

15 LET

ZAKONA O DOSTOPU DO
INFORMACIJ JAVNEGA
ZNAČAJA

1. LETO

SPLOŠNE UREDBE
O VARSTVU
PODATKOV

LETNO POROČILO

Informacijskega pooblaščenca za leto 2018



'18

UVODNA BESEDA INFORMACIJSKE POOBLAŠČENKE

Spoštovani,

Isto 2018 je bilo na obeh področjih dela Informacijskega pooblaščenca v določeni meri prelomno, tako vsebinsko kot glede na izzive in obseg dela. Na področju dostopa do informacij javnega značaja smo obeležili 15. obletnico uveljavitve Zakona o dostopu do informacij javnega značaja (ZDIJZ). Področje varstva osebnih podatkov pa je v preteklem letu brez dvoma zaznamoval začetek uporabe Splošne uredbe o varstvu podatkov (Splošne uredbe), ki pomeni prelomnico in prinaša številne novosti v načinu varstva osebnih podatkov v Evropski uniji (EU) in posledično tudi na nacionalni ravni. Hkrati je bila sprejeta prenovljena Konvencija Sveta Evrope o varstvu podatkov, s katero se ta trend sprememb širi bistveno preko meja EU.

Na področju dostopa do informacij javnega značaja je Informacijski pooblaščenec leta 2018 obravnaval 549 pritožbenih postopkov in znova zaznal nekaj pozitivnih kazalnikov: na eni strani to kaže na večjo seznanjenost prosilcev s pravico dostopa do informacij javnega značaja in na drugi boljše odzivanje zavezancev na njihove zahteve. Trend rasti števila pritožbenih zadev zadnjih nekaj let se je nadaljeval tudi leta 2018, kar kaže, da so prosilci s postopkom uresničevanja pravice do pravnega varstva dobro seznanjeni in ga tudi uporabljajo. Pritožbeni postopek je za prosilce v celoti brezplačen in relativno hiter, zato Informacijski pooblaščenec ocenjuje, da je z njim zagotovljeno učinkovito pravno varstvo pravice dostopa do informacij javnega značaja. Informacijski pooblaščenec je leta 2018 še skrajšal povprečni čas reševanja pritožbenih zadev, in sicer je ta znašal 32 dni. Klub temu da Informacijski pooblaščenec sodelovanje z zavezanci ocenjuje kot zgledno (leta 2018 zoper njih ni uvedel nobenega postopka zaradi prekrškov po ZDIJZ, ZInFP ali ZMed), pa ugotavlja, da je leta 2018 znova naraslo število pritožb zaradi t. i. molka organa in da je bilo, po letu 2017, ko je ta trend padel, spet vloženih več pritožb zoper občine.

Tudi leta 2018 je Informacijski pooblaščenec prejel številna zaprosila za mnenja in stališča, ki jih nudi v okviru neformalnega svetovanja, na podlagi primerov iz prakse, ki jih je že obravnaval. Navedeno kaže, da so bili zavezanci v tem letu aktivni in odzivni ter so se z vprašanji pogosto obrnili na Informacijskega pooblaščenca tudi izven pritožbenega postopka, torej tudi takrat, ko jim zakon tega ne nalaga. Da so zavezanci z Informacijskim pooblaščencem pripravljeni sodelovati in da upoštevajo njegova priporočila, izhaja tudi iz relativno majhnega deleža upravnih sporov, ki so sproženi zoper odločbe Informacijskega pooblaščenca; zavezanci in prosilci odločitve Informacijskega pooblaščenca spoštujejo in sprejemajo.

Na področju varstva osebnih podatkov je Informacijski pooblaščenec leta 2018 posvetil učinkovitemu začetku uporabe nove Splošne uredbe, tako z vidika ozaveščanja zavezancev ter posameznikov o novostih, podajanja pripomb v okviru postopka priprav novega zakona o varstvu osebnih podatkov kot tudi z vidika reorganizacije in krepitev organa s ciljem zagotavljanja učinkovitega izvajanja nadzora in uveljavljanja pravic posameznikov ter drugih pristojnosti Informacijskega pooblaščenca v novih okvirih in ob bistvenem porastu pripada novih zadev. Informacijski pooblaščenec je podobno kot v preteklih letih tudi leta 2018 prejel veliko prijav s strani posameznikov. Informacijski pooblaščenec je leta 2018 vodil 1029 inšpeksijskih zadev (57 % več kot leto pred tem). Občutno povečanje števila prijav je nedvomno rezultat večje ozaveščenosti posameznikov, saj se je o Splošni uredbi v medijih veliko govorilo in pisalo. Z majem 2018 je Informacijski pooblaščenec postal član novega telesa EU – Evropskega odbora za varstvo podatkov, katerega odločitve so zavezujoče tudi za Slovenijo.

Izkušnje prvega leta uporabe Splošne uredbe kažejo, da pomeni neposredna uporaba Splošne uredbe velik izliv, ki bo terjal precejšnjo pozornost tudi v prihodnjih letih. Še posebej glede na to, da Slovenija Direktive, ki se nanaša na organe pregona, še ni prenesla v svoj pravni red in ni sprejela predpisov za izvedbo Splošne uredbe. To v praksi pomeni številne pravne negotovosti tako za podjetja in druge organizacije, uveljavljanje pravic posameznikov kot tudi izvajanje nadzora. Informacijski pooblaščenec na primer še nima možnosti izrekanja upravnih glob po Splošni uredbi.

Informacijski pooblaščenec si bo tudi v prihodnje aktivno prizadeval za ohranjanje težko dosežene ravni transparentnosti javnega sektorja ter se hkrati soočal z izzivi, ki jih na področju varstva podatkov prinašajo novi predpisi in nove tehnologije. Na obeh področjih, tako pri varovanju pravice dostopa do informacij javnega značaja kot tudi pravice do varstva osebnih podatkov, bo glavno vodilo učinkovito varstvo in zagotavljanje pravic posameznikov v sodelovanju z zavezanci in stroko.



VIR: Jože Suhadolnik, Delo, d.d.

Mojca Prelesnik,
informacijska pooblaščenka

A handwritten signature in black ink, appearing to read "Mojca Prelesnik".

STRNJEN PREGLED LETA 2018

Dostop do informacij javnega značaja

Informacijski pooblaščenec je na področju dostopa do informacij javnega značaja tudi leta 2018 zabeležil trend rasti števila pritožbenih zadev, hkrati pa uspešno občutno skrajšal čas obravnave posamezne zadeve. Med izzivi velja izpostaviti vnovičen porast števila pritožb zaradi t. i. molka organa in znova večje število vloženih pritožb zoper občine. Leta 2018 je hkrati stopila v veljavo novela ZDIJZ-F, ki v členu 26.a določa, da je stranka v postopku z zahtevo za dostop do informacije javnega značaja ali ponovne uporabe samo prosilec, če je predmet odločanja dostop do podatkov, za katere je z zakonom določeno, da so javni. S tem je uredila institut stranske udeležbe posebej glede na splošno ureditev v zakonodaji, ki ureja upravni postopek.

Glede na ugotovitve in izkušnje iz obravnave konkretnih pritožbenih zadev Informacijski pooblaščenec ob koncu leta podaja naslednje ugotovitve in priporočila za delo zavezancev v prihodnje:

I. Zavezanci naj pri obravnavi zahtev več pozornosti namenijo postopkovnim vprašanjem, še posebej pripravi obrazložitev zavnih odločb.

II. Z vidika izjem, na katere so se sklicevali zavezanci v postopkih, velja opozoriti na povečanje števila pritožbenih zadev, v katerih je šlo za t. i. izjemo notranjega delovanja. Po ugotovitvah Informacijskega pooblaščenca zavezanci to izjemo razlagajo preširoko in ne da bi konkretno izkazali škodo, ki bi nastala z razkritjem zahtevanih dokumentov.

III. Ker je Informacijski pooblaščenec leta 2018 obravnaval tudi nekaj primerov, ko so zavezanci zavnili dostop do podatkov v zvezi z delovnimi razmerji javnih uslužbencev z obrazložitvijo, da gre za varovane osebne podatke, velja poudariti, da se pravna podlaga za posredovanje teh podatkov javnosti tudi po uveljavitvi Splošne uredbe ni spremenila.

IV. Ker je Informacijski pooblaščenec v praksi naletel na primere, ko so zavezanci zaradi obstoja zakonske izjeme dostop do zahtevane informacije zavnili v celoti, ne da bi upoštevali pravilo delnega dostopa iz 7. člena ZDIJZ, velja opozoriti, da če dokument ali njegov del le delno vsebuje varovane informacije in jih je mogoče iz dokumenta izločiti, ne da bi to ogrozilo njihovo zaupnost, mora organ slediti pravilu delnega dostopa in prosilca seznaniti z vsebino preostalega, nevarovanega dela dokumenta.

V. V zvezi z ugotovitvijo iz prejšnje točke Informacijski pooblaščenec pripominja, da se pravilo delnega dostopa nanaša tudi na inšpekcijske prijave in druge dokumente iz teh postopkov, ki niso varovani absolutno in v celoti.

Varstvo osebnih podatkov

Na področju varstva osebnih podatkov je leta Informacijskega pooblaščenca tako na področju nadzora kot na področju reševanja pritožb in še posebej pri preventivni dejavnosti obarval predvsem začetek uporabe Splošne uredbe.

Bistvene novosti, ki jih prinaša Splošna uredba, so nove in okrepljene pravice posameznika, poleg obstoječih predvsem pravica do prenosljivosti podatkov. Precej večji poudarek je na transparentnosti obdelave, torej glede zagotavljanja preglednih in lahko dostopnih informacij posameznikom o obdelavi njihovih podatkov. Splošna uredba določa tudi nove obveznosti upravljavcev in obdelovalcev podatkov, kot so obveznost izvajanja ustreznih varnostnih ukrepov in obveznost uradnega obveščanja o kršitvah varstva osebnih podatkov, imenovanje pooblaščenih oseb za varstvo podatkov, izvajanje ocen učinka. Upravljavci niso več dolžni prijavljati zbirk osebnih podatkov v register zbirk osebnih podatkov, ostajajo pa dolžnosti sprejema popisa zbirk (t. i. evidence dejavnosti obdelave), ki se krepijo in uvajajo tudi za (pogodbene) obdelovalce. Splošna uredba bistveno bolj poudarja načelo odgovornosti in preventivne ukrepe, poleg omenjenih mehanizmov zagotavljanja skladnosti pa uvaja tudi možnost potrjevanja sektorskih kodeksov ravnanja in certifikacije.

Prijave, ki jih je leta 2018 prejel Informacijski pooblaščenec, so se nanašale na naslednje sume kršitev določb Splošne uredbe in ZVOP-1: nezakonito razkrivanje osebnih podatkov, posredovanje osebnih podatkov nepooblaščenim uporabnikom in nezakonita objava osebnih podatkov, nezakonita obdelava osebnih podatkov pri izvajanju neposrednega trženja, nezakonito zbiranje oz. zahtevanje osebnih podatkov, nezakonito izvajanje videonadzora, neustrezeno zavarovanje osebnih podatkov, nezakonit vpogled v osebne podatke, obdelava osebnih podatkov v nasprotju z namenom zbiranja.

Informacijski pooblaščenec je v 101 prekrškovnem postopku leta 2018 izdal le 20 glob in 22 opominov, čemur je nedvomno botrovala odsotnost procesne ureditve izrekanja upravnih glob po Splošni uredbi v slovenskem pravnem redu.

Z uporabo Splošne uredbe je bistveno večji pomen dobilo tudi mednarodno sodelovanje Informacijskega pooblaščenca, predvsem v okviru novoustanovljenega Evropskega odbora za varstvo podatkov (Odbor). Gre za organ EU s svojstvom pravne osebe, v katerem sodelujejo predstavniki vseh 28 neodvisnih nadzornih organov EU in EGS (Islandija, Norveška in Lichtenštajn), Evropske komisije in Evropskega nadzornika za varstvo podatkov; odbor nadomešča Delovno skupino za varstvo podatkov iz člena 29 (Article 29 Working Party). Odločitve odbora so za nacionalne organe pravno zavezujoče, sam postopek obravnave inšpekcijskih primerov s čezmejnim elementom in določenih mehanizmov za zagotavljanje skladnosti zahteva tudi obravnavo na ravni odbora. Splošna uredba namreč v poglavju IIV zapoveduje tesno sodelovanje med nadzornimi organi za varstvo osebnih podatkov v državah članicah EU in EGS (Islandija, Norveška in Lichtenštajn) pri čezmejnih primerih, in sicer preko:

- **sodelovanja v postopkih čezmejnega nadzora po načelu »vse na enem mestu« (angl. one stop shop)** (člen 60 Splošne uredbe);
- **mehanizmov vzajemne pomoči** med organi za varstvo osebnih podatkov v državah članicah EU (člen 61 Splošne uredbe);
- **skupnega ukrepanja** organov za varstvo osebnih podatkov v državah članicah EU (člen 62 Splošne uredbe);
- v okviru postopkov sodelovanja nadzornih organov s **sprejemanjem pravno zavezujočih odločitev odbora v okviru mehanizma za skladnost** (z izdajo mnenj po členu 64, reševanjem sporov po členu 65 ter reševanjem nujnih primerov po členu 66 Splošne uredbe) v zvezi z nacionalnimi nadzornimi organi, da se zagotovi dosledno uporabo Splošne uredbe;
- **sprejemanja splošnih smernic** za podrobnejšo opredelitev pogojev evropske zakonodaje o varstvu podatkov, s čimer svojim deležnikom zagotavlja dosledno razlago njihovih pravic in obveznosti;
- **svetovanja Evropski komisiji** v zvezi z vprašanji varstva podatkov in pripravo evropskih predpisov s področja varstva podatkov;
- **promocije sodelovanja in izmenjave izkušenj** med nacionalnimi nadzornimi organi za varstvo podatkov.

Informacijski pooblaščenec je leta 2018 na ravni EU aktivno sodeloval tudi v petih delovnih telesih EU, ki se ukvarjajo z nadzorom nad izvajanjem varstva osebnih podatkov v okviru velikih informacijskih sistemov EU, in sicer Europola, Schengenskega sistema SIS II, sistema za nadzor na področju carin CIS, sistema za vizni nadzor VIS in sistema Eurodac.

Informacijski pooblaščenec je leta 2018 prejel 106 pritožb posameznikov v zvezi s krštvami pravice do seznanitve z lastnimi osebnimi podatki, pravice do seznanitve z lastno zdravstveno dokumentacijo in pravice do seznanitve z zdravstveno dokumentacijo s strani drugih upravičenih oseb. Vložene pritožbe so večinoma zadevale upravljavce iz javnega sektorja (zlasti državne organe, občine in javne zavode), med upravljavci iz zasebnega sektorja pa zlasti banke, zavarovalnice, operaterje elektronskih komunikacij ter druga podjetja, društva in zasebne izvajalce zdravstvene dejavnosti.

Splošna uredba daje veliko težo novemu načelu odgovornosti. Informacijski pooblaščenec je zato leta 2018 okreplil delovno področje, ki skrbi za področje skladnosti, preventive in informacijskih tehologij, kjer delujejo strokovnjaki s pravnimi, tehnološkimi in komunikološkimi znanji, ki so potrebna za ustrezeno pripravo gradiv in komunikacijo z zavezanci. Z namenom ustreznega informiranja zavezancev in učinkovitega izvajanja teh obveznosti je Informacijski pooblaščenec vzpostavil številne postopke ter pripravil gradiva, med drugim smernice o pogodbeni obdelavi, smernice o ocenah učinkov na varstvo osebnih podatkov, smernice o prenosu osebnih podatkov v tretje države in mednarodne organizacije, smernice za oblikovanje izjave o varstvu osebnih podatkov na spletnih straneh, kodeks obnašanja pri zbiranju osebnih podatkov, smernice Informirani potrošniki – komu dajemo katere osebne podatke in zakaj. Novost preteklega leta so tudi infografike, ki posamezna tematska področja, kljub kompleksnosti tem, predstavijo na enostaven in učinkovit način: npr. pravne podlage za javni in zasebni sektor, vključno z veljavno privolitvijo, neposredno trženje.

Informacijski pooblaščenec je ob evropskem dnevu varstva osebnih podatkov organiziral poseben dogodek na temo novosti Splošne uredbe ter izvedel 109 pro bono predavanj različnim zbornicam in združenjem v javnem in zasebnem sektorju ter na konferencah in seminarjih. S ciljem podpore zavezancem je konec leta 2018 javnosti predstavil evropski projekt RAPiD.Si (Raising Awareness on Data Protection and the GDPR in Slovenia), katerega glavni namen je izobraževanje in ozaveščanje manjših in srednje velikih podjetij ter posameznikov o reformi zakonodajnega okvira s področja varstva osebnih podatkov. Projekt sofinancira Evropska unija.

LETO 2018 V ŠTEVILKAH



40

zaposlenih za nedoločen čas



1.833.399,66

EUR proračuna

Varstvo osebnih podatkov



1029
inšpekcijskih postopkov
+57%



101
prekrškovni postopek



2192
pisnih mnenj
+70%



3230
ustnih mnenj
+62%



81
postopkov odločanja o
vodilnem nadzornem organu



68
prijav kršitev varnosti



6
mnenj na prejete ocene učinka



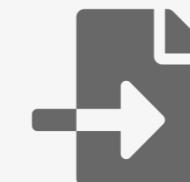
1920
imenovanih pooblaščenih oseb
za varstvo podatkov



1
kodeks v potrditev



30
mednarodnih sodelovanj
"vse na enem mestu"



549
vloženih pritožb



288
izdanih odločb



236
pozivov zaradi molka



36
in camera ogledov



32 dni
povprečen čas reševanja
pritožbenih zadev
-13%



6
novih smernic



6
obrazcev za zavezance



3
infografike



109
predavanj



64
mnenj na predpise



287
pisnih prošenj za pojasnila

Ostalo



6

novih smernic



6

obrazcev za zavezance



64
mnenj na predpise

KAZALO

1.1 NASTANEK IN OSEBNA IZKAZNICA INFORMACIJSKEGA POOBLAŠČENCA	2	3.5.1 OBVEZNOSTI UPRAVLJAVCEV	98
1.1.1 ORGANIZIRANOST	4	3.5.2 POGODBENA OBDELAVA	99
1.2 KLJUČNA PODROČJA DELOVANJA IN PRISTOJNOSTI	7	3.5.3 EVIDENCE OBDELAV	100
1.3 FINANČNO POSLOVANJE V LETU 2018	16	3.5.4 PRIJAVA KRŠITEV VARNOSTI OSEBNIH PODATKOV	100
2.1 PRAVNA UREDITEV NA PODROČJU DOSTOPA DO INFORMACIJ JAVNEGA ZNAČAJA.....	22	3.5.5 OCENE UČINKOV NA VARSTVO OSEBNIH PODATKOV	103
2.2 ŠTEVILO VLOŽENIH PRITOŽB IN REŠENIH ZADEV.....	28	3.5.6 POOBLAŠČENE OSEBE ZA VARSTVO PODATKOV	105
2.3 ŠTEVILO VLOŽENIH TOŽB IN SODB	30	3.5.7 KODEKSI RAVNANJA IN POTRJEVANJE.....	106
2.4 STATISTIKA PO POSAMEZNIH PODROČJIH	31	3.5.8 AKTIVNOSTI IZOBRAŽEVANJA IN OZAVEŠČANJA	107
2.5 STORJENI PREKRŠKI PO ZDIJZ, ZInfP IN ZMeD	34	3.6 MEDNARODNO SODELOVANJE	112
2.6 IZBRANI PRIMERI NA PODROČJU DOSTOPA DO INFORMACIJ JAVNEGA ZNAČAJA.....	34	3.6.1 SODELOVANJE V EVROPSKEM ODBORU ZA VARSTVO PODATKOV	112
2.7 AKTIVNOSTI IZOBRAŽEVANJA IN OZAVEŠČANJA	49	3.6.2 SODELOVANJE V DRUGIH NADZORNIH TELESIH EVROPSKE UNIJE	116
2.7.1 DAN PRAVICE VEDETI V ZNAMENJU 15. OBLETNICE ZAKONA O DOSTOPU DO INFORMACIJ JAVNEGA ZNAČAJA.....	49	3.6.3 SODELOVANJE V DRUGIH MEDNARODNIH TELESIH	117
2.7.2 NAGRADA AMBASADOR TRANSPARENTNOSTI 2018.....	51	3.7 SPLOŠNA OCENA STANJA VARSTVA OSEBNIH PODATKOV	120
2.7.3 MEDNARODNO SODELOVANJE	52		
2.8 SPLOŠNA OCENA IN PRIPOROČILA	53		
3.1 KONCEPT VARSTVA OSEBNIH PODATKOV V REPUBLIKI SLOVENIJI	58		
3.2 INŠPEKCIJSKI NADZOR V LETU 2018	62		
3.2.1 INŠPEKCIJSKI NADZOR V JAVNEM SEKTORU.....	65		
3.2.2 INŠPEKCIJSKI NADZOR V ZASEBNEM SEKTORU	66		
3.2.3 PREKRŠKOVNI POSTOPKI	68		
3.2.4 SODELOVANJE PRI ČEZMEJNIH INŠPEKCIJSKIH NADZORIH.....	71		
3.2.5 IZBRANI PRIMERI OBDELAVE OSEBNIH PODATKOV	74		
3.3 DRUGI UPRAVNI POSTOPKI	83		
3.3.1 DOPUSTNOST IZVAJANJA BIOMETRIJSKIH UKREPOV	83		
3.3.2 POVEZOVANJE JAVNIH EVIDENC	84		
3.3.3 PRENOS OSEBNIH PODATKOV V TRETJE DRŽAVE	87		
3.3.4 PRAVICE POSAMEZNIKOV	91		
3.4 PRIPRAVA MNENJ IN POJASNIL.....	94		
3.4.1 SPLOŠNA POJASNILA.....	94		
3.4.2 MNENJA NA PREDPISE	95		
3.5 SKLADNOST IN PREVENTIVA	98		

UPORABLJENE KRATICE IN OKRAJŠAVE ZAKONOV

ZDIJZ - Zakon o dostopu do informacij javnega značaja

Splošna uredba - Splošna uredba o varstvu podatkov

ZVOP-1 - Zakon o varstvu osebnih podatkov

ZInfP - Zakon o Informacijskem pooblaščencu

ZVOP-2 - Predlog novega Zakona o varstvu osebnih podatkov

ZUP - Zakon o splošnem upravnem postopku

Zmed - Zakon o medijih

ZPacP - Zakon o pacientovih pravicah

ZPLD-1 - Zakon o potnih listinah

ZOlzk-1 - Zakon o osebni izkaznici

ZEKom-1 - Zakon o elektronskih komunikacijah

ZCKR - Zakon o centralnem kreditnem registru

ZPotK-2 - Zakon o potrošniških kreditih

ZBan-2 - Zakon o bančništvu

ZMat - Zakon o maturi

ZOsn - Zakon o osnovni šoli

ZTP - Zakon o tajnih podatkih

ZKP - Zakon o kazenskem postopku

ZZPISI - Zakon o zagotavljanju pogojev za izvedbo strateške investicije na razvojnem območju

ZIN - Zakon o inšpekcijskem nadzoru

ZDRS - Zakon o državljanstvu Republike Slovenije

ZGD-1 - Zakon o gospodarskih družbah

ZASP - Zakon o avtorski in sorodnih pravicah

ZSSve - Zakon o sodnem svetu

ZP-1 - Zakon o prekrških

ZVrt - Zakon o vrtcih

ZDR-1 - Zakon o delovnih razmerjih

ZDru-1 - Zakon o društvih

ZVO-1 - Zakon o varstvu okolja

O INFORMACIJSKEM POOBLAŠČENCU – POD SVOJO STREHO ZDRUŽUJE DOSTOP DO INFORMACIJ JAVNEGA ZNAČAJA IN VARSTVO OSEBNIH PODATKOV

1.1 NASTANEK IN OSEBNA IZKAZNICA INFORMACIJSKEGA POOBLAŠČENCA

POMEMBNO

Informacijski pooblaščenec je samostojen in neodvisen državni organ s pristojnostmi na področju dveh z Ustavo Republike Slovenije zavarovanih temeljnih človekovih pravic, pravice dostopa do javnih informacij in pravice do varstva osebnih podatkov.

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

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

ZInfP je v slovenski pravni red prinesel pomembne novosti. S tem zakonom je bil namreč ustanovljen nov državni organ, Informacijski pooblaščenec, ki izvaja številne pristojnosti tako na področju dostopa do informacij javnega značaja kot tudi na področju varstva osebnih podatkov. Poleg določb, ki urejajo položaj in imenovanje informacijskega pooblaščenca, ZInfP vsebuje tudi določbe o nadzornikih za varstvo osebnih podatkov, o nekaterih posebnostih postopka pred Informacijskim pooblaščencem ter nekatere kazenske določbe.

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.

OSEBNA IZKAZNICA



Republika Slovenija
Informacijski pooblaščenec
Dunajska cesta 22
1000 Ljubljana



Telefon: 01 230 97 30
Faks: 01 230 97 78
E-pošta: gp.ip@ip-rs.si



www.ip-rs.si



Pooblaščena oseba za varstvo podatkov:
dpo@ip-rs.si



Prijava kršitev varnosti:
prijava-krsitev@ip-rs.si

1.1.1 ORGANIZIRANOST

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

Informacijski pooblaščenec opravlja svoje naloge v naslednjih notranjih organizacijskih enotah:

- kabinet Informacijskega pooblaščenca,
- sektor za informacije javnega značaja,
- sektor za varstvo osebnih podatkov,
- administrativno-tehnična služba.

ORGANIGRAM PO DELOVNIH PODROČJIH

INFORMACIJSKI POOBLAŠČENEC

ADMINISTRATIVNO-TEHNIČNA SLUŽBA

PODROČJE VARSTVA OSEBNIH PODATKOV

Inšpekcijski nadzor in prekrški

Mednarodno sodelovanje in nadzor

Odločanje o pravicah posameznikov

Skladnost in preventiva

Zakonodaja

Izdajanje odločb o biometriji, povezovanju evidenc in prenosu

Svetovanje in izobraževanje

PODROČJE DOSTOPA DO INFORMACIJ JAVNEGA ZNAČAJA

Reševanje pritožb pri dostopu do IJZ

Reševanje pritožb pri ponovni uporabi IJZ

Reševanje pritožb po Zakonu o medijih

Neformalno svetovanje in izobraževanje

31. 12. 2018 je bilo pri Informacijskem pooblaščenu zaposlenih 43 uslužbencev, od tega 40 za nedoločen čas ter 3 za določen čas (nadomeščanje zaradi porodniškega dopusta in projektni sodelavec V). Izobrazbena struktura zaposlenih je razvidna iz preglednice.

Izobrazbena struktura zaposlenih pri Informacijskem pooblaščencu na dan 31. 12. 2018

	Srednja strokovna šola	Višja strokovna šola	Visoka strokovna šola, univerzitetni program	Univerzitetna izobrazba	Magisterij	Doktorat	Skupaj
Pooblaščenka				1			1
Namestniki			2	2	2		4
Vodja mednarodnega sodelovanja in nadzora				1			1
Generalna sekretarka				1	1		1
Državni nadzorniki za varstvo osebnih podatkov			6	6	1	13	
Svetovalci pooblaščenca			10	3			13
Asistent svetovalca				1			1
Raziskovalec			1	2			3
Sistemski administrator			1				1
Strokovna sodelavka za finančne in kadrovske zadeve			1				1
Poslovna sekretarka			1				1
Dokumentalistka			1				1
Projektni sodelavci	2						2
Skupaj	2	2	3	22	13	1	43

1.2 KLJUČNA PODROČJA DELOVANJA IN PRISTOJNOSTI

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 (ZDIJZ), ima Informacijski pooblaščenec pristojnosti pritožbenega organa, kot jih določa 2. člen ZInfP. To pomeni, da odloča o pritožbi prosilca, če je zavezanc za dostop do informacij javnega značaja:

1. zahtevo za dostop do informacij javnega značaja zavrnil ali zavrgel;
2. na zahtevo ni odgovoril v predpisanim 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 pooblaščencu pristojnosti podeljuje tudi **Zakon o medijih** (ZMed) (45. člen). Po ZMed se zavnilni odgovor zavezanca na vprašanje, ki ga zastavi predstavnik medija, šteje kot zavnilna 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.

Na delo Informacijskega pooblaščenca na področju varstva osebnih podatkov je v letu 2018 zelo vplival začetek uporabe Splošne uredbe, ki se uporablja neposredno v vseh državah članicah EU od 25. 5. 2018. Do tega datuma je imel Informacijski pooblaščenec pristojnosti, ki sta mu jih dajala Zakon o varstvu osebnih podatkov (ZVOP-1) in 2. člen ZInfP, in sicer:

1. opravljanje inšpekcijskega nadzora nad izvajanjem določb ZVOP-1 in drugih predpisov, ki urejajo varstvo ali obdelavo osebnih podatkov, tj. obravnavanje prijav, pritožb, sporočil in drugih vlog, v katerih je izražen sum kršitve zakona, ter opravljanje preventivnega inšpekcijskega nadzora pri upravljavcih osebnih podatkov s področja javnega in zasebnega sektorja (pristojnost je določena v 2. členu ZInfP);
2. odločanje o pritožbi posameznika, kadar upravljač osebnih podatkov ne ugodi zahtevi posameznika glede njegove pravice do seznanitve z zahtevanimi podatki, do izpisov, seznamov, vpogledov, potrdil, informacij, pojasnil, prepisovanja ali kopiranja po določbah zakona, ki ureja varstvo osebnih podatkov (pristojnost je določena v 2. členu ZInfP);
3. vodenje postopkov o prekrških s področja varstva osebnih podatkov (hitri postopek);
4. vodenje in vzdrževanje registra zbirk osebnih podatkov in zagotavljanje, da je register ažuren ter javno dostopen prek svetovnega spleta (28. člen ZVOP-1);
5. omogočanje vpogleda in prepisa podatkov iz registra zbirk osebnih podatkov, praviloma isti dan, najpozneje pa v osmih dneh (29. člen ZVOP-1);
6. odločanje 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 odločb o zagotavljanju ustrezne ravni varstva osebnih podatkov v tretjih državah (63. člen ZVOP-1);
8. vodenje postopkov ugotavljanja ustrezne ravni varstva osebnih podatkov v tretjih državah na podlagi ugotovitev inšpekcijskega nadzora in drugih informacij (64. člen ZVOP-1);
9. 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 le delno zagotavlja ustrezno raven varstva osebnih podatkov, je v seznamu navedeno tudi, v katerem delu je ustrezna raven zagotovljena (66. člen ZVOP-1);
10. vodenje upravnih postopkov za izdajo dovoljenj o iznosu osebnih podatkov v tretjo državo (70. člen ZVOP-1);
11. vodenje upravnih postopkov za izdajo dovoljenj za povezovanje javnih evidenc in javnih knjig, kadar katera od zbirk osebnih podatkov, ki naj bi se jih povezalo, vsebuje občutljive osebne podatke ali pa je za izvedbo povezovanja potrebna uporaba istega povezovalnega znaka, npr. EMŠO ali davčne številke (84. člen ZVOP-1);

12. vodenje upravnih postopkov 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. sodelovanje 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. dajanje in objava predhodnih mnenj državnim organom ter nosilcem javnih pooblastil o usklajenosti določb predlogov predpisov z zakoni in drugimi predpisi, ki urejajo osebne podatke;
15. dajanje in objava neobveznih mnenj o skladnosti kodeksov poklicne etike, splošnih pogojev poslovanja oz. njihovih predlogov s predpisi s področja varstva osebnih podatkov;
16. priprava, dajanje in objava neobveznih navodil in priporočil glede varstva osebnih podatkov na posameznem področju;
17. objava (na spletni strani ali na drug primeren način) predhodnih mnenj o usklajenosti predlogov zakonov in drugih predpisov z zakonom in drugimi predpisi s področja varstva osebnih podatkov ter zahtev za oceno ustavnosti predpisov, objava odločb in sklepov sodišč, ki se nanašajo na varstvo osebnih podatkov, ter izdaja neobvezna mnenja, pojasnila, stališča in priporočila glede varstva osebnih podatkov na posameznih področjih (49. člen ZVOP-1);
18. dajanje izjav za javnost o opravljenih nadzorih in priprava letnega poročila o svojem delu v preteklem letu;
19. sodelovanje v delovnih skupinah za varstvo osebnih podatkov, oblikovanih znotraj EU, ki združujejo neodvisne institucije za varstvo osebnih podatkov držav članic (v Delovni skupini po členu 29 Direktive 95/46/EC in v nadzornih organih, ki se ukvarjajo z nadzorom obdelave osebnih podatkov v Schengenskem informacijskem sistemu, v informacijskem sistemu za carino, v okviru Europola ter v skupini za nadzor Eurodaca).

