strani profesionalnega »hekerja«, ki je na modemu in stari arhivski enoti omogočil UPnP-protokol. Glede na to, da vgrajena strojna oprema ni omogočala natančne diagnostike, ISP pa ni omogočal beleženja sledljivosti zunanjih dostopov, ker podatki niso bili namenjeni dostopanju z interneta, pogodbeni obdelovalec zatrjevanega ni mogel izkazati. Pogodbeni obdelovalec je navedel še, da je takoj po telefonskem klicu Informacijskega pooblaščenca dostop do stare arhivske enote onemogočil tako, da jo je fizično odklopil iz sistema, naštel pa je tudi druge ukrepe, ki jih je izvedel po incidentu, da bi preprečil nadaljnje nepooblaščen dostope.

Ob upoštevanju vseh pridobljenih dokazov in pojasnil v postopku inšpekcijskega nadzora je Informacijski pooblaščenec zaključil, da pogodbeni obdelovalec v okviru pooblastil, ki jih je zavezanec nanj prenesel s pogodbo, ni zagotovil učinkovitih organizacijskih, tehničnih in logično-tehničnih ukrepov za zavarovanje dostopa do mrežnega vmesnika in stare arhivske enote (npr. s požarno pregrado ali z uporabniškim imenom in geslom), ki je vsebovala celotno datotečno strukturo zavezanca, na kateri so bili shranjeni dokumenti z osebnimi podatki večjega števila posameznikov. Zaradi tega je lahko kateri koli uporabnik svetovnega spleta zgolj z vnosom določene URL-vrstice v spletni brskalnik prosto dostopal do vseh osebnih podatkov v shranjenih dokumentih, ker pa pogodbeni obdelovalec tudi ni zagotavljal sledljivosti obdelave osebnih podatkov, ni bilo možno ugotoviti niti tega, kdo je dostopal do podatkov. Navedeno kršitev določb 24. in 25. člena ZVOP-1 je Informacijski pooblaščenec obravnaval v okviru pooblastil, ki jih ima kot prekrškovni organ, in pogodbenemu obdelovalcu izrekel globo.

3.9.9. Zbiranje podatkov o vzrokih za bolniško odsotnost

Informacijski pooblaščenec je na podlagi informacij, da je določen delodajalec (zavezanec) sprejel Pravilnik o zmanjševanju bolniške odsotnosti (Pravilnik), ki predvideva zbiranje osebnih podatkov o zdravstvenem stanju delavcev, uvedel postopek inšpekcijskega nadzora, katerega predmet je bilo preverjanje zakonitosti zbiranja osebnih podatkov na obrazcih, ki so priloga navedenega Pravilnika.

Splošna pravna podlaga za obdelavo osebnih podatkov je urejena v 8. členu ZVOP-1, ki določa, da se osebni podatki lahko obdelujejo le, če obdelavo osebnih podatkov in osebne podatke, ki se obdelujejo, določa zakon ali če je za obdelavo določenih osebnih podatkov podana osebna privolitve posameznika. Področna zakona v smislu 8. člena ZVOP-1 v konkretnem primeru predstavljata Zakon o evidencah na področju dela in socialne varnosti⁵⁶ in Zakon o delovnih razmerjih⁵⁷. ZEPDSV določa vrste evidenc, ki jih morajo voditi delodajalci, in njihovo vsebino, 48. člen ZDR-1 pa določa, da se osebni podatki delavcev lahko zbirajo, obdelujejo, uporabljajo in dostavljajo tretjim osebam samo, če je to določeno s tem ali drugim zakonom ali če je to potrebno zaradi uresničevanja pravic in obveznosti iz delovnega razmerja ali v zvezi z delovnim razmerjem. Iz navedene določbe ZDR-1 tako izhaja, da delodajalec lahko zbira le tiste podatke zaposlenih, ki so določeni s tem ali drugim zakonom ali če je to potrebno zaradi uresničevanja pravic in obveznosti iz delovnega razmerja ali v zvezi z delovnim razmerjem. Pri tem so mišljene pravice in obveznosti obeh, torej delavca in delodajalca.

Po preučitvi obrazcev je Informacijski pooblaščenec ugotovil, da so obrazci predvidevali tudi zbiranje občutljivih osebnih podatkov delavcev oziroma podatkov o njihovem zdravstvenem stanju (vrsta bolezni ali poškodbe ter diagnoza) ter podatkov o zasebnih življenjskih navadah delavca in vzrokih za pogost bolniški stalež, kar je poleg nezakonitega zbiranja osebnih podatkov predstavljajo tudi prekomeren poseg v zasebnost delavcev. Zavezanec za zbiranje navedenih podatkov (namen je bil izboljšanje zdravja in počutja zaposlenih ter posledično zmanjšanje bolniških odsotnosti) ni imel podlage v zakonu (ZDR-1, ZEPDSV, Zakona o varnosti in zdravju pri delu⁵⁸), osebna privolitve delavcev (na katero se je skliceval zavezanec) pa je načeloma v delovnih razmerjih zaradi podrejenega položaja delavca oziroma izrazite neenakosti moči strank izključena. Delavec je namreč pri izražanju svoje volje v odnosu do delodajalca šibkejša stranka in bistveno manj svoboden, kot to velja v drugih razmerjih, kjer sta pogodbeni stranki v prirejenem položaju. O privolitvi kot podlagi za zbiranje osebnih podatkov v delovnih razmerjih je mogoče govoriti le v redkih situacijah, ko gre za obdelave osebnih podatkov za namene izvajanja povsem neobveznih, dodatnih dejavnosti oziroma procesov, ki jih lahko delavec odkloni brez bojazni, da bo to kakor koli vplivalo na njegovo delovno razmerje – kadar torej ne gre za obdelavo osebnih podatkov delavcev, povezano z izpolnjevanjem pravic in obveznosti iz delovnega razmerja. V konkretnem primeru je Informacijski pooblaščenec ugotovil, da ni šlo za enega izmed povsem prostovoljnih procesov, ki z izvrševanjem pravic in obveznosti iz delovnega razmerja ne bi bil nikakor povezan, saj je bil vsak delavec po prihodu iz bolniške dolžan izpolniti obrazce, ki so bili priloga Pravilnika, na obrazcih pa pri spornih kategorijah osebnih podatkov tudi ni bilo izrecno označeno, da je posredovanje le-teh neobvezno. Navedeno vodi do zaključka, da ureditev, kakršna je veljala pri zavezancu, delavcu ni jasno sporočala, ali je podatke dolžan posredovati, ter mu ni omogočala svobodne presoje, katere osebne podatke bo posredoval. S tem pa v konkretnem primeru tudi ni mogoče govoriti o privolitvi kot podlagi za zbiranje ter hrambo osebnih podatkov delavcev, ki jih je zavezanec zbiral skladno s Pravilnikom.

Zavezanec je po seznanitvi z ugotovljenimi nepravilnostmi in pozivu Informacijskega pooblaščenca k njihovi odpravi obrazce, ki so priloga Pravilnika, ustrezno prilagodil, vse izpolnjene obrazce pa je uničil.

Delodajalec lahko v zvezi z bolniškimi odsotnostmi zbira podatke o režimu gibanja delavca (navodila zdravnika o počitku ali dopustnem gibanju) in o predvidenem času odsotnosti, ker brez njih ne more ukrepati ob sumu zlorabe bolniškega staleža in organizirati dela oziroma zagotoviti nadomeščanja odsotnega delavca. Podatke lahko pridobi od zaposlenega ali od njegovega osebnega zdravnika, ki pa podatkov ni dolžan posredovati. Delodajalec ima pravno podlago tudi za pridobitev podatka o razlogu začasne zadržanosti od dela, ker ga potrebuje za obračun nadomestila plače med začasno zadržanostjo, nima pa pravne podlage za pridobitev diagnoze bolezni oziroma poškodbe. Podatek o razlogu pri bolniški odsotnosti do 30 dni je razviden iz bolniškega lista (npr. bolezen, poškodba izven dela, poklicna bolezen, poškodba pri delu, nega), ki ga prinese delavec, pri odsotnosti nad 30 dni pa iz odločbe ZZZS, ki jo prejme tudi delodajalec.

V zvezi z dolžnostjo delodajalca po 6. členu ZVZD-1 (priprava ter izvajanje načrta za promocijo zdravja na delovnem mestu) pa Informacijski pooblaščenec pojasnjuje, da ukrepi za promocijo zdravja niso namenjeni posameznim delavcem, ampak gre za sistematične ciljne aktivnosti in ukrepe, ki so namenjeni vsem delavcem in se izvajajo za vse delavce pod enakimi pogoji, z namenom ohranjanja in krepitev telesnega in duševnega zdravja zaposlenih. Gre za kombinacijo

⁵⁶ Uradni list RS, št. 40/2006, v nadaljevanju ZEPDSV,

⁵⁷ Uradni list RS, št. 21/2013 s spremembami, nadaljevanju ZDR-1,

⁵⁸ Uradni list RS, št. 43/2011, v nadaljevanju ZVZD-1.

sprememb fizičnega in socialnega okolja ter z zdravjem povezanega življenjskega sloga⁵⁹. Zato lahko delodajalec zbira informacije o življenjskem slogu ter življenjskih navadah delavcev, tudi z uporabo vprašalnikov, vendar po oceni Informacijskega pooblaščenca za pripravo načrta ne potrebuje osebnih podatkov, pač pa lahko predmetni načrt ter ukrepe, usmerjene v promocijo zdravja na delovnem mestu, določi ter izvaja na podlagi informacij, ki jih dobi od delavcev z izpolnitvijo anonimnega vprašalnika.