POMEMBNO

Začetek uporabe Splošne uredbe terja sprejetje novega Zakona o varstvu osebnih podatkov (ZVOP-2), s katerim bi se v Republiki Sloveniji zagotovilo izvajanje Splošne uredbe, vendar pa ta zakon do konca leta 2018 ni bil sprejet. Zato se poleg Splošne uredbe še vedno uporablja tudi ZVOP-1, in sicer tiste določbe, ki jih uredba ne ureja in ki z njo niso v nasprotju. Tako Informacijski pooblaščenec še vedno opravlja vse zgoraj navedene naloge po ZVOP-1, razen nalog, navedenih od 4. do vključno 10. točke.

- Splošna uredba** določa naloge Informacijskega pooblaščenca kot nadzornega organa v členu 57:
- (a) spremlja in zagotavlja uporabo te uredbe;
 - (b) spodbuja ozaveščenost in razumevanje javnosti o tveganjih, pravilih, zaščitnih ukrepih in pravicah v zvezi z obdelavo; posebna pozornost se posveti dejavnostim, ki so namenjene izrecno otrokom;
 - (c) v skladu s pravom države članice svetuje nacionalnemu parlamentu, vladi ter drugim institucijam in organom o zakonodajnih in upravnih ukrepih v zvezi z varstvom pravic in svoboščin posameznikov pri obdelavi;
 - (d) spodbuja ozaveščenost upravljavcev in obdelovalcev glede njihovih obveznosti na podlagi te uredbe;
 - (e) vsakemu posamezniku, na katerega se nanašajo osebni podatki, na zahtevo zagotovi informacije o uresničevanju njegovih pravic na podlagi te uredbe in v ta namen, če je ustrezno, sodeluje z nadzornimi organi v drugih državah članicah;
 - (f) obravnava pritožbe, ki jih vloži posameznik, na katerega se nanašajo osebni podatki, oz. v skladu s členom 80 telo, organizacija ali združenje, v ustremnem obsegu preuči vsebino pritožbe in v razumnem roku obvesti pritožnika o poteku in rezultatu preiskave, zlasti če je potrebna nadaljnja preiskava ali usklajevanje z drugim nadzornim organom;
 - (g) sodeluje z drugimi nadzornimi organi, med drugim z izmenjavo informacij, in jim zagotavlja medsebojno pomoč, da se zagotovi doslednost pri uporabi in izvajanju te uredbe;
 - (h) izvaja preiskave o uporabi te uredbe, tudi na podlagi informacij, ki jih prejme od drugega nadzornega organa ali drugega javnega organa;
 - (i) spremlja razvoj na zadevnem področju, kolikor vpliva na varstvo osebnih podatkov, predvsem razvoj informacijskih in komunikacijskih tehnologij ter trgovinskih praks;
 - (j) sprejema standardna pogodbena določila iz člena 28(8) in točke (d) člena 46(2);
 - (k) vzpostavi in vzdržuje seznam v zvezi z zahtevo po oceni učinka v zvezi z varstvom podatkov v skladu s členom 35(4);
 - (l) svetuje glede dejanj obdelave iz člena 36(2);
 - (m) spodbuja pripravo kodeksov ravnanja v skladu s členom 40(1) ter poda mnenje in odobi take kodekse ravnanja, ki zagotavljajo zadostne zaščitne ukrepe, v skladu s členom 40(5);
 - (n) spodbuja vzpostavitev mehanizmov potrjevanja za varstvo podatkov ter pečatov in označb za varstvo podatkov v skladu s členom 42(1) in odobi merila potrjevanja v skladu s členom 42(5);
 - (o) kadar je ustrezno, izvaja redne preglede potrdil, izdanih v skladu s členom 42(7);
 - (p) oblikuje in objavi merila za pooblastitev telesa za spremljanje kodeksov ravnanja v skladu s členom 41 in organa za potrjevanje v skladu s členom 43;

- (q) opravi pooblastitev telesa za spremljanje kodeksov ravnanja v skladu s členom 41 in organa za potrjevanje v skladu s členom 43;
- (r) odobri pogodbena določila in določbe iz člena 46(3);
- (s) odobri zavezujoča poslovna pravila v skladu s členom 47;
- (t) prispeva k dejavnostim odbora;
- (u) hrani notranjo evidenco kršitev te uredbe in sprejetih ukrepov v skladu s členom 58(2) ter
- (v) opravlja vse druge naloge, povezane z varstvom osebnih podatkov.

Skladno s členom 55(3) Splošne uredbe Informacijski pooblaščenec ni pristojen za nadzor dejanj obdelave sodišč, kadar delujejo kot sodni organ.

Informacijski pooblaščenec ima pristojnosti še po **Zakonu o pacientovih pravicah (ZPacP)**, **Zakonu o potnih listinah (ZPLD-1)**, **Zakonu o osebni izkaznici (ZOIzk)**, **Zakonu o elektronskih komunikacijah (ZEKom-1)**, **Zakonu o centralnem kreditnem registru (ZCKR)**, **Zakonu o potrošniških kreditih (ZPotK-2)**, **Uredbi o sistemih brezpilotnih zrakoplovov** in [Uredbi o izvajanju Uredbe \(EU\) o državljanski pobudi](#).

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 pacientovi 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 četrtim 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 oz. 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 določajo, v kakšnih primerih in na kakšen način lahko upravljavci osebnih podatkov kopirajo potne listine oz. 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;
- 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 terminalske 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 bančništvu (ZBan-2) 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 oz. vključitev v sistem izmenjave informacij ter za zagotavljanje zaupnosti podatkov, ki se zbirajo v sistemu izmenjave informacij. Pred določitvijo teh aktov Banka Slovenije pridobi mnenje Informacijskega pooblaščenca, ki izvaja inšpekcijski nadzor v zvezi z zbiranjem in obdelavo osebnih podatkov v centralnem kreditnem registru in sistemu izmenjave informacij v skladu z ZVOP-1. V skladu z 31. členom ZCKR Informacijski pooblaščenec z namenom preprečevanja in odvračanja ravnanj, ki pomenijo nezakonito obdelavo osebnih podatkov, javno objavi informacije v zvezi z ukrepi nadzora in sankcijami zaradi prekrška, ki jih je izrekel.

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 oz. 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 pooblaščencu 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. 2011 o državljanski pobudi](#) s področja varstva osebnih podatkov.

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

Z vstopom Republike Slovenije v schengensko območje je Informacijski pooblaščenec prevzel nadzor nad izvajanjem 128. člena **Konvencije o izvajanju Schengenskega sporazuma**. 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.

INFORMACIJSKI POOBLAŠČENEC

[Splošna uredba o varstvu podatkov](#)

[Zakon o varstvu osebnih podatkov](#)

[Zakon o elektronskih komunikacijah](#)

[Zakon o pacientovih pravicah](#)

[Zakon o osebni izkaznici](#)

[Zakon o potnih listinah](#)

[Zakon o centralnem kreditnem registru](#)

[Zakon o potrošniških kreditih](#)

[Uredba o sistemu brezpilotnih zrakoplovov](#)

[Uredba o izvajanju Uredbe o drž. pobudi](#)

Zakon o dostopu do informacij javnega značaja

Zakon o medijih

1.3 FINANČNO POSLOVANJE V LETU 2018

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.

Za izvajanje svojih nalog je imel Informacijski pooblaščenec za leto 2018 veljavni proračun na integralnih postavkah 1.833.399,66 EUR, od tega na postavki plače 1.490.391,00 EUR, na postavki materialni stroški 238.008,66 EUR in na postavki investicije 105.000,00 EUR. Evidentiranih odredb na integralnih postavkah je bilo na dan 31. 12. 2018 1.786.004,17 EUR, od tega na postavki plače 1.458.915,66 EUR, na postavki materialni stroški 222.537,12 EUR in na postavki investicije 104.551,45 EUR.

Proračun Informacijskega pooblaščenca 2014-2018

Proračunsko leto	Veljavni proračun
2014	1.247.110,10 EUR
2015	1.243.661,35 EUR
2016	1.335.457,02 EUR
2017	1.459.747,90 EUR
2018	1.833.399,66 EUR

Informacijski pooblaščenec je leta 2018 razpolagal z namenskimi sredstvi v znesku 7.317,92 EUR in donacijami za sodelovanje v projektih, ki so bili financirani s strani EU. Porabe za namenska sredstva in donacije leta 2018 ni bilo.

V proračun leta 2019 bo Informacijski pooblaščenec prenesel 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 7608 – Tekoča proračunska rezerva pri Ministrstvu za finance je bilo leta 2018 preneseno 164.000,00 EUR iz integralnih postavk.

Podrobnejši pregled prejetih, porabljenih in neporabljenih finančnih sredstev po posameznih postavkah je razviden iz naslednje tabele.

Proračun Informacijskega pooblaščenca 2018

	Veljavni proračun v EUR	Evidentirane odredbe v EUR	Razpoložljiv proračun v EUR konec leta
	1.840.720,71	1.786.004,17	54.716,54
PODPORAMI			
OPRAVLJANJE DEJAVNOSTI	1.833.399,66	1.786.004,17	47.395,49
PP 1271 Materialni stroški	238.008,66	222.537,12	15.471,54
PP 1273 Investicije	105.000,00	104.551,45	448,55
PP 1267 Plače	1.490.391,00	1.458.915,60	31.475,40
NAMENSKA SREDSTVA	7.317,92	0,00	7.317,92
7459 Namenska sr. kupnine	7.317,92	0	7.317,92
DONACIJE	3,13	0,00	3,13
PP 9958 Mednarodna spl. str.	0,14	0	0,14
PP130134 projekt Taiex	2,99	0,00	2,99

Za materialne stroške je bilo leta 2018 porabljenih 222.537,12 EUR, kar predstavlja 93,50 % glede na veljavni proračun za leto 2018.

POMEMBNO

Informacijski pooblaščenec se je s 1. 8. 2018 preselil v nove najete poslovne prostore na lokaciji Dunajska cesta 22, Ljubljana. Poraba sredstev je bila večja zaradi najemnin in obratovalnih stroškov ter stroškov selitve in ureditve prostorov.

Materialni stroški so obsegali: pisarniški material, čiščenje poslovnih prostorov, spremljanje medijev in arhiviranje – kliping, nakup drobnega inventarja, storitve strokovnega svetovanja in nadzora ter izdelave načrta notranje opreme, stroške zdravniških pregledov zaposlenih, stroške za energijo, vodo, komunalne storitve, pošto in komunikacijo, prevozne stroške in vzdrževanje dveh službenih vozil (gorivo za službeni vozili, stroški, povezani s selitvijo z lokacije Zaloška 59 na lokacijo Dunajska 22), taksi storitve, izdatke za službena potovanja, stroške za tekoče vzdrževanje (popravila ter vzdrževanja poslovnega prostora Zaloška 59, zavarovanje, fiksni obratovalni stroški na lokaciji Dunajska 22, tekoče vzdrževanje nelicenčne programske opreme ter druge opreme – vzdrževanje spletnega mesta ter evidence prisotnosti), poslovne najemnine in zakupnine (najemnina za poslovne prostore in parkirne prostore, odmera NUSZ, razne naročnine in najemnine – IUS-INFO in prekrškovni portal), drugi operativni odhodki (plačila po sodbah sodišč, kvote Javnemu jamstvenemu, preživninskemu in invalidskemu skladu, izobraževanja zaposlenih). Iz postavke materialni stroški je Informacijski pooblaščenec leta 2018 prerazporedil 80.000,00 EUR prostih pravic porabe v Tekočo proračunsко rezervo pri Ministrstvu za finance. Proste pravice porabe in ostanek sredstev na postavki plače je nastal iz naslova neuspešno izvedenih dodatnih zaposlitev, kot je bilo prvotno načrtovano.

Za investicije je bilo do konca leta 2018 porabljenih 104.551,45 EUR. Sredstva so bila porabljenata nakup: pisarniškega pohištva (pohištvo za neopremljene najete poslovne prostore, arhivske omare za kletne prostore ter drugo pisarniško pohištvo), pisarniške opreme, strojne računalniške opreme (prenosni in stacionarni računalniki, monitorji, tiskalnik), strežnikov in diskovnih sistemov, nakup opreme za varovanje, telekomunikacijske opreme, nakup druge opreme in napeljav ter nakup nematerialnega premoženja (licenca Amebis BesAna). Konec leta 2018 je na postavki investicije ostalo 448,55 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 1.458.915,60 EUR oz. 97,89 % glede na veljavni proračun za leto 2018.**

POMEMBNO

Glede na predhodna leta se je poraba sredstev povečala zaradi sprostitve napredovanj, višjih regresov za letni dopust ter dodatnih zaposlitev v skladu s kadrovskim načrtom in novimi pristojnostmi Informacijskega pooblaščenca na področju uveljavitev Splošne uredbe in nove Direktive Evropskega parlamenta in Sveta o varstvu posameznikov pri obdelavi osebnih podatkov, ki jih pristojni organi obdelujejo za namene preprečevanja, preiskovanja, odkrivanja ali pregona kaznivih dejanj ali izvrševanja kazenskih sankcij. Uveljavitev Splošne uredbe v Republiki Sloveniji je za Informacijskega pooblaščenca pomenila prevzem številnih novih nalog in zadolžitev, ki zahtevajo dodatne zaposlitve.

Iz postavke plače je Informacijski pooblaščenec leta 2018 prerazporedil 84.000,00 EUR prostih pravic porabe v tekočo proračunsko rezervo pri Ministrstvu za finance. Proste pravice porabe in ostanek sredstev na postavki plače je nastal iz naslova neuspešno izvedenih dodatnih zaposlitev, kot je bilo prvotno načrtovano.

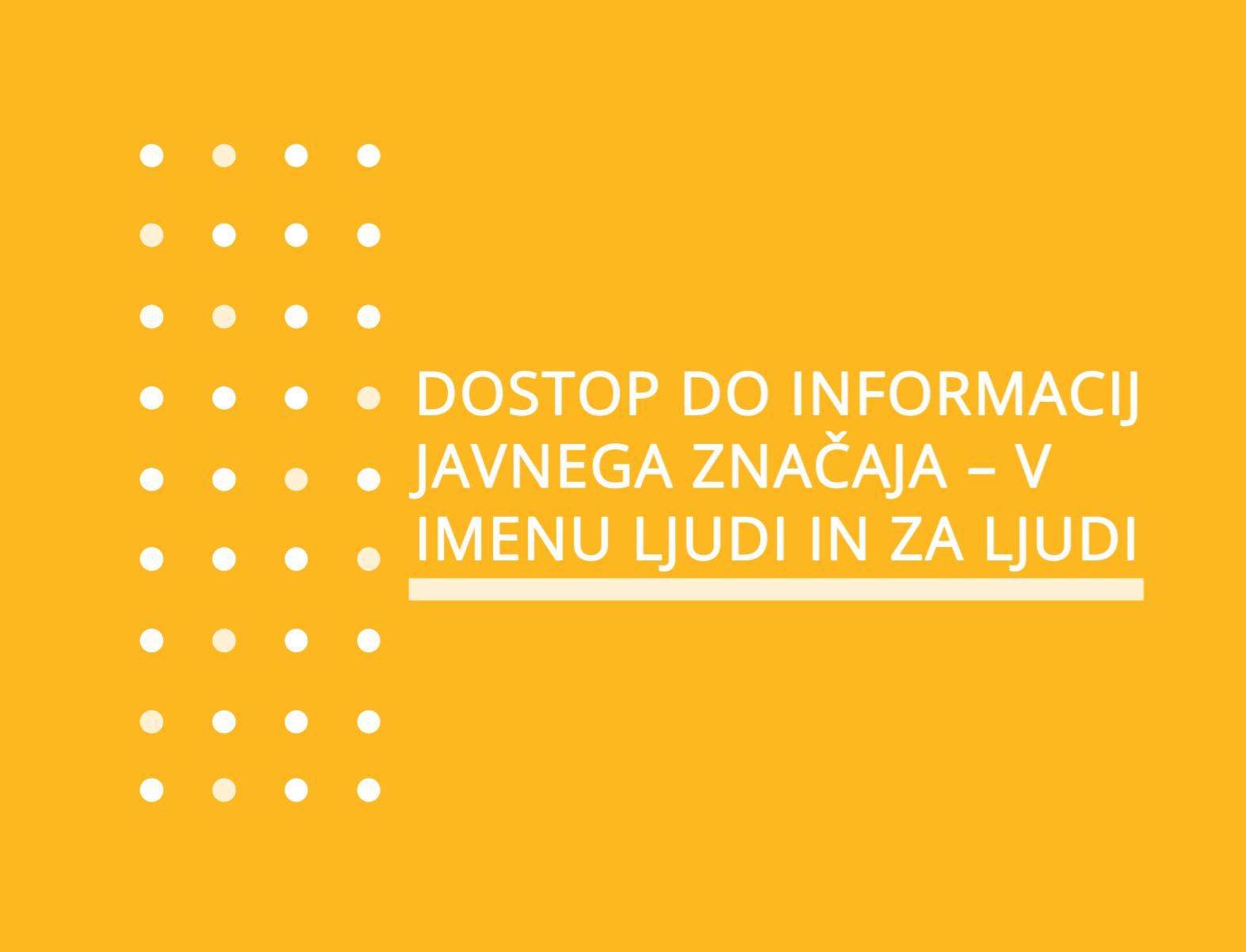
Namenska sredstva kupnine – v leto 2018 je bilo preneseno **7.317,92 EUR** finančnih sredstev kupnin. Leta 2018 na postavko ni bilo prilivov niti ni bilo porabe. Preostanek finančnih sredstev v višini 7.317,92 EUR se prenese v leto 2019.

Mednarodna spletna stran info-commissioners.org – iz leta 2018 je bilo preneseno 0,14 EUR finančnih sredstev. Leta 2018 na tej postavki ni bilo porabe. Projekt se leta 2019 konča, preostanek sredstev se bo nakazal na podračun izvrševanja proračuna.

Projekt Taiex – iz leta 2016 je v bilo v leto 2018 preneseno 2.99 EUR finančnih sredstev na postavko projekt Taiex. Na to postavko leta 2018 ni bilo prilivov niti ni bilo porabe. Projekt se leta 2019 konča, preostanek sredstev se bo nakazal na podračun izvrševanja proračuna.

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 je financirala Evropska komisija, ki jo zastopa Izvajalska agencija za raziskave, trajal je 36 mesecev. Osredotočen je bil na izboljšanje metodologije za certificiranje varnostnih izdelkov, med drugim upoštevajoč vidike varstva osebnih podatkov. Zaposleni Informacijskega pooblaščenca kot enega izmed partnerjev projekta so sodelovali pri pripravi gradiv, izvedbi analiz, raziskav in drugih aktivnosti projekta, napoteni so bili na misije in sestanke, povezane s projektom, na katerih so se izvajale posamezne naloge s področja varstva osebnih podatkov, ki jih je pokrival projekt, izvajali so tudi predstavitve, seminarje in delavnice za ciljne skupine projekta. Zaključno finančno poročilo je bilo po koncu projekta v roku oddano že maja 2017, vendar je Evropska komisija od vseh sedmih partnerjev v projektu zahtevala več dodatnih pojasnil; finančno poročilo je bilo s strani Evropske komisije sprejeto šele decembra 2017. Za sodelovanje v projektu bo Informacijski pooblaščenec prejel namenska finančna sredstva, in sicer 132.400,00 EUR. Leta 2018 je veljavni proračun na PP 140084 Pooblaščenec-CRISP znašal 13.441,00 EUR, dovoljena poraba je bila samo 8.209,48,00 EUR, glede na prejeta sredstva v vseh letih. Porabljenih je bilo 8.126,28 EUR, in sicer za pokrivanje stroškov zaposlenih ter za pokrivanje stroškov službene poti. Informacijski pooblaščenec je zadnje nakazilo sredstev v višini 29.520,86 prejel 21. 12. 2018. Projekt se je leta 2018 končal, preostanek sredstev bo leta 2019 nakazan na podračun izvrševanja proračuna.



DOSTOP DO INFORMACIJ JAVNEGA ZNAČAJA – V IMENU LJUDI IN ZA LJUDI

2.1 PRAVNA UREDITEV NA PODROČJU DOSTOPA DO INFORMACIJ JAVNEGA ZNAČAJA

Pravica dostopa do informacij javnega značaja je zagotovljena že z Ustavo Republike Slovenije. 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 tako tudi zaščitena na ustavnem ravni, se je začela uveljavljati šele 11 let po sprejetju Ustave RS, in sicer s sprejetjem Zakona o dostopu do informacij javnega značaja. Dotlej so se posamezne določbe o javnosti informacij pojavljale le v nekaterih zakonih; celostno jih je uredil šele ZDIJZ, ki je začel veljati leta 2003.

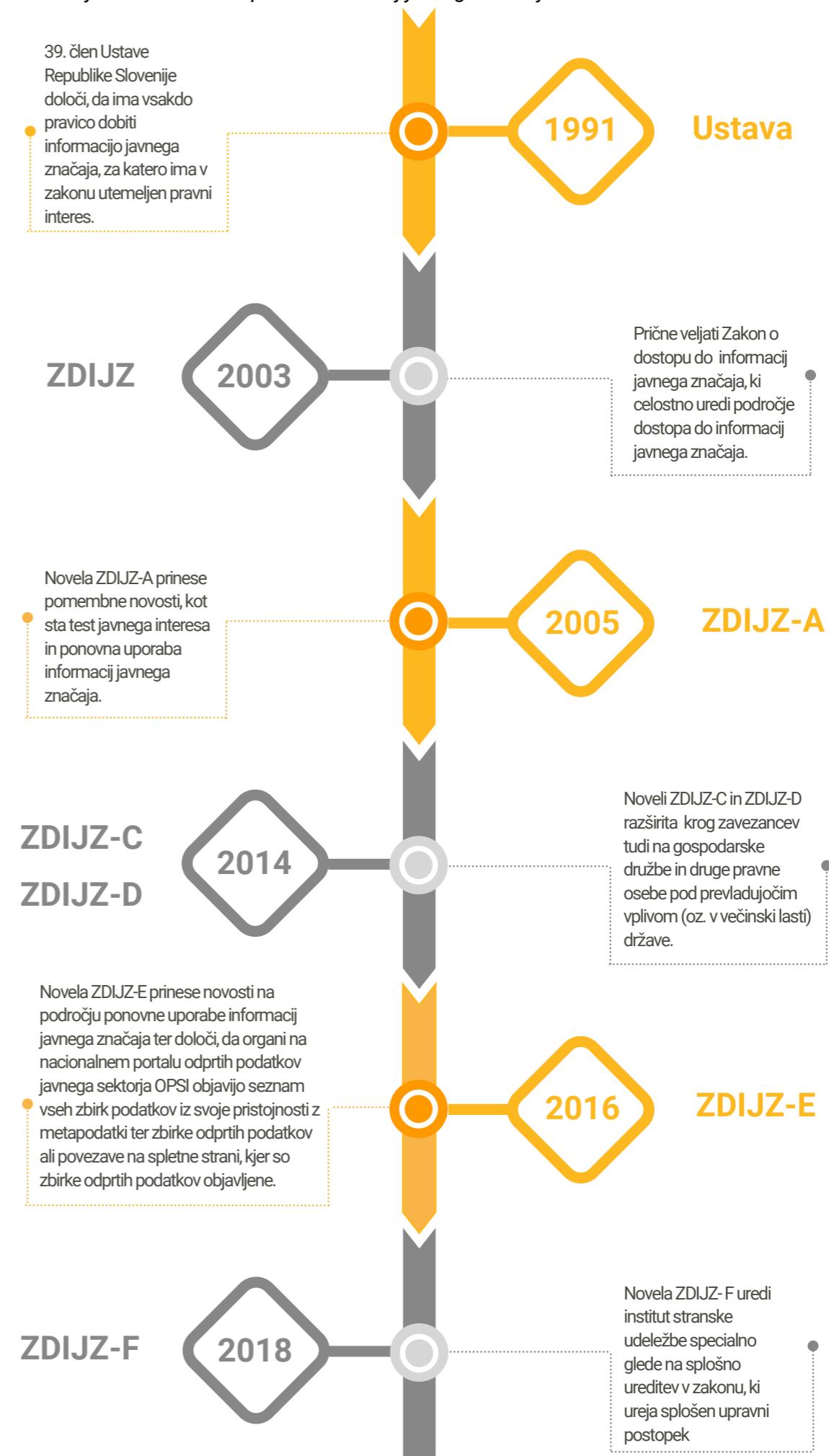
ZDIJZ sledi usmeritvam mednarodnih aktov in EU. Njegov namen je zagotoviti javnost in odprtost delovanja javne uprave ter vsakomur omogočiti dostop do javnih informacij, torej tistih, ki so povezane z delovnimi področji organov javne uprave. Zakon je uredil postopek, ki vsakomur omogoča prost dostop 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 razveljavitevi 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-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 noveli ZDIJZ-C in ZDIJZ-D. Najpomembnejša sprememba, ki sta jo prinesli, je, da se je obveznost posredovanja informacij javnega značaja z organov javnega sektorja razširila tudi na gospodarske družbe in druge pravne osebe pod prevladujočim vplivom (oz. v večinski lasti) države, občin ali drugih oseb javnega prava ter da je AJPES 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 krepita tudi transparentnost in odgovorno ravnanje pri upravljanju s finančnimi sredstvi poslovnih subjektov pod prevladujočim vplivom oseb javnega prava. Nadzor javnosti, omejen zgolj na državne organe, občine in širši javni sektor, se je izkazal za nezadostnega. Finančna in gospodarska kriza preteklih let je namreč povečala občutljivost javnosti za korupcijo, zlorabo oblasti in slabo upravljanje. K večji transparentnosti 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-E, 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 spletni strani, kjer so objavljene zbirke odprtih podatkov. 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 je spremenila 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 značaja, s katero je sprejela enotni stroškovnik za posredovanje informacij javnega značaja. S tem je 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.

Leta 2018 je stopila v veljavo novela ZDIJZ-F, ki v členu a26.a določa, da je stranka v postopku z zahtevo za dostop do informacije javnega značaja ali ponovne uporabe samo prosilec, če je predmet odločanja dostop do podatkov, za katere je z zakonom določeno, da so javni. S tem je uredila institut stranske udeležbe specialno glede na splošno ureditev v zakonodaji, ki ureja upravni postopek.



POMEMBNO

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.

Kdo so zavezanci za posredovanje informacij javnega značaja?

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. poenostavljeni postopek odločanja o zahtevah (npr. ne izdajo zavrnitve 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.

Kako do informacije javnega značaja?

Informacije javnega značaja so **prosto dostopne vsem**, zato pravnega interesa za njihovo pridobitev ni treba izkazovati, dovolj sta radovednost ter želja po znanju in obveščenosti. Vsak prosilec ima na zahtevo pravico pridobiti informacijo javnega značaja, in sicer tako, da jo **dobi na vpogled ali da dobije njen prepis, fotokopijo ali elektronski zapis**. Zavezanci 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 zavezanci prosilcu zaračuna materialne stroške. Če zavezanci prosilcu zahtevane informacije javnega značaja ne posreduje, ima prosilec v 15 dneh pravico vložiti pritožbo zoper zavrnitvo odločbo ali obvestilo, s katerim je zavezanci zahtevalo zavrnitev. O pritožbi odloča Informacijski pooblaščenec. Prav tako ima prosilec pravico do pritožbe, če mu zavezanci na zahtevo v zakonskem roku ni odgovoril (oz. je v molku) ali če informacije ni dobil v obliku, v kateri jo je zahteval.

Kje so izjeme?

Zavezanci 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 oz. 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. Zavezanci 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.

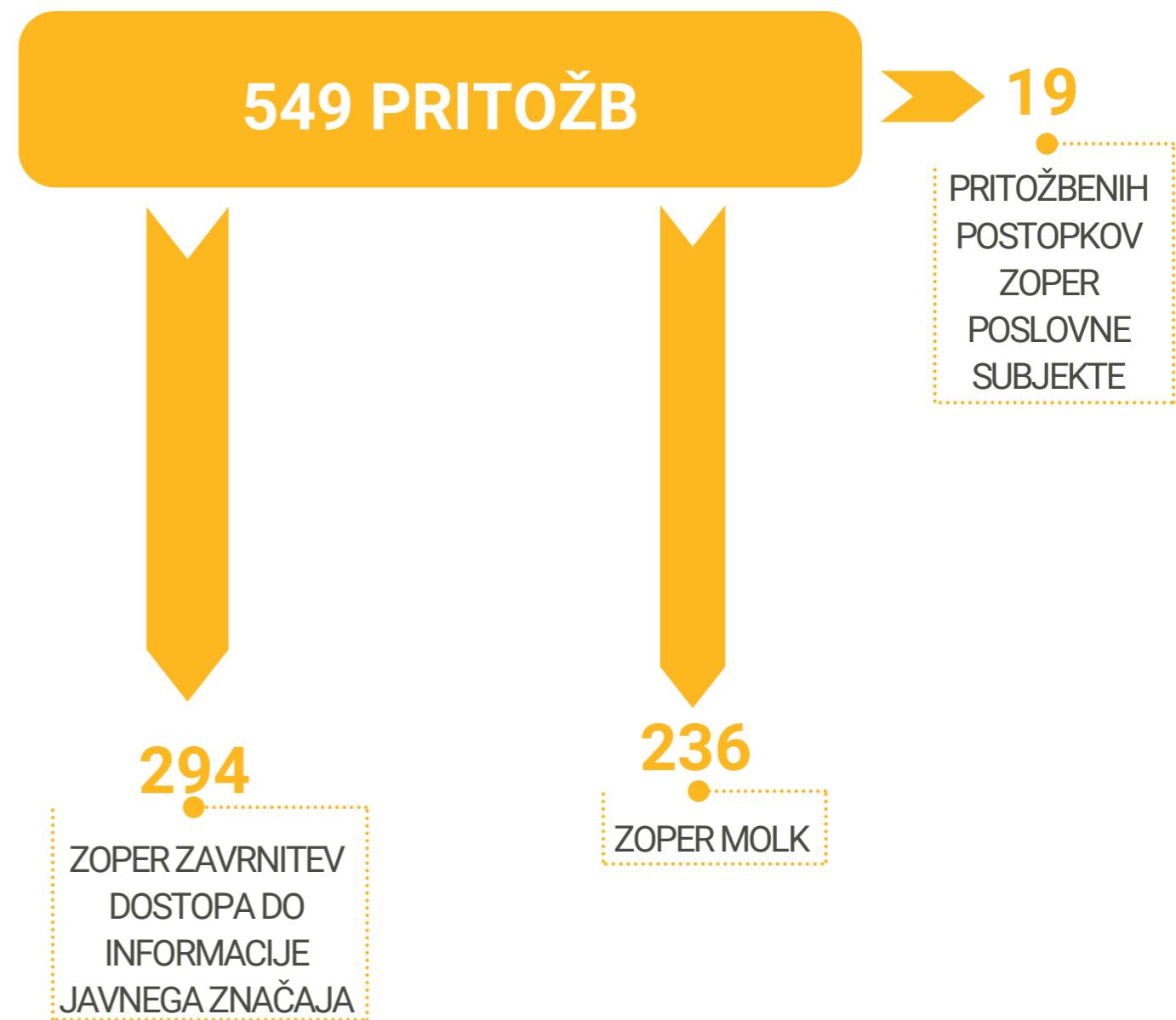
Če dokument, ki ga zahteva prosilec, delno vsebuje informacije iz 5.a ali 6. člena ZDIJZ, to ni razlog, da bi zavezanci zavrnili dostop do celotnega dokumenta. Če je te informacije mogoče iz dokumenta izločiti, ne da bi to ogrozilo njihovo zaupnost, se jih prekrije, prosilcu pa se posreduje preostali del informacij javnega značaja. Zavezanci mora namreč v skladu z 19. členom Uredbe o posredovanju in ponovni uporabi informacij javnega značaja varovane podatke prekriti in prosilcu omogočiti vpogled v preostanek dokumenta (ali fotokopije ali elektronskega zapisa).

Kaj pa zahteva na podlagi Zakona o medijih?

Če poda zahtevo za posredovanje informacij medij na podlagi 45. člena ZMed, je postopek nekoliko drugačen, saj informacije po ZMed niso enake informacijam javnega značaja po določbah ZDIJZ. Informacije za medije so širši pojem kot informacije javnega značaja, saj med prve sodi tudi priprava odgovorov na vprašanja (pojasnila, razlage, analize, komentarji). Če medij zahteva odgovor na vprašanje, se njegova vloga [obravnava po določbah ZMed](#), če pa zahteva dostop do dokumenta, se njegova vloga obravnava po ZDIJZ. Medij mora vprašanje vložiti pisno po navadni ali elektronski pošti (digitalno potrdilo ali elektronski podpis nista potrebna), zavezanc pa ga mora o zavrnitvi ali delni zavrnitvi pisno obvestiti do konca naslednjega delovnega dne. V nasprotnem primeru mora zavezanc 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 zavezanc posredovati najpozneje v treh dneh. Če zavezanc 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 ŠTEVILLO VLOŽENIH PRITOŽB IN REŠENIH ZADEV

Pritožbeni postopki v 2018



Leta 2018 je Informacijski pooblaščenec vodil 549 pritožbenih postopkov, od tega 313 postopkov zaradi zavrnitve dostopa do zahtevane informacije (med njimi je bilo 19 pritožbenih postopkov zoper poslovne subjekte pod prevladujočim vplivom oseb javnega prava) in 236 postopkov zaradi t. i. molka organa (neodzivnosti).

V okviru pritožbenih postopkov zoper odločbe, s katerimi so zavezanci zavrnili zahteve po dostopu do informacij javnega značaja ali zahteve po njihovi ponovni uporabi, je Informacijski pooblaščenec izdal 288 odločb, sedem sklepov o ustavitev postopkov zaradi umika pritožbe, v petih primerih je pritožbo s sklepom zavrgel (tri pritožbe so bile prepozne, dve pa nedovoljeni), dva pritožbena postopka pa je združil v enega. Pri reševanju pritožb je opravil 36 ogledov in camera, tj. ogledov brez prisotnosti stranke, ki zahteva dostop do informacije javnega značaja, na katerih je ugotavljal dejansko stanje pri organu.

Informacijski pooblaščenec je v pritožbenih postopkih zaradi molka zavezance najprej pozval, naj o zahtevi prosilca čim prej odločijo. V večini primerov so zavezanci po pozivu Informacijskega pooblaščenca o zahtevi prosilca odločili na način, da so mu posredoovali zahtevane informacije, ali pa da so mu izdali zavrnitno odločbo, zoper katero se je prosilec lahko pritožil pri Informacijskem pooblaščencu. V 22 primerih je Informacijski pooblaščenec prosilcem pojasnil, da za reševanje njihove vloge ni pristojen, in jim svetoval, kako ravnati, v 21 primerih pa je pritožbo s sklepom zavrgel, in sicer v 19 primerih zaradi preuranjenosti, v dveh primerih pa zaradi pomanjkljive vloge oz. zato, ker prosilec vloge kljub pozivu v določenem roku ni dopolnil. Sedem posameznikov je pritožbe umaknilo, ker so prejeli zahtevano dokumentacijo, v enem primeru pa je Informacijski pooblaščenec vlogo odstopil v reševanje pristojnemu organu.

Leta 2018 je Informacijski pooblaščenec prejel 287 pisnih prošenj za pomoč in različnih vprašanj posameznikov glede dostopa do informacij javnega značaja, v okviru dežurstev v času uradnih ur pa je prejel 640 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.



287 pisnih prošenj za pomoč



640 klicev

2.3 ŠTEVILLO VLOŽENIH TOŽB IN SODB

Pritožba zoper odločbo Informacijskega pooblaščenca ni dopustna, mogoče pa je sprožiti upravni spor. Leta 2018 je bilo zoper odločbe Informacijskega pooblaščenca na Upravnem sodišču vloženih 34 tožb, tj. zoper 11,8 % 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.

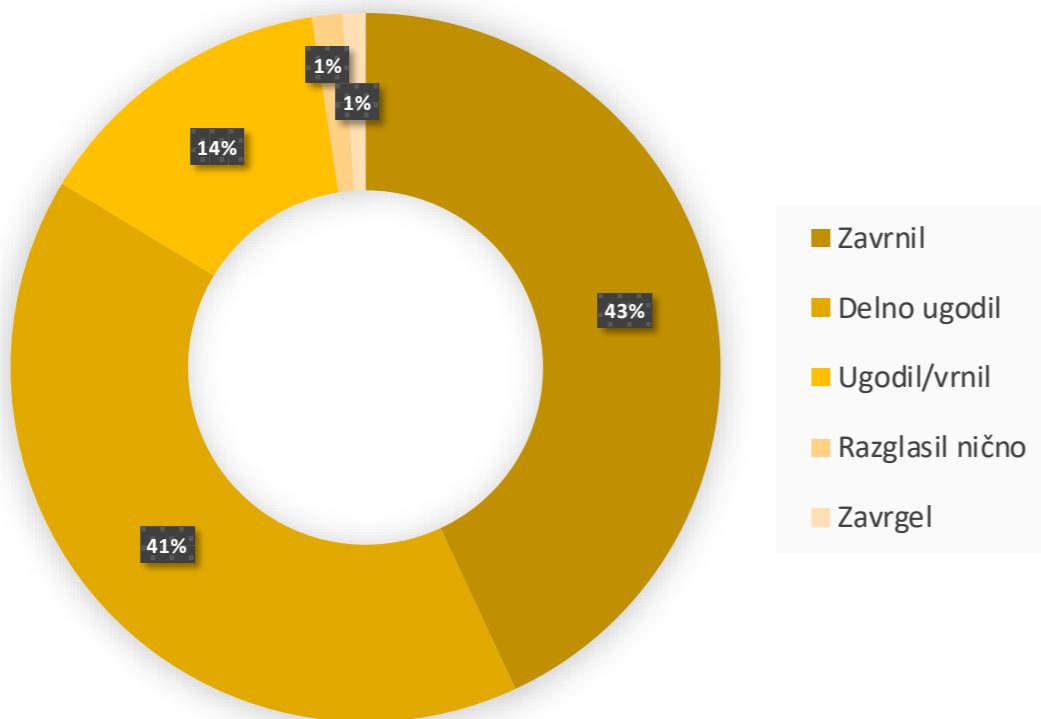
Upravno sodišče je leta 2018 odločilo o 40 tožbah, ki so bile vložene zoper odločbe Informacijskega pooblaščenca, in:

- tožbo zavrnilo – 22,
- tožbi ugodilo, izpodbijano odločbo oz. del odločbe odpravilo in zadevo vrnilo Informacijskemu pooblaščencu v ponovno odločanje – 7,
- tožbo zavrglo – 6,
- tožbi ugodilo in izpodbijano odločbo v enem delu spremenilo tako, da se pritožba zavrne – 2,
- postopek ustavilo zaradi umika tožbe – 2,
- tožbi deloma ugodilo, odločbo v tem delu odpravilo in vrnilo organu prve stopnje v ponoven postopek – 1.

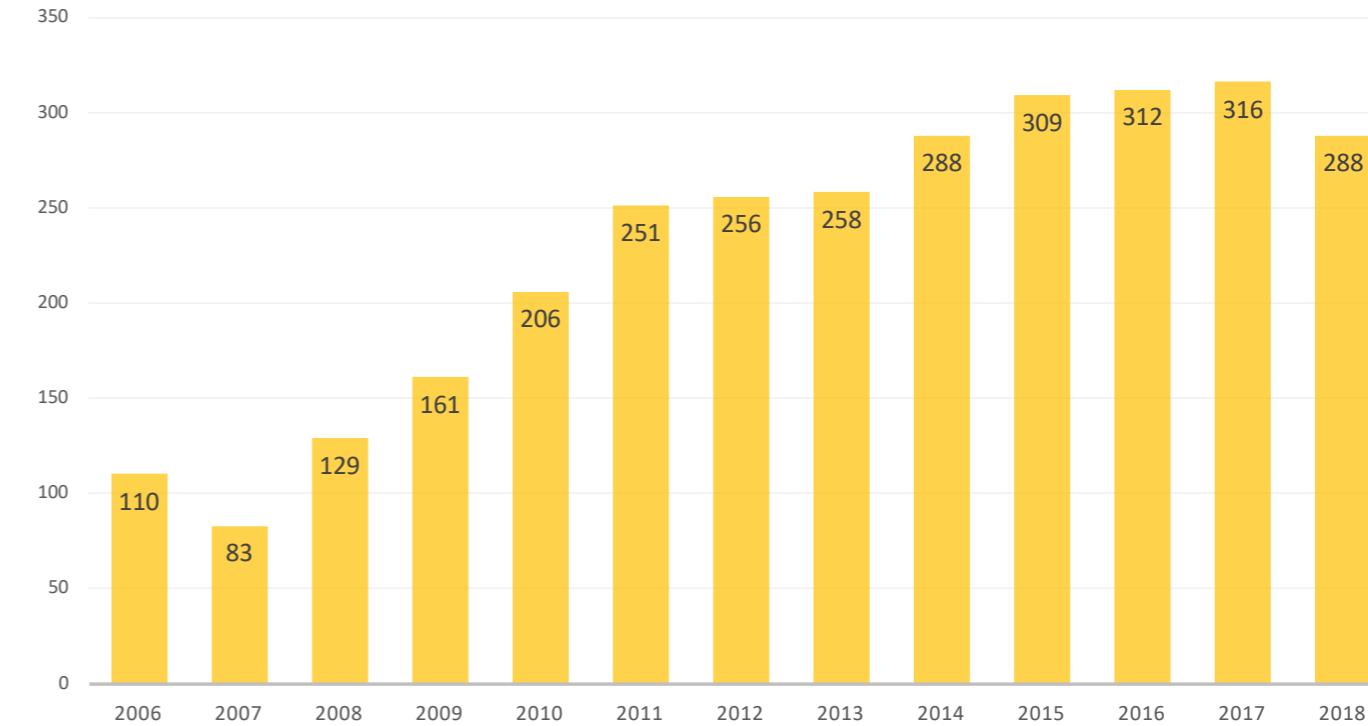
Leta 2018 ni bila vložena nobena revizija zoper sodbo Upravnega sodišča. Do konca leta 2018 je Informacijski pooblaščenec prejel dve odločitvi Vrhovnega sodišča v zvezi z revizijami zoper sodbe Upravnega sodišča; Vrhovno sodišče je eno revizijo, ki jo je vložil zavezanc, zavrnilo, eni reviziji, ki jo je prav tako vložil zavezanc, pa je ugodilo. V slednji je sodbo Upravnega sodišča spremenilo tako, da je tožbi zavezanca ugodilo in izpodbijano odločbo Informacijskega pooblaščenca v enem delu spremenilo tako, da je pritožbo prosilca zavrnilo. Prosilec je nato kot stranka z interesom zoper sodbo Vrhovnega sodišča in sodbo Upravnega sodišča vložil ustavno pritožbo, ki jo je Ustavno sodišče sprejelo v obravnavo, sprejelo pa je tudi prosilčeve pobudo za začetek postopka za oceno ustavnosti tretjega odstavka 18.a člena Zakona o maturi (ZMat) ter osmega odstavka 64. člena in 65. člena Zakona o osnovni šoli (ZOsni).

2.4 STATISTIKA PO POSAMEZNIH PODROČJIH

Odločitve Informacijskega pooblaščenca glede prejetih pritožb



Število izdanih odločb na področju dostopa do informacij javnega značaja med letoma 2006 in 2018.

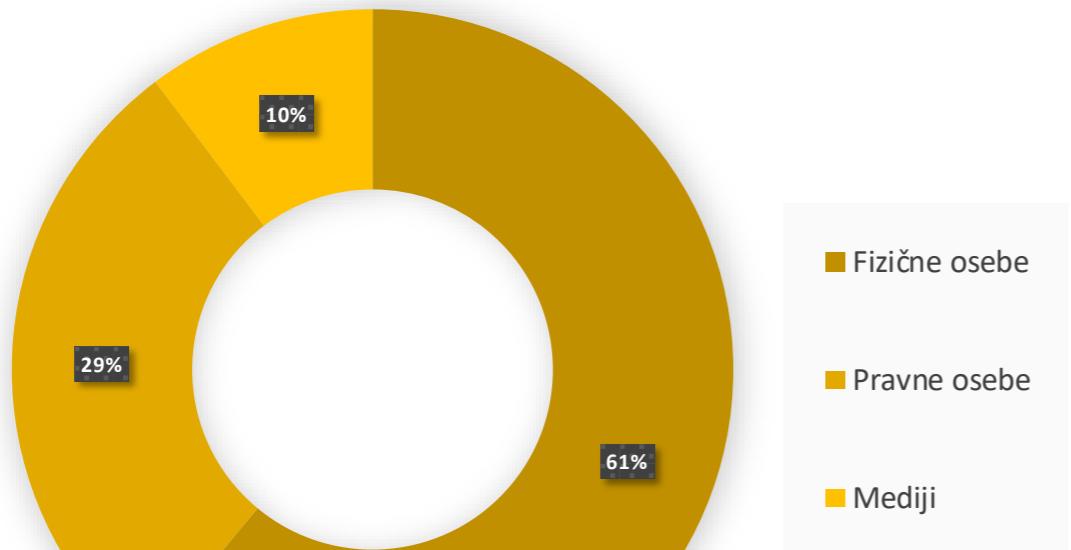


Informacijski pooblaščenec je leta 2018 v pritožbenih postopkih izdal 288 meritornih odločb, v katerih je:

- pritožbo zavrnili – 124,
- pritožbi delno ali v celoti ugodil oz. rešil zadevo v korist prosilca – 117,
- pritožbi ugodil in zadevo vrnil v ponovno odločanje prvostopenjskemu organu – 40,
- odločbo prvostopenjskega organa razglasil za nično – 4,
- pritožbo zavrgel – 3.

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

- državni organi – 131, od tega ministrstva in organi v sestavi ter upravne enote 109, sodišča, vrhovno državno tožilstvo, državno odvetništvo pa 22,
- javni skladi, zavodi, agencije, izvajalci javnih služb, nosilci javnih pooblastil in druge pravne osebe javnega prava – 86,
- občine – 50,
- poslovni subjekti pod prevladujočim vplivom države, občin ali drugih oseb javnega prava – 21.



V 172 primerih so bili prosilci fizične osebe, v 81 primerih so se pritožile pravne osebe zasebnega sektorja, novinarji in medijske hiše so se pritožili 29-krat, pravne osebe javnega sektorja pa šestkrat.

2.5 STORJENI PREKRŠKI PO ZDIJZ, ZInfP IN ZMeD

Leta 2018 Informacijski pooblaščenec ni uvedel nobenega postopka zaradi prekrškov po ZDIJZ, ZInfP ali ZMed, je pa izdal odločbo o prekršku v postopku iz leta 2017, s katero je odgovorni osebi organa izrekel globo zaradi prekrška po drugem odstavku 39. člena ZDIJZ. Informacijski pooblaščenec je namreč ugotovil, da je organ po prejemu zahteve za dostop do informacij javnega značaja trajno izbrisal zahtevane dokumente z namenom, da informacija ne bi bila dostopna javnosti.

2.6 IZBRANI PRIMERI NA PODROČJU DOSTOPA DO INFORMACIJ JAVNEGA ZNAČAJA

Razpolaganje z nepristranskimi in objektivnimi informacijami je v javnem interesu

Prosilec (Transparency International Slovenija) je želel prejeti dopis, ki ga je Zavod RS za blagovne rezerve naslovil na Komisijo za preprečevanje korupcije (v nadalnjem besedilu organ) glede odstranitve transakcij iz aplikacije Erar. Organ je odločil, da je dopis prosto dostopna informacija javnega značaja, priloga k dopisu pa ne, pri čemer se je skliceval na izjemo iz 1. točke prvega odstavka 6. člena ZDIJZ (varstvo tajnih podatkov). Priloga (tj. seznam transakcij) je namreč vsebovala podatke o finančnih transakcijah pri nabavah zaščitnih tehničnih ovir in je bila označena s stopnjo »internal« po Zakonu o tajnih podatkih (ZTP). Pri izvedbi testa javnega interesa je organ ocenil, da javni interes za razkritje dokumenta ni bil podan. V pritožbenem postopku je Informacijski pooblaščenec ugotovil, da ZDIJZ kot izjemo po določbi 1. točke prvega odstavka 6. člena dovoljuje samo tiste informacije, ki so ustrezno opredeljene kot tajne po ZTP in ki za to izpolnjujejo materialni in formalni kriterij. Ob vpogledu v seznam transakcij je Informacijski pooblaščenec ugotovil, da sta izpolnjena dva elementa formalnega kriterija – dokument je bil vidno označen s stopnjo tajnosti, oceno možnih škodljivih posledic je podpisala za to pooblaščena oseba. Manjkal pa je tretji kriterij, saj ocena škodljivih posledic ni izpolnjevala vseh pogojev skladno z 11. členom ZTP. ZTP določa, da mora pooblaščena oseba določiti stopnjo tajnosti podatka ob njegovem nastanku oz. ob začetku izvajanja naloge organa, katere rezultat bo tajen podatek. Informacijski pooblaščenec je ugotovil, da so bili izvirni podatki, ki jih je vseboval seznam transakcij, javno objavljeni v aplikaciji Erar od dne 5. 11. 2015 do 28. 6. 2016. Ocena možnih škodljivih posledic (ki se je sicer nanašala samo na izpis, tj. seznam transakcij) je bila izdelana šele 24. 6. 2016. To pomeni prepozno, saj je nastala več kot sedem mesecev po tem, ko je bil javno objavljen prvi podatek iz seznama oz. en dan po objavi zadnjega podatka iz seznama transakcij, torej nedvomno po nastanku izvirnega dokumenta in tudi po začetku izvajanja naloge Zavoda, katere rezultat naj bi bil tajen podatek.

Niti organ niti Zavod tudi nista uspela izkazati, da bi z razkritjem zahtevanega dokumenta nastale ali bi očitno lahko nastale škodljive posledice za varnost države ali za njene politične in gospodarske koristi, konkretno za delovanje ali izvajanje nalog organa na enem izmed področij, navedenih v 5. členu ZTP.

To je pomenilo, da v obravnavani zadevi tudi materialni kriterij za določitev tajnosti podatka ni bil podan. Zavodu, ki je dokumentu določil stopnjo tajnosti, je zato Informacijski pooblaščenec naložil umik stopnje tajnosti. Pri tem je Informacijski pooblaščenec za razkritje zahtevane informacije ugotovil tudi obstoj prevladujočega javnega interesa. Vsi podatki, ki so se nahajali v seznamu transakcij, so bili določeno obdobje javno objavljeni v spletni aplikaciji Erar. Dejstvo, da so bile zaščitne tehnične ovire nabavljenе in postavljenе na meji, ni bilo sporno. Iz obširnega poročanja v javnih občilih se je lahko vsak seznanil s tem, da je Slovenija na meji za regulacijo migracijskih tokov uporabila zaščitne tehnične ovire in kakšne vrste so te ovire, prav tako so sredstva javnega obveščanja obširno poročala o tem, kakšne težave so se ob tem pojavljale. O tem obstajajo tudi uradni podatki (npr. v odgovoru na poslansko vprašanje). Za pravilno in celovito seznanitev javnosti s podatki o porabi javnih sredstev v zvezi z nabavo in postavitvijo zaščitnih tehničnih ovir je bilo torej v javnem interesu, da se seznam transakcij razkrije v celoti. Kot se je Informacijski pooblaščenec prepričal z vpogledom v ta seznam, iz njega niso bili razvidni nobeni tehnični podatki (npr. geolokacija zaščitnih tehničnih ovir, časovna dinamika postavitve po posameznih delih meje, časovna dinamika dobave zaščitnih tehničnih ovir, način postavitve ipd.), ki bi lahko vplivali na učinkovitost regulacije migracijskih tokov na meji. Nedvomno je v javnem interesu, da v demokratični družbi javnost razpolaga z nepristranskimi in objektivnimi informacijami, na podlagi katerih se lahko informirano odloča v/o javnopravnih zadevah in tudi vrši nadzor nad porabo javnih sredstev. To je skladno tudi s 3. in z 39. členom Ustave RS. Ker so bile v obravnavanem primeru izražene okoliščine, ki so bile v prid javnemu interesu, je Informacijski pooblaščenec organu naložil razkritje zahtevanega dokumenta. Tehtanje vseh okoliščin je v danem primeru nedvomno pripeljalo do zaključka, da je javni interes za razkritje zahtevanih informacij močnejši od interesa, da se ti podatki zavarujejo zaradi varovanja tajnih podatkov.

KLJUČNE BESEDE: tajni podatki, test interesa javnosti, odločba številka 090-298/2017

Višina izplačil skupaj z imeni in priimki mentorjev pri zaključevanju študijskih programov so prosto dostopni podatki

Prosilka (novinarka) je želela po Zakonu o medijih prejeti informacijo, koliko izplačil je Pravna fakulteta v Mariboru oz. Univerza v Mariboru nakazala z naslova postavke »znanstveni magistrski študijski program« za celotno študijsko leto 2015/2016 in koliko za obdobje od junija do septembra 2016 posameznim profesorjem in drugim sodelavcem. Organ je zahtevo zavrnil s sklicevanjem na izjemo po drugem odstavku 5.a člena ZDIJZ, ker se je zahteva nanašala na podatke, ki bodo pridobljeni oz. sestavljeni zaradi nadzornega postopka. Na Univerzi v Mariboru (v nadalnjem besedilu organ) je bila namreč v teku revizija notranjega poslovanja članic, pri kateri so se preverjala tudi izplačila profesorjem. V pritožbenem postopku je Informacijski pooblaščenec ugotovil, da je pritožba dovoljena, ker zahtevana informacija izhaja iz dokumenta »Bruto plačila po pogodbah in

ceniku Univerze v Mariboru za sodelovanje v komisijah in za mentorstvo pri zaključevanju starih magistrskih programov«. Informacijski pooblaščenec je odločil, da finančni nadzor s strani revizijske hiše ne ustreza pogoju izjeme po drugem odstavku 5.a člena ZDIJZ. Po navedeni izjemi lahko organ prosilcu zavrne dostop do zahtevane informacije ali njen ponovno uporabo, če se zahteva nanaša na podatek, ki je pridobljen ali sestavljen zaradi nadzornega postopka, ki ga v skladu z zakonom vodi Banka Slovenije, organ, pristojen za nadzor trga vrednostnih papirjev ali zavarovalniški nadzor, ali drug nadzorni organ, specializiran za finančni nadzor, če je nadzorni postopek še v teku. Kot izhaja iz navedene določbe, ki v okviru »nadzornih organov« izrecno navaja Banko Slovenije, organ, pristojen za nadzor trga vrednostnih papirjev ali zavarovalniški nadzor, je zakonodajalec nadzorne postopke, ki jih je želel varovati, vezal na institucije, ki opravljajo oblastne, javnopravne naloge na področju finančnega nadzora. V obravnavanem primeru je Informacijski pooblaščenec ocenil, da revizijskih družb ni mogoče uvrstiti med »drug nadzorni organ«. Zakonodajalec je z navedbo »ali drug nadzorni organ, specializiran za finančni nadzor« dopustil možnost, da se v okviru te izjeme varujejo tudi drugi »nadzorni postopki«, ki niso našteti, če gre za »organe«, ki izpolnjujejo pogoj, da so »specializirani za finančni nadzor« (tak organ je po praksi Informacijskega pooblaščenca npr. Računsko sodišče RS). Vendar pri revizijskih družbah ni mogoče zaznati »oblastnih, javnopravnih nalog nadzora«, kar je namen te izjeme. Informacijski pooblaščenec pri odločjanju o zadevi po uradni dolžnosti ni ugotovil obstoja katere koli izjeme od prostega dostopa po 5.a členu ali po prvem odstavku 6. člena ZDIJZ. V dokumentu so sicer navedena imena in priimki mentorjev, vendar so ti podatki povezani s porabo javnih sredstev, zato ne sodijo med varovane osebne podatke. Imena in priimki posameznikov skupaj s podatkom o višini izplačila predstavljajo podatke, ki so skladno z določbo 1. alineje tretjega odstavka 6. člena ZDIJZ prosto dostopne informacije javnega značaja. Tako iz prakse Informacijskega pooblaščenca kot iz upravno-sodne prakse izhaja, da je pojem javnih sredstev treba razlagati široko (zajema tudi sredstva, pridobljena na trgu) in da se z njim ne zajema le proračunskih sredstev.

Ker je bila pritožba prosilke utemeljena, je Informacijski pooblaščenec organu odredil posredovanje dokumenta »Bruto plačila po pogodbah in ceniku Univerze v Mariboru za sodelovanje v komisijah in mentorstvu pri zaključevanju starih magistrskih programov«.

KLJUČNE BESEDE: osebni podatki, mediji, odločba številka 090-277/2017

Zakaj dokumenti kazenskega postopka, ki je še v teku, niso prosto dostopne informacije javnega značaja?

Prosilec je od Vrhovnega državnega tožilstva (v nadalnjem besedilu organ) želel prejeti pravnomočne sklepe o uvedbi štirih preiskav zoper konkretno fizične osebe. Organ je zahtevo zavrnil s sklicevanjem na izjemo varstva postopka kazenskega pregona po 6. točki prvega odstavka 6. člena ZDIJZ. Nesporočno je bilo dejstvo, da so zahtevani dokumenti (tj. sklepi o uvedbi preiskave) predmet

odprtih, še ne pravnomočno končanih, (pred)kazenskih postopkov. Dostop do zahtevanih informacij javnega značaja bi škodoval interesom oz. učinkoviti izvedbi (pred)kazenskih postopkov, pa tudi zasebnosti vpletenih oseb oz. varstvu njihovih osebnih podatkov. S samim dostopom do zahtevanih informacij bi bila dodatno ogrožena tudi verodostojnost izpovedi prič. Prosilec se ni strinjal z argumentom organa, da bi razkritje zahtevanih informacij vplivalo na pričanja prič, zato je vložil pritožbo. Informacijski pooblaščenec je v pritožbenem postopku ugotovil, da so bili postopki kazenskega pregona v vseh obravnavanih primerih še v teku in da bi izvedbi teh postopkov lahko nastala nepopravljiva škoda, če zaradi razkritja zahtevanih sklepov določenih preiskovalnih opravil (tudi zaslišanja prič) ne bi bilo mogoče več opraviti. Organ je prepričljivo pojasnil, da bi razkritje lahko povzročilo nepopravljive posledice za samo izvedbo (pred)kazenskih postopkov, sodnih preiskav in glavnih obravnav (če bo do njih prišlo), ker so se v vseh obravnavanih primerih dokazi še zbirali oz. še niso bile zaslišane vse priče in se še niso izvedli drugi dokazi. Pri ugotavljanju obstaja izjeme po 6. točki prvega odstavka 6. člena ZDIJZ je Informacijski pooblaščenec smiselno sledil tudi namenu določb Zakona o kazenskem postopku (ZKP). Da je izjeme po ZDIJZ treba presojati v povezavi s posameznimi procesnimi zakoni, izhaja tudi iz upravno-sodne prakse (sodba št. I U 542/2013 z dne 11. 9. 2013 (tč. 13 obrazložitve), sodba št. I U 2287/2011/6 z dne 9. 5. 2012 (tč. 9 obrazložitve)). V zvezi s podatki v zahtevanih sklepih izvedba delnega dostopa na podlagi 7. člena ZDIJZ ni bila mogoča. Prav tako pri obravnavanem primeru ni bilo moč uporabiti 7.a člena ZDIJZ, saj je šele neobstoj izjeme po 6. točki prvega odstavka 6. člena ZDIJZ eden izmed pogojev, ki morajo biti kumulativno podani, da se na podlagi 7.a člena ZDIJZ lahko razkrijejo taksativno našteti podatki iz obtožnega akta. Informacijski pooblaščenec je ocenil tudi, da javni interes za razkritje ni podan. Rezultat testa je bil vezan tudi na časovno točko, zlasti na dejstvo, da so bili obravnavani postopki še v teku in v fazah, v katerih se je kaznivo dejanje še raziskovalo in so se dokazi še zbirali. Po ustaljeni upravno-sodni praksi za razkritje ne zadošča niti medijska odmevnost dogodka, temveč je javni interes glede razkritja podan, če so ogrožene take vrednote, kot je življenje, zdravje ali varnost ljudi in podobno. Takšne vrednote v konkretnem primeru niso bile ogrožene, zato je Informacijski pooblaščenec pritožbo prosilca zavrnil.