Informacijski pooblaščenec dodaja, da prakse delodajalca, da skupaj z delavcem prouči možnosti za zmanjšanje bolniške odsotnosti, ne ocenjuje kot sporne. Kljub temu pa mora delodajalec pri tem upoštevati pravico delavca do zasebnosti ter se, razen v primerih, ko bi bil pri delavcu zaznan razlog za pogoste bolniške odsotnosti na strani delodajalca oziroma v povezavi z delovnim procesom, vzdržati pridobivanja informacij o podrobnejših razlogih za bolniško odsotnost ter presoje, ali ima delavec možnost število svojih odsotnosti glede na okoliščine iz zasebnega življenja zmanjšati. To pomeni, da je z vidika preprečevanja pogostih bolniških odsotnosti konkretnega delavca dopustno izključno pridobivanje informacij, ki se nanašajo na delavčevo počutje v službi, njegovo sposobnost za delo in občutek (pre)obremenjenosti zaradi določenega dela.

3.9.10. Posredovanje videoposnetka tatvine in njegova objava na Facebooku

Informacijski pooblaščenec je bil obveščen, da je na Facebooku objavljen videoposnetek tatvine iz avtomobila, ki je bil parkiran na javni površini. Ker je iz prejetega obvestila izhajal sum nezakonitega snemanja javnih površin in nezakonite obdelave (posredovanja in objave) osebnih podatkov, je Informacijski pooblaščenec uvedel postopek inšpekcijskega nadzora zoper izvajalca videonadzora (zavezanec).

V postopku je bilo ugotovljeno, da je posameznik na Facebooku objavil videoposnetek, ki prikazuje tatvino. Namen objave videoposnetka je bil čim hitrejša prepoznavna tatu, čeprav je posameznik, ki je videoposnetek objavil, kaznivo dejanje kot oškodovanec že naznanil policiji, ki je videoposnetek dogodka pri zavezancu tudi zasegla. Posameznik je videoposnetek nezakonito pridobil pri zavezancu, ki izvaja videonadzor nad vhodom na svojo parcelo, pri čemer pa zajame tudi cesto, kjer je bilo parkirano vozilo, iz katerega so bile odtujene posameznikove stvari. Informacijski pooblaščenec je posameznika pozval, da sporni videoposnetek odstrani s svojega Facebook profila, kar je tudi storil.

Informacijski pooblaščenec je ugotovil, da zavezanec ni imel pravne podlage za posredovanje videoposnetka posamezniku, čeprav je šlo za odtujitev njegovih stvari. Glede na to, da se zavezanec šteje med upravljavce osebnih podatkov v zasebnem sektorju, bi lahko osebne podatke (videoposnetek) posredoval na podlagi zakona ali osebnih privolitvev posameznikov na posnetku, kot to določata prvi odstavek 8. in 10. člena ZVOP-1. Ker so videoposnetki so osebni podatki, bi lahko posameznik na podlagi 30. in 31. člena ZVOP-1, ki določata vsebino pravice do seznanitve z lastnimi osebnimi podatki in postopek seznanitve, pridobil videoposnetek, na katerem se nahaja, vendar pa bi moral zavezanec kot upravljavec osebnih podatkov (zbirke videoposnetkov) pred posredovanjem videoposnetka podobe drugih posameznikov na posnetku prekriti (tudi podobo tatu), česar pa ni storil. Celoten posnetek tatvine lahko pridobi policija kot organ pregona na podlagi Zakona o nalogah in pooblastilih policije in Zakona o kazenskem postopku, kar je policija v konkretnem primeru tudi storila, posameznik pa bi lahko kot oškodovanec videoposnetek pridobil od policije, vendar ga ne bi smel objaviti na Facebooku. Posamezniki, ki imajo status stranke v določenem postopku, lahko praviloma na podlagi procesnih zakonov pridobijo podatke iz spisov (npr. upravnih ali sodnih), vendar teh podatkov ne smejo posredovati nepooblaščenim osebam, uporabljajo jih lahko le za zakonite namene, npr. za varovanje pravic pred pristojnimi organi.

V zvezi s snemanjem ceste, ki ni v zavezančevi lasti, Informacijski pooblaščenec pojasnjuje, da lahko izvajalec videonadzora s kamerami, s katerimi snema vhode v svoje poslovne prostore oziroma vhode na varovano območje, ki se nahajajo ob javni cesti, zajame tudi del te ceste, katerega nadzor je po naravi stvari nujen, da se zagotovi uresničitev namenov, zaradi katerih se videonadzor izvaja (npr. varovanje premoženja, nadzor nad vstopi in izstopi). Ker pri tem posameznik tudi mimoidoče, s čimer posega v njihovo zasebnost, Informacijski pooblaščenec dodaja, da lahko videoposnetke pregleduje le v skladu z nameni, ki jih za uvedbo videonadzora določa ZVOP-1. To pomeni, da lahko v primeru incidenta (npr. poškodovanja ali odtujitve premoženja) vpogleda

⁵⁹ Smernice za promocijo zdravja na delovnem mestu, http://www.mz.gov.si/fileadmin/mz.gov.si/pageuploads/javno_zdravje_2015/zdr_na_del_mestu/Smernice_promocija_zdravja_na_delovnem_mestu-januar_2017.pdf.

v arhiv videoposnetkov, kar mora ustrezno evidentirati, ni pa dopustno stalno spremljanje žive slike.

3.10. Splošna ocena stanja varstva osebnih podatkov in priporočila

Informacijski pooblaščenec je leta 2017 v okviru izvajanja inšpekcijskega nadzora na področju varstva osebnih podatkov obravnaval:

- 655 inšpekcijskih zadev, od tega 226 na področju javnega in 429 na področju zasebnega sektorja, in
- 105 prekrškovnih zadev.

Poleg inšpekcijskih in prekrškovnih postopkov je Informacijski pooblaščenec leta 2017 prejel in obravnaval še:

- 1.289 zaprosil za pisna mnenja in pojasnila s področja varstva osebnih podatkov,
- 16 vlog za izdajo dovoljenja za povezovanje zbirk osebnih podatkov,
- štiri vloge za izdajo dovoljenja za izvajanje biometrijskih ukrepov,
- 29 vlog za izdajo dovoljenja za iznos osebnih podatkov,
- 110 pritožb zaradi zavrnitve zahteve za seznanitev z lastnimi osebnimi podatki.

Od skupaj 655 inšpekcijskih zadev je bilo 559 zadev obravnavanih zaradi prejetih prijav, 96 pa jih je bilo obravnavanih na lastno pobudo. Na področju javnega sektorja je bilo vloženi 189 prijav in pritožb, na področju zasebnega sektorja pa 370. Število prijav zaradi suma kršitev predpisov s področja varstva osebnih podatkov je bilo podobno kot v preteklih letih. Največ prijav je bilo vloženi zaradi posredovanja osebnih podatkov nepooblaščenim uporabnikom, zaradi nezakonitega zbiranja oziroma zahtevanja osebnih podatkov, zaradi uporabe osebnih podatkov za namene neposrednega trženja (zlasti zaradi suma nezakonitega pridobivanja osebnih podatkov za te namene ter zaradi neupoštevanja zahteve posameznika po prenehanju uporabe osebnih podatkov za te namene), zaradi izvajanja videonadzora in nezakonite uporabe posnetkov (zlasti v delovnih prostorih), zaradi neustreznega zavarovanja osebnih podatkov, zaradi uporabe osebnih podatkov v nasprotju z namenom njihovega zbiranja ter zaradi nezakonitega vpogledovanja v osebne podatke.

Podobno kot v preteklih letih je Informacijski pooblaščenec pri obravnavi prejetih prijav od skupaj 559 obravnavanih prijav v 221 primerih (39 % prejetih prijav) že na podlagi preučitve navedb v sami prijavi in priložene dokumentacije presodil, da opisana ravnanja ne pomenijo kršitve predpisov s področja varstva osebnih podatkov. Najpogostejši razlog za tako veliko število neutemeljenih prijav je še vedno ta, da prijavitelji pogosto premalo poznajo predpise s področja varstva osebnih podatkov in pristojnosti Informacijskega pooblaščenca, Informacijski pooblaščenec pa poleg takšnih prijav, ki so vložene z namenom vzpostavitve zakonitega stanja in iz upravičenih razlogov, še vedno 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 poskus reševanja medsebojnih sporov in uveljavljanja takšnih zasebnih interesov, ki jih v postopku inšpekcijskega nadzora Informacijskega pooblaščenca sploh ni mogoče uveljavljati. Veliko število neupravičeno vloženi prijav ter nujnost njihove obravnave ovirata opravljanje t. i. preventivnega inšpekcijskega nadzora na področjih, kjer bi se ta moral intenzivneje izvajati. Državni nadzornik, ki zadevo obravnava, vsem takšnim prijaviteljem pošlje pisno obvestilo, v katerem obrazloži razloge, zaradi katerih opisano ravnanje 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.

Velik problem pri obravnavi prejetih prijav ter izvajanju inšpekcijskega nadzora nasploh predstavljajo tudi zavezanci, ki nimajo poslovnih prostorov, ampak le poštni nabiralnik, ter zavezanci, ki imajo v Poslovni register kot pooblaščenice osebe za zastopanje vpisane tuje državljanke. V večini primerov gre za zavezance, ki se ukvarjajo s spletno prodajo ter osebne podatke zbirajo in uporabljajo za vsiljivo neposredno trženje.

Opozoriti je treba tudi na povečanje števila prijav zaradi nezakonitega zbiranja oziroma zahtevanja osebnih podatkov, ki je bilo v veliki meri posledica pomanjkljivega oziroma neustreznega informiranja posameznika, od katerega se osebni podatki pridobivajo. V postopku inšpekcijskega nadzora se je namreč izkazalo, da je imel upravljavec osebnih podatkov za zbiranje zahtevanih osebnih podatkov sicer ustrezno zakonsko podlago, vendar pa posamezniku, od katerega je podatke pridobival, ni

podal ustreznih informacij o namenu zbiranja le-teh, zaradi česar je posameznik upravičeno posumil, da za zbiranje osebnih podatkov nima ustrezne pravne podlage, in je podal prijavo Informacijskemu pooblaščenču. Upravljevalec osebnih podatkov mora namreč v primeru pridobivanja osebnih podatkov posamezniku ob pridobivanju osebnih podatkov skladno z določbami 19. člena ZVOP-1 zagotoviti naslednje informacije: o upravljavcu osebnih podatkov in njegovem sedežu, o namenu obdelave osebnih podatkov ter druge informacije, če je to potrebno, da se zagotovi zakonita in poštena obdelava (informacije o uporabnikih osebnih podatkov, informacije o tem, ali je zbiranje osebnih podatkov obvezno ali prostovoljno ter o možnih posledicah, če posameznik ne bo prostovoljno podal podatkov, ter informacije o pravici do vpogleda, prepisa, kopiranja, dopolnitve, popravka, blokiranja in izbrisa osebnih podatkov). Nova evropska Splošna uredba o varstvu podatkov, ki se bo začela uporabljati 25. maja 2018, je glede zagotavljanja informacij, ki jih je treba zagotoviti posamezniku v primeru, ko se osebni podatki pridobivajo neposredno od njega, še zahtevnejša kot veljavni ZVOP-1, saj v drugem in tretjem odstavku člena 13 določa še precej širši nabor informacij, ki jih je treba zagotoviti posamezniku.