KLJUČNE BESEDE: kazenski postopek, odločba številka 090-307/2017

Za sodelovanje v javni razpravi mora javnost imeti pravico do celovitih in popolnih informacij

Prosilec je od Ministrstva za gospodarski razvoj in tehnologijo (v nadalnjem besedilu organ) zahteval dostop do Pogodbe o izvedbi strateške investicije, ki so jo podpisale država, občina Hoče - Slivnica in družba Magna Steyr. Organ je zahtevo zavrnil s sklicevanjem na poslovno skrivnost po 2. točki prvega odstavka 6. člena ZDIJZ, saj je ugotovil, da je zahtevani pogodbni priložen sklep stranskega udeleženca in da je celotna pogodba opredeljena kot poslovna skrivnost. Tudi stranski udeleženec je opozoril, da gre za investicijo v visoko konkurenčni panogi in ima zato upravičen interes, da

specifike svoje naložbe ohrani tajne. Čeprav je Informacijski pooblaščenec v pritožbenem postopku ugotovil, da je predmetna pogodba po subjektivnem kriteriju opredeljena kot poslovna skrivnost stranskega udeleženca, jo je bil organ dolžan posredovati prosilcu na podlagi drugega odstavka 6. člena ZDIJZ. Javni interes za razkritje zahtevane pogodbe je prevladal nad interesom stranskega udeleženca, da bi ohranil poslovno skrivnost. Strateška investicija, na izvedbo katere se je zahtevana pogodba nanašala, namreč ni bila zgolj predmet medijske pozornosti, ampak je v lokalni skupnosti in tudi v širši javnosti sprožila številne dileme in vprašanja, kot npr. ali je bila sklenitev zahtevane pogodbe transparentna in gospodarna z vidika porabe javnih sredstev, katere pravice in obveznosti iz te pogodbe izhajajo za pogodbene stranke, kakšni bodo vplivi investicije na okolje ter posledično na zdravje ljudi in kvaliteto njihovega življenja, kolikšen bo finančni učinek za državo oz. občino. Da bi javnost lahko sodelovala v odprti javni razpravi v zvezi z obravnavano strateško investicijo, mora imeti pravico do celovitih in popolnih informacij, med katere so sodile tudi informacije iz zahtevane pogodbe. Dejstvo je bilo, da je bila zahtevana pogodba sklenjena na podlagi 9. člena Zakona o zagotavljanju pogojev za izvedbo strateške investicije na razvojnem območju (ZZPISI) v Občini Hoče - Slivnica in da je konkretno urejala pravice in obveznosti strank, ki so morale biti določene skladno z ZZPISI in sklepom Vlade RS. Informacijski pooblaščenec je ocenil, da bi bilo povsem v nasprotju z namenom določbe ZZPISI o varovanju javne koristi, če bi se javnosti dostop do zahtevane pogodbe onemogočil, saj brez podatkov iz te pogodbe ne bi bilo mogoče preveriti, ali se z obravnavano strateško investicijo resnično varuje interese Republike Slovenije in javno korist. V prid razkritju je bilo tudi dejstvo, da se mora vsakdo, ki želi skleniti pogodbo s subjektom javnega prava, podrediti posebnemu načinu sklepanja pravnih poslov. Posredno je bila zahtevana pogodba povezana s finančnim učinkom, ki se je kazal v tem, da je v zvezi z izvedbo predmetne strateške investicije organ s stranskim udeležencem podpisal Pogodbo o dodelitvi finančne spodbude, na podlagi katere je bila ta strateška investicija s strani države sofinancirana v višini 18.600.000 evrov. Vsi podatki v zahtevani pogodbi so bili navedeni v okvirih določb ZZPISI in Sklepa Vlade RS ter niso razkrivali podrobnejše časovnice projekta, dinamike investiranja in poslovnih načrtov, zato je Informacijski pooblaščenec menil, da je bila ocena stranskega udeleženca, da bi razkritje pogodbe omogočalo sklepanje na dodatne informacije in posledično poslabšalo njegov konkurenčni položaj, pretirana. Omejitev gospodarske pobude je prestala tudi vse tri vidike t. i. strogega testa sorazmernosti, zato je ustavno dopustna.

KLJUČNE BESEDE: poslovna skrivnost, test interesa javnosti, odločba številka 090-7/2018

Prednost ima interes javnosti, ne interes in koristi javnega zavoda

Prosilka (novinarka) je od Javnega zavoda Lekarne Ljubljana (v nadalnjem besedilu organ) zahtevala posredovanje Strateškega načrta Lekarne Ljubljana 2018–2022. Organ je zahtevo zavrnil s sklicevanjem na izjemo varstva poslovne skrivnosti po 2. točki prvega odstavka 6. člena ZDIJZ. Prosilka je v pritožbi navedla, da je strateški dokument razvoja javnega zavoda v javnem interesu in ta javni interes pretehta interes javnega zavoda po zapiranju informacij. Informacijski pooblaščenec je v pritožbenem postopku navedbi pritrdil. Ob pregledu Strateškega načrta 2018–2022 in preučitvi sprejetega pravilnika in sklepa organa o poslovni skrivnosti, je Informacijski pooblaščenec ugotovil, da strateški načrt kot tak v pravilniku in v sklepu ni bil opredeljen kot poslovna skrivnost. Kot poslovna skrivnost so bili opredeljeni le podatki, ki se nanašajo na tržno dejavnost. Ob pregledu kazala dokumenta je Informacijski pooblaščenec ugotovil, da se nobeno od poglavij ne nanaša na tržno dejavnost organa, temveč na sam organ kot celoto. Za izpolnitev subjektivnega kriterija bi morala biti podana izrecna odredba o tem, kateri podatki se štejejo za poslovno skrivnost. Po objektivnem kriteriju poslovne skrivnosti pa je nujno, da je potreba po varstvu očitna (tako tudi upravno-sodna praksa, npr. sodba št. U 32/2008-25 z dne 8. 10. 2008 in sodba št. U 284/2008-35 z dne 27. 5. 2009), česar organ v konkretnem primeru sploh ni izkazoval. Ker gre pri delovanju organa za izvajanje javne službe, kar je v javnem interesu, bi se moral organ zavedati tudi tega, da ima pri tem izreden pomen nadzor javnosti in da so posledično njegovi interesi in koristi pri izvajanju te dejavnosti omejeni. Dokument je predstavljal načrt in strategijo delovanja javnega zavoda kot celote, organ ga je bil dolžan sprejeti skladno z zakonom, ki ureja njegovo javnopravno delovanje, podatki v njem pa so se nanašali na javno službo. Strateški načrt javnega zavoda, katerega vsebina se nanaša na izvajanje javne službe, tako ne more predstavljati izjeme od prostega dostopa po 2. točki prvega odstavka 6. člena ZDIJZ. Poleg tega je bil za razkritje zahtevanega dokumenta podan javi interes. V dokumentu so bili predstavljeni strategija razvoja, cilji in načrti javnega zavoda kot celote (in ne zgolj njegovega tržnega dela), pri čemer je šlo za podatke, pomembne za celotno javnost, za uporabnike javnega zavoda in za vse tiste, zaradi katerih je vzpostavljen javnopravni režim na tem področju. Ker ima javnost absolutno pravico biti seznanjena s tem, kakšen je strateški načrt razvoja največjega javnega zavoda, ki svoje delo opravlja na področju zagotavljanja zdravil pri zdravljenju in izdelkov za podporo zdravljenja in ohranitve zdravja, je Informacijski pooblaščenec organu naložil, da prosilki posreduje zahtevani dokument v celoti.

KLJUČNE BESEDE: poslovna skrivnost, test interesa javnosti, odločba številka 090-118/2018

Argumentacija organov o varovanju tajnosti vira je največkrat preširoka

Prosilec je od Inšpektorata RS za šolstvo in šport (v nadalnjem besedilu organ) zahteval vse informacije javnega značaja, ki jih je organ izdelal sam, v sodelovanju z drugim organom ali pridobil od drugih oseb zoper določen javni zavod (oz. v zvezi z njim). Organ je zahtevo delno zavrnil s sklicevanjem na izjeme varstva osebnih podatkov, varstva tajnosti vira prijave, varstva notranjega delovanja, varstva poslovne skrivnosti, varstva dokumenta v postopku izdelave in varstva upravnega postopka, pri čemer je prosilcu posredoval 258 strani zahtevanih dokumentov, za katere je ocenil, da so prosto dostopne informacije javnega značaja. Organ je navedel, da do dneva izdaje izpodbijane odločbe trije inšpekcijski postopki niso bili zaključeni, zato vse do njihovega zaključka in še pred preverbo odrejenih ukrepov zaradi vodenja upravnega postopka vseh zahtevanih dokumentov ne more posredovati javnosti. Ocenil je namreč, da seznanitev javnosti pred seznanitvijo stranke v postopku (konkretnega javnega zavoda) z zaključkom postopka in morebitnim obveščanjem pobudnika o izvedenih in izvršenih ukrepih na podlagi določb Zakona o inšpekcijskem nadzoru (ZIN) (24. člen) in Zakona o šolski inšpekciji (11. člen) pomeni odstopanje od načel inšpekcijskega postopka. Informacijski pooblaščenec je v pritožbenem postopku ugotovil, da bi lahko v predmetni zadevi odloči po delih, zato je izdal delno odločbo v delu, ki se je nanašal na varstvo upravnega postopka in varstvo tajnosti vira prijave. ZDIJZ določa, da organ prosilcu zavrne dostop do zahtevane informacije, če se zahteva nanaša na podatek, ki je bil pridobljen ali sestavljen zaradi upravnega postopka, in bi njegovo razkritje škodovalo izvedbi tega postopka. Organ ob sklicevanju na izjemo po 7. točki prvega odstavka 6. člena ZDIJZ ni pojasnil, v kakšni fazi so upravljeni postopki, o katerih posameznih dokumentih iz predmetnih zadev je odločal niti kako bi razkritje posameznega dokumenta vplivalo oz. škodovalo izvedbi konkretnega upravnega postopka. Kot take se izpodbijane odločbe ni dalo preizkusiti, zato jo je Informacijski pooblaščenec v tem delu vrnil organu prve stopnje v ponovno odločanje z navodili, da se opredeli do vsakega posameznega dokumenta in posamezno oceni in obrazloži obstoj izjeme varstva upravnega postopka. Glede izjeme po tretjem odstavku 5.a člena ZDIJZ (varovanje tajnosti vira) je Informacijski pooblaščenec ugotovil, da je organ za del dokumentov napačno zaključil, da je bila podana navedena izjema, in da pri njih ni mogoče uporabiti instituta delnega dostopa iz 7. člena ZDIJZ. Skladno z drugim odstavkom 16. člena ZIN je inšpektor dolžan varovati tajnost vira prijave in vira drugih informacij, na podlagi katerih opravlja inšpekcijski nadzor. Z drugim odstavkom 16. člena ZIN je varovana identiteta tega vira, medtem ko podatki ali obvestila, ki jih je ta vir dal, skladno s prvim odstavkom 16. člena ZIN uživajo varstvo pred razkritjem le, če so opredeljeni kot poslovna skrivnost ali druga tajnost. Tako je Informacijski pooblaščenec ugotovil, da je prost dostop mogoč, saj je šlo ali za anonimne prijave ali za dokumente, pri katerih je vir prijave mogoče prekriti in ga s tem varovati na način, da ni več določljiv. Pri teh dokumentih je torej delni dostop v smislu 7. člena ZDIJZ mogoč. S prekritjem določenih podatkov v teh dokumentih se posledično ni dalo sklepiti na določenega posameznika, saj ni šlo za tolikšno vsebnost in koncentracijo informacij, da bi bilo iz njih mogoče razbrati vir prijave. Enako je veljalo za anonimne

prijave, ki so bile podane splošno, čeprav so se nanašale na konkretno problematiko pri določenem javnem zavodu. Vsebina teh prijav je bila splošna in iz nje niso izhajali podatki, na podlagi katerih bi lahko sklepal na določenega prijavitelja. Ker je bila v tem delu pritožba utemeljena, je Informacijski pooblaščenec ugodil prosilcu; organ mu je moral omogočiti dostop do zahtevanih dokumentov na način, da je prekril zgolj varovane podatke.

KLJUČNE BESEDE: upravni postopek, tajnost vira, številka odločbe 090-155/2018

Pri tehtanju javnega interesa ni splošnih odločitev

Prosilkajena Ministrstvo za notranje zadeve vložila zahtevo za posredovanje seznama posameznikov, ki so bili od leta 2007 do vložitve zahteve izredno naturalizirani. Glede na to, da se je prosilka v dopolnitvi zahteve sklicevala na javni interes, je o zahtevi skladno s prvo alinejo drugega odstavka 21. člena ZDIJZ odločila Vlada RS (v nadalnjem besedilu organ). Organ je dostop do imen in priimkov 3979 posameznikov, ki so bili izredno naturalizirani, zavrnil s sklicevanjem na izjemo varstva osebnih podatkov po 3. točki prvega odstavka 6. člena ZDIJZ. Po mnenju organa prevladajoč javni interes za razkritje določenih osebnih podatkov ni bil podan. Navedel je še, da je bil ta primer z vidika »množičnosti« bistveno drugačen od primera iz leta 2012 (odločba Informacijskega pooblaščenca, št. 090-148/2012/8), ko je Informacijski pooblaščenec odločal o dostopu do podatka o tem, ali je konkretna posameznica pridobila slovensko državljanstvo z izredno naturalizacijo. V pritožbenem postopku se je Informacijski pooblaščenec najprej opredelil do svoje odločbe z dne 19. 10. 2012, št. 090-148/2012/8, in poudaril, da zgolj zato, ker je v navedeni odločbi odločil, da je podan javni interes za dostop do odločbe in pravnega mnenja za konkretno posameznico, to per se ne pomeni, da so vsa imena in priimki izredno naturaliziranih v registru državljanstev prosto dostopne informacije javnega značaja. Pri testu javnega interesa namreč ni generalnih odločitev, ki bi veljale za vse »podobne« ali »istovrstne« informacije. S to odločbo Informacijski pooblaščenec ni posegel v zakonsko ureditev evidence državljanstev in njihovo dostopnost po Zakonu o državljanstvu Republike Slovenije (ZDRS), temveč je zgolj v konkretnem primeru odločil, da interes javnosti prevlada nad sicer varovanimi osebnimi podatki konkretno posameznice. Tokrat zahtevan seznam imen in priimkov 3979 oseb je predstavljal zbirko osebnih podatkov, ki se vodi v okviru registra državljanstev, za namene po ZDRS, ki ne omogoča prostega dostopa. Izjemoma je mogoče izjemo varstva osebnih podatkov preseči s testom javnega interesa, vendar le, če bi se izkazalo, da je podan javni interes za razkritje za vsakega posameznika posebej, torej za vsako od 3979 oseb. Prosilka je pri izkazovanju javnega interesa izhajala iz dvoma o pravilnosti vodenja postopkov oz. je navedla, da so posamezniki izredno naturalizirani v imenu vseh državljanov Republike Slovenije, zato je to v javnem interesu. Informacijski pooblaščenec je ocenil, da zgolj »splošna nadzorna funkcija javnosti« zagotovo ni zadosten argument javnega interesa, da bi lahko posegli v varovane osebne podatke vrste posameznikov. Obstajati bi moralo nekaj več, torej javni interes za razkritje vsakega posameznika posebej, česar pa

Informacijski pooblaščenec ni ugotovil. Testa javnega interesa za 3979 oseb niti ni bilo mogoče konkretno izvajati, zlasti ne na podlagi informacij, ki so bile predmet presoje. Po oceni Informacijskega pooblaščenca morebitni dvom o nepravilnostih pri enem postopku ne more predstavljati zadostne pravne podlage za razkritje imen in priimkov 3979 oseb. Informacijski pooblaščenec je izvedel še ustavni test sorazmernosti. Ugotovil je, da prosilka sicer zasleduje ustavno doposten oz. legitimen cilj, to je pravico javnosti, da se seznaní z informacijami glede podelitev izrednega državljanstva. Gre namreč za pravico, ki je vezana na ugotavljanje nacionalnega interesa, kar pomeni, da je v tem obsegu presežena strogo osebna pravica posameznika do vprašanja pravne pripadnosti določeni državi in da zajema širše interese države. Vendar pa je Informacijski pooblaščenec ob tem ugotovil, da v obravnavanem primeru niso izpolnjeni vsi trije pogoji testa sorazmernosti za obdelavo oz. prost dostop do osebnih podatkov 3979 oseb (nujnost, primernost in načelo sorazmernosti v ožjem pomenu). Zato je zaključil, da poseg v ustavno pravico do varstva osebnih podatkov ni doposten, in je pritožbo prosilke zavrnil.

KLJUČNE BESEDE: osebni podatek, test interesa javnosti, odločba številka 090-139/2018

Analize tal kot okoljski podatki so absolutno javne

Prosilec (Društvo Proteus – okoljsko gibanje Bela krajina) je na Kmetijsko gozdarsko zbornico Slovenije – Zavod Novo mesto (v nadalnjem besedilu organ) naslovil zahtevo za posredovanje vseh analiz zemlje s kmetije v Črnomlju. Organ je zahtevo zavrnil, ker z dokumenti ne razpolaga oz. ker niso informacije javnega značaja, saj so del njegove tržne dejavnosti. V razlogih je navedel, da je izvajal aktivnosti, povezane z analizami tal in izdelavo gnojilnih načrtov, v dveh primerih. Prvi pri izvajanjу javne naloge »Vnos podatkov in dokumentov za izdelane Programe aktivnosti v letih 2015 in 2016« po naročilu Ministrstva za kmetijstvo, gozdarstvo in prehrano in drugič pri izvajaju čiste tržne dejavnosti, in sicer izvedbe storitve »Hitri talni/rastlinski N-test in Načrt gnojenja«. Za ti dve storitvi je zatrjeval, da je to njegova tržna dejavnost. V zvezi z izvajanjem javne naloge vnosa podatkov in dokumentov je navedel, da je obsegala vnos podatkov in skenirane dokumentacije v spletno aplikacijo, ki je v lasti Agencije RS za kmetijske trge in razvoj podeželja. Zatrdil je, da ni lastnik ali upravljavec te aplikacije, zato tudi nima nikakršnih pooblastil za posredovanje informacij, ki so sestavni del baz podatkov, s katerimi upravlja Agencija RS za kmetijske trge in razvoj podeželja. Poleg tega je prosilec v svoji zahtevi poimensko navedel osebo, zato tudi v primeru, ko bi na dokumentih prekril osebne podatke, ne bi mogel zagotoviti varstva osebnih podatkov fizične osebe. Prosilec je v pritožbi opozoril na dejstvo, da gre pri zahtevanih dokumentih za okoljske podatke, ki so javni po določbah Zakona o varstvu okolja (ZVO-1) (4. točka drugega odstavka 110. člena). Gre namreč za sum škodljivih emisij v zemljo s pretiranim gnojenjem, kar neposredno ogroža podtalnico in rodovitnost zemlje. Informacijski pooblaščenec je v pritožbenem postopku opravil ogled brez prisotnosti strank, t. i. ogled in camera, ter pridobil vse konkretnе zahtevane analize, ki jih je

organ vnašal v aplikacijo Agencije RS za kmetijske trge in razvoj podeželja skladno z javno nalogo po protokolu vnosa. Navedbe organa, da ni lastnik ali upravljavec aplikacije in zato nima nikakršnih pooblastil za posredovanje zahtevanih informacij, je Informacijski pooblaščenec štel za neutemeljene. Izvajanje javnopravnih nalog enega javnopravnega subjekta po naročilu drugega javnopravnega subjekta namreč ni mogoče šteti za dejavnost, ki bi bila izvzeta iz dometa ZDIJZ. Iz prvega odstavka 1. člena ZDIJZ izhaja, da ZDIJZ ureja postopek glede dostopa do informacij javnega značaja, s katerimi organi že razpolagajo, torej ki že obstajajo. Informacija javnega značaja je po prvem odstavku 4. člena ZDIJZ informacija, ki izvira iz delovnega področja organa, nahaja pa se v obliki dokumenta, zadeve, dosjeja, registra, evidence ali drugega dokumentarnega gradiva (v nadalnjem besedilu: dokument), ki ga je organ izdelal sam, v sodelovanju z drugim organom ali ga je pridobil od drugih oseb. Prav tako za odločitev v zadevi niso bile relevantne navedbe organa, da so analize tal in gnojilni načrti last kmetovalca, ki jih je pridobil proti plačilu na trgu in so rezultat izvajanja povsem tržne dejavnosti in ne del izvajanja javne službe. Informacijski pooblaščenec je namreč ugotovil, da po 142. členu Uredbe o ukrepih kmetijsko-okoljska-podnebna plačila, ekološko kmetovanje in plačila območjem z naravnimi ali drugimi posebnimi omejitvami iz Programa razvoja podeželja Republike Slovenije za obdobje 2014–2020 Agencija med drugim izvaja tudi kontrolo izpolnjevanja obveznosti v zvezi z upravičenostjo do plačil za ukrepe razvoja podeželja. Analize tal, ki jih je kmetovalec priložil organu, so del dokumentacije in izkazujejo izpolnjevanje pogojev za pridobivanje plačil ter jih Agencija, oz. po njenem navodilu organ, poseduje zaradi izvajanja javne naloge, ki sodi v njeno, oz. njegovo, delovno področje. Informacijski pooblaščenec je torej ugotovil, da organ razpolaga z vsemi zahtevanimi dokumenti in da gre pri teh za okoljske podatke, ki so po drugi alineji tretjega odstavka 6. člena ZDIJZ »absolutno javne informacije javnega značaja«. S tem ZDIJZ sledi določilom Konvencije o dostopu do informacij, udeležbi javnosti pri odločanju in dostopu do pravnega sredstva v okoljskih zadevah (v nadalnjem besedilu Aarhuška konvencija), po kateri morajo biti od vseh informacij javnega značaja javnosti najbolj dostopne prav okoljske informacije, saj so te ključne za trajnostni razvoj in učinkovito sodelovanje javnosti pri upravljanju z okoljem. Aarhuški konvenciji sledi tudi ZVO-1, ki v 13. členu določa, da so okoljski podatki javni. Med okoljske podatke sodijo vse informacije o tem, kar kakor koli posega v okolje, torej v tisti del narave, kamor seže ali bi lahko segel vpliv človekovega delovanja (3. člen ZVO-1); med te informacije brez dvoma sodijo tudi rezultati analize tal. Ker za okoljske informacije ne velja nobena izjema od prostega dostopa, je Informacijski pooblaščenec sklenil, da so tudi Nmin testi prosto dostopne informacije javnega značaja. Tudi Upravno sodišče RS je v sodbi št. I U 1435/2016-38 z dne 18. 7. 2018 zavzelo stališče, da kadar gre za okoljske informacije, razlage pojma »delovno področje« iz ZDIJZ zaradi (sekundarnega) prava EU, ki vključuje tudi Aarhuško konvencijo, ni mogoče enostavno prenesti iz sistema razmejitve med javno službo in tržno dejavnostjo, saj to razmejevanje (kot ga zagovarja organ v izpodbijani odločbi), pravo EU in interpretacija le-tega s strani Sodišča EU (vključno z Aarhuško konvencijo) ne pozna. Osebni podatki (ime in priimek) kmetovalca ter naslov ali sedež kmetijskega gospodarstva niso varovani osebni podatki, saj podatki v zvezi s kmetijsko dejavnostjo,

ki jo izvaja kmetijsko gospodarstvo, vpisano v register kmetijskih gospodarstev, ne uživajo varstva osebnih podatkov. Informacijski pooblaščenec je tako pritožbi prosilca ugodil in organu naložil, da prosilcu posreduje vse zahtevane analize tal.

KLJUČNE BESEDE: okoljski podatki, osebni podatek, številka odločbe 090-128/2018

Neobjavljeni avtorsko delo lahko predstavlja tudi poslovno skrivnost

Prosilec je od Javnega zavoda Avditorij Portorož (v nadalnjem besedilu organ) želel prejeti dokumentacijo v zvezi z javnim razpisom za 38. festival Melodij morja in sonca Portorož 2018. Želel je pridobiti seznam vseh prejetih prijav na razpis, zaznamke o morebitni izločitvi prijav zaradi neizpolnjevanja pogojev ali nepopolnosti prijave, zvočne posnetke skladb, opredelitev načina izbora skladb, ocene oz. opredelitve do ocenjevanih skladb posameznih članov žirije, točkanje skladb posameznih članov žirije in seštevek točk ter zapisnik izbora z morebitnimi prilogami. Organ je zahtevo zavrnil s sklicevanjem na izjemo varstva osebnih podatkov po 3. točki prvega odstavka 6. člena ZDIJZ. Informacijski pooblaščenec je v pritožbenem postopku ugotovil, da je razkritje osebnih podatkov v zvezi z izbranimi skladbami skladno s 1. alinejo tretjega odstavka 6. člena ZDIJZ, ki določa, da se dostop do podatkov dovoli, ko gre za podatke, ki hkrati pomenijo tudi podatke o porabi javnih sredstev. V razpisnih pogojih je bilo nedvoumno zapisano, da naj bi bile na festivalu podeljene (denarne) nagrade, poleg tega naj bi organizator prijaviteljem skladb, ki so bile izbrane za sodelovanje na festivalu, izplačal po 400,00 EUR bruto na prijavitelja. Skladbe, ki jih je izbrala strokovna komisija in so bile izvedene na festivalu, so bile torej neposredno povezane s porabo javnih sredstev, zato osebni podatki (imena in priimki prijaviteljev izbranih skladb) niso varovani. Za podatke o prijaviteljih neizbranih skladb je Informacijski pooblaščenec ugotovil, da so zaupni, saj Informacijski pooblaščenec ni našel pravne podlage za njihovo razkritje. Prav tako so varovani osebni podatki naslovi (prebivališč) vseh prijaviteljev skladb (izbranih in neizbranih), saj niso v neposredni zvezi s porabo javnih sredstev. Za stvaritve, s katerimi posamezni prijavitelji niso uspešno konkurirali na javnem razpisu (naslovi, izvajalci in zvočni posnetki neizbranih skladb), je Informacijski pooblaščenec ocenil, da so poslovna skrivnost prijaviteljev po drugem odstavku 39. člena Zakona o gospodarskih družbah (ZGD-1). Glede na to, da so prijavitelji na razpis lahko prijavili le avtorska dela, ki še niso bila predvajana javnosti, je bilo očitno, da bi prizadetim strankam z razkritjem njihovih del nastala občutna škoda. Skladbe kot glasbeno delo z besedilom ali brez besedila so avtorska dela individualne intelektualne stvaritve s področja književnosti, znanosti in umetnosti, ki so varovana po Zakonu o avtorski in sorodnih pravicah (ZASP). Enako varstvo kot samo delo uživajo tudi osnutek, sestavni deli in naslov avtorskega dela, ki so sami po sebi individualne intelektualne stvaritve (6. člen ZASP). Avtor ima po 17. členu ZASP izključno pravico odločiti, ali, kdaj in kako bo njegovo delo prvič objavljeno. S tem je ustvarjalec nekega dela (konkretno prijavljene skladbe) nagrajen z »ekskluzivo« nad izkoriščanjem lastnega dela in truda; kakršno koli drugačno ravnanje tretjih oseb

bi lahko vplivalo na njegov položaj na trgu in mu s tem povzročilo občutno škodo. Glede na to, da avtorska pravica pripada avtorju na podlagi same stvaritve dela (14. člen ZASP), je Informacijski pooblaščenec odločil, da se lahko ta stvaritev do odločitve avtorja o prvi objavi varuje kot poslovna skrivnost. Le tako se nosilci avtorskih in drugih sorodnih pravic lahko obnašajo poslovno, tržno, ekonomsko zanimivo, hkrati pa onemogočajo kakršno koli protipravno prilaščanje njihovih stvaritev. Podatki, ki se nanašajo na izbrane skladbe (naslovi, izvajalci in njihovi zvočni posnetki), pa so zaradi določbe 1. alineje tretjega odstavka 6. člena ZDIJZ prosto dostopne informacije javnega značaja. Tudi pri razkrivanju imen in priimkov članov strokovne komisije je bilo treba upoštevati 1. alinejo tretjega odstavka 6. člena ZDIJZ. Vsi člani strokovne komisije so bili v komisijo imenovani z odločitvijo organa in so torej v imenu in na račun organa opravljeni javno funkcijo. Poleg tega je bilo treba pri objavi imen in priimkov članov komisij upoštevati 10. člen Uredbe o posredovanju in ponovni uporabi informacij javnega značaja. Ta določa, da mora organ v svetovni splet posredovati dokumentacijo o najmanj naslednjih javno dostopnih informacijah javnega značaja v zvezi s postopki javnih razpisov, ki jih vodi: javni razpis in razpisno dokumentacijo, člane komisij za izvedbo postopkov javnih razpisov, prejemnike in višino prejetih sredstev ter zaključno poročilo ali povzetek o poteku in rezultatih porabljenih sredstev. Upoštevajoč navedene argumente ter na podlagi dokumentov, ki so se nahajali v upravni zadevi št. 090/172/2018, je Informacijski pooblaščenec organu naložil, da prosilcu omogoči delni dostop do zapisnika komisije festivala.

KLJUČNE BESEDE: osebni podatek, poslovna skrivnost, odločba številka 090-172/2018

Postopki obravnave tujcev na državni meji niso del notranjega delovanja policije

Prosilec (Amnesty International Slovenije) je od Policije (v nadalnjem besedilu organ) zahteval posredovanje navodil in usmeritev glede ravnanja policistov na terenu v okoliščinah povečanih migracijskih pritiskov. Organ se je pri zavrnitvi skliceval na izjemo notranjega delovanja in varstva osebnih podatkov. Navedel je, da dokumenti vsebujejo osebne podatke javnih uslužbencev, zaposlenih v policiji (ime, priimek, naziv in funkcijo), kot tudi udeležencev delovnega sestanka, pripravljavcev ali podpisnikov dokumentov policije in imena javnih uslužbencev, ki so bili dodeljeni v kadrovsko pomoč. Razkritje imen javnih uslužbencev kot podpisnikov dokumentov po mnenju organa po 1. alineji tretjega odstavka 6. člena ZDIJZ ni bilo sporno, drugače pa je bilo z razkritjem imen javnih uslužbencev, ki so bili dodeljeni v kadrovsko pomoč. Ti so seveda opravljali svoje delovne naloge, toda razkritje njihovih imen bi lahko povzročilo motnjo v delovanju organa, kar pa predstavlja izjemo po 11. točki prvega odstavka 6. člena ZDIJZ. Na podlagi imen bi bilo mogoče sklepati, kolikšna je kadrovska pomoč in kje je pričakovati manjše število policistov, kar bi lahko zmanjšalo učinkovitost in uspešnost operativnega dela policije. Poleg tega je šlo za dokumente za notranjo rabo organa z vsebino, ki je bila namenjena izključno enotam, prejemnicam sporočil. Dokumenti so vsebovali operativne informacije, pridobljene tudi iz analize tveganja pri čezmejni kriminaliteti in nedovoljenih

migracijah. Ugotovitve analiz tveganja so bile podlaga za načrtovanje in izvajanje ukrepov preprečevanja, odkrivanja in preiskovanja organizirane čezmejne kriminalitete ter nedovoljenih migracij. Ugotovitve analiz tveganja so bile osredotočene tudi na posebnosti nezakonitega priseljevanja državljanov določenih držav. Javna predstavitev teh ugotovitev bi lahko povzročila neželene učinke pri širši javnosti ter posredno vplivala na delovno-operativno okolje policije in drugih deležnikov, ki so bili vključeni v postopanje z nezakonitimi migrantmi. Po oceni organa načrtovani ukrepi (ki so izhajali iz analize tveganja) in s tem taktike delovanja organa pri opravljanju njegovih temeljnih nalog, ki so navedene v Zakonu o nalogah in pooblastilih policije, ne morejo biti razkriti. Pri tem gre tudi za varovanje skupnega varnostnega prostora EU. Če bi bila javnost seznanjena s sredstvi, podrobnnimi operativnimi in tehničnimi postopki policije pri preprečevanju nedovoljenih (nezakonitih) migracij, z načinom operativnega obveščanja in poročanja v določenem času oz. ob določenem dogodku, z izvajanjem poostrenega nadzora in konkretnimi aktivnostmi, kdaj, katere enote, na katerem območju, s kakšnimi sredstvi izvajajo poostren nadzor, kako se ta izvaja in kaj vse se spremlja, kje in koliko začasnih tehničnih ovir bi bilo treba še postaviti na zunanjih schengenskih meji, bi to bistveno zmanjšalo učinkovitost slovenske policije pri preprečevanju nezakonitih migracij ter na drugi strani izrazito povečalo verjetnost nezakonitih prehodov državne meje in schengenskega območja in olajšalo čezmejno kriminalitetu. Razkritje operativnih informacij in taktike delovanja bi lahko hitro vplivalo na poslabšanje varnostnih razmer. Ne nujno samo v Sloveniji, temveč tudi znotraj schengenskega območja oz. v skupnem varnostnem prostoru EU. Prosilec je odločitvi organa oporekal, ker je bila vsebina dokumentov prekomerno prekrita in tako ni bilo mogoče potrditi, da so bili vsi postopki pri nadzoru državne meje »zakoniti, enotni in usklajeni«. Informacijski pooblaščenec je pritožbi delno ugodil. Prosilec je že v zahtevi, kot kasneje tudi v pritožbi, navedel, da ni želel prejeti osebnih imen policistov in osebnih podatkov tretjih oseb, zato Informacijski pooblaščenec posledično teh podatkov v tem pritožbenem postopku sploh ni presojal. Skladno z utečeno prakso Informacijskega pooblaščenca dokumenti, iz katerih izhaja »zunanje« delovanje, ki je usmerjeno navzven in se nanaša na razmerje do zunanjih subjektov in do posameznikov, npr. do oseb, obravnavanih v policijskih postopkih, niso dokumenti, namenjeni le internemu delu organa. V pritožbenem postopku je Informacijski pooblaščenec ugotovil, da organ ni izkazal motenj, ki bi zaradi razkritja zahtevanih dokumentov nastale v njegovem delovanju. Za obstoj te izjeme bi bilo treba izkazati konkretne motnje, ki bi organu nastale z razkritjem zahtevanih informacij (tako tudi sodba št. I U 1176/2010-12 z dne 30. 11. 2011). Dokazno breme glede razlogov za nastanek motenj v delovanju organa je vedno na strani organa, dokazni standard »bi razkritje povzročilo motnje« pa je dokazni standard »onkraj dvoma«. Informacijski pooblaščenec je organu tako naložil razkritje tistih delov zahtevanih dokumentov, ki so vsebinsko predstavljeni le splošne ugotovitve oz. zaključke, brez konkretnih opisov posameznih postopkov in metod dela, ki bi se nanašali na policijsko delo. Poleg tega je bil za razkritje podan tudi prevladajoč javni interes. Informacijski pooblaščenec je bil mnenja, da se ima javnost pravico seznaniti z informacijami o tem, ali policija obmejne postopke izvaja zakonito, enotno, predvidljivo in v okviru zaupanih ji zakonskih pooblastil. Vsak posameznik, ki se

zajde v postopkih pred represivno-varnostnimi organi, med katere spada tudi policija, ima pravico biti seznanjen s tem, kako se ti postopki dejansko operativno izvajajo, kaj lahko v takšnem postopku pričakuje in kakšne pravice so mu v njem priznane oz. bi mu morale biti priznane. Postopki obravnave tujcev na državni meji (ne glede na status migrant/begunec/prebežnik) niso del »interne strategije« organa, ampak gre za vprašanje pravilnosti izvajanja zakonskih nalog, ki so določene z veljavnimi predpisi. Informacijski pooblaščenec se je strinjal s pritožbeno navedbo, da če organ navaja, da so vsi postopki nadzora državne meje zakoniti, enotni in usklajeni, mora imeti javnost pravico te navedbe preveriti. Delovanje organa v postopkih z osebami, ki jih je obravnaval na meji in ki so regulirani z veljavno slovensko in mednarodno zakonodajo, ne bi smelo biti tajno. V teh postopkih je šlo za obravnavo posameznikov, ki so bili kot subjekti po mednarodnem pravu, ki zavezuje Slovenijo, upravičeni do priznanja določenih pravic. Vprašanje, ali jim je policija v postopkih obravnave te pravice tudi priznavala, je v javnem interesu. Informacijski pooblaščenec je ob tem upošteval, da je bil prosilec v konkretnem primeru nevladna organizacija, ki je informacije zahtevala zaradi javne razprave in nadzora civilne družbe nad policijo. Da gre za pomembno okoliščino, ki lahko pretehta v smeri razlogov za razkritje zahtevanih informacij, izhaja tudi iz zadnje sodbe Upravnega sodišča RS št. IU 1688/2016-27 z dne 17. 10. 2018. Posledično je Informacijski pooblaščenec pritožbi prosilca delno ugodil in organu naložil posredovanje dokumentov v obliki delnega dostopa.

KLJUČNE BESEDE: notranje delovanje organa, test interesa javnosti, odločba številka 090-223/2018

Podatek o začasni odstranitvi sodnika iz sodniške službe je prosto dostopna informacija javnega značaja

Prosilec (novinar) je od Vrhovnega sodišča RS (v nadalnjem besedilu organ) želel prejeti odločbo v zvezi z začasno odstranitvijo sodnika iz sodniške službe. Organ je zahtevo zavrnil zaradi varstva osebnih podatkov po 3. točki prvega odstavka 6. člena ZDIJZ in obstoja izjeme varstva sodnega postopka po 8. točki prvega odstavka 6. člena ZDIJZ. V postopku na prvi stopnji je ugotovil, da se ta izjema nanaša tudi na disciplinski postopek, ki se zoper sodnike vodi pred disciplinskim sodiščem pri Sodnem svetu. Informacijski pooblaščenec se s trditvami organa ni strinjal, saj je predmetni disciplinski postopek poseben postopek, katerega pravila so določena v Zakonu o sodnem svetu (ZSSve), ne gre torej za pravdni, nepravdni ali drug sodni postopek. Temeljno načelo (katerega kolikor disciplinskega postopka je, da disciplinski organ ravna po procesnem redu, ki ga urejajo sprejeta pravila. Če se v teh pravilih sklicuje na smiselnouporabo pravil kazenskega, pravdnega ali drugega sodnega postopka, to še ne pomeni, da gre tudi dejansko za tovrstni postopek. V konkretnem primeru pogoji za obstoj izjeme iz 8. točke prvega odstavka 6. člena ZDIJZ niso bili izpolnjeni. Je pa Informacijski pooblaščenec v zvezi z zahtevanim dokumentom ugotovil, da vsebuje osebne podatke posameznikov (sodnikov). Ker razkritje osebnega podatka predstavlja vrsto obdelave osebnih

podatkov po členu 4 drugega pododstavka Splošne uredbe, je za presojo dopustnosti razkritja treba upoštevati splošne podlage za obdelavo osebnih podatkov, opredeljene v členu 6 Splošne uredbe. Iz tega člena kot splošno pravilo izhaja, da je obdelava osebnih podatkov (torej tudi razkritje podatkov javnosti) zakonita (dopustna) med drugim takrat, če je obdelava potrebna za izpolnitve zakonske obveznosti, ki velja za upravljavca (točka c), ali pri izvajanju javne oblasti, dodeljene upravljavcu (točka e). Zakonsko podlago za obdelavo osebnih podatkov, upoštevajoč točko c prvega odstavka člena 6 Splošne uredbe, lahko predstavlja tudi ZDIJZ. Razkritje osebnih podatkov v postopku dostopa do informacij javnega značaja je dopustno v primeru, ko gre za osebne podatke, ki hkrati pomenijo na primer tudi podatke o porabi javnih sredstev ali podatke, povezane z opravljanjem javne funkcije ali delovnega razmerja javnega uslužbenca (1. alineja tretjega odstavka 6. člena ZDIJZ), ali ko organ odloči, da je treba podatke razkriti zaradi prevladujočega javnega interesa (drugi odstavek 6. člena ZDIJZ). Informacijski pooblaščenec je tako ugotovil, da imena in priimki funkcionarjev (sodnikov oz. sodnice), ki so izvajali svoje naloge in so v zahtevanem dokumentu navedeni v kontekstu opravljanja svoje funkcije, niso varovani osebni podatki. Ti osebni podatki so na podlagi tretjega odstavka 6. člena ZDIJZ prosto dostopni. Enako velja za ime in priimek sodnika, ki mu je bil izrečena začasna odstranitev iz sodniške službe. Informacija je v neposredni zvezi z opravljanjem njegove funkcije in kot taka prosto dostopna. ZDIJZ vsebuje izjeme, ki pomenijo pomemben poseg v posameznikovo informacijsko zasebnost, zato mora funkcionar (oz. javni uslužbenec) dopustiti tiste meje posega v njegovo informacijsko zasebnost, ki jih je zakonodajalec določil z namenom preglednosti porabe javnih sredstev ali v zvezi z izvajanjem javne funkcije (oz. delovnim razmerjem). V neposredni zvezi z opravljanjem javne funkcije so tudi navedbe pravnih podlag očitanih disciplinskih kršitev. Točka c prvega odstavka člena 5 Splošne uredbe določa, da morajo biti osebni podatki ustrezni, relevantni in omejeni na to, kar je potrebno za namene, za katere se obdelujejo (»najmanjši obseg podatkov«). Namen ZDIJZ je zagotoviti javnost in odprtost delovanja organov, kar pomeni, da razkrivanje opisov dejanskega stanja domnevnih kršitev oz. način izvršitve očitanih kršitev ni mogoče razkrivati na podlagi 1. alineje tretjega odstavka 6. člena ZDIJZ, saj gre za navedbe, ki niso neposredno povezane z opravljanjem javne funkcije (oz. delovnega razmerja). Po oceni Informacijskega pooblaščenca bi dostop do informacij, ki vsebujejo z vidika zasebnosti relevantno sporočilo o določljivem posamezniku, pomenil prekomeren poseg v zasebnost te osebe, kar bi bilo tudi v nasprotju z načelom sorazmernosti. Informacijski pooblaščenec je v obravnavanem primeru še ugotovil, da poznavanje informacij iz določenega dokumenta ni razlog za zavrnitev dostopa do samega dokumenta, ki vsebuje te informacije, zato bi organ pri dostopu do zahtevanega dokumenta moral upoštevati tudi institut delnega dostopa. Glede informacij, za katere je Informacijski pooblaščenec ocenil, da so varovane, ni zaznal javnega interesa.

KLJUČNE BESEDE: osebni podatek, ostali sodni postopki, številka odločbe 090-234/2018

2.7 AKTIVNOSTI IZOBRAŽEVANJA IN OZAVEŠČANJA

Načelo transparentnosti je eden temeljnih postulatov vsake demokratične družbe, zato mora (p)ostati eno vodilnih načel delovanja organov javnega sektorja. Odprtost in preglednost delovanja javnih organov je bistvenega pomena za njihovo boljše delovanje, kar na drugi strani prinaša koristi vsem članom družbe. Zato Informacijski pooblaščenec pozornost namenja tudi aktivnostim ozaveščanja strokovne in splošne javnosti, s katerimi spodbuja dobro prakso na področju dostopa do informacij javnega značaja.

2.7.1 DAN PRAVICE VEDETI V ZNAMENJU 15. OBLETNICE ZAKONA O DOSTOPU DO INFORMACIJ JAVNEGA ZNAČAJA

Leta 2002 je bil 28. september izbran za svetovni dan pravice vedeti, ko so se različne organizacije civilne družbe iz številnih držav povezale v organizacijo Freedom of Information Advocates Network (FOIANet). Dogodek obeležujemo tudi v Sloveniji. Informacijski pooblaščenec je svetovni dan pravice vedeti leta 2018 posvetil praznovanju 15. obletnice uveljavljanje Zakona o dostopu do informacij javnega značaja. Ob tej priložnosti je pod pokroviteljstvom predsednika Republike Slovenije, gospoda Boruta Pahorja, organiziral strokovni posvet z naslovom »Iz teorije v prakso pri iskanju informacij javnega značaja – 15 let Zakona o dostopu do informacij javnega značaja«. Udeležencem posveta sta bila predstavljena razvoj pravice dostopa do informacij javnega značaja ter praksa Informacijskega pooblaščenca.

Pooblaščenec je pomemben mejnik obeležil tudi z izdajo publikacije [Vodnik po praksi Informacijskega pooblaščenca](#), v kateri so nanizani številni odmevni in zanimivi primeri. Vodnik je nastal z željo po predstavitvi 15-letnega delovanja organa ter z namenom, da bo uporaben priomoček zavezancem – z njegovo pomočjo se bodo ti laže soočali z izviri, ki jih prinaša delo na področju zagotavljanja informacij javnega značaja.

POMEMBNO

Vodnik po praksi Informacijskega pooblaščenca podaja strnjen pregled najodmevnnejših primerov in je prosto dostopen na spletni strani Informacijskega pooblaščenca.

Naslovica publikacije *Vodnik po praksi Informacijskega pooblaščenca*



2.7.2 NAGRADA AMBASADOR TRANSPARENTNOSTI 2018

Pomembno je, da opozorimo na delo tistih, ki delajo dobro, in jih nagradimo, zato Informacijski pooblaščenec ob svetovnem dnevu pravice vedeti vsako leto podeli nagrado **Ambasador transparentnosti**. Leta 2018 je nagrado prejela ekipa novinarjev oddaje Tarča RTV Slovenija, ki že od leta 2003 skrbi za pronicljive prispevke, s čimer prispeva k boljšemu pretoku informacij v našem okolju ter k promociji pravice dostopa do informacij javnega značaja. Ekipa Tarče je skozi leta mnogo zgodb odkrila, razkrila in osvetlila prav s pomočjo Zakona o dostopu do informacij javnega značaja, s čimer je pokazala, da je zavezana načelu transparentnosti.

Prejemniki nagrade Ambasador transparentnosti 2018



2.7.3 MEDNARODNO SODELOVANJE

Na povabilo hrvaškega Informacijskega pooblaščenca se je 11. in 12. maja 2018 Informacijski pooblaščenec udeležil mednarodne konference z naslovom »15 let dostopa do informacij javnega značaja v Republiki Hrvaški«. Na konferenci so s prispevki sodelovali predavatelji iz Hrvaške, Združenih držav Amerike, Velike Britanije, Španije, Črne gore, Makedonije, Albanije in Slovenije. Informacijski pooblaščenec je predstavil referat na temo prakse dostopa do informacij javnega značaja v Republiki Sloveniji s poudarkom na zlorabi pravice in sodni praksi na to temo.

Informacijski pooblaščenec se je 26. in 27. novembra 2018 udeležil tudi delavnice »Freedom of Information, Case Handling Workshop« v Budimpešti na Madžarskem. To je bila prva mednarodna delavnica na temo reševanja konkretnih primerov iz prakse organov, pristojnih za nadzor nad dostopom do informacij javnega značaja. Delavnice so se udeležili predstavniki iz različnih evropskih držav (Madžarska, Albanija, Hrvaška, Nemčija, Kosovo, Maroko, Slovenija, Srbija, Velika Britanija), Gibraltarja in Južne Afrike.

Predstavljene so bile različne nacionalne ureditve postopkov dostopa do informacij javnega značaja, posebna pozornost je bila posvečena konkretnim primerom iz prakse: udeleženci so se osredotočili na dileme, težave in ovire, s katerimi se srečujejo uradne osebe pri vodenju in odločanju v pritožbenih postopkih dostopa do informacij javnega značaja.

Vsaka sekcija je bila sestavljena iz prispevkov posameznih udeležencev. Informacijski pooblaščenec je svojim predavanjem sodeloval v 1. in 4. sekciiji.

2.8 SPLOŠNA OCENA IN PRIPOROČILA

Informacijski pooblaščenec je leta 2018 praznoval 15. obletnico uveljavitve Zakona o dostopu do informacij javnega značaja. Leta 2003, ko se je zakon pričel uporabljati, se verjetno nihče ni zavedal, kakšne spremembe v delovanju organov javnega sektorja bo povzročil. Iz sistema, v katerem je bilo javnosti dostopnih relativno malo informacij, smo vstopili v sistem popolne odprtosti, kjer le zakon določa izjeme od proste dostopnosti in kjer je postalo načelo transparentnosti eno vodilnih načel delovanja javnega sektorja.

Kot že nekaj preteklih let je Informacijski pooblaščenec tudi leta 2018 zaznal nekaj pozitivnih kazalnikov, ki na eni strani kažejo večjo seznanjenost prosilcev s pravico dostopa do informacij in na drugi strani boljše odzivanje zavezancev na njihove zahteve. Trend rasti števila pritožbenih zadev, ki ga je zaznati že zadnjih nekaj let, se je nadaljeval tudi leta 2018, kar kaže na to, da so prosilci s postopkom uresničevanja pravice do pravnega varstva dobro seznanjeni in se zanj pogosto odločajo. Pritožbeni postopek je za prosilce v celoti brezplačen in relativno hiter, zato Informacijski pooblaščenec ocenjuje, da je na ta način zagotovljeno učinkovito pravno varstvo pravice dostopa do informacij javnega značaja. Ob tem je Informacijski pooblaščenec leta 2018 še zmanjšal povprečen čas reševanja pritožbenih zadev – ta je znašal 32 dni (za primerjavo: leta 2017 je bil povprečen čas reševanja pritožbenih zadev 37 dni, leta 2016 pa 47 dni). Pripomniti velja, da je zakonski rok, ki ga za reševanje tovrstnih zadev določa Zakon o splošnem upravnem postopku (ZUP), dva meseca.



Tudi leta 2018 je Informacijski pooblaščenec prejel številna zaprosila za mnenja in stališča, ki jih nudi v okviru neformalnega svetovanja, na podlagi primerov iz prakse, ki jih je že obravnaval. To kaže, da so bili zavezanci v tem letu aktivni in odzivni ter da so se z vprašanji pogosto obrnili na Informacijskega pooblaščenca izven pritožbenega postopka, torej tudi takrat, ko jih zakon tega ne nalaga. Da so tako zavezanci kot prosilci pripravljeni sodelovati z Informacijskim pooblaščencem in da upoštevajo njegova priporočila, izhaja tudi iz relativno majhnega deleža upravnih sporov, sproženih zoper odločbe Informacijskega pooblaščenca – leta 2018 je bilo teh le zoper 11,8 % izdanih odločb. Informacijski pooblaščenec primere iz svoje prakse redno objavlja na svoji spletni strani, trudi se, da so ti dostopni pregledno in ažurno, da bi tako olajšal delo zavezancem in čim učinkoviteje seznanjal javnost s pomenom te temeljne človekove pravice.

Klub temu da Informacijski pooblaščenec sodelovanje z zavezanci ocenjuje kot zgledno (leta 2018 zoper njih ni uvedel nobenega postopka zaradi prekrškov po ZDIJZ, ZInfP ali ZMed), pa ugotavlja, da je leta 2018 znova naraslo število pritožb zaradi t. i. molka organa in da je bilo, po letu 2017, ko je ta trend padel, to leto vnovič vloženih več pritožb zoper občine. Glede na konkretnе primere, ki jih je obravnaval, Informacijski pooblaščenec večjega števila pritožb ne more v celoti pripisati neodzivnosti organov, delno je to namreč posledica povečanja števila vloženih zahtev pri organih prve stopnje, delno pa za primere t. i. nejasnih zahtev, ki se lahko obravnavajo na različnih pravnih podlagah. V praksi je Informacijski pooblaščenec namreč zaznal primere, ko isti prosilec od enega organa (npr. občine) večkrat zahteva dostop do dokumentov na različnih pravnih podlagah (npr. ne samo po ZDIJZ, ampak tudi kot npr. občinski svetnik, prijavitelj ali stranka postopka). Ker je v takšnih primerih lahko sporno, po kateri pravni podlagi je organ dolžan voditi postopek, lahko to vodi tudi v (neutemeljene) pritožbene postopke.

Leta 2018 je Informacijski pooblaščenec obravnaval 21 pritožb zoper odločitve poslovnih subjektov pod prevladujočim vplivom, kar je sicer več kot leto poprej, še vedno pa gre za relativno majhen delež (3,8 %) vseh pritožbenih zadev (549), ki jih je obravnaval Informacijski pooblaščenec.

V zvezi s ponovno uporabo je Informacijski pooblaščenec leta 2018 vodil en pritožbeni postopek. 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 se pritožbenega postopka ne poslužujejo 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 OPSI Ministrstva za javno upravo. Potencialni ponovni uporabniki tako 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 pooblaščencem.

POMEMBNO

Na podlagi konkretnih pritožbenih primerov Informacijski pooblaščenec podaja naslednje ugotovitve in priporočila za nadaljnje delo zavezancev:

I. Zavezanci naj pri obravnavi zahtev več pozornosti namenijo postopkovnim vprašanjem, še posebej pripravi obrazložitev zavrnih odločb. V primerih, ko zahtevo prosilca zaradi obstoja zakonskih izjem zavrnejo, je namreč ključno, da popolnoma ugotovijo dejansko stanje in se konkretno opredelijo do vsebine zahtevanih dokumentov. Iz obrazložitve mora biti razvidno, o katerih dokumentih so odločali ter v katerem delu je bila zahteva prosilca zavrnjena. Razlogi, zakaj je bil dostop do zahtevanih dokumentov zavrnjen, morajo biti pojasnjeni tako, da je prosilcem razumljivo in skladno z izrekom odločbe. Leta 2018 je Informacijski pooblaščenec namreč zaznal povečanje števila pritožbenih zadev, pri katerih so bile zaradi pomanjkljive obrazložitve podane kršitve pravil postopka, kar je vplivalo tudi na pravico prosilcev do učinkovitega pravnega sredstva.

II. Z vidika izjem, na katere so se sklicevali zavezanci v postopkih, velja opozoriti na povečanje števila pritožbenih zadev, v katerih je šlo za t. i. izjemo notranjega delovanja. Po ugotovitvah Informacijskega pooblaščenca zavezanci to izjemo razlagajo preširoko in ne da bi konkretno izkazali škodo, ki bi nastala z razkritjem zahtevanih dokumentov. Ker se navedena izjema nanaša zlasti na različna interna navodila, zapisnike in načrte dela, Informacijski pooblaščenec opozarja, da vsak dokument, ki je interne narave, ne ustrezza tej izjemi. Iz načela prostega dostopa, ki je določeno v 5. členu ZDIJZ, namreč izhaja, da lahko organ zahtevo za dostop do informacije zavrne le v primeru, če izkaže, da je zatrjevana izjema dejansko podana. Povedano drugače: dokazno breme je pri organu, v nasprotnem primeru je treba šteti, da gre za prosto dostopno informacijo.

III. Ker je Informacijski pooblaščenec leta 2018 obravnaval tudi nekaj primerov, ko so zavezanci zavrnili dostop do podatkov v zvezi z delovnimi razmerji javnih uslužbencev z obrazložitvijo, da gre za varovane osebne podatke, velja poudariti, da se pravna podlaga za posredovanje teh podatkov javnosti tudi po uveljavitvi Splošne uredbe ni spremenila. Določba tretjega odstavka 6. člena ZDIJZ te podatke namreč določa kot absolutno javne. Takšna je tudi dolgoletna praksa Informacijskega pooblaščenca in praksa Upravnega sodišča.

IV. Ker je Informacijski pooblaščenec v praksi zaznal primere, ko zavezanci zaradi obstoja zakonske izjeme dostop do zahtevane informacije zavrnejo v celoti, ne da bi upoštevali pravilo delnega dostopa iz 7. člena ZDIJZ, velja opozoriti, da če dokument ali njegov del le delno vsebuje varovane informacije in jih je mogoče iz dokumenta izločiti, ne da bi to ogrozilo njihovo zaupnost, mora organ slediti pravilu delnega dostopa in prosilca seznaniti z vsebino preostalega, nevarovanega dela dokumenta.

V. V zvezi z ugotovitvijo iz prejšnje točke je v praksi zaznati povečanje števila primerov glede dostopa do dokumentov iz inšpekcijskih postopkov, zato Informacijski pooblaščenec pripominja, da se pravilo delnega dostopa nanaša tudi na inšpekcijske prijave in druge dokumente iz teh postopkov, ki niso varovani absolutno in v celoti, ampak le v delih, v katerih gre za varovane podatke, ki predstavljajo zakonske izjeme (npr. varujejo se osebni podatki, podatki o prijavitelju ..., ne pa celotna, tudi npr. anonimna prijava).



VARSTVO OSEBNIH PODATKOV – VARSTVO TEMELJNE ČLOVEKOVE PRAVICE

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 doposten, če je v zakonu določno opredeljeno, kateri osebni podatki se smejo obdelovati, namen njihove obdelave, zagotovljeno pa mora biti tudi ustrezeno varstvo in zavarovanje osebnih podatkov. Namen obdelave osebnih podatkov mora biti ustavno doposten, 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. Ključni sistemski zakon glede varstva osebnih podatkov je bil do 25. 5. 2018 Zakon o varstvu osebnih podatkov.

POMEMBNO

Leto 2018 je prineslo reformo varstva osebnih podatkov v EU.

V času od sprejema Direktive o varstvu osebnih podatkov 95/46/ES leta 1995 je z razvojem sodobnih informacijsko-komunikacijskih tehnologij prišlo do obsežnih sprememb v obsegu, intenzivnosti in prenosih osebnih podatkov (npr. z razvojem in širitevijo uporabe računalništva v oblaku, družbenih omrežij, pametnih telefonov), ki so terjale prilagoditve in posodobitve zakonodajnega okvira. Enotna in posodobljena zakonodaja o varstvu podatkov je bistvena za zagotovitev temeljne pravice posameznikov do varstva osebnih podatkov, razvoj digitalnega gospodarstva ter okrepitev boja proti mednarodnemu kriminalu in terorizmu. 4. 5. 2016 sta bila v Uradnem listu Evropske unije objavljena ključna gradnica novega zakonodajnega svežnja EU o varstvu osebnih podatkov, in sicer:

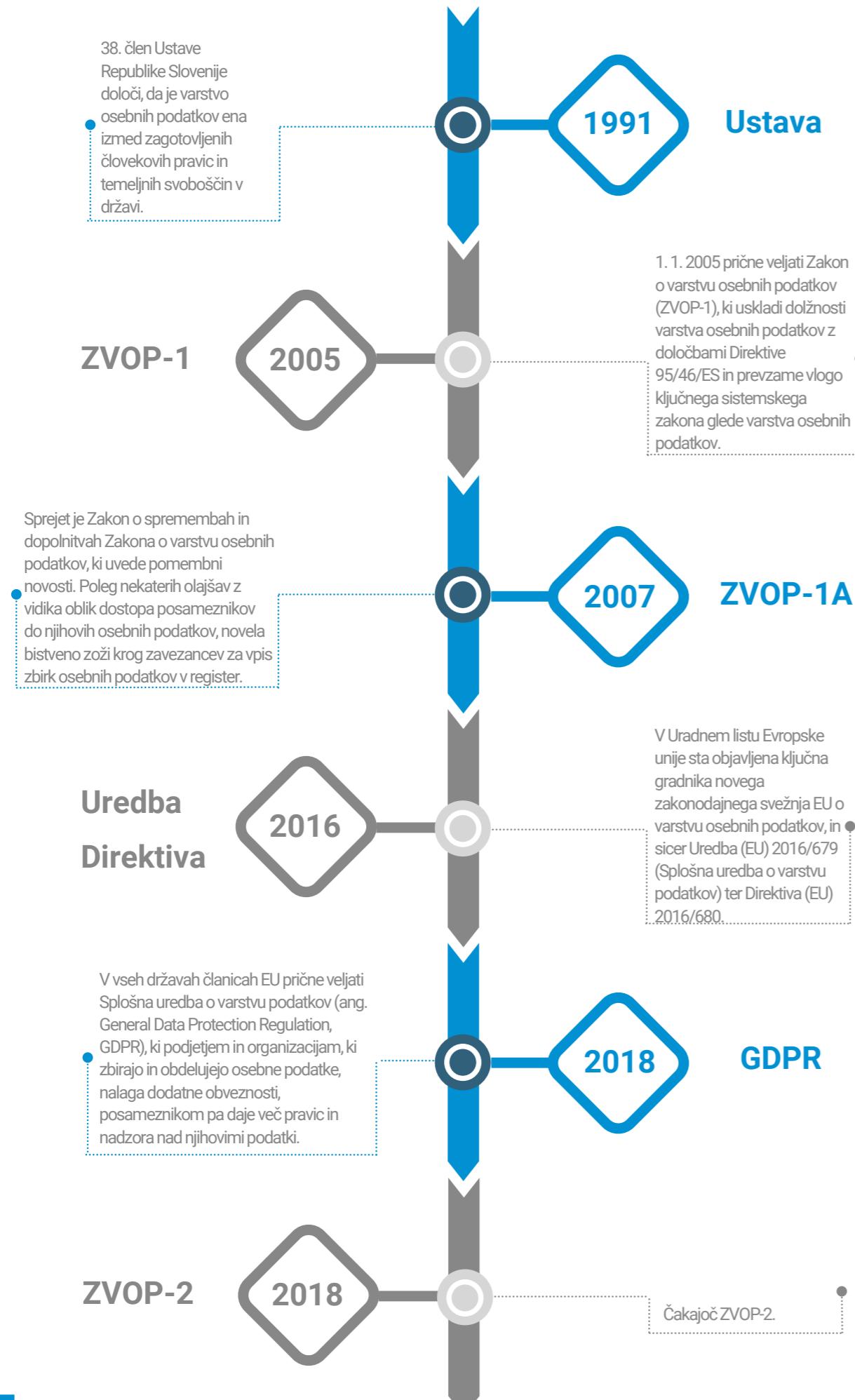
- [Uredba \(EU\) 2016/679 Evropskega parlamenta in Sveta z dne 27. 4. 2016 o varstvu posameznikov pri obdelavi osebnih podatkov in o prostem pretoku takih podatkov ter o razveljavitvi Direktive 95/46/ES \(Splošna uredba o varstvu podatkov\)](#),
- [Direktiva \(EU\) 2016/680 Evropskega parlamenta in Sveta z dne 27. 4. 2016 o varstvu posameznikov pri obdelavi osebnih podatkov, ki jih pristojni organi obdelujejo za namene preprečevanja, preiskovanja, odkrivanja ali pregona kaznivih dejanj ali izvrševanja kazenskih sankcij, in o prostem pretoku takih podatkov ter o razveljavitvi Okvirnega sklepa Sveta 2008/977/PNZ \(Direktiva LED\)](#).