Poleg obravnave prejetih prijav je Informacijski pooblaščenec tudi leta 2017 okrepljeno izvajal t. i. načrtovan *ex offo* inšpekcijski nadzor na področjih, na katerih glede na oceno tveganja obstaja bodisi večja verjetnost kršitve predpisov s področja varstva osebnih podatkov ali pa zaradi občutljivosti obdelave osebnih podatkov v primeru morebitnih kršitev obstaja nevarnost večjih škodljivih posledic za posameznike, na katere se osebni podatki nanašajo. Pri opravljanju teh obsežnejših oziroma temeljitejših inšpekcijskih nadzorov je Informacijski pooblaščenec posebno pozornost namenil preverjanju in zagotavljanju informacijske varnosti, katere namen je preprečevanje nepooblaščenih obdelav osebnih podatkov ter naključnega ali nepooblaščenega uničevanja ali izgube le-teh, ki se vsako leto izvajajo skladno z letnim načrtom. Načrtovani inšpekcijski nadzor nad spoštovanjem določb ZVOP-1 se je leta 2017 izvajal na ministrstvih, v upravnih enotah, zdravstvenih zavodih, pri večjih pogodbenih obdelovalcih osebnih podatkov, v turističnih agencijah, pri sindikatih in njihovih zvezah ter pri društvih in njihovih zvezah.

Informacijski pooblaščenec podobno kot v preteklih poročilih ugotavlja, da se je ozaveščenost tako splošne kot strokovne javnosti glede zasebnosti in varstva osebnih podatkov precej izboljšala in se še vedno izboljšuje. Osnovne težave glede poznavanja zakonodaje so bile presežene, pri čemer pa Informacijski pooblaščenec pri upravljavcih osebnih podatkov in njihovih pogodbenih obdelovalcih na različnih področjih pri opravljanju inšpekcijskega nadzora še vedno ugotavlja precej nepravilnosti in pomanjkljivosti. Med najpogostejše ugotovljene nepravilnosti in pomanjkljivosti sodijo zlasti nedefinirani ali pomanjkljivo definirani organizacijski, tehnični in logično-tehnični postopki in ukrepi za zavarovanje osebnih podatkov v notranjih aktih upravljavcev, pomanjkljivo ali neustrezno zagotavljanje notranje in zunanje sledljivosti obdelave osebnih podatkov, neizdelani sezname oseb, ki so odgovorne za posamezne zbirke osebnih podatkov, in oseb, ki lahko zaradi narave svojega dela obdelujejo določene osebne podatke, sporočanje neustreznih ali pomanjkljivih informacij posameznikom ob zbiranju njihovih osebnih podatkov, prekomerno in nesorazmerno izvajanje videonadzora v delovnih prostorih ter uporaba posnetkov za nadzor nad zaposlenimi, neupoštevanje zahtev posameznikov po prenehanju uporabe osebnih podatkov za neposredno trženje, pomanjkljive pogodbe s pogodbenimi obdelovalci ter preusmeritve in nepooblaščenno prebiranje službene elektronske pošte nekdanjih zaposlenih.

Zelo pogoste so tudi nepravilnosti in pomanjkljivosti v zvezi z vodenjem ažurnih katalogov zbirk osebnih podatkov ter s tem povezanim posredovanjem podatkov v register zbirk osebnih podatkov, pri čemer je treba opozoriti, da se bo z uveljavitvijo Splošne uredbe o varstvu podatkov register zbirk osebnih podatkov nehal voditi, dozdajšnje kataloge zbirk osebnih podatkov pa bodo upravljavci (razen nekaterih izjem) morali nadomestiti z vodenjem evidenc obdelave osebnih podatkov, kot to določa člen 30 Splošne uredbe o varstvu podatkov. Slednji k vodenju evidenc dejavnosti obdelave zavezuje tudi pogodbeni obdelovalci osebnih podatkov, ki to dejavnost izvajajo v imenu upravljavcev; po ZVOP-1 pogodbeni obdelovalci takšnih evidenc niso bili dolžni voditi.

Zavezanci opisane nepravilnosti in pomanjkljivosti praviloma prostovoljno odpravijo že na podlagi opozorila, ki jim ga v postopku izreče državni nadzornik za varstvo osebnih podatkov, zaradi česar izdaja inšpekcijske (ureditvene) odločbe praviloma ni potrebna, opozoriti pa je treba, da prostovoljna odprava ugotovljenih nepravilnosti zavezanca ne odvezuje prekrškovne, kazenske in odškodninske odgovornosti.

Varstvo osebnih podatkov v evropskem prostoru so leta 2017 v veliki meri zaznamovale priprave na Splošno uredbo (EU) 2016/679 Evropskega parlamenta in Sveta z dne 27. 4. 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, angl. *General Data Protection Regulation – GDPR*).

Splošna uredba o varstvu podatkov je začela veljati 25. 5. 2016, njene določbe pa bodo vse države članice začele uporabljati v dveh letih. Na uporabo Splošne uredbe o varstvu podatkov so se večji upravljavci že začeli pripravljati, pri manjših upravljavcih, ki so bili po ZVOP-1 deležni določenih izjem (npr. glede priprave katalogov in prijave zbirk osebnih podatkov v register Informacijskega pooblaščenca), pa se je izkazalo, da nekateri zakonodajci o varstvu osebnih podatkov niso dobro poznali. To se je izkazalo na predstavitvah Splošne uredbe na konferencah, okroglih mizah, posvetih in ob dnevu varstva osebnih podatkov, ko so se pojavljala številna vprašanja, ki se niso nanašala na bodočo ureditev po Splošni uredbi, temveč na obstoječa pravila po ZVOP-1 in področnih zakonih, ki urejajo ravnanje z osebnimi podatki (npr. na delovno-pravnem področju). Podobno situacijo so zaznali tudi državni nadzorni organi drugih držav članic Evropske unije, vnovič pa se je tudi izkazalo, kako nevarne so delne izjeme, saj nekateri zavezanci delne izjeme razumejo kot popolne izjeme od dolžnosti upoštevanja pravil o varstvu osebnih podatkov.

Leta 2017 se je začela tudi priprava novega ZVOP-2, katerega nosilec je Ministrstvo za pravosodje. ZVOP-2 naj bi implementiral uredbo v naš pravni red in uredil področja, kjer lahko države članice ohranijo več maneverskega prostora (npr. pravila glede zdravstvenih, biometrijskih in genetskih podatkov), razmerje do drugih področij (npr. informacije javnega značaja, pravica do svobode izražanja, arhivarska, statistična in znanstveno-raziskovalna dejavnost) ter določene postopkovne vidike (npr. glede uveljavljanja pravic posameznika, prekrškovnih in upravnih postopkov glede varstva osebnih podatkov). Informacijski pooblaščenec je na osnutke ZVOP-2 za javno razpravo podal obširna mnenja.

Poseben izziv za določene upravljavce in obdelovalce osebnih podatkov predstavlja imenovanje pooblaščenih oseb za varstvo osebnih podatkov. Gre za institut, ki je v praksi prisoten kvečjemu v velikih bankah in zavarovalnicah, Splošna uredba pa določa precej širok krog zavezancev, ki bodo morali imenovati tovrstno osebo, in sicer ko:

- obdelavo opravlja javni organ ali telo, razen sodišč, kadar deluje kot sodni organ;
- temeljne dejavnosti upravljavca ali obdelovalca zajemajo dejanja obdelave, pri katerih je treba zaradi njihove narave, obsega in/ali namenov posameznike, na katere se osebni podatki nanašajo, redno in sistematično obsežno spremljati, ali
- temeljne dejavnosti upravljavca ali obdelovalca zajemajo obsežno obdelavo posebnih vrst podatkov v zvezi s kazenskimi obsodbami in prekrški.

Zelo pomembno bo, da bodo pooblaščenice osebe imele izkušnje na področju prakse in zakonodaje o varstvu osebnih podatkov, predvsem pa bo pomembna podpora vodstva, ki bo moralo v njih prepoznati notranji nadzorni organ, ki zastopa interese organizacije v smislu zmanjševanja tveganj, da pride do kršitev zakonodaje. Naloge pooblaščenih oseb so namreč nadzorne, svetovalne in obveščevalne, za skladnost z zakonodajo pa je odgovorno vodstvo.

Preventivno delovanje

Tudi leta 2017 je Informacijski pooblaščenec posebno pozornost posvetil preventivnim vidikom svojega delovanja. S ciljem **izobraževanja** upravljavcev in drugih zavezancev je izvedel več kot 100 brezplačnih predavanj domačim slušateljem. V stalnem stiku je 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. Podal je tudi več kot **100 mnenj na predloge zakonov** in drugih predpisov, ki se nanašajo na različne vidike urejanja, zbiranja in obdelave osebnih podatkov.

Maja 2017 je na Bledu potekalo prvo zasedanje **pobude »Initiative 2017«**, v okviru katere je Informacijski pooblaščenec gostil predstojnike nadzornih organov za varstvo osebnih podatkov iz Hrvaške, Srbije, Bosne in Hercegovine, Črne gore, Kosova in Makedonije. Namen pobude »Initiative 2017« je združiti moči nadzornih organov za varstvo osebnih podatkov z območja nekdanje skupne države, saj se soočamo s podobnimi strokovnimi vprašanji in izzivi. Tudi številna podjetja in organizacije javnega sektorja v regiji čezmejno zbirajo in izmenjujejo osebne podatke, zato je

zagotavljanje ustrezne in čim bolj enotne ravni varstva osebnih podatkov pomembno z gospodarskega vidika. Med ključnimi področji, o katerih je tekla razprava, so bili učinkovita implementacija novih evropskih standardov varstva osebnih podatkov, varstvo osebnih podatkov v telekomunikacijskem sektorju in učinkovit nadzor varstva osebnih podatkov v sektorju organov pregona. Udeleženci so se strinjali, da bo lahko ena od oblik sodelovanja v prihodnje izvedba regionalnih preventivnih preiskav na področju varstva osebnih podatkov s ciljem prepoznave dobrih praks in uvedbe visokih standardov varstva osebnih podatkov v izbranih sektorjih v vseh državah v regiji.

Predstojniki nadzornih organov so v okviru razprav soglašali, da danes učinkovitega varstva osebnih podatkov ne more biti brez dobrega mednarodnega sodelovanja med različnimi nadzornimi organi. To lahko glede na skupne gospodarske in zgodovinske okvire pomembno obogati kakovost dela vsakega od nadzornih organov na tem območju. Predstojniki so ob tej priložnosti zato podpisali deklaracijo o medsebojnem sodelovanju, s katero so se dogovorili za redna letna srečanja, katerih cilj bo izmenjava strokovnih stališč, izkušenj in dobrih praks pri reševanju izzivov nadzora nad varstvom osebnih podatkov.

Informacijski pooblaščenec uživa visok ugled pri kolegih iz držav nekdanje skupne države, kjer so že do zdaj pogosto prevzeli zakonodajne in praktične rešitve iz Slovenije, zato je prevzel vodilno vlogo pri združevanju in izmenjavi dobrih praks na področju varstva osebnih podatkov v regiji. Želi si tudi, da bi pobuda na področju varstva človekovih pravic dodatno prispevala h krepitvi dobrih odnosov med državami.

Kot enega temeljnih preventivnih orodij za pravočasni pristop k varstvu osebnih podatkov Informacijski pooblaščenec omogoča **neformalno izvedbo ocen učinkov na varstvo osebnih podatkov**. Leta 2017 se je tako na Informacijskega pooblaščenca obrnilo **več kot 100 upravljavcev** in obdelovalcev iz javnega in zasebnega sektorja, ki so pripravljali zakonodajo, rešitve ali projekte in se želeli o tveganjih pravočasno premisliti ter se tako izogniti kršitvam zakonodaje.

Izdali je tudi nove **smernice** ter napotke za upravljavce osebnih podatkov. Smernice za centre za socialno delo podajajo odgovore na najpogosteje zastavljena vprašanja glede varstva osebnih podatkov, s katerimi se srečujejo delavci na centrih za socialno delo, pa tudi stranke v postopkih, uporabniki storitev in upravljavci, ki posredujejo oziroma pridobivajo osebne podatke od centrov za socialno delo.

Leta 2017 je Informacijski pooblaščenec pripravil prve smernice po Splošni uredbi o varstvu podatkov, in sicer Smernice o ocenah učinkov na varstvo osebnih podatkov. Ocena učinka je orodje za identifikacijo, analizo in zmanjševanje tveganj glede nezakonitih ravnanj z osebnimi podatki, do katerih lahko pride pri določenem projektu, sistemu ali uporabi tehnologije. Ocene učinkov predstavljajo enega temeljnih preventivnih mehanizmov Splošne uredbe o varstvu osebnih podatkov in upravljavci, ki stremijo k odgovornemu ravnanju z osebnimi podatki posameznikov, bi morali prepoznati ocene učinka kot orodje, ki je primarno v njihovem interesu. Namenjeno je namreč pravočasni identifikaciji tveganj in sprejemu ustreznih ukrepov za obvladovanje tveganj, s čimer lahko upravljavci in obdelovalci preprečijo, da bi prišlo do kršitve zakonodaje. Kršitve namreč prinašajo možnost visokih kazni, obveznost poročanja o zaznanih kršitvah (v določenih primerih tudi obveščanje vseh prizadetih posameznikov), kar lahko vodi v zahtevne popravilne ukrepe, sankcije, negativno publiciteto in izgubo zaupanja. Zaupanje v odgovorno ravnanje s podatki posameznikov bi moralo biti v informacijski družbi, kjer so osebni podatki najpomembnejša valuta, ključno. Podjetja in institucije, ki bodo prepoznale pomen svobodne izbire posameznika in zaupanja v odgovorno ravnanje s podatki, bodo uspešnejša od tistih, ki ne bodo izvajala ukrepov za ohranitev in dvig zaupanja.

Veliko pozornosti je Informacijski pooblaščenec namenil ozaveščanju o Splošni uredbi o varstvu podatkov. V ta namen je pripravil **posebno podstran**⁶⁰, na kateri objavlja različna gradiva, med drugim je tam že objavljeno naslednje gradivo:

- Splošna uredba o varstvu osebnih podatkov – pogosta vprašanja in odgovori,

⁶⁰ <https://www.ip-rs.si/zakonodaja/reforma-evropskega-zakonodajnega-okvira-za-varstvo-osebni-podatkov/>

- informativni letak – 10 korakov za pripravo na GDPR,
- informativni letak – Kaj prinaša nova Splošna uredba (EU) o varstvu podatkov?
- informativni letak Evropske komisije za mala in srednja podjetja,
- povzetki posvetovanja z zainteresiranimi deležniki – Fablab (Bruselj, 5.– 6. april 2017).

Upravljavcem in obdelovalcem lahko zelo pomagajo mnenja in smernice na evropski ravni, ki jih Informacijski pooblaščenec pripravlja v sodelovanju z informacijskimi pooblaščenici iz drugih držav v okviru Delovne skupine iz člena 29. Leta 2017 so bila objavljena naslednja mnenja in smernice:

- Mnenje o ključnih vprašanjih Direktive o varstvu podatkov pri preprečevanju, odkrivanju in preiskovanju kaznivih dejanj (EU št. 2016/680) (WP 258, 29. 11. 2017),
- po javni razpravi revidirane Smernice o prenosljivosti podatkov (WP 242, 5. 4. 2017),
- po javni razpravi revidirane Smernice o pooblaščenih osebah za varstvo podatkov (WP 243, 5. 4. 2017),
- po javni razpravi revidirane Smernice za določitev vodilnega nadzornega organa za upravljavce ali obdelovalce (WP 244, 5. 4. 2017),
- po javni razpravi revidirane Smernice o oceni učinka na varstvo podatkov (WP 248 rev. 1, 4. 10. 2017),
- Smernice o privolitvi po Uredbi 2016/679 (WP 259, 28. 11. 2017).

Zlasti **smernice o privolitvi** bodo lahko v precejšnji pomoč upravljavcem, saj bodo nekateri od njih morali privolitve posameznikov vnovič pridobiti, zelo koristne pa so tudi **smernice o pooblaščenih osebah**, saj natančno pojasnjujejo, kdo mora pooblaščen osebo za varstvo osebnih podatkov imenovati, kakšne so naloge te osebe in njen položaj.

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 e-Uprave in 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 2017 so na primer nastopili na Workshop of National Data Protection Authorities Experts On Civil Drones Applications (Bruselj), Datacenter conference, na XVI. dnevih delovnega prava in socialne varnosti, konferenci Informatika v javni upravi 2017, konferenci Mreža znanja – Arnes, 8. mednarodni konferenci Dnevi korporativne varnosti, sodelovali so pri Pripravi gospodarstva na uveljavitev GDPR (GZS) na sejmu Feel the Future, na strokovnem srečanju zdravstvene informatike (SDMI), na konferenci GDPR/ZVOP-2, strokovnem posvetu IT-revizorjev (ISACA), strokovnem posvetu Združenja bank Slovenije, Dnevih korporativne varnosti in številnih drugih. Konec leta je Informacijski pooblaščenec v sodelovanju z zvezo potrošnikov Slovenije pripravil prijavo na EU razpis Rights, Equality and Citizenship Programme, Call: REC-AG-2017 (Call for proposals for action grants under 2017 Rights, Equality and Citizenship Work Programme), Topic: REC-RDAT-TRAI-AG-2017. Razpis je primarno namenjen nadzornim organom za varstvo osebnih podatkov, podpira pa ozaveščevalne aktivnosti o varstvu osebnih podatkov, ki imajo dve ključni ciljni skupini javnosti: mala in srednje velika podjetja ter splošno javnost. V okviru dvoletnega projekta Raising Awareness on Data Protection and the GDPR in Slovenia – RAPID.SI bo vzpostavljena posebna telefonska linija, na kateri bodo predstavniki podjetij lahko dobili nasvete, pripravljana bodo ozaveščevalna gradiva, vzpostavljeni bosta dve spletni mesti, organizirana pa bodo tudi predavanja. Projekt se bo predvidoma začel izvajati julija 2018.



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 2017 je Informacijski pooblaščenec izdal več kot 100 mnenj na predloge sprememb zakonov ter na predloge novih zakonov in drugih predpisov. Pri tem je zaznal 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.