Splošna uredba o varstvu podatkov (angl. General Data Protection Regulation – GDPR, Splošna uredba) je začela veljati 25. 5. 2016, uporabljati pa se je začela 25. 5. 2018. Rok za prenos določb Direktive (EU) 2016/680 v nacionalno zakonodajo je bil dve leti.

Splošna uredba prinaša nove in okrepljene pravice posameznika, poleg obstoječe pravice do dostopa do osebnih podatkov ter pravice do popravka ureja še pravico do pozabe, izbrisu, omejitve obdelave, ugovora in prenosljivosti podatkov. Precej večji poudarek je na transparentnosti obdelave – tj. glede zagotavljanja preglednih in lahko dostopnih informacij posameznikom o obdelavi njihovih podatkov. Splošna uredba določa tudi nove obveznosti upravljalcev in obdelovalcev podatkov, kot so obveznost izvajanja ustreznih varnostnih ukrepov in obveznost uradnega obveščanja o kršitvah varstva osebnih podatkov, imenovanje pooblaščenih oseb za varstvo podatkov, izvajanje ocen učinka. Upravljavci niso več dolžni prijavljati zbirk osebnih podatkov v register zbirk osebnih podatkov, ostajajo pa dolžnosti sprejema popisa zbirk (t. i. evidence dejavnosti obdelave); te dolžnosti se krepijo in uvajajo tudi za (pogodbene) obdelovalce. Splošna uredba bistveno bolj poudarja načelo odgovornosti in preventivne ukrepe, poleg omenjenih mehanizmov zagotavljanja skladnosti uvaja tudi možnost potrjevanja sektorskih kodeksov ravnanja in certifikacije.

V Splošni uredbi je potrjena obstoječa obveznost držav članic glede ustanovitve neodvisnega nadzornega organa na nacionalni ravni. Njegov cilj je tudi vzpostavitev mehanizmov, s katerimi bi zagotovili doslednost pri izvajanju zakonodaje o varstvu podatkov v vsej EU. Bistveno je, da bo v primeru, ko bo obdelava osebnih podatkov potekala v več kot eni državi članici, za nadzor nad temi dejavnostmi po načelu sodelovanja »vse na enem mestu« odgovoren vodilni nadzorni organ, tj. organ tiste države članice, v kateri je glavni ali edini sedež upravljalca ali obdelovalca. Ostali nadzorni organi bodo v postopkih nadzora sodelovali kot zadevni organi.

Splošna uredba zajema tudi ustanovitev Evropskega odbora za varstvo podatkov (angl. European Data Protection Board, EDPB). V odboru sodelujejo predstavniki vseh 28 neodvisnih nadzornih organov EU in EGS (Islandija, Norveška in Lichtenštajn), Evropske komisije in Evropskega nadzornika za varstvo podatkov; odbor nadomešča Delovno skupino za varstvo podatkov iz člena 29 (Article 29 Working Party).



3.2 INŠPEKCIJSKI NADZOR V LETU 2018

Postopek inšpekcijskega nadzora, ki ga izvaja Informacijski pooblaščenec oz. državni nadzorniki za varstvo osebnih podatkov, poleg ZVOP-1, Zakona o informacijskem pooblaščencu (ZInfP) in Splošne uredbe urejata še Zakon o inšpekcijskem nadzoru (ZIN) in Zakon o splošnem upravnem postopku (ZUP). Informacijski pooblaščenec v inšpekcijskih postopkih nadzira izvajanje določb Splošne uredbe, ZVOP-1 in vseh tistih predpisov, ki urejajo področje varstva osebnih podatkov.

V okviru inšpekcijskega nadzora Informacijski pooblaščenec nadzira zlasti:

- zakonitost in preglednost obdelave osebnih podatkov;
- ustreznost ukrepov varnosti osebnih podatkov ter izvajanje postopkov in ukrepov za zagotovitev varnosti osebnih podatkov;
- izvajanje določb Splošne uredbe, ki urejajo posebne izraze načela odgovornosti (uradno obveščanje nadzornih organov in posameznikov o kršitvi varnosti, ocene učinka, pooblaščene osebe za varstvo osebnih podatkov, evidence dejavnosti obdelav);
- izvajanje določb Splošne uredbe glede prenosa osebnih podatkov v tretje države ali mednarodne organizacije in o njihovem posredovanju tujim uporabnikom osebnih podatkov;
- izvajanje določb Splošne uredbe glede obdelave na podlagi pogodbe o obdelavi osebnih podatkov.

Splošna uredba daje Informacijskemu pooblaščencu v členu 58 naslednja inšpekcijska pooblastila:

1. Preiskovalna pooblastila:

- da upravljavcu in obdelovalcu ter, če je ustrezno, predstavniku upravljavca ali obdelovalca odredi, naj zagotovi vse informacije, ki jih potrebuje za opravljanje svojih nalog;
- da izvaja preiskave v obliki pregledov na področju varstva podatkov;
- da izvaja pregledne potrdil skladnosti obdelav (certifikatov);
- da upravljavca ali obdelovalca uradno obvesti o domnevni kršitvi uredbe;
- da od upravljavca ali obdelovalca pridobi dostop do vseh osebnih podatkov in informacij, ki jih potrebuje za opravljanje svojih nalog;
- da pridobi dostop do vseh prostorov upravljavca ali obdelovalca, vključno z vso opremo in sredstvi za obdelavo podatkov, v skladu s pravom Evropske unije ali postopkovnim pravom države članice.

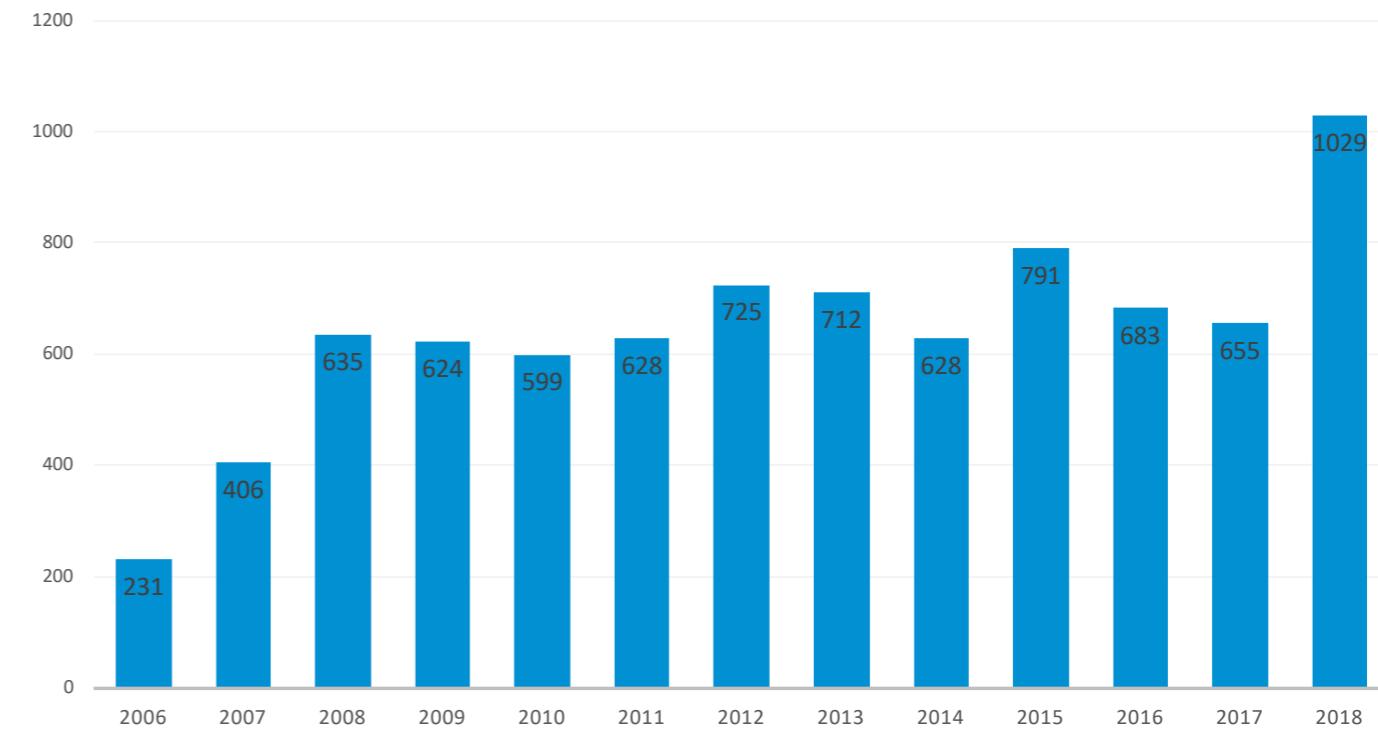
2. Popravljalna pooblastila:

- da izda upravljavcu ali obdelovalcu opozorilo, da bi predvidena dejanja obdelave verjetno kršila določbe uredbe;
- da upravljavcu ali obdelovalcu izreče opomin, kadar so bile z dejanji obdelave kršene določbe uredbe;
- da upravljavcu ali obdelovalcu odredi, naj ugodi zahtevam posameznika, na katerega se nanašajo osebni podatki, glede uresničevanja njegovih pravic na podlagi uredbe;
- da upravljavcu ali obdelovalcu odredi, naj dejanja obdelave, če je to ustrezno, na določen način in v določenem roku uskladi z določbami uredbe;
- da upravljavcu odredi, naj posameznika, na katerega se nanašajo osebni podatki, obvesti o kršitvi varstva osebnih podatkov;
- da uvede začasno ali dokončno omejitev obdelave, vključno s prepovedjo obdelave;
- da v zvezi s pravico posameznika odredi popravek ali izbris osebnih podatkov oz. omejitev obdelave in o takšnih ukrepih uradno obvesti uporabnike, ki so jim bili osebni podatki razkriti;
- da prekliče potrdilo ali organu za potrjevanje odredi preklic potrdila, izdanega v skladu s členoma 42 in 43, ali da organu za potrjevanje odredi, naj ne izda potrdila, kadar zahteve v zvezi s potrdilom niso ali niso več izpolnjene;
- da glede na okoliščine posameznega primera poleg ali namesto ukrepov iz tega odstavka naloži upravno globo v skladu s členom 83;
- da odredi prekinitev prenosov podatkov uporabniku v tretji državi ali mednarodni organizaciji.

POMEMBNO

Informacijski pooblaščenec je leta 2018 zaradi suma kršitev določb ZVOP-1 in Splošne uredbe vodil 1.029 inšpekcijskih zadev, od tega 330 v javnem in 699 v zasebnem sektorju. V primerjavi z letom 2017 to predstavlja kar 57-odstotni porast inšpekcijskih postopkov. Zoper pravne osebe javnega sektorja je na podlagi prijav uvedel 279 inšpekcijskih zadev, 51 postopkov je uvedel po uradni dolžnosti, zoper zavezance v zasebnem sektorju je na podlagi prijav odprl 660 inšpekcijskih zadev, 39 postopkov pa je začel po uradni dolžnosti.

Število inšpekcijskih zadev med letoma 2006 in 2018



Posameznemu državnemu nadzorniku za varstvo osebnih podatkov je bilo leta 2017 dodeljenih v povprečju 61, leta 2018 pa 92 inšpekcijskih zadev, kar predstavlja 51-odstotno povečanje obsega dodeljenih zadev.

Število dodeljenih inšpekcijskih zadev na posameznega nadzornika leta 2018 v primerjavi z letom 2017



Dodeljenih inšpekcijskih zadev
na nadzornika v 2018:

92

Prijave, ki jih je prejel Informacijski pooblaščenec, so se nanašale na naslednje sume kršitev določb Splošne uredbe in ZVOP-1:

Prijave glede na sume kršitve določb Uredbe in ZVOP-1

Sum kršitve	Število prijav
nezakonito razkrivanje osebnih podatkov: posredovanje osebnih podatkov nepooblaščenim uporabnikom in nezakonita objava osebnih podatkov	269
nezakonita obdelava osebnih podatkov pri izvajanju neposrednega trženja	171
nezakonito zbiranje oz. zahtevanje osebnih podatkov	138
nezakonito izvajanje videonadzora	97
neustrezno zavarovanje osebnih podatkov	69
nezakonit vpogled v osebne podatke	58
obdelava osebnih podatkov v nasprotju z namenom zbiranja	49
razno (zavrnitev posredovanja ali izbrisala osebnih podatkov; obdelava osebnih podatkov po preteku roka hrambe; uporaba netočnih podatkov; kršitev pravice do seznanitve; sumi kršitev, ki ne sodijo v pristojnost Informacijskega pooblaščenca)	88

3.2.1 INŠPEKCIJSKI NADZOR V JAVNEM SEKTORJU

Informacijski pooblaščenec je zaradi suma kršitev določb Splošne uredbe in ZVOP-1 zoper pravne osebe javnega sektorja na podlagi prijav odprl 279 inšpeksijskih zadev. V 96 primerih je Informacijski pooblaščenec prijaviteljem pisno pojasnil, zakaj v prijavi opisano ravnanje ne pomeni kršitev zakonodaje s področja varstva osebnih podatkov oz. zakaj uvedba postopka inšpeksijskega nadzora ni možna ali smiselna. Na podlagi devetih prijav je Informacijski pooblaščenec takoj izrekel ukrep v skladu z zakonom, ki ureja prekrške, ker je po preučitvi prijav zaključil, da uvedba inšpeksijskih postopkov ne bi bila smiselna, saj je šlo za enkratna dejanja v preteklosti, ki jih z inšpeksijskimi ukrepi za nazaj ni več možno preprečiti ali odpraviti, in ker je bilo prijavi priloženih dovolj dokazov o storitvi prekrška. V petih primerih je Informacijski pooblaščenec prijavitelje napotil na pravico do seznanitve z lastnimi osebnimi podatki, tri prijave je odstopil v reševanje pristojnim organom, v enem primeru pa ni uvedel postopka, ker prijavitelj ni posredoval svojih podatkov, zaradi česar ga ni mogel pozvati k posredovanju dodatnih podatkov, ki bi bili potrebni za uvedbo inšpeksijskega postopka.

Po preučitvi prejetih prijav je bilo zaradi utemeljenega suma kršitev določb Splošne uredbe in ZVOP-1 začetih 165 inšpeksijskih postopkov, 51 jih je bilo začetih po uradni dolžnosti, skupaj torej 216. V javnem sektorju je bilo opravljenih 22 inšpeksijskih pregledov, za odpravo ugotovljenih nepravilnosti je Informacijski pooblaščenec 17 zavezancem javnega sektorja izrekel ukrepe v obliki opozorila na zapisnik (10), predodločbe (6)¹ in ureditvene odločbe (1). Zavezanci so naložene ukrepe izvršili.

Leta 2018 so bili v javnem sektorju zaključeni 104 inšpeksijski postopki. Informacijski pooblaščenec v 49 postopkih ni zaznal kršitev določb Splošne uredbe ali ZVOP-1, 28 postopkov je ustavil, ker so zavezanci ugotovljene nepravilnosti odpravili, 27 postopkov pa je ustavil zato, ker je šlo za kršitve, ki so predstavljale enkratna dejanja v preteklosti, ki jih z inšpeksijskimi ukrepi za nazaj ni bilo več mogoče odpraviti. Zoper en sklep o ustavitvi postopka je zavezanci vložil tožbo na Upravno sodišče RS.

Informacijski pooblaščenec je prejel eno sodbo Upravnega sodišča RS v zvezi s tožbo, vloženo leta 2017 zoper sklep o ustavitvi inšpeksijskega postopka. Sodišče je tožbo zavrnilo.

3.2.2 INŠPEKCIJSKI NADZOR V ZASEBNEM SEKTORJU

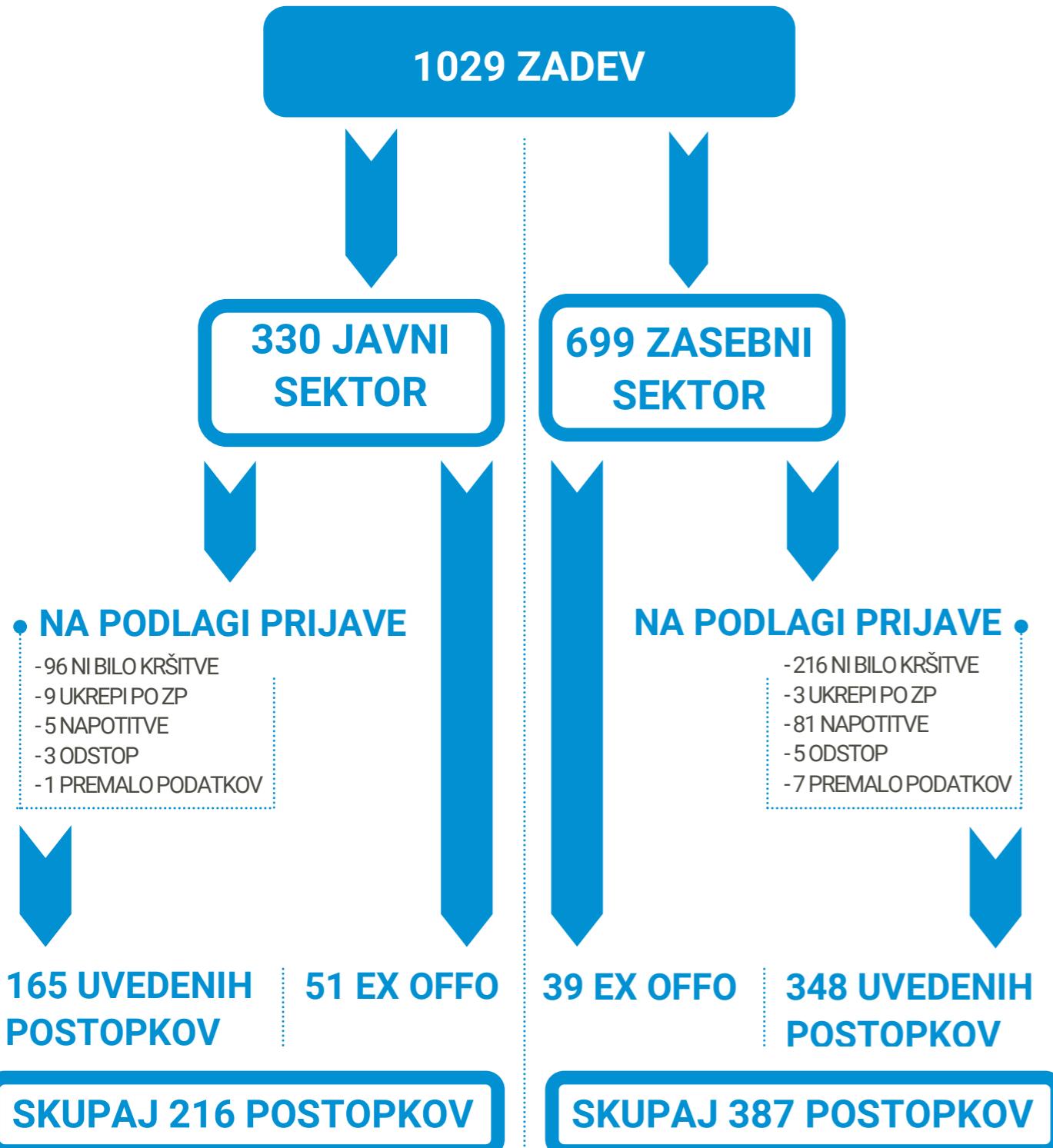
Informacijski pooblaščenec je zoper zavezance v zasebnem sektorju na podlagi prijav odprl 660 zadev. V 216 primerih so bili prijavitelji obveščeni, da Informacijski pooblaščenec postopka inšpeksijskega nadzora ne bo uvedel, ker iz njihove prijave ne izhaja suma kršitev določb Splošne uredbe in ZVOP-1 ali ker postopek ne bi bil smiseln, 81 prijaviteljev pa je napotil na pravice, ki jih morajo pri upravljavcih osebnih podatkov uveljavljati sami (največkrat na pravico do seznanitve z lastnimi osebnimi podatki in pravico do ugovora). V sedmih primerih Informacijski pooblaščenec postopka inšpeksijskega nadzora ni mogel uvesti zaradi pomanjkanja podatkov, pet prijav je odstopil v reševanje pristojnim institucijam, od tega je v štirih primerih naznanil suma storitve kaznivega dejanja, na podlagi treh prijav pa je takoj uvedel postopke o prekršku.

Informacijski pooblaščenec je po preučitvi prejetih prijav začel 348 postopkov inšpeksijskega nadzora, 39 jih je uvedel po uradni dolžnosti, skupaj torej 387. Državni nadzorniki za varstvo osebnih podatkov so v zasebnem sektorju opravili 81 inšpeksijskih ogledov, za odpravo ugotovljenih nepravilnosti so zavezancem izrekli ukrepe v 26 predodločbah, 13 opozorilih na zapisnik in treh ureditvenih odločbah. En zavezanc je zoper odločbo vložil tožbo, preostali so naložene ukrepe v dodeljenem jim roku izvršili.

¹ 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 praks treba pred izdajo ureditvene odločbe dati možnost, da se izjaví 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.

Leta 2018 je Informacijski pooblaščenec pri zavezancih v zasebnem sektorju s sklepom ustavil 188 postopkov; 84 postopkov je ustavil, ker ni bilo kršitev določb ZVOP-1, 71 postopkov je ustavil po tem, ko so zavezanci odpravili ugotovljene nepravilnosti, 33 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 zavezanc vložil tožbo na Upravno sodišče RS.

Pregled inšpekcijskih zadev v javnem in zasebnem sektorju leta 2018

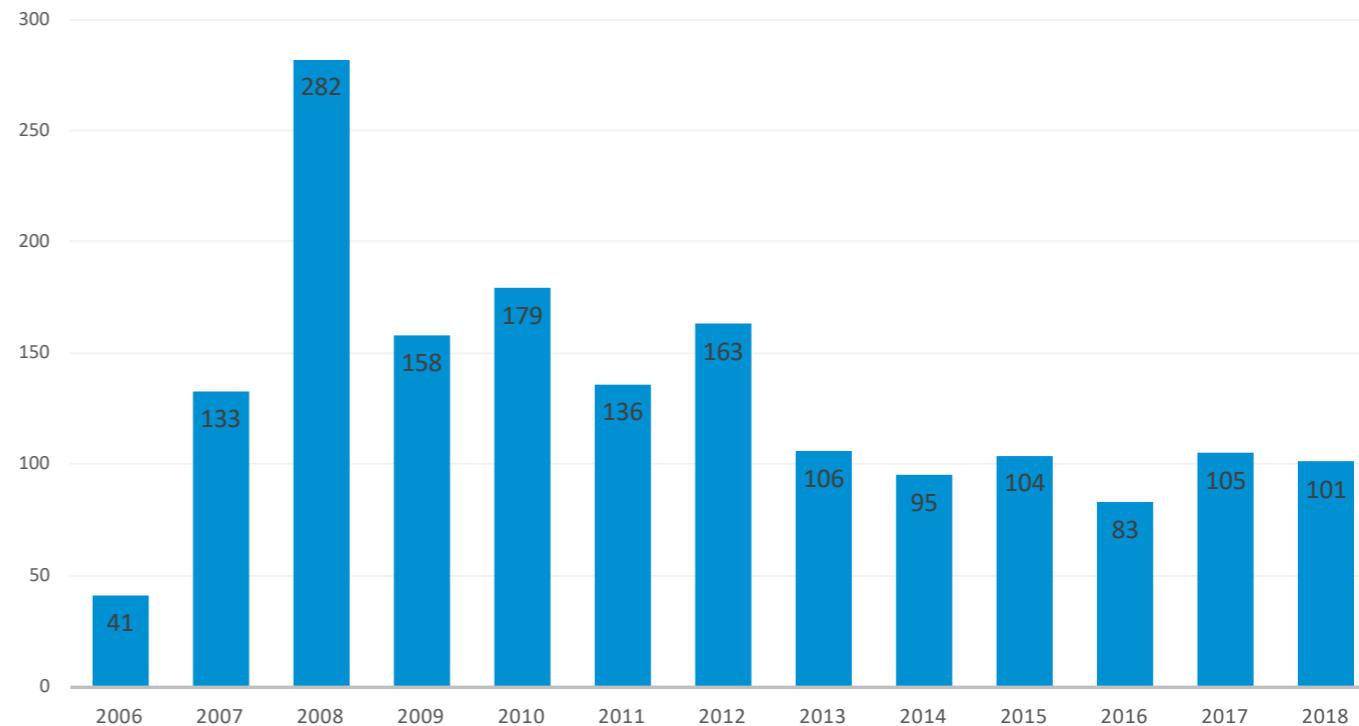


3.2.3 PREKRŠKOVNI POSTOPKI

POMEMBNO

Informacijski pooblaščenec je zaradi suma kršitev določb ZVOP-1 leta 2018 uvedel 101 postopek o prekršku, od tega je 42 postopkov uvedel zoper pravne osebe javnega sektorja in njihove odgovorne osebe, 31 zoper pravne osebe zasebnega sektorja in njihove odgovorne osebe, 28 pa zoper posameznike (v to število so vključeni tudi postopki zoper odgovorne osebe državnih organov in samoupravnih lokalnih skupnosti, saj v skladu z Zakonom o prekrških (ZP-1) Republika Slovenija in samoupravne lokalne skupnosti za prekrške ne odgovarjajo, odgovarjajo le njihove odgovorne osebe – teh je bilo 25).

Število uvedenih postopkov o prekršku med letoma 2006 in 2018



Za ugotovljeni prekršek lahko prekrškovni organ v skladu s 53. členom izreče opozorilo, če je storjeni prekršek neznaten in če pooblaščena uradna oseba oceni, da je glede na pomen dejanja opozorilo zadosten ukrep. Če je storjen hujši prekršek, prekrškovni organ izda odločbo o prekršku, s katero kršitelju izreče sankcijo. V skladu s 4. členom ZP-1 sta sankciji za prekršek globa in opomin, glede na 57. člen ZP-1 pa se lahko globa izreče tudi v obliki plačilnega naloga.

Informacijski pooblaščenec je ustavil dva postopka o prekršku, tri predlagatelje za uvedbo postopka o prekršku pa je obvestil, da postopka ne bo uvedel.

POMEMBNO

Informacijski pooblaščenec je v prekrškovnih postopkih leta 2018 izdal:

- 9 opozoril ter
- 42 odločb o prekršku (20 glob in 22 opominov).

Poleg opozoril, ki so bila izrečena v prekrškovnih postopkih, je Informacijski pooblaščenec v skladu z načelom ekonomičnosti izrekel tudi 42 opozoril po 53. členu ZP-1 v okviru postopkov inšpekcijskega nadzora.

Kršitelji so zoper izdane odločbe o prekršku vložili sedem zahtev za sodno varstvo (zoper 16,7 % 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.

Preglednica: Kršitve varstva osebnih podatkov leta 2018

Vrsta kršitve	Število kršitev (v okviru enega postopka je lahko več kršitev)
nezakonita obdelava osebnih podatkov (8. člen ZVOP-1)	37
neustrezno zavarovanje osebnih podatkov (24. in 25. člen ZVOP-1)	33
nezakonit namen zbiranja in nadaljnje obdelave osebnih podatkov (16. člen ZVOP-1)	11
neustrezno urejena pogodbena obdelava osebnih podatkov (11. člen ZVOP-1)	10
kršitve določb v zvezi z izvajanjem videonadzora (74., 75., 76. in 77. člen ZVOP-1)	7
nepravilnosti v zvezi z vzpostavitvijo katalogov zbirk osebnih podatkov in posredovanjem podatkov v register zbirk osebnih podatkov (26. in 27. člen ZVOP-1)	7
kršitve določb o neposrednem trženju (72. in 73. člen ZVOP-1)	6
nezakonito kopiranje osebnih dokumentov (4.a člen ZPLD in 4. člen ZOlzk)	4
neizpolnjevanje ukrepov, izrečenih v postopkih inšpekcijskega nadzora, kršitve določb ZIN	3
neustrezno zavarovanje občutljivih osebnih podatkov (14. člen ZVOP-1)	1
nezakonita obdelava občutljivih osebnih podatkov (13. člen ZVOP-1)	1
pomanjkljivo obveščanje posameznika o obdelavi osebnih podatkov (19. člen ZVOP-1)	1

POMEMBNO

Informacijski pooblaščenec poudarja, da je na vodenje prekrškovih postopkov in izrekanje sankcij za ugotovljene kršitve zelo vplival nesprejem ZVOP-2, saj ni mogel uvesti postopka za prekrške in izreči sankcije za kršitve določb Splošne uredbe; to je lahko storil le za kršitve tistih členov ZVOP-1, ki še veljajo.

Leta 2018 je Informacijski pooblaščenec prejel osem sodb, s katerimi so okrajna sodišča odločila o zahtevah za sodno varstvo, ki so jih storilci vložili zoper odločbe o prekrških, izdane v letih 2016, 2017 in 2018:

- zahteva za sodno varstvo je bila zavrnjena kot neutemeljena, odločba Informacijskega pooblaščenca pa potrjena – 4,
- zahtevi za sodno varstvo je bilo delno ugodeno tako, da je bila odločba o prekršku Informacijskega pooblaščenca spremenjena glede odločitve o sankciji in je bil storilcem namesto globe izrečen opomin, sicer pa je bila zahteva za sodno varstvo zavrnjena kot neutemeljena – 2,
- postopek o prekršku je bil ustavljen – 2.

Informacijski pooblaščenec je prejel tudi sodbo Vrhovnega sodišča Republike Slovenije o zahtevi za varstvo zakonitosti, ki jo je Vrhovno državno tožilstvo vložilo na pobudo kršitelja zoper sodbo okrajnega sodišča v zvezi z odločbo Informacijskega pooblaščenca. Vrhovno sodišče je zahtevi za varstvo zakonitosti ugodilo in postopek o prekršku zoper storilki zaradi zastaranja ustavilo, saj sta od dneva, ko je okrajno sodišče prejelo zahtevo za sodno varstvo, do dneva izdaje sodbe pretekli več kot dve leti.

3.2.4 SODELOVANJE PRI ČEZMEJNIH INŠPEKCIJSKIH NADZORIH

Splošna uredba v poglavju 7 zapoveduje tesno sodelovanje med nadzornimi organi za varstvo osebnih podatkov v državah članicah EU in EGS (Islandija, Norveška in Lichtenštajn) pri čezmejnih primerih, in sicer prek naslednjih mehanizmov:

- **sodelovanje po načelu »vse na enem mestu«** (angl. one stop shop), ki predvideva, da postopek nadzora v čezmejnem primeru obdelave osebnih podatkov vodi t. i. vodilni organ in pri tem sodeluje z drugimi organi za varstvo osebnih podatkov (člen 60 Splošne uredbe);
- **vzajemna pomoč** med organi za varstvo osebnih podatkov v državah članicah EU (člen 61 Splošne uredbe);
- **skupno ukrepanje** organov za varstvo osebnih podatkov v državah članicah EU (člen 62 Splošne uredbe).

Sodelovanje po mehanizmu »vse na enem mestu« se lahko prične, ko je ugotovljeno, kateri nadzorni organ bo v postopku prevzel vlogo vodilnega in kateri organi bodo v postopku sodelovali kot zadevni organi. Vodilni organ prihaja iz tiste države članice EGS, kjer ima upravljačec osebnih podatkov, ki posluje čezmejno, glavno ustanovitev – sedež, ki prevzema odgovornost za obdelavo osebnih podatkov. Nadzorni organi iz drugih držav članic EGS pa se postopku nadzora priključijo kot zadevni organi, kadar ima upravljačec na njihovem ozemlju npr. podružnice ali poslovne enote oz. kadar obdelava osebnih podatkov pomembno vpliva na posameznike v teh državah članicah. Glavni organ v postopku inšpekcijskega nadzora vodi sodelovanje z drugimi organi ter pripravi osnutek odločbe, zadevni organi pa lahko izrazijo svoje zadržke. V primeru nestrinjanja med vodilnim in zadevnimi organi o sporu odloči Evropski odbor za varstvo osebnih podatkov.

Sodelovanje v okviru vseh treh mehanizmov poteka prek informacijskega sistema za notranji trg (Internal Market Information System, IMI) Evropske komisije; ta zagotavlja varno in zaupno komunikacijo med nadzornimi organi ter omogoča izvajanje posameznih faz in postopkov čezmejnega sodelovanja, v za to določenih rokih.

Leta 2018 (podatki na dan 8. 1. 2019) je bilo v informacijskem sistemu za notranji trg registriranih:

- 255 čezmejnih primerov upravljavcev ali obdelovalcev osebnih podatkov, pri katerih naj bi prišlo do kršitev Splošne uredbe (176 jih je bilo pričetih na podlagi prijave ali pritožbe posameznikov, ostale so organi pričeli po uradni dolžnosti ex offo).

V okviru teh primerov so bili izvedeni različni mehanizmi sodelovanja (v okviru enega primera je lahko izvedenih več postopkov):

- 397 postopkov vzajemne pomoči med nadzornimi organi za varstvo osebnih podatkov v različnih državah članicah EU in EGS ter
- 43 postopkov po mehanizmu »vse na enem mestu«, od katerih sta bila ob koncu leta 2018 dva postopka zaključena, 21 jih je bilo v fazi osnutka odločbe in 20 v fazi konzultacije med organi.

Poleg tega je bilo pričetih 574 postopkov ugotavljanja, kdo je v določnem primeru čezmejne obdelave osebnih podatkov s sumom kršitve Splošne uredbe t. i. vodilni organ, ki bo vodil sodelovanje z drugimi organi v postopku nadzora.

Sodelovanje Informacijskega pooblaščenca v čezmejnih postopkih inšpekcijskega nadzora, ki so bili pričeti v obdobju od uveljavitve Splošne uredbe do konca koledarskega leta, torej od 25. 5. 2018 do 31. 12. 2018:

V **81 postopkih ugotavljanja vodilnega organa** čezmejnega postopka nadzora po členu 56 Splošne uredbe se je Informacijski pooblaščenec opredelil za zadevni organ:

- ker je tudi sam prijel prijavo domnevne kršitve varstva osebnih podatkov v čezmejnem primeru,
- ker ima upravljačec osebnih podatkov, zoper katerega teče postopek v drugi državi članici, v Sloveniji poslovno enoto ali je bil tu ustanovljen,
- ker storitve upravljavca, zoper katerega teče postopek v drugi državi članici, uporabljajo posamezniki v Sloveniji in jih vprašanje domnevne kršitve varstva osebnih podatkov pomembno zadeva. Tu gre največkrat za priljubljene ponudnike komunikacijskih spletnih storitev oz. spletnne velikane: Facebook, Google, Amazon, Apple, PayPal, WhatsApp, Twitter, Instagram, Microsoft itd. Večina naštetih podjetij ima v EU sedež na Irskem, kar pomeni, da je irski nadzorni organ za varstvo osebnih podatkov vodilni v teh postopkih inšpekcijskega nadzora in sodelovanja², organi iz drugih držav članic pa v postopku sodelujejo v skladu s pooblastili, ki jih določa Splošna uredba.

Na temelju omenjenih postopkov ugotavljanja vodilnega nadzornega organa je bilo pozneje pričetih **30 postopkov čezmejnega sodelovanja pri inšpekcijskem nadzoru** nad podjetji, ki poslujejo čezmejno, po mehanizmu »vse na enem mestu« (člen 60 Splošne uredbe), v katerih Informacijski pooblaščenec sodeluje kot zadevni organ. Leta 2018 ni bil končan nobeden od postopkov; večinoma so bili še v fazi konzultacije med organi.

² Podrobnosti primerov so na voljo v letnem poročilu Irskega nadzornega organa za varstvo osebnih podatkov, ki je na voljo na <https://www.data-protection.ie/sites/default/files/uploads/2019-03/DPC%20Annual%20Report%202018.pdf>.

Informacijski pooblaščenec je sodeloval v šestih postopkih vzajemne pomoči po členu 61 Splošne uredbe, saj je bil s strani drugih nadzornih organov iz EU zaprošen za podajo pojasnil glede konkretnih čezmejnih primerov, ki jih obravnavajo, ali glede usmeritev pri obravnavi določene tematike.

Sodelovanje Informacijskega pooblaščenca v čezmejnih postopkih nadzora:

- 81 postopkov določitve vodilnega in zadevnih nadzornih organov,
- 30 primerov sodelovanja v mehanizmu »vse na enem mestu« (kot zadevni nadzorni organ),
- 6 postopkov vzajemne pomoči drugim nadzornim organom.

Primeri čezmejnega sodelovanja Informacijskega pooblaščenca zadevajo predvsem priljubljena multinacionalna spletna podjetja, tj. Facebook, Google, Twitter, LinkedIn, Amazon, Apple idr., ter skladnost njihovih praks s Splošno uredbo na različnih področjih:



zakonitost obdelave osebnih podatkov s strani ponudnikov družbenih omrežij in priljubljenih komunikacijskih storitev ter drugih upravljavcev, še posebej z vidika uporabe osebnih podatkov posameznikov za namen personaliziranega oglaševanja in ciljanja;



ustreznost njihovih politik zasebnosti in obveščanja posameznikov o obdelavi osebnih podatkov;



izvrševanje pravic posameznikov (npr. do seznanitve z lastnimi osebnimi podatki, do prenosljivosti podatkov);



kršitve varnosti osebnih podatkov, npr. zaradi izkoriščanja varnostnih ranljivosti.

3.2.5 IZBRANI PRIMERI OBDELAVE OSEBNIH PODATKOV

V nadaljevanju so predstavljeni primeri obdelave osebnih podatkov, v zvezi s katerimi so se posamezniki leta 2018 največkrat obrnili na Informacijskega pooblaščenca, in primeri, v katerih se je praksa po začetku uporabe Splošne uredbe bistveno spremenila.

Neposredno trženje in pravice posameznika

Informacijski pooblaščenec je prejel zelo veliko prijav, v katerih so posamezniki navedli, da s strani različnih ponudnikov prejemajo sporočila, čeprav v to niso privolili. Posamezniki so želeli, da Informacijski pooblaščenec preveri, kje so ponudniki pridobili njihove osebne podatke.

V takšnih primerih Informacijski pooblaščenec praviloma ni uvedel postopka inšpeksijskega nadzora, ker je privolitev le ena od šestih možnih pravnih podlag za zakonito obdelavo osebnih podatkov po členu 6 Splošne uredbe, kar pomeni, da lahko upravljavec v določenih primerih osebne podatke obdeluje tudi brez privolitve posameznika, pri čemer je dovolj, da mu posreduje informacije iz člena 13 in/ali 14 Splošne uredbe. Takšen primer je obdelava osebnih podatkov na podlagi točke (f) člena 6(1) Splošne uredbe, ki je zakonita, če je potrebna zaradi zakonitih interesov, za katere si prizadeva upravljavec ali tretja oseba, razen kadar nad takimi interesi prevladajo interesi ali temeljne pravice in svoboščine posameznika. Obdelava osebnih podatkov za neposredno trženje se skladno z uvodno določbo (47) Splošne uredbe lahko šteje za opravljeno v zakonitem interesu, prav tako pa se kot obdelava, ki je potrebna za izvajanje zakonitih interesov, za katere si prizadeva upravljavec, lahko šteje tudi obdelava osebnih podatkov za namene, da upravljavec posameznika zaprosi in od njega pridobi še kakšno dodatno novo privolitev. Če je upravljavec osebne podatke posameznika pridobil na zakonit način (npr. iz javno dostopnih virov ali v okviru zakonitega opravljanja dejavnosti), jih lahko uporabi tudi za namene neposrednega trženja po navadni pošti. Kje je upravljavec pridobil osebne podatke in ali jih obdeluje na zakoniti pravni podlagi, lahko posameznik preveri sam, in sicer tako, da na upravljavca skladno s členom 15 Splošne uredbe naslovi zahtevo za seznanitev z lastnimi osebnimi podatki, na podlagi katere mu mora upravljavec med drugim posredovati tudi informacije o viru pridobitve osebnih podatkov. Na podlagi člena 21 Splošne uredbe lahko posameznik pri upravljavcu kadar koli ugovarja obdelavi osebnih podatkov, ki temelji na točki (f) člena 6(1), kamor spada tudi obdelava osebnih podatkov za namene neposrednega trženja, uveljavlja pa lahko tudi pravico do izbrisala osebnih podatkov (pravica do pozabe) iz člena 17 Splošne uredbe. Prenehanje obdelave osebnih podatkov za namene neposrednega trženja lahko posameznik od upravljavca pisno ali na drug dogovorjeni način zahteva tudi na podlagi 73. člena ZVOP-1, ki določa, da je upravljavec osebnih podatkov dolžan v 15 dneh ustrezno preprečiti uporabo osebnih podatkov za namen neposrednega trženja ter o tem v nadaljnjih petih dneh pisno ali na drug dogovorjeni način obvestiti posameznika, ki je to zahteval.

Pravice iz poglavja III (členi 13 do 22) Splošne uredbe so pravice posameznika, ki jih pri upravljavcu lahko uveljavlja zgolj on sam. Informacijski pooblaščenec je nadzorni organ, ki v primeru kršitve pravic deluje kot pritožbeni organ, kar pomeni, da lahko posameznik, če upravljačev njegovo zahtevo v celoti zavrne ali nanjo ne odgovori v enomesečnem roku, na Informacijskega pooblaščenca naslovi pritožbo. Pritožbo lahko posreduje tudi, če upravljačev ne ravna v skladu s 73. členom ZVOP-1.

Fotografiranje otrok na prireditvah v šolah in vrtcih

Informacijski pooblaščenec je v prejel številna vprašanja zaskrbljenih staršev, osnovnih šol in vrtcev glede (ne)dopustnosti fotografiranja nastopov otrok s strani staršev, zaradi česar je dne 7. 12. 2018 pripravil sporočilo za javnost in ga objavil na svoji spletni strani. V sporočilu je poudaril, da v zvezi z navedenim po začetku uporabe Splošne uredbe ni nobenih sprememb, kar pomeni, da nova zakonodaja ni uvedla novih pravil glede fotografiranja otrok in staršem tudi ne prepoveduje fotografiranja lastnega otroka na noveletnem ali drugem nastopu. V primeru fotografiranja ali snemanja otrok s strani staršev pa gre praviloma za obdelavo osebnih podatkov, ki se izvaja za osebno uporabo oz. v zasebne namene. Takšno fotografiranje ali snemanje zato ne predstavlja kršitve določb ZVOP-1 in Splošne uredbe, saj se glede na določbo točke (c) drugega odstavka člena 2 Splošne uredbe le-ta ne uporablja za obdelavo osebnih podatkov (torej tudi za fotografiranje ali snemanje) s strani fizične osebe med potekom popolnoma osebne in domače dejavnosti. Informacijski pooblaščenec zato meni, da ukrep nekaterih vzgojno-izobraževalnih institucij, ki so staršem absolutno prepovedale fotografirati ali snemati svoje otroke na šolski ali vrtčevski prireditvi, ni bil ustrezan. Najprimernejše bi bilo, da bi šole in vrtci starše na začetku prireditve opozorile na dopustnost snemanja in fotografiranja ter na nadaljnjo uporabo posnetkov in fotografij. Starši morajo namreč paziti, da fotografij drugih otrok ne posredujejo tretjim osebam – zlasti to velja za objavo na spletu in družbenih omrežjih – brez soglasja njihovih staršev. Če šolsko ali vrtčevsko prireditve snema ali fotografira šola ali vrtec, gre lahko za obdelavo osebnih podatkov, ki so del zbirk osebnih podatkov, katerih upravljačev je vrtec ali šola, zato mora za takšno obdelavo obstajati ustrezna pravna podlaga. Ker objave fotografij Zakon o vrtcih (ZVrt) in Zakon o osnovni šoli (ZOsn) ne določata, lahko skladno z drugim odstavkom 9. člena ZVOP-1 v povezavi z drugim odstavkom člena 6 Splošne uredbe pravno podlago za objavo predstavlja le osebna privolitev posameznika. Glede na to, da so v vrtcih in osnovnih šolah mladoletni otroci, ki poslovne sposobnosti še nimajo, morajo namesto njih privolitev podati njihovi starši ali drugi zakoniti zastopniki. Osebno (pisno) privolitev staršev za objavo določenih osebnih podatkov otrok določata tudi Pravilnik o zbiranju in varstvu osebnih podatkov na področju osnovnošolskega izobraževanja v 6. členu in Pravilnik o zbiranju in varstvu osebnih podatkov na področju predšolske vzgoje v 16. členu.

Gre za osebne podatke, ki po naravi, vsebini ali namenu ne posegajo v zasebnost otrok (npr. razstave izdelkov, skupinski posnetki na fotografijah, videoposnetki, zvočni ali filmski posnetki javnih nastopov na prireditvah ipd.). To pomeni, da bi vrtec ali šola pred objavo fotografij morala pretehtati, ali so primerne za objavo oz. ali na kakršen koli način posegajo v zasebnost otrok. Pri objavi fotografij na spletu je namreč treba upoštevati predvsem dejstvo, da so dostopne vsakomur in da se jih lahko nekontrolirano kopira in objavlja na drugih spletnih straneh, pri čemer je nemogoče odpraviti škodljive posledice, ki bi lahko nekomu nastale zaradi objave določene fotografije.

V primeru, da gre za javno prireditve, organizator prireditve (šola, vrtec) posebnih osebnih privolitev udeležencev za splošno fotografiranje prireditve in objavo ni dolžan pridobiti, če udeležence predhodno seznaniti s snemanjem in objavo posnetkov na ustrezen način (jim posreduje informacije iz člena 13 Splošne uredbe). Vsak posameznik, ki se udeleži javne prireditve, se mora namreč zavedati, da na takšni prireditvi obstaja večja verjetnost, da bo posnet in da bo fotografija objavljena v različnih medijih z namenom predstavitve samega dogodka.

Obdelava osebnih podatkov ob včlanitvi v sindikat in za namen obračuna sindikalne članarine

Podatek o članstvu v sindikatu se po členu 9(1) Splošne uredbe šteje med posebne vrste osebnih podatkov (po ZVOP-1 je bil to občutljiv osebni podatek). Neposredno pravno podlago za obdelavo osebnih podatkov članov znotraj sindikatov predstavlja točka (d) člena 9(2) Splošne uredbe, ki določa, da je dopustna obdelava osebnih podatkov, ki jo izvajajo sindikati v okviru svojih zakonitih dejavnosti z ustreznimi zaščitnimi ukrepi pod pogojem, da se obdelava nanaša samo na člane ali nekdanje člane sindikata ali na osebe, ki so v rednem stiku z njim v zvezi z njegovimi nameni, ter da se osebni podatki ne posredujejo zunaj tega telesa brez privolitve posameznikov, na katere se osebni podatki nanašajo. To pomeni, da sindikati za zbiranje osebnih podatkov posameznikov za namene včlanitve in zakonitih dejavnosti sindikata (kot so opredeljene v zakonu ali aktih sindikata) ne potrebujejo njihove osebne privolitve, ampak jih morajo zgolj ustrezno (v pristopni izjavi ali na drug ustrezni način) seznaniti z vsemi informacijami o obdelavi, kot to zahteva člen 13 Splošne uredbe. Čeprav se posameznik prostovoljno odloči, ali se bo včlanil v sindikat in s tem sprejel tudi akte (npr. statut, različne pravilnike, ki določajo uveljavljanje pravic članov), v katerih je opredeljeno njegovo delovanje, to ne pomeni, da lahko sindikat zbira katere koli osebne podatke, saj mora, tako kot vsi upravljači, osebne podatke obdelovati skladno z načelom sorazmernosti oz. z načelom najmanjšega obsega podatkov iz točke (c) člena 5(1) Splošne uredbe. Zakonitost in veljavnost včlanitve v sindikat se presoja glede na civilnopravne predpise. Delodajalec na podlagi tretjega odstavka 207. člena Zakona o delovnih razmerjih (ZDR-1) na zahtevo sindikata v skladu z aktom sindikata, katerega član je delavec, zagotavlja tehnično izvedbo obračuna in plačevanja sindikalne članarine za delavca. Delavec lahko plačuje sindikalno članarino na dva načina, in sicer tako, da jo

plačuje sindikatu neposredno sam, ali pa tako, da tehnično izvedbo obračuna in plačevanja sindikalne članarine zagotavlja delodajalec, ki v konkretnem primeru ni upravljavec zbirke osebnih podatkov v zvezi z nakazili sindikalne članarine niti pogodbeni obdelovalec sindikata, ampak uporabnik teh podatkov. Zato mora sindikat, če omogoča plačevanje članarine na oba načina, kot upravljavec zbirke ob včlanitvi oz. tudi kasneje, če pride do spremembe, pridobiti ustreznar pooblastila svojih članov za izvajanje plačila članarine prek delodajalca. Če je plačevanje sindikalne članarine možno zgolj prek delodajalca, mora sindikat posameznika ob včlanitvi s tem seznaniti in navesti vrste osebnih podatkov, ki jih bo posredoval delodajalcu za ta namen. Sindikat posreduje delodajalcu le tiste podatke, ki jih potrebuje za izvedbo nakazila članarine, in ne kopij pristopnih izjav.

Obdelava podatkov o družinskih članih potencialnega kreditojemalca iz centralnega kreditnega registra s strani bank

Informacijski pooblaščenec je prejel več prijav zoper banke zaradi pridobivanja osebnih podatkov iz centralnega kreditnega registra za družinske člane (predvsem partnerje) potencialnih kreditojemalcev. Ob obravnavi prijav je ugotovil, da so banke v skladu z določbami ZPotK-2 dolžne oceniti kreditno sposobnost potrošnika, in sicer na podlagi potrebnih, zadostnih in sorazmernih informacij o prihodkih in izdatkih oz. premoženskem stanju potrošnika, ki jih pridobijo od potrošnika in izzbirk osebnih podatkov, ki se vodijo na podlagi zakona, ki ureja sistem izmenjave informacij o boniteti oz. zadolženosti fizičnih oseb (tj. ZCKR). V skladu z 19. členom ZCKR lahko člani sistema za namene ocenjevanja kreditnega tveganja fizične osebe ali poslovnega subjekta, ki je izrazil interes za sklenitev kreditnega posla ali s katerim so kreditni posel sklenili, dostopajo do vseh podatkov, ki se o tej fizični osebi ali poslovnom subjektu obdelujejo v sistemu izmenjave informacij.

Informacijski pooblaščenec je zaključil, da niti ZPotK-2 niti ZCKR bankam ne dajeta pravne podlage za to, da bi iz centralnega kreditnega registra pridobivale osebne podatke kogar koli drugega kot kreditojemalca. Banke osebnih podatkov iz registra ne morejo pridobiti niti na podlagi privolitve posameznika. Banka Slovenije, ki je vzpostavila centralni kreditni register in ga tudi upravlja, je namreč del javnega sektorja, osebni podatki v javnem sektorju pa se skladno s prvim odstavkom 9. člena ZVOP-1 lahko obdelujejo, če obdelavo osebnih podatkov in osebne podatke, ki se obdelujejo, določa zakon, na podlagi osebne privolitve pa se lahko obdelujejo le, če tako določa zakon. Ker niti ZPotK-2 niti ZCKR ne predvidevata privolitve za pridobivanje osebnih podatkov iz centralnega kreditnega registra, banke niti na podlagi privolitve nimajo osnove za pridobivanje osebnih podatkov partnerjev potencialnih kreditojemalcev ali drugih družinskih članov. Banka bi osebne podatke partnerjev oz. drugih družinskih članov potencialnih kreditojemalcev sicer lahko pridobila prek pravice fizične osebe do seznanitve z lastnimi osebnimi podatki, ki jo ZCKR opredeljuje v 22. členu, torej bi osebne podatke iz centralnega kreditnega registra pridobila od posameznikov, na katere se ti podatki nanašajo, potem ko bi jih ti sami pridobili iz centralnega kreditnega registra na podlagi

zahteve za seznanitev, ki bi jo vložili pri Banki Slovenije ali članu sistema. Takšno pridobivanje osebnih podatkov bi se z vidika določb Splošne uredbe lahko štelo za zakonito le v primeru, če bi banka potencialnemu kreditojemalcu in njegovim družinskim članom ob zaprosilu za posredovanje osebnih podatkov posredovala jedrnate, pregledne in razumljive informacije iz člena 13 Splošne uredbe, zlasti informacije iz točke (c) prvega odstavka (namene, za katere se osebni podatki obdelujejo, in pravno podlago za njihovo obdelavo) in točke (e) drugega odstavka (ali je zagotovitev osebnih podatkov statutarna ali pogodbena obveznost ali pa obveznost, ki je potrebna za sklenitev pogodb, ter ali mora posameznik, na katerega se osebni podatki nanašajo, zagotoviti osebne podatke ter kakšne so morebitne posledice, če se taki podatki ne zagotovijo).

Videonadzor v delovnih prostorih in spremljanje žive slike kamer

Videonadzor znotraj delovnih prostorov se skladno s 77. členom ZVOP-1 lahko izvaja le v izjemnih primerih, kadar je to nujno za varnost ljudi ali premoženja ali za varovanje tajnih podatkov ter poslovne skrivnosti, vendar tega namena ni možno doseči z milejšimi sredstvi. Informacijski pooblaščenec pojasnjuje, da namestitev kamer na delovnih mestih (npr. v proizvodnji in gostinskih lokalih) sama po sebi še ni nezakonita, če so bile te nameščene zaradi varovanja zgoraj navedenih dobrin in če so izpoljeni drugi pogoji, ki jih za uvedbo videonadzora določa ZVOP-1. Problematična je, kot se je izkazalo v postopkih inšpekcijskega nadzora, predvsem ureditev dostopnih pravic do videonadzornega sistema ter omogočanje dostopa do žive slike. Dostop do žive slike, pogosto gre celo za oddaljen dostop prek katere koli naprave, povezane v internet (mobilni telefon, prenosnik), imajo predvsem nadrejeni, ki živo sliko spremljajo po lastni presoji in v nasprotju z nameni uvedbe videonadzora, največkrat zaradi nadzora nad opravljanjem dela posameznih delavcev. Takšno ravnanje ni v skladu s 16. členom ZVOP-1 in točko (b) člena 5 Splošne uredbe, iz katerih izhaja, da se osebni podatki, ki so bili zbrani za določene, izrecne in zakonite namene, ne smejo nadalje obdelovati na način, ki ni združljiv s temi nameni.

Zgoraj navedeno ne pomeni, da a priori ni mogoče izključiti možnosti, da delodajalec omogoča spremljanje dogajanja v delovnih prostorih prek žive slike, vendar je potrebno obdelavo osebnih podatkov, ki jo predstavlja vpogled v živo sliko, upravičiti skozi namene, zaradi katerih se videonadzor izvaja. Spremljanje žive slike mora biti namenjeno izključno varovanju premoženja ter zagotavljanju varnosti ljudi, slednje pa je po sami naravi stvari mogoče doseči le z nepreklenjenim spremljanjem žive slike med delovnim procesom (ne z občasnimi, naključnimi vpogledi) s strani za to pooblaščene osebe, npr. varnostnika, in ne osebe, ki je pooblaščena za nadzor nad izpolnjevanjem obveznosti delavcev. Delavec, pooblaščen za zagotavljanje varnosti, bo lahko namreč neposredno ob zaznanem incidentu (požar, tatvina, neuporaba zaščitnih sredstev, poškodba delavca ...) ustrezeno ukrepal ter preprečil nastanek (večje) škode oz. hujše poškodbe delavca, kar je nenazadnje namen izvajanja videonadzora v delovnih prostorih. Verjetnost, da se bo incident zgodil ravno v trenutku, ko

bo vodja ali drugi nadzorni delavec naključno vpogledal v videonadzorni sistem, pa je zanemarljiva, zaradi česar je tudi spremjanje žive slike s strani vodstvenih delavcev neutemeljeno. Ti so namreč zadolženi predvsem za skrb za izpolnjevanje delovnih obveznosti delavcev, pri čemer jim možnost spremjanja dogajanja prek žive slike predstavlja sredstvo za prikriti nadzor nad delom delavcev, kar pa je v nasprotju z nameni, zaradi katerih je dopustno izvajati videonadzor v delovnih prostorih. Še posebej to velja v primerih, ko je vodstvenim delavcem dostop do žive slike omogočen prek oddaljenega dostopa, kar jim omogoča, da nadzirajo delovni proces tudi izven delovnega časa.

Glede na zgoraj navedeno morajo delodajalci, ki izvajajo videonadzor znotraj delovnih prostorov, določiti osebo oz. osebe, ki imajo dostop do arhiva videoposnetkov, v izjemnih primerih pa tudi osebo, ki bo v skladu z zakonitimi nameni videonadzora spremljala živo sliko. Tudi pooblašcene osebe lahko arhiv videoposnetkov pregledujejo le v skladu z nameni, ki jih za uvedbo videonadzora določa ZVOP-1 (npr. takrat, ko pride do poškodovanja ali odtujitve premoženja ali ogrožanja ljudi), pri čemer morajo zagotavljati ustrezen sledljivost vpogledov v videoposnetke (kdo, kdaj, katere videoposnetke, iz kakšnih razlogov oz. za kakšen namen jih je obdeloval). Pregledovanje arhiva videoposnetkov ali spremjanje žive slike izključno z namenom nadzora nad zaposlenimi pomeni kršitev določb ZVOP-1 in nedoposten poseg v zasebnost zaposlenih, do katere so upravičeni tudi na delovnem mestu.

Nezakoniti vpogledi v zdravstvene osebne podatke in pridobitev podatkov o posameznikih, ki so opravili vpoglede

Informacijski pooblaščenec vsako leto prejme nekaj prijav zaradi suma nezakonitih vpogledov v zdravstvene osebne podatke, v katerih posamezniki zahtevajo tudi pridobitev seznama oseb, ki so obdelovale njihove osebne podatke. Postopek inšpeksijskega nadzora, v katerem preverja zakonitost obdelave osebnih podatkov določenega posameznika, ki se vodijo v določeni zbirki, Informacijski pooblaščenec uvede zgolj v primeru, če posameznik v prijavi izkaže konkretnе razloge za sum, da so zaposleni pri določenem upravljavcu v določenem obdobju nezakonito vpogledovali v njegove osebne podatke oz. da so njegove osebne podatke obdelovali za nezakonite namene (npr. da določena oseba razpolaga s podatki, ki jih je lahko pridobila izključno z nezakonitim vpogledom v zbirko osebnih podatkov). Zgolj domneva, da so nekateri zaposleni, ki imajo dostop do osebnih podatkov, z njimi nepooblaščeno razpolagali in jih obdelovali, za uvedbo inšpeksijskega postopka ni dovolj.

V primeru potrjenega suma nezakonitega vpogleda v podatke o zdravstvenem stanju, ki se po členu 9(1) Splošne uredbe štejejo med posebne vrste osebnih podatkov, Informacijski pooblaščenec kršitelju praviloma izreče globo. Zaposleni v določeni zdravstveni ustanovi namreč lahko v osebne podatke pacienta vpogledajo le, če sodelujejo v procesu njegove zdravstvene obravnave ali iz drugih

zakonitih razlogov (npr. za namen izdaje računa za opravljene zdravstvene storitve ali za namen obveznega sporočanja določenih primerov policiji). Ob tem dodaja, da se nekateri posamezniki, katerih osebna imena so zabeležena v dnevnikih sledljivosti obdelave osebnih podatkov, čeprav niso imeli zakonitega razloga za vpogled v osebne podatke, želijo izogniti odgovornosti na način, da zatrjujejo, da v podatke niso vpogledali oni, ampak nekdo drug z uporabo njihovega gesla. Tudi v takšnem primeru Informacijski pooblaščenec kršiteljem izreče globo, vendar ne zaradi nezakonite obdelave osebnih podatkov, ampak zaradi neustreznega zavarovanja gesel, katerega posledica je bila, da so neznane osebe z uporabo njihovih gesel nepooblaščeno in nezakonito obdelovale osebne podatke pacientov. Ker ima vsak zaposleni, ki dostopa do zbirke osebnih podatkov pacientov v informacijskem sistemu, svoje uporabniško ime in geslo, se mora na začetku obdelave (npr. vnos, popravljanje, izpis podatkov ali samo vpogled v podatke) prijaviti v sistem in po zaključku obdelave iz njega odjaviti. Še posebej je to pomembno, kadar vsak zaposleni nima svojega računalnika oz. kadar več zaposlenih uporablja en računalnik. Če se zaposleni ne odjavlja iz sistema in več oseb (kljub temu, da je upravljavec določil posamične dostopne pravice) uporablja isto geslo, tudi ni zagotovljena ustreza notranja sledljivost obdelave osebnih podatkov, ki jo ZVOP-1 nalaga upravljavcem v 5. točki prvega odstavka 24. člena kot enega izmed ukrepov za zavarovanje osebnih podatkov in ki je bistvenega pomena za odkrivanje nepooblaščenih vpogledov v osebne podatke.