Informacijski pooblaščenec je leta 2017 podal mnenje, pripombe oziroma je sodeloval pri pripravi naslednjih predpisov (v zvezi z nekaterimi je podal več mnenj):

- Osnutek Zakona o dostopnosti spletišč in mobilnih aplikacij,
- Predlog Zakona o trgu finančnih instrumentov,
- Predlog novele Zakona o javnem interesu v mladinskem sektorju,
- Predlog Zakona o notariatu,
- Predlog Zakona o konzularni zaščiti,
- Predlog novele Zakona o rejniški dejavnosti,
- Predlog Zakona o spremembah in dopolnitvah Zakona o javnih uslužbencih (tri mnenja),
- Predlog Zakona o spremembah in dopolnitvah Zakona o zbirkah podatkov s področja zdravstvenega varstva,
- Predlog Slovenskega zavarovalnega združenja za spremembe in dopolnitve Zakona o zavarovalništvu (dve mnenji),
- Predlog Zakona o spremembah in dopolnitvah Zakona o kmetijstvu (tri mnenja),
- Predlog Uredbe o izvajanju uredbe (EU) o skupni ribiški politiki,
- Predlog Zakona o spremembah in dopolnitvah Zakona o divjadi in lovstvu (dve mnenji),
- Predlog Uredbe o vodenju in vzdrževanju Poslovnega registra Slovenije,
- Predlog Uredbe o spremembah in dopolnitvah Uredbe o sodnem registru,
- Predlog Pravilnika o evidenci prekrškovnih organov, evidenci pravnomočnih sodb oziroma sklepov o prekrških, skupni evidenci kazenskih točk v cestnem prometu ter skupni informacijski infrastrukturi (dve mnenji),
- Predlog Pravilnika o priznavanju organizacij proizvajalcev in združenj organizacij proizvajalcev v sektorjih sadje in zelenjava, oljčno olje in namizne oljke ter hmelj,
- Predlog Zakona o sodnih izvedencih, cenilcih in tolmačih,
- Predlog Pravilnika o priznanju skupine proizvajalcev za skupno trženje,
- Predlog Pravilnika o naročanju in upravljanju čakalnih seznamov ter najdaljših dopustnih čakalnih dobah,
- Predlog Pravilnika o poslovanju državnega odvetništva (VI., X. in XII. poglavje – tri mnenja),
- Predlog Pravilnika o usposabljanju za varno delo s traktorjem in traktorskimi priključki (štiri mnenja),
- Osnutek Zakona o nepremičninskem posredovanju,
- Sporazum o zaposlovanju državljanov Republike Srbije v Republiki Sloveniji,
- Predlog Zakona o dolgotrajni oskrbi in obveznem zavarovanju za dolgotrajno oskrbo,
- Spremembe 19. in 21. člena Zakona o centralnem kreditnem registru (dve mnenji),
- Predlog Zakona o spremembah in dopolnitvah Zakona o varstvu okolja,
- Osnutek Odredbe o določitvi programa strokovnega usposabljanja za varnostnika čuvaja,
- Predlog direktive o interoperabilnosti elektronskih cestninskih sistemov ter lažji čezmejni izmenjavi informacij o neplačilih cestninah v Uniji,
- Predlog Zakona o informacijski varnosti (dve mnenji),
- Predlog Uredbe o spremembah in dopolnitvah Uredbe o izvajanju ukrepa Sheme kakovosti za kmetijske proizvode in živila iz Programa razvoja podeželja Republike Slovenije za obdobje 2014–2020,
- Predlog Zakona o evidentiranju dejanske rabe zemljišč javne cestne in javne železniške infrastrukture (dve mnenji),
- Uredba o načinu in obveznostih izvajanja javne službe kmetijskega svetovanja,
- Pravilnik o tehničnih pogojih, ki jih morajo izpolnjevati video elektronska identifikacijska sredstva,
- Uredba o javni službi nalog rastlinske genske banke,
- Uredba o javnih službah strokovnih nalog v proizvodnji kmetijskih rastlin,



- Predlog Pravilnika o evidenci posebnih kultur,
- Predlog Zakona o izobraževanju odraslih (dve mnenji),
- Predlog Srednjeročnega programa statističnih raziskovanj 2018–2022,
- Predlog Pravilnika o vzpostavitvi, vzdrževanju in upravljanju Registra dejanskih lastnikov (dve mnenji),
- Predlog osnutka besedila Izvedbenega sporazuma med Republiko Albanijo, Republiko Avstrijo, Bosno in Hercegovino, Republiko Bolgarijo, Madžarsko, Republiko Makedonijo, Republiko Moldavijo, Črno goro, Romunijo, Republiko Srbijo in Republiko Slovenijo o varstvu podatkov,
- Predlog Zakona o spremembah in dopolnitvah Zakona o izvrševanju kazenskih sankcij (dve mnenji),
- Spremembe Poslovnika občinskega sveta Občine Prevalje,
- Predlog Pravilnika o obrazcu vloge za izdajo potrdila A1 (dve mnenji),
- Osnutek Pravilnika o izvajanju notranje kontrole, pooblaščenca, hrambi in varstvu podatkov, strokovnem usposabljanju ter upravljanju evidenc pri zavezancih,
- Osnutek Pravilnika o reševanju na smučiščih,
- Pravilnik o določitvi pogojev za ugotavljanje in preverjanje istovetnosti stranke z uporabo sredstev elektronske identifikacije,
- Osnutek nove Odredbe o določitvi programa strokovnega usposabljanja za varnostnika,
- Osnutek Predloga Pravilnika o spremembah in dopolnitvah Pravilnika o policijskih pooblastilih,
- Osnutek Predloga Uredbe o izvajanju Uredbe (EU) št. 2015/847 Evropskega parlamenta in sveta z dne 20. maja 2015 o informacijah, ki spremljajo prenose sredstev, in razveljavitvi Uredbe,
- Predlog Sporazuma o avtomatizirani izmenjavi podatkov o DNA, daktiloskopskih podatkov in podatkov iz registrov vozil,
- Novela Zakona o pacientovih pravicah,
- Predlog dopolnjene nove Uredbe o upravnem poslovanju,
- Predlog Zakona o spremembah in dopolnitvah Zakona o izvršbi in zavarovanju (dve mnenji),
- Dopolnjen predlog sprememb Zakona o motornih vozilih (dve mnenji),
- Predlog Uredbe o izvajanju podukrepa pomoč za zagon dejavnosti, namenjene razvoju majhnih kmetij iz Programa razvoja podeželja Republike Slovenije za obdobje 2014–2020,
- Osnutek Pravilnika o izvajanju Zakona o varnosti na smučiščih,
- Predlog Uredbe o izvajanju Uredbe (EU) o preglednosti poslov financiranja z vrednostnimi papirji in ponovne uporabe,
- Predlog sprememb Zakona o lokalni samoupravi,
- Osnutek predloga Zakona o spremembah in dopolnitvah Zakona o pravnem varstvu v postopkih javnega naročanja,
- Predlog Zakona o spremembah in dopolnitvah Zakona o cestah (dve mnenji),
- Osnutek predloga Zakona o plačilnih storitvah, storitvah izdajanja elektronskega denarja in plačilnih sistemih,
- Predlog Zakona o spremembah in dopolnitvah Zakona o varuhu človekovih pravic,
- Predlog Pravilnika o kazenski evidenci in evidenci vzgojnih ukrepov,
- Predlog Pravilnika o spremembah in dopolnitvah Pravilnika o obliki in vsebini vpisnikov in pomožnih knjig pri prekrškovnih organih,
- Predlog Zakona o spremembah in dopolnitvah Zakona o integriteti in preprečevanju korupcije,
- Predlog Zakona o spremembah in dopolnitvah Zakona o cestninjenju (dve mnenji),
- Predlog Direktive Evropskega parlamenta in Sveta o nekaterih vidikih pogodb o dobavi digitalnih vsebin, COM (2015) 634 final,
- Osnutek Zakona o državni meteorološki, hidrološki, oceanografski in seizmološki službi (dve mnenji),
- Mnenje EDPS na 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 Zakona o izvrševanju Uredbe Evropske unije o preglednosti poslov financiranja z vrednostnimi papirji in ponovne uporabe,
- Predlog Zakona o spremembah in dopolnitvah Zakona o organizaciji in financiranju vzgoje in izobraževanja,
- Predlog Zakona o spremembah in dopolnitvah Zakona o strokovnih in znanstvenih naslovih,
- Predlog nove Uredbe o varstvu posameznikov pri obdelavi osebnih podatkov s strani institucij, organov, uradov in agencij Unije in o prostem pretoku takih podatkov,
- Predlog Zakona o varstvu pred ionizirajočimi sevanji in jedrski varnosti,
- Predlog Zakona o spremembah in dopolnitvah Zakona o kazenskem postopku,
- Predlog Zakona o spremembah in dopolnitvah Energetskega zakona,

- Predlog Zakona o spremembah in dopolnitvah Zakona o izdelkih iz plemenitih kovin,
- Predlog Zakona o probaciji (dve mnenji),
- Določbi 7. in 17. člena Sodnega reda (tri mnenja),
- Predlog načina vzpostavitve Evidence o preizkusih znanja v zvezi s 101.a členom Zakona o mednarodni zaščiti,
- Predlog Zakona o spremembah in dopolnitvah Zakona o poslovnem registru,
- Predlog Pravilnika o skupnih oznakah ob hkratnem izvajanju nalog nadzornika in reševalca na smučišču,
- Predlog Zakona o službi v Slovenski vojski,
- Predlog Zakona o obrambi,
- Predlog Zakona o spremembah in dopolnitvah Zakona o skupnosti študentov,
- Predlog Uredbe o izvajanju ukrepov iz Operativnega programa za izvajanje Evropskega sklada za pomorstvo in ribištvo v Republiki Sloveniji za obdobje 2014–2020, ki se izvajajo v skladu z javnimi razpisi,
- Zakon o dajatvah za motorna vozila,
- Osnutek predloga Pravilnika o spremembah in dopolnitvah Pravilnika o vsebinah vlog za izdajo dovoljenj dimnikarskim družbam in licenc dimnikarjem (dve mnenji),
- Osnutek predloga Pravilnika o dopolnilnem usposabljanju in dimnikarski izkaznici (dve mnenji),
- Osnutek predloga Sporazuma o čezmejni izmenjavi podatkov o elektronskem receptu in povzetku podatkov o pacientih,
- Predlog sprememb Zakona o izenačevanju možnosti invalidov,
- Predlog Uredbe o izvedbi ukrepov kmetijske politike za leto 2017,
- Predlog uredbe Evropskega parlamenta in Sveta o sodelovanju med nacionalnimi organi, odgovornimi za izvrševanje zakonodaje o varstvu potrošnikov,
- Predlog Zakona o osebni asistenci,
- Predlogi novih uredb o uporabi SIS,
- Predlog Gradbenega zakona,
- Predlog Zakona o spremembah in dopolnitvah Zakona o zdravstveni dejavnosti,
- Predlog Zakona o pooblaščenih arhitektih in inženirjih,
- Predlog Zakona o kakovosti in varnosti,
- Predlog Zakona o urejanju prostora.

4.2. Sodelovanje z javnostmi

Informacijski pooblaščenec je leta 2017 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.

Spletna stran Informacijskega pooblaščenca www.ip-rs.si, ki je bila prenovljena leta 2016, 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 najpogostejše 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;
- 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 2017 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 2017 je izdal smernice za centre za socialno delo in smernice Ocene učinkov na varstvo podatkov po Splošni uredbi o varstvu podatkov. S pomočjo smernic naj bi upravljavci dobili priporočila, kako naj v praksi zadostijo zahtevam ZVOP-1. Namen smernic je namreč podati skupne praktične napotke za upravljavce zbirk osebnih podatkov na jasn, razumljiv in uporaben način ter s tem odgovoriti na najpogosteje zastavljena vprašanja s področja varstva osebnih podatkov, s katerimi se srečujejo posamezni upravljavci. Pravno podlago za izdajo smernic Informacijskemu pooblaščenca daje 49. člen ZVOP-1, ki med drugim določa, da Informacijski pooblaščenec daje neobvezna mnenja, pojasnila in stališča o vprašanih s področja varstva osebnih podatkov in jih objavlja na spletni strani ali na drug primeren način ter pripravlja in daje neobvezna navodila in priporočila glede varstva osebnih podatkov na posameznem področju.

Informacijski pooblaščenec publikacij že dalj časa ne tiska, ampak jih objavi 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 sodeloval na različnih izobraževalnih konferencah, delavnicah in okroglih mizah. Leta 2017 so zaposleni pri Informacijskem pooblaščenca izvedli kar **132 brezplačnih predavanj** za različne strokovne javnosti in zavezance na obeh področjih delovanja, tj. za upravljavce osebnih podatkov (100 predavanj) in zavezance za posredovanje informacij javnega značaja (32 predavanj).

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 **posvet z naslovom Pravice posameznikov in dolžnosti upravljavcev osebnih podatkov po novi evropski Splošni uredbi o varstvu podatkov** v dvorani Zdravniške zbornice Slovenije. Dogodek je bil namenjen iskanju odgovorov na vprašanja, katere novosti in izboljšave ter tudi izzive prinaša evropska reforma varstva osebnih podatkov za posameznike in njihove pravice ter seveda za upravljavce. Evropa je s sprejemom nove evropske Splošne uredbe o varstvu podatkov naredila pomemben korak za zagotavljanje učinkovitejšega varstva osebnih podatkov. Pomen tega področja in dejstvo, da so osebni podatki valuta sodobnega sveta, najbolj nazorno ponazarja sam postopek sprejemanja uredbe: Evropska reforma varstva osebnih podatkov je rezultat večletnih razprav – od prvega predloga uredbe do njenega sprejetja so minila štiri leta, v tem času pa so odločevalci na osnovni predlog od različnih interesnih skupin dobili kar 4000 amandmajev.

Informacijska pooblaščenka Mojca Prelesnik je poudarila, da zaradi hitrega razvoja sodobnih tehnologij Direktiva o varstvu podatkov iz leta 1995 ni več sledila zahtevam sodobne e-družbe in novim načinom obdelav osebnih podatkov, zato je EU sprejela Splošno uredbo o varstvu podatkov, ki se bo začela uporabljati 25. maja 2018. Do takrat bodo potrebne prilagoditve, saj ureja številna področja podrobneje ali drugače kot trenutno še veljavni ZVOP-1. Tako se na primer posameznikovo soglasje k obdelavi njegovih osebnih podatkov nikoli ne predvideva, ampak mora posameznik s tem jasno in aktivno soglašati. Upravljalci bodo o kršitvah varstva osebnih podatkov obvezani obveščati, nova pravila za obravnave kršitev bodo presegala meje ene same države članice EU. Globe za kršitelje bodo bistveno višje, javni sektor, pri bolj tveganih obdelavah in podatkih pa tudi podjetja, bodo morali imenovati posebno odgovorno osebo za varstvo podatkov. Nova je tudi ureditev obdelav osebnih podatkov v več kot eni državi članici – načelo »vse na enem mestu« prinaša pristojnost organa ene države članice, četudi bodo v določenem postopku obdelovani podatki državljanov različnih držav EU.

Predstavniki upravljavcev, resornega ministrstva in različnih strokovnjakov za varstvo osebnih podatkov so predstavili svoj pogled na pomen varstva osebnih podatkov in odprli razpravo o nalogah pri pripravah na izvajanje uredbe v letu 2017: dr. Andrej Možina, predsednik Zdravniške zbornice Slovenije, je predstavil pomen varstva občutljivih osebnih podatkov v zdravstvu; Boris Koprivnikar, minister za javno upravo, je predstavil prispevek z naslovom Kaj država ve o tebi?; Peter Pavlin z Ministrstva za pravosodje se je osredotočil na implementacijo Splošne uredbe o varstvu podatkov in vprašanje zagotovitve pravne varnosti ter velike pomembnosti človekove pravice do varstva osebnih podatkov; namestnik informacijske pooblaščenke mag. Andrej Tomšič je predstavil nove pravice, ki jih prinaša uredba; novinar Domen Savič je prikazal možnost seznanitve z lastnimi osebnimi podatki v praksi; svetovalec pri Informacijskem pooblaščenku mag. Urban Brulc je predstavil pravico do seznanitve z lastnimi osebnimi podatki in lastno zdravstveno dokumentacijo po uveljavitvi uredbe; pravico do varstva zasebnosti in varstva osebnih podatkov z vidika pacienta je predstavila varuhinja pacientovih pravic Duša Hlade Zore.

Že tradicionalno je Informacijski pooblaščenec podelil **priznanja za dobro prakso na področju varstva osebnih podatkov**:

- **Priznanje ambasador zasebnosti** je prejelo podjetje TIBOPO, d. o. o., za pristop k razvoju sistema mDrive, ki želi izboljšati prometno varnost (gre za sistem za nadzor dvoročnega upravljanja z vozili, ki na podlagi analize slike iz kamere detektira položaj rok na volanu in s tem pomaga reševati motnje pozornosti oziroma distrakcije, kot je npr. telefoniranje, pisanje SMS-sporočil ali prehranjevanje med vožnjo), saj so se že ob snovanju sistema zavedali pomena zasebnosti in so pripravili predhodno oceno učinka na varstvo osebnih podatkov. S tem so pravočasno zmanjšali možne negativne vplive na varstvo osebnih podatkov in v sam sistem vgradili primerne varovalke.
- **Priznanje za dobro prakso na področju varovanja osebnih podatkov v javnem sektorju** je prejela Podružnična šola Podkum, Osnovna šola Ivana Skvarče Zagorje ob Savi. Šola je zmagala na natečaju za najboljšo učno uro na temo zasebnosti in varstva osebnih podatkov, ki ga je Informacijski pooblaščenec pripravil v evropskem projektu ARCADES. Uvajanje poučevanja varstva osebnih podatkov in zasebnosti na spletu že pri mlajših otrocih je primer odlične prakse in zato zgled vsem šolam.
- **Priznanje za dobro prakso na področju varovanja osebnih podatkov v zasebnem sektorju** je prejelo podjetje Elektro Ljubljana, d. d., in sicer zaradi zavedanja pomena varstva osebnih podatkov, ki je pri tej družbi vpeljano v sam sistem dela. Odraža se v zavesti zaposlenih in v tehničnih rešitvah za preprečevanje zlorab. Proaktivnost za dvig ravni varstva osebnih podatkov je razvidna iz celovitega pristopa k organizacijskim in tehničnim procesom.
- Posebna priznanja družbam, ki so leta 2016 pridobile **certifikat po standardu za varovanje informacij ISO/IEC 27001** in s tem izkazale visoko raven varovanja osebnih podatkov: Doctrina, d. o. o., Imagine, d. o. o., ISKRAEMECO, d. d., ISKRATEL, d. o. o., PRO Servis, d. o. o., in VIBOR, 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). Dogodki, ki na ta dan potekajo po vsem svetu, opozarjajo na pravico dostopa do informacij javnega značaja kot temeljno človekovo pravico, ki prispeva k bolj odprti in demokratični družbi ter posameznikom in civilni družbi omogoča aktivno



udeležbo v pomembnih javnopravnih zadevah. Leta 2017 je Informacijski pooblaščenec ta dan posvetil transparentnosti porabe javnega denarja; dogodek je nosil naslov **Nadzor nad porabo javnega denarja – imam pravico vedeti**. Pomembna funkcija pravice vedeti, ki je pomembno orodje za doseg odprtega, preglednega in odgovornega delovanja javne uprave, je namreč tudi nadzorna funkcija, v okviru katere se imajo državljani pravico seznaniti z informacijami o tem, kako in za kakšne namene organi javnega sektorja porabljajo javni denar. Boljši dostop do informacij o porabi javnega denarja povečuje kakovost odločanja in prispeva k racionalnejši porabi javnih sredstev ter zmanjšuje korupcijska tveganja.

Udeležence posveta sta nagovorila informacijska pooblaščenka Mojca Prelesnik in Mitja Bervar, predsednik Državnega sveta, v prostorih katerega je potekal posvet. Informacijska pooblaščenka je poudarila, da lahko le transparentna družba zagotavlja in podpira človekove pravice. V času, ko se zaradi številnih družbenih in političnih razlogov, pa tudi zaradi hitrega tehnološkega razvoja krepi potreba po nadzoru, na dolgi rok le odprtost in transparentnost krepi zaupanje državljanov v javno oblast. Svoj nagovor je končala z mislijo, da transparentnost podatkov o porabi javnih sredstev ne sme biti sama sebi namen, ampak je predvsem vzvod, s katerim se zmanjšujejo korupcijska tveganja in s katerim se aktivira druge družbene vzvode. Na tem področju mora tudi javnost prevzeti odgovorno vlogo, in to tako, da informacije postavi v pravičen kontekst in prek njih opozori na vprašanja, ki pomembno vplivajo na življenje ljudi. Transparentnost je orodje za doseg cilja, to pa sta predvsem povečanje zaupanja državljanov v javni sektor in možnost sodelovanja v družbeno pomembnih odločitvah.