Obdelava osebnih podatkov članov društva

Informacijski pooblaščenec je glede na pravne podlage, kot jih ureja Splošna uredba, zavzel stališče, da osebna privolitev ni več "osnovna in izključna" pravna podlaga za obdelavo osebnih podatkov članov društva, ampak se pri obdelavi osebnih podatkov za namen delovanja društva pravne podlage presojojo zlasti v okviru točk (b) in (f) člena 6(1).

Združevanje v društva je glede na Zakon o društvih (ZDru-1) prostovoljno in namenjeno skupnemu sodelovanju pri uresničevanju določenih skupnih interesnih ciljev, kar sovpada z značilnostmi obligacijskega razmerja pri družbeni pogodbi po OZ (skupen namen, skupno prispevanje k uresničevanju ciljev, prostovoljno oz. svobodno združevanje). Včlanitev v društvo se zato lahko obravnava kot sklenitev pogodbe, članstvo v društvu pa kot pogodbeno razmerje, saj član z včlanitvijo prevzame določene obveznosti in hkrati pridobi določene pravice glede sodelovanja v društvu (razmerje med članom in društrom ali zvezo društev je opredeljeno v aktih društva in zvezze). Glede na navedeno je podlaga za obdelave osebnih podatkov, ki so neločljivo povezane s samim članstvom v društvu in delovanjem društva, v skladu z nameni, ki so opredeljeni v temeljnem in drugih aktih društva (npr. vodenje seznama članov društva, vabiljenje članov društva na zbor članov in podobno), točka (b) člena 6(1) Splošne uredbe, ki določa, da je obdelava osebnih podatkov zakonita, če je potrebna za izvajanje pogodbe, katere pogodbena stranka je posameznik, na katerega se nanašajo osebni podatki, ali za izvajanje ukrepov na zahtevo takega posameznika pred sklenitvijo pogodbe.

Ustrezno pravno podlago za obdelavo osebnih podatkov članov društva lahko predstavlja tudi točka (f) člena 6(1) Splošne uredbe, po kateri je obdelava zakonita, če je potrebna zaradi zakonitih interesov, za katere si prizadeva upravljavec ali tretja oseba, razen kadar nad takimi interesi prevladajo interesi ali temeljne pravice in svoboščine posameznika, na katerega se nanašajo osebni podatki, ki zahtevajo varstvo osebnih podatkov, zlasti kadar je posameznik, na katerega se nanašajo osebni podatki, otrok. Bistvo konkretne podlage za obdelavo je tehtanje posega v interes, pravice in svoboščine posameznika, ki ga morajo opraviti društva kot upravljavci, poleg tega morajo posamezniku, ko se osebni podatki na tej pravni podlagi zbirajo neposredno od njega, ob zbiranju med drugim zagotoviti tudi informacije o zakonitih interesih, za katere si prizadeva upravljavec ali tretja oseba (točka (d) člena 13(1) Splošne uredbe). Informacije iz člena 13(1, 2) Splošne uredbe mora društvo posamezniku zagotoviti ob vsakem pridobivanju osebnih podatkov, ne glede na to, na kateri pravni podlagi pridobiva podatke. Društvo mora informacije skladno s členom 12(1) Splošne uredbe zagotoviti v jedrnati, pregledni, razumljivi in lahko dostopni obliki ter v jasnom in preprostem jeziku.

Osebna privolitev kot temelj za obdelavo osebnih podatkov članov društev (točka (a) člena 6(1) Splošne uredbe) bi prišla v poštev predvsem v situacijah, ko gre za obdelavo zunaj namenov, ki so v neposredni zvezi z delovanjem društva, zlasti v primeru posredovanja osebnih podatkov tretjim osebam (npr. objava na spletni strani društva). Javna objava osebnih podatkov namreč predstavlja zelo velik poseg v zasebnost posameznika, ki je redko upravičen z vidika izvajanja nalog društva (kot izvajanja pogodbe) ali kot zakoniti interes društva, ki prevlada nad pravico posameznika, zato je v takem primeru ustrezno, da društvo od posameznikov pridobi osebno privolitev, ki posameznikom v največji meri zagotavlja oblast nad njihovimi osebnimi podatki. Privolitev mora biti po Splošni uredbi konkretna, informirana in razumljiva izjava, dana z nedvoumnim pritrdilnim dejanjem in dokazljiva. Zato privolitve članov, ki so jih društva pridobila pred začetkom uporabe Splošne uredbe na način splošnega strinjanja s pravili, določenimi v aktih društva, niso več ustrezne – skladno z uvodno določbo 171 Splošne uredbe bi morala društva za vse obdelave osebnih podatkov, ki niso potrebne za izvajanje temeljnih dejavnosti društva, pridobiti nove privolitve.

Nadzor nad multinacionalnimi ponudniki sodobnih komunikacijskih storitev

Ponudniki zelo priljubljenih spletnih storitev, družbenih omrežij in komunikacijskih platform (Facebook, Google, Instagram, Twitter, WhatsApp, Viber idr.) so z uvedbo Splošne uredbe pristali pod večjim pritiskom glede svojih praks obdelave osebnih podatkov njihovih uporabnikov. Njihov poslovni model najpogosteje temelji na storitvi, ki je za uporabnika sicer brezplačna, a se monetizira s pomočjo personaliziranega in ciljanega oglaševanja, ki temelji na zbiranju ogromnih količin podatkov posameznikov, njihovi analizi, tudi s pomočjo umetne inteligence, ter predvidevanjih interesov, želja in potreb posameznikov, ki so jim prikazani zanje relevantni oglasi. Te prakse uporabe osebnih podatkov so običajnemu uporabniku storitev najpogosteje nevidne, ne zaveda se jih in je o njih pomanjkljivo obveščen, hkrati pa imajo lahko zelo velik negativen vpliv na njegovo pravico do varstva osebnih podatkov in zasebnosti. Lahko vodijo v diskriminacijo in družbeno razslojevanje. Problematika personaliziranih oglasov je postala še posebej pereča ob zadnjih razkritijih glede uporabe podatkov posameznikov za namen politične promocije pred volitvami in referendumi, in sicer na družbenem omrežju Facebook³.

Splošna uredba je organom za varstvo osebnih podatkov v EU prinesla težko pričakovana in nujno potrebna nova orodja za nadzor nad tehnološkimi velikani te vrste. Ena bistvenih novosti je širši teritorialni domet Splošne uredbe, ki jo morajo, glede na člen 3 upoštevati tudi podjetja, ki niso ustanovljena v EU, hkrati pa ponujajo storitve državljanom EU ali spremljajo njihovo vedenje. Višje varstvo pravic posameznikov zagotavljajo tudi strožje določbe glede profiliranja, obveščanja posameznikov in izvajanja njihovih pravic ter večje odgovornosti podjetij za vnaprejšnjo presojo, kakšne učinke ima lahko obdelava določenih podatkov na posameznika. Nenazadnje pa je Splošna uredba prinesla ključno novost – izboljšane možnosti operativnega sodelovanja nadzornih organov za varstvo osebnih podatkov pri nadzoru tovrstnih primerov čezmejnih praks. Sodelovanje temelji na načelu »vse na enem mestu«, ki predvideva, da postopek nadzora v čezmejnem primeru obdelave osebnih podatkov vodi t. i. vodilni organ, ki pri tem sodeluje z drugimi organi za varstvo osebnih podatkov. Le z enotnim pristopom lahko namreč nadzorni organi na ravni EU bolj učinkovito vplivajo na aktivnosti multinacionalnih ponudnikov sodobnih spletnih storitev, komunikacijskih platform in družbenih omrežij, ki so na škodo pravicam posameznikov. Konkretni primeri nadzora v teku zadevajo vprašanja zakonitosti obdelave osebnih podatkov, še posebej z vidika uporabe za namen personaliziranega oglaševanja, ustreznosti politik zasebnosti in obveščanja posameznikov o obdelavi osebnih podatkov; izvrševanja pravic posameznikov ter kršitev varstva osebnih podatkov zaradi vdorov v informacijske sisteme in pomanjkljivega zavarovanja osebnih podatkov⁴.

³ Omenjene primere je obravnaval nadzorni organ za varstvo osebnih podatkov iz Združenega kraljestva. Omrežju Facebook je izrekel gobo v višini 500.000 evrov.

⁴ Podrobnosti so objavljene v letnem poročilu Irskega nadzornega organa za varstvo osebnih podatkov. <https://www.dataprotection.ie/sites/default/files/uploads/2019-03/DPC%20Annual%20Report%202018.pdf>

3.3 DRUGI UPRAVNI POSTOPKI

3.3.1 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 78.–81. členu ZVOP-1. Informacijski pooblaščenec mora v skladu s tretjim odstavkom 80. člena ZVOP-1 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**. 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 oz. 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 oz. avtentifikacijo ali za ugotavljanje identitete oz. identifikacijo).

POMEMBNO

Informacijski pooblaščenec je leta 2018 prejel štiri vloge za izdajo dovoljenja za uvedbo biometrijskih ukrepov, izdal pa je šest odločb (tri v zadevah iz leta 2017). Dvema upravljavcema je dovolil izvajanje biometrijskih ukrepov z uporabo čitalnika prstnih odtisov, in sicer za vstop v varno sistemsko sobo, v kateri se nahaja temeljna poslovno-tehnična infrastruktura in informacijsko-komunikacijsko vozlišče, ter za vstop v komoro (t. i. »čisti prostor«), v kateri poteka priprava avtolognih celičnih zdravil. Zavrnil je vloge štirih upravljavcev, ki so žeeli biometrijske ukrepe uvesti za evidentiranje delovnega časa in/ali odklepanje vrat.

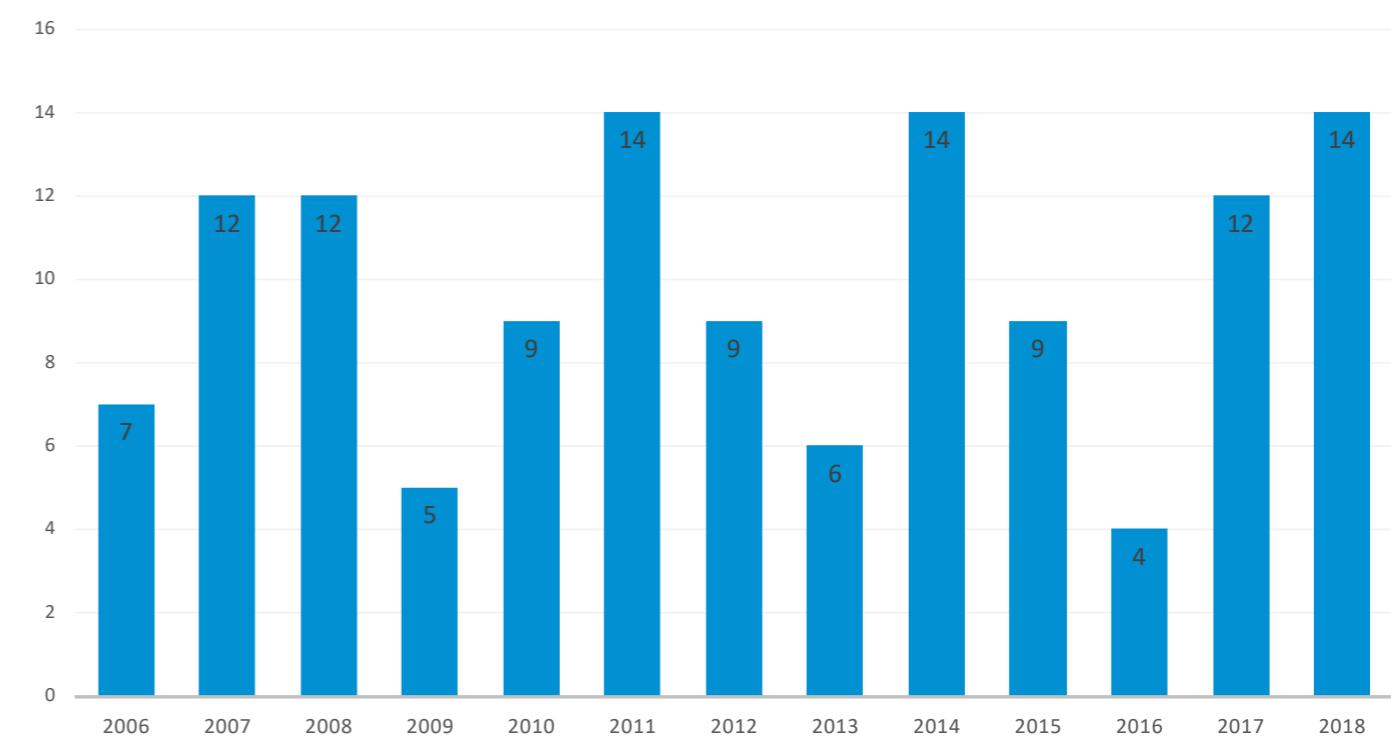
3.3.2 POVEZOVANJE JAVNIH EVIDENC

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 predstavlja obdelava in narava osebnih podatkov, ki se obdelujejo. Poleg ugotavljanja ustreznosti zavarovanja osebnih podatkov mora Informacijski pooblaščenec pri odločanju o izdaji dovoljenja za povezovanje zbirk osebnih podatkov opraviti tudi vsebinski preizkus, ali za povezovanje zbirk osebnih podatkov obstaja ustrezna zakonska podlaga. V okviru povezave zbirk osebnih podatkov se lahko posredujejo oz. obdelujejo le tiste vrste osebnih podatkov, ki jih določa veljavna zakonodaja. Povezovanje zbirk 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 več povezanih zbirk. Zbirk 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.

POMEMBNO

Informacijski pooblaščenec je leta 2018 prejel 14 vlog za pridobitev dovoljenja za povezovanje zbirk osebnih podatkov. Izdal je 10 odločb, s katerimi je upravljavcem dovolil povezovanje zbirk osebnih podatkov.

Število vlog za izdajo odločbe glede povezljivosti zbirk osebnih podatkov med letoma 2006 in 2018



Izdane odločbe glede povezovanja javnih evidenc

Upravljavec 1	Zbirka osebnih podatkov 1	Upravljavec 2	Zbirka osebnih podatkov 2	Povezovalni znak
1. Ministrstvo za infrastrukturo, Uprava RS za pomorstvo	Vpisnik morskih čolnov	Ministrstvo za notranje zadeve Finančna uprava RS	Centralni register prebivalstva Register davčnih zavezancev	EMŠO Davčna številka
Ministrstvo za infrastrukturo, Uprava RS za pomorstvo	Evidenca pooblastil pomorščakov, potrdil in overitev o priznanju, ki se izdajajo na podlagi mednarodnih konvencij	Ministrstvo za notranje zadeve	Centralni register prebivalstva	EMŠO
2. Ministrstvo za finance, Urad RS za preprečevanje pranja denarja	Evidenca podatkov o osebah in transakcijah iz 68. in 69. člena ZPPDFT-1, Evidenca o prejetih pobudah iz 99. in 100. člena ZPPDFT-1, Evidenca obvestil in informacij iz 101. in 102. člena ZPPDFT-1 ter Evidenca mednarodnih zaprosil iz 105. in 106. člena ZPPDFT-1	Ministrstvo za infrastrukturo, Uprava RS za pomorstvo	Vpisnik čolnov	EMŠO ali davčna številka
3. Študentska organizacija Slovenije	Evidenca upravičencev do subvencionirane študentske prehrane	Zavod za zdravstveno zavarovanje Slovenije	Evidenca o zavarovanih osebah obveznega zdravstvenega zavarovanja	EMŠO
4. Zavod RS za zaposlovanje	Evidenca brezposelnih oseb	Agencija RS za javnopravne evidence in storitve	Poslovni register Slovenije	EMŠO
5. Ministrstvo za obrambo	Vpisnik čolnov	Ministrstvo za infrastrukturo, Uprava RS za pomorstvo	Vpisnik čolnov	EMŠO ali davčna številka
6. Študentska organizacija Slovenije	Evidenca študentskega dela	Ministrstvo za notranje zadeve	Centralni register prebivalstva	EMŠO
7. Finančna uprava RS	Evidenca o odmeri davka na dedičnine in darila, Evidenca o odmeri davka na promet nepremičnin	Ministrstvo za okolje in prostor, Geodetska uprava RS	Register nepremičnin	EMŠO
8. Sklad kmetijskih zemljišč in gozdov RS	Evidenca o pravnih in stvarnih lastnostih nepremičnin, s katerimi gospodari	Ministrstvo za notranje zadeve	Centralni register prebivalstva	EMŠO
9. Ministrstvo za izobraževanje, znanost in šport	Evidenčni in analitski informacijski sistem visokega šolstva Republike Slovenije, Evidenca študentov in diplomantov (eVŠ – EŠD), Centralna evidenca udeležencev vzgoje in izobraževanja (CEUVIZ)	Agencija M servis, d.o.o.	Evidenca o dijakih in študentih, članih študentskega servisa	EMŠO
10. Ministrstvo za izobraževanje, znanost in šport	Evidenčni in analitski informacijski sistem visokega šolstva Republike Slovenije, Evidenca študentov in diplomantov (eVŠ – EŠD), Centralna evidenca udeležencev vzgoje in izobraževanja (CEUVIZ)	Študentski servis, d.o.o.	Evidenca o članih	EMŠO

3.3.3 PRENOS OSEBNIH PODATKOV V TRETJE DRŽAVE

PRENOSI DO 24. MAJA 2018

Skladno z določbami ZVOP-1 je bil Informacijski pooblaščenec na področju iznosa oz. prenosa osebnih podatkov v tretje države do dne 24. 5. 2018 pristojen za:

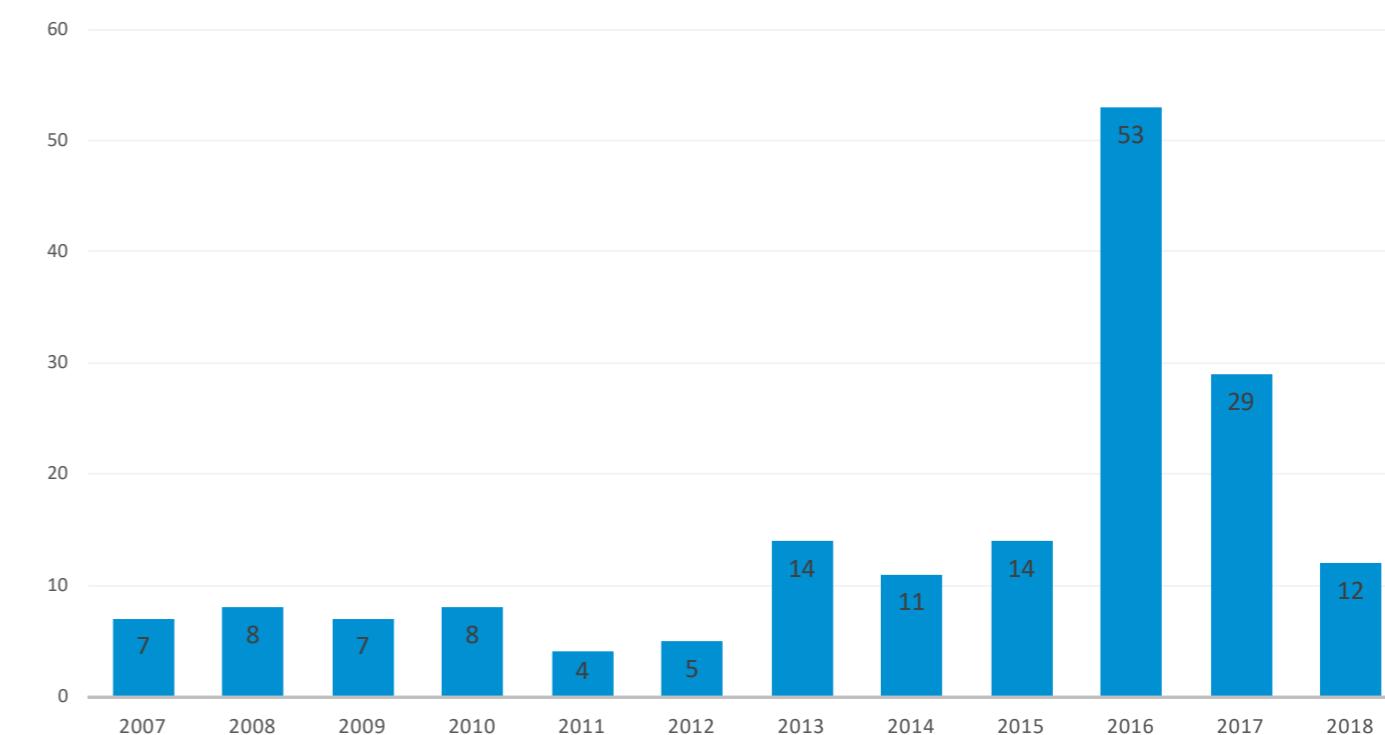
- izdajo odločb o zagotavljanju ustrezone ravni varstva osebnih podatkov v tretjih državah (63. člen);
- vodenje postopkov ugotavljanja ustrezone ravni varstva osebnih podatkov v tretjih državah na podlagi ugotovitev inšpekcijskega nadzora in drugih informacij (64. člen);
- vodenje seznama tretjih držav,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

Informacijski pooblaščenec je kot pristojni nadzorni organ za varstvo osebnih podatkov glede na določbe 7. točke prvega odstavka 70. člena ZVOP-1 v postopku odločanja o izdaji posebnega dovoljenja za iznos osebnih podatkov v tretjo državo preverjal, ali so upravljavci osebnih podatkov (izvozniki podatkov) zagotavljali ustreze postopke in ukrepe zavarovanja osebnih podatkov ter ali so v določbah pogodb ali v splošnih pogojih poslovanja navedli ustreze možnosti njihovega uresničevanja in varstva podatkov. Poleg tega je Informacijski pooblaščenec pri odločanju o izdaji posebnega dovoljenja (odločbe) glede iznosa osebnih podatkov v tretje države opravil tudi vsebinski preizkus, ali za posredovanje oz. za razkrivanje, širjenje in dajanje določenih osebnih podatkov na razpolago drugi pravni osebi obstaja ustreza pravna podlaga.

POMEMBNO

Informacijski pooblaščenec je leta 2018 prejel 12 vlog za prenos osebnih podatkov, od tega 8 vlog do dne 24. 5. 2018. Skupno je do 24. 5. izdal 12 odločb (štiri za vloge, vložene leta 2017), s katerimi je odobril prenos podatkov. Skupaj je izdal 12 odločb in z njimi desetim družbam dovolil, da osebne podatke prenašajo in jih posredujejo svojim obdelovalcem v tretjih državah. Družbe bodo podatke prenašale večinoma v ZDA in Srbijo, pa tudi v Izrael, Novo Zelandijo in Indijo. Trem družbam je dovolil, da prenašajo podatke povezanim družbam znotraj mednarodne skupine družb.

Število vlog za izdajo odločbe glede iznosa osebnih podatkov med letoma 2007 in 2018.



Sedem družb bo prenašalo osebne podatke, ki se nanašajo na zaposlene, nekatere med njimi pa tudi podatke o kandidatih za zaposlitev, štipendistih in iskalcih zaposlitev. Nadalje bodo družbe prenašale osebne podatke svojih strank, potrošnikov, poslovnih partnerjev (dobaviteljev, izvajalcev, svetovalcev), podatke, ki se nanašajo na uporabnike bančnih kartic, ter podatke pacientov in zdravstvenih delavcev.

Nameni iznosa osebnih podatkov, ki so jih navedle družbe, so uporaba raznih oblačnih storitev, upravljanje in gostovanje aplikacij za razvoj človeških virov, koriščenje podpornih storitev za digitalne platforme, uporaba sistemov za upravljanje odnosov s strankami, zagotavljanje drugih IT-storitev (npr. IT-infrastruktura).

PRENOSI PO SPLOŠNI UREDBI O VARSTVU PODATKOV

Splošna uredba ureja prenos podatkov v tretje države in v mednarodne organizacije v V. poglavju.

Prenos je dovoljen, če obstaja ena izmed naslednjih pravnih podlag:

1. Evropska komisija izda odločbo, da država, ozemlje, določen sektor v državi ali mednarodna organizacija, v katero se osebni podatki prenašajo, zagotavlja ustrezeno raven njihovega varstva (člen 45). V veljavi ostajajo tudi odločbe o zagotavljanju ustrezne ravni varstva osebnih podatkov v tretjih državah, ki jih je na podlagi 63. člena ZVOP-1 sprejel Informacijski pooblaščenec;
2. izvoznik podatkov zagotovi ustrezne zaščitne ukrepe na podlagi členov 46 in 47;
3. gre za posebne primere, ki so določeni v členu 49, v katerih so mogoča odstopanja.

POMEMBNO

Po Splošni uredbi dovoljenje Informacijskega pooblaščenca za prenos podatkov v tretje države ali mednarodne organizacije v večini primerov ni več potrebno.

V določenih primerih pa je še zmeraj treba pridobiti dovoljenje oz. odločbo glede ustreznosti zaščitnih ukrepov iz člena 46, ki predstavljajo podlago za prenos podatkov. Dovoljenje je potrebno:

- ko gre za prenos podatkov v tretjo državo na podlagi pogodbenih določil, ki jih kot ustrezne zaščitne ukrepe sama določita izvoznik in uvoznik podatkov (točka (a) člena 46(3));
- ko gre za prenos podatkov med javnimi organi na podlagi določb, ki se vstavijo v upravne dogovore (točka (b) člena 46(3));
- če se podatki prenašajo na podlagi zavezujocih poslovnih pravil, mora le-te predhodno odobriti pristojni nadzorni organ (člen 47(1)).

Informacijski pooblaščenec leta 2018 od dne 25. 5. ni izdal nobene odločbe. Izdal pa je šest sklepov, s katerimi je zaključil postopke, in sicer en sklep o ustavitvi postopka (vlagatelj je vlogo umaknil) in pet sklepov o zavrnjenju zaradi nepristojnosti. Vlagatelji so od Informacijskega pooblaščenca zahtevali, da v skladu s 63. in 64. členom ZVOP-1 ugotovi, da določene države (Srbija, Črna gora, Bosna, Egipt) zagotavljajo ustrezeno raven varstva osebnih podatkov. V skladu z določbami Splošne uredbe Informacijski pooblaščenec za to ni (več) pristojen, zato je zahteve s sklepom zavrgel.

POMEMBNO

Informacijski pooblaščenec je decembra 2018 izdal prenovljene smernice o prenosu, v katerih je podrobno predstavljena ureditev prenosov v tretje države in mednarodne organizacije po Splošni uredbi o varstvu podatkov. Smernice glede prenosa osebnih podatkov v tretje države in mednarodne organizacije so dostopne na [tej povezavi](#).

Smernice glede prenosa osebnih podatkov v tretje države in mednarodne organizacije



Smernice glede prenosa osebnih podatkov

v tretje države in mednarodne organizacije po Splošni uredbi o varstvu podatkov

3.3.4 PRAVICE POSAMEZNIKOV

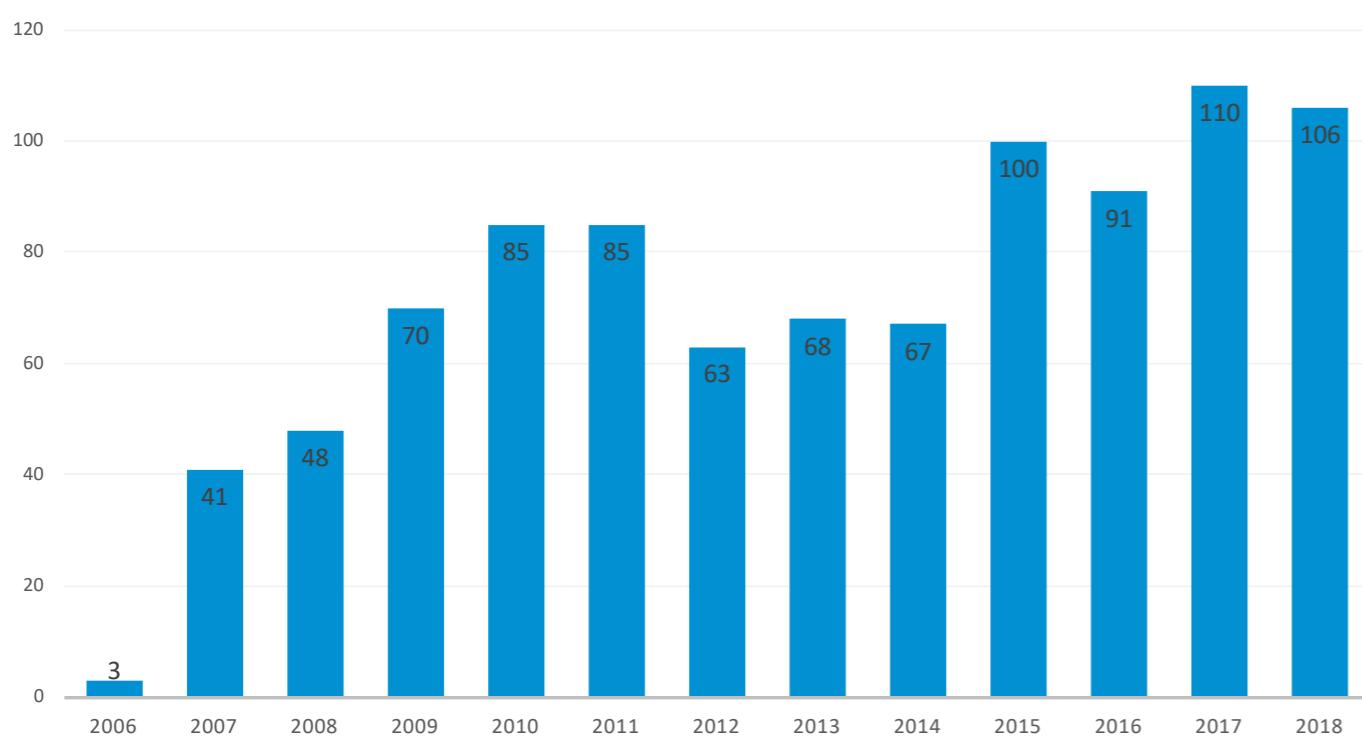
POMEMBNO

Informacijski pooblaščenec je leta 2018 prejel 106 pritožb posameznikov v zvezi s kršitvami:

- **pravice do seznanitve z lastnimi osebnimi podatki,**
- **pravice do seznanitve z lastno zdravstveno dokumentacijo in**
- **pravice do seznanitve z zdravstveno dokumentacijo s strani drugih upravičenih oseb.**

Že več let zapored je prejel več kot sto pritožb v enem letu.

Število pritožb v zvezi s pravico do seznanitve z lastnimi osebnimi podatki med letoma 2006 in 2018.



Vložene pritožbe so v 56 primerih zadevale upravljavce iz javnega sektorja (zlasti državne organe, občine in javne zavode), 50 pritožb pa se je nanašalo na upravljavce iz zasebnega sektorja (zlasti banke, zavarovalnice, operaterje elektronskih komunikacij ter druga podjetja, društva in zasebne izvajalce