Ker je transparentnost na področju porabe javnega denarja pomembna tema, je Informacijski pooblaščenec k sodelovanju povabil tako predstavnike državnih institucij kot predstavnike civilne družbe, ki so problematiko predstavili iz različnih zornih kotov. Predsednik Računskega sodišča Tomaž Vesel je predstavil pogled Računskega sodišča na načelo transparentnosti pri nadzoru nad porabo javnega denarja; Urška Ban, poslanka Državnega zbora RS in predsednica Odbora za finance in monetarno politiko ter članica Komisije za nadzor javnih financ, se je osredotočila na fiskalno transparentnost kot načelo dobrega upravljanja z javnim denarjem, in sicer v luči pristojnosti in odgovornosti Državnega zbora; Borut Smrdel, predsednik Državne revizijske komisije, ki bdi nad pravilnostjo postopkov javnega naročanja, je predstavil načelo transparentnosti, ki je pomemben vzvod za zagotavljanje pravilnosti in gospodarnosti v postopkih javnega naročanja; mag. Mateja Prešeren, vodja Službe za transparentnost, integriteto in politični sistem na Ministrstvu za javno upravo, je vprašanje nadzora nad porabo javnega denarja predstavila z vidika vse pomembnejše proaktivne objave informacij; Jure Brankovič, novinar oddaje Tarča na RTV Slovenija, ki je odprl številne odmevne medijske zgodbe o (ne)transparentni porabi javnega denarja, je svoj novinarsko-kritični pogled predstavil v prispevku *Kako ustaviti javnost?*, Sebastijan Peterka, vodja projektov, katerih namen je krepitev preglednosti in transparentnosti delovanja javnega sektorja ter nadzor nad porabo javnega denarja, in raziskovalec pri Transparency International Slovenija, pa je na primeru Zavoda RS za blagovne rezerve opozoril, da je zapoznelost informacij enaka zavrnitvi.

Informacijski pooblaščenec je podelil tudi **priznanje ambasador transparentnosti** za dobro prakso na področju dostopa do informacij javnega značaja. Prejela ga je Uprava RS za varno hrano, veterinarstvo in varstvo rastlin, ki med drugimi opravlja naloge na področjih varstva potrošnikov, varne hrane, varovanja zdravja in dobrobiti živali ter varstva rastlin. Ker gre za področja, ki so za zdravje ljudi še posebej pomembna, sta dobra obveščenost javnosti in hiter dostop do informacij bistvena. Uprava je v zadnjih letih dokazala, da je pri svojem delu zavezana transparentnosti, tudi proaktivni. S široko objavo informacij in ugotovitev iz postopkov inšpekcijskih nadzorov (npr. iz nadzorov nad pekarnami, gostinskimi obrati in čebelarji) je lahko za zgled ostalim inšpekcijskim organom. Dokazala je, da je načelo varstva podatkov iz inšpekcijskih postopkov v praksi mogoče uspešno uravnovežiti z načelom javnosti delovanja. Tako je javnosti zagotovila boljši dostop do informacij in omogočila javno razpravo o skupnih zadevah v javnem interesu.

Informacijski pooblaščenec je 15. 5. 2017 na Bledu gostil **ustanovno zasedanje pobude Initiative 2017**, na katerem so sodelovali predstojniki nadzornih organov za varstvo osebnih podatkov iz Hrvaške, Srbije, Bosne in Hercegovine, Črne gore, Kosova in Makedonije. Pobuda Informacijskega pooblaščenca za Initiative 2017 sledi zgledu nordijskih držav, ki si delijo podobne zgodovinske, kulturne in pravne okvire in katerih nadzorni organi za varstvo osebnih podatkov tesno sodelujejo ter si izmenjujejo izkušnje. Namen pobude Initiative 2017 je združiti moči nadzornih organov za varstvo osebnih podatkov z območja nekdanje skupne države, saj se soočajo s podobnimi strokovnimi vprašanji in izzivi. Tudi številna podjetja in organizacije javnega sektorja v regiji čezmejno zbirajo in izmenjujejo osebne podatke, zato je zagotavljanje ustrezne in čim bolj enotne ravni varstva osebnih podatkov pomembno z gospodarskega vidika.

Med ključnimi področji, o katerih je tekla razprava, so bili učinkovita implementacija novih evropskih standardov varstva osebnih podatkov, varstvo osebnih podatkov v telekomunikacijskem sektorju in učinkovit nadzor varstva osebnih podatkov v sektorju organov pregona. Udeleženci so se strinjali, da bo lahko ena od oblik sodelovanja v prihodnje izvedba regionalnih preventivnih preiskav na področju varstva osebnih podatkov s ciljem prepoznavne dobrih praks in uvedbe visokih standardov varstva osebnih podatkov v izbranih sektorjih v vseh državah v regiji.

Predstojniki nadzornih organov so v okviru razprav soglašali, da učinkovitega varstva osebnih podatkov ne more biti brez dobrega mednarodnega sodelovanja med različnimi nadzornimi organi. To lahko glede na skupne gospodarske in zgodovinske okvire pomembno obogati kakovost dela vsakega od nadzornih organov na tem območju. Predstojniki so podpisali deklaracijo o medsebojnem sodelovanju, s katero so se dogovorili za redna letna srečanja, katerih cilj bo izmenjava strokovnih stališč, izkušenj in dobrih praks pri soočanju z izzivi, ki jih predstavlja nadzor nad varstvom osebnih podatkov.

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 2017 na ravni EU aktivno 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 Cooperation, Technology, E-government ter Future of Privacy),
- v Skupnem nadzornem organu za Europol, ki se je z uveljavitvijo Uredbe o Europolu maja 2017 preoblikoval v Europolov Odbor za sodelovanje (za nadzor nad obdelavo osebnih podatkov v okviru Eurolpa je po Uredbi o Europolu primarno pristojen Evropski nadzorni organ za varstvo osebnih podatkov (EDPS), ki pa je pri tem dolžan tesno sodelovati z nacionalnimi organi za varstvo osebnih podatkov),
- v Skupnem nadzornem organu za carino,
- na koordinacijskih sestankih EDPS in nacionalnih organov za varstvo osebnih podatkov za nadzor nad SIS II,
- na koordinacijskih sestankih EDPS in nacionalnih organov za varstvo osebnih podatkov za nadzor nad CIS,
- na koordinacijskih sestankih EDPS in nacionalnih organov za varstvo osebnih podatkov za nadzor nad VIS,
- na koordinacijskih sestankih EDPS in nacionalnih organov za varstvo osebnih podatkov za nadzor nad Eurodac.

WP29, ki Evropski komisiji daje strokovna mnenja s področja varstva osebnih podatkov, je bila leta 2017 osredotočena predvsem na priprave na uporabo Splošne uredbe o varstvu podatkov. Skupina je sodelovala tudi pri prvem pregledu delovanja t. i. Ščita zasebnosti EU–ZDA, ki skladno z dogovorom med Evropsko komisijo in ameriško vlado iz leta 2016 omogoča enostaven prenos osebnih podatkov iz EU certificiranim organizacijam v ZDA.

WP29 je leta 2017 sprejela naslednje pomembne smernice in mnenja:

- Smernice o pravici do prenosljivosti podatkov (WP 242),
- Smernice o pooblaščenih osebah za varstvo osebnih podatkov (»DPO«) (WP 243),
- Smernice o vodilnem nadzornem organu (WP 244),
- Mnenje št. 01/2017 o predlogu Uredbe o zasebnosti in elektronskih komunikacijah (2002/58/ES) (WP 247),
- Smernice o oceni učinka na varstvo podatkov (DPIA) (WP 248),
- Mnenje 2/2017 o obdelavi podatkov pri delu (WP 249),
- Smernice o uradnem obvestilu nadzornemu organu o kršitvi varstva osebnih podatkov po Uredbi 2016/679 (WP 250),
- Smernice o avtomatiziranem posameznem sprejemanju odločitev in oblikovanju profilov za namene Uredbe 2016/679 (WP 251),



- Mnenje št. 03/2017 o obdelavi osebnih podatkov v okviru sodelovalnih inteligentnih prometnih sistemov (C-ITS) (WP 252),
- Smernice o uporabi in določanju upravnih glob za namene Uredbe 2016/679 (WP 253),
- Delovni dokument o kriteriju skladnosti (WP 254),
- Delovni dokument o zavezujočih poslovnih pravilih za obdelovalce osebnih podatkov (WP 256),
- Delovni dokument o zavezujočih poslovnih pravilih za upravljavce osebnih podatkov (WP 257),
- Mnenje o nekaterih ključnih vprašanjih t. i. Direktive o kazenskem pregonu 2016/680 (WP 258),
- Smernice o privolitvi po Uredbi 2016/679 (WP 259),
- Smernice o transparentnosti v skladu z Uredbo 2016/679 (WP 260).

V okviru WP29 je Informacijski pooblaščenec aktivno sodeloval predvsem v štirih njenih podskupinah, in sicer v podskupinah Cooperation, Technology, E-government ter Future of Privacy, delo v okviru ostalih podskupin WP29 pa je zaradi pomanjkanja resursov le spremljal.

Informacijski pooblaščenec je tudi leta 2017 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 pooblaščenecv in organov za varstvo osebnih podatkov in zasebnosti s celega sveta. Delovna skupina je na zasedanjih v Washingtonu in Parizu sprejela štiri nove delovne dokumente, ki so pomemben znak konsenza glede določenih vprašanj varstva osebnih podatkov na mednarodni ravni, predvsem glede izzivov, ki jih prinašajo nove tehnologije. Delovni dokument o vprašanjih zasebnosti in varnosti pri delovanju platform za e-učenje (https://www.datenschutz-berlin.de/pdf/publikationen/working-paper/2017/25042017_en_2.pdf) naslavlja izzive, ki jih prinaša IT-podprto učenje. Obseg zbranih podatkov o učečih je lahko neprimerno večji, o njih je možno zbirati tudi zdravstvene podatke (npr. nagnjenost k disleksiji, napovedovanje učnih težav ipd.), zato delovni dokument obravnava tovrstna tveganja ter podaja priporočila za šole, ponudnike platform, zakonodajalce in nadzorne organe za varstvo osebnih podatkov. Drugi delovni dokument pa predstavlja poziv k upoštevanju temeljnih demokratičnih načel ter poziv k vpeljavi strožjih mehanizmov nadzora nad delovanjem obveščevalnih služb. Delovni dokumenti IWGDPT pogosto predstavljajo pomemben prispevek k mednarodnim resolucijam o varstvu osebnih podatkov, kar velja tudi za ta delovni dokument. Na srečanju v Parizu sta bila sprejeta delovna dokumenta o nadgradnji strojne programske opreme (angl. *firmware*) ter o varovanju osebnih podatkov registrantov spletnih domen v t. i. *whois* direktoriju, ki ga vodi ICANN (International Corporation for Assigned Names and Numbers). Dokumenta bosta po pregledu javno objavljena na spletni strani delovne skupine (<https://www.datenschutz-berlin.de/working-paper.html>).

V okviru Sveta Evrope je predstavnik Informacijskega pooblaščenca tudi leta 2017 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 junija in novembra na plenarnih zasedanjih obravnaval vprašanja procesa dokončanja in sprejema posodobljene Konvencije št. 108, ki poteka od začetka leta 2011, ter stanje pridruženja držav h Konvenciji 108 in k dodatnemu protokolu. 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. Odbor je leta 2017 aktivno pripravljal Priporočilo glede zaščite zdravstvenih podatkov in Vodič glede uporabe osebnih podatkov v policijskem sektorju ter sodeloval z drugimi odbori pri pripravi Smernic glede varovanja zasebnosti v medijih. Pripravljati je začel novo poročilo o umetni inteligenci.

4.3.2. Ostale mednarodne dejavnosti

Leta 2017 je Informacijski pooblaščenec dal pobudo za Initiative 20i7 z namenom združiti moči nadzornih organov za varstvo osebnih podatkov z območja nekdanje Jugoslavije, saj se ti soočajo s podobnimi strokovnimi vprašanji in izzivi. Tudi številna podjetja in organizacije javnega sektorja v regiji čezmejno zbirajo in izmenjujejo osebne podatke, zato je zagotavljanje ustreznih in čim bolj enotnih ravni varstva osebnih podatkov pomembno z gospodarskega vidika. Cilj Initiative 20i7 je tesno sodelovanje in izmenjava dobrih praks na področju varstva osebnih podatkov v regiji, ki lahko kot pobuda na področju varstva človekovih pravic dodatno prispeva h krepitvi dobrih odnosov med državami. Na prvem srečanju Initiative 20i7, ki je maja potekalo na Bledu, so predstojniki nadzornih organov za varstvo osebnih podatkov iz Hrvaške, Srbije, Bosne in

Hercegovine, Črne gore, Kosova, Makedonije in Slovenije razpravljali o implementaciji novih evropskih standardov varstva osebnih podatkov, varstvu osebnih podatkov v telekomunikacijskem sektorju in učinkovitem nadzoru varstva osebnih podatkov v sektorju organov pregona. Udeleženci so se strinjali, da bo lahko ena od oblik sodelovanja izvedba regionalnih preventivnih preiskav na področju varstva osebnih podatkov s ciljem prepoznave dobrih praks in uvedbe visokih standardov varstva osebnih podatkov v izbranih sektorjih v vseh državah v regiji. Predstojniki so podpisali deklaracijo o medsebojnem sodelovanju, s katero so se dogovorili za redna letna srečanja, katerih cilj bo izmenjava strokovnih stališč, izkušenj in dobrih praks pri soočanju z izzivi ob nadzoru nad varstvom osebnih podatkov.

Informacijski pooblaščenec je leta 2017 gostil predstavnike sorodnih institucij iz Turčije in Makedonije ter jim predstavil svoje delovanje in dobre prakse s področij, za katera je pristojen.

Informacijski pooblaščenec je leta 2017 pripravil odgovore na 98 vprašanj in vprašalnikov tujih organov za varstvo osebnih podatkov, mednarodnih organizacij, akademskih in raziskovalnih inštitucij ter tujih nevladnih organizacij.

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 2017 Informacijski pooblaščenec ni prejel nobene pritožbe zaradi nezakonite obdelave osebnih podatkov iz SIS II kot tudi ne zaradi neizvajanja oziroma neustreznega izvajanja pravice do seznanitve z lastnimi osebnimi podatki iz SIS II.

Predstavnica Informacijskega pooblaščenca je kot državna strokovnjakinja sodelovala pri izvedbi Schengenske evalvacije Švedske na področju varstva podatkov.

4.3.3. Sodelovanje na mednarodnih srečanjih

Leta 2017 so se zaposleni pri Informacijskem pooblaščenču poleg sestankov v okviru mednarodnih dejavnosti (delovne skupine EU, projekti) udeležili tudi naslednjih mednarodnih konferenc:

- 22.–24. februar, Berlin, Nemčija: European Information Commissioners and Ombudsmen meeting,
- 23. marec, Bruselj, Belgija: CPC/Data Protection Workshop,
- 23.–26. marec, Strasbourg, Francija: Konferenca »Promoting dialogue between the European Court of Human Rights and the media freedom community«,
- 4.–6. april, Bruselj, Belgija: FabLab,
- 19.–21. junij, Manchester, Velika Britanija: 29th European Case Handling Workshop,
- 6.–8. september, Tartu, Estonija: Konferenca »E-Volution of Data Protection«,
- 10.–15. september, Trier, Nemčija: European Data Protection Law: ERA Summer Course,
- 19.–21. september, Manchester, Velika Britanija: ICIC Manchester 2017,
- 23. september–1. oktober, Hongkong: 39th International Conference of Data Protection and Privacy Commissioners (the 39th ICDPPC),
- 23. oktober, Bruselj, Belgija: Stakeholder workshop on GDPR implementation and health data,
- 6.–8. december, Podgorica, Črna gora: Konferenca »Anti corruption week – Free Access to Information«,
- 11. december, Bruselj, Belgija: Meeting Taskforce 11/12.



4.3.4. Projekti Informacijskega pooblaščenca

4.3.4.1. Projekt CRISP



Informacijski pooblaščenec je med letoma 2014 in 2017 sodeloval v konzorciju EU FP7 projekta CRISP (https://cordis.europa.eu/project/rcn/185503_en.html), katerega namen je bil 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: poleg **varnosti** sistema sta s pomočjo te metodologije ocenjeni tudi dimenziji **zaupanja** in **učinkovitosti**, pa tudi vpliv sistema na morebitne kršitve **človekovih pravic s posebnim poudarkom na varstvu osebnih podatkov** in to, kako sistem prispeva k skladnosti z novo Splošno uredbo o varstvu podatkov (t. i. STEFi dimenzije).

Slika 17: Shematski prikaz dimenzij STEFi za evalvacijo varnostnih sistemov



Projekt se je uspešno zaključil aprila 2017. V zadnjem letu projekta je Informacijski pooblaščenec vodil delo celotnega konzorcija kot vodja Delovnega paketa 7. Pri tem so bile opravljene naslednje aktivnosti:

- Izvajale so se aktivnosti za dvigovanje zaupanja v predlagano rešitev za evalvacijo, in sicer s pripravo informacijskega gradiva, 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 je bil izveden postopek standardizacije pristopa evalvacije na podlagi STEFi dimenzij v obliki dokumenta CEN Workshop Agreement (CWA); to je dokument dobre prakse, ki ga potrdijo organizacije, ki se formalno registrirajo v postopek sprejema, in velja tri leta z možnostjo podaljšanja. Dokument CRISP CWA »Guidelines for the evaluation of installed security systems, based on STEFi criteria« opredeljuje metodologijo za evalvacijo in navaja primere meril, ki temeljijo na posamezni dimenziji STEFi, med drugim tudi merila, ki zagotavljajo skladnost z določbami nove Splošne

uredbe o varstvu podatkov. CRISP CWA predstavlja najpomembnejši prispevek projekta CRISP; marca 2017 ga je potrdilo evropsko standardizacijsko telo CEN in takrat je bil tudi objavljen na <ftp://ftp.cencenelec.eu/EN/ResearchInnovation/CWA/CWA1714700.pdf>.

- Informacijski pooblaščenec je vse dejavnosti, izvedene v okviru Delovnega paketa 7, predstavil v podrobnem poročilu za Evropsko komisijo, ki je dostopno na povezavi http://crisproject.eu/wp-content/uploads/2017/05/CRISP_D7.1_Consolidated-WP7-report.pdf.

V konzorciju projekta CRISP so sodelovali: 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 bil sofinanciran s strani Sedmega okvirnega programa Evropske skupnosti za raziskave, tehnološki razvoj in predstavitvene dejavnosti (številka dogovora 607941).



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

Jasna Duralija, svetovalka

Alenka Jerše, namestnica informacijske pooblaščenke

mag. Eva Kalan Logar, državna nadzornica za varstvo osebnih podatkov

mag. Kristina Kotnik Šumah, namestnica informacijske pooblaščenke

mag. Andrej Tomšič, namestnik informacijske pooblaščenke

Oblikovanje:

Anže Novak in **Bons, d. o. o.**

Lektorirala:

Katja Klopčič Lavrenčič

Informacijski pooblaščenec Republike Slovenije

Zaloška cesta 59

1000 Ljubljana

www.ip-rs.si

gp.ip@ip-rs.si

Ljubljana, maj 2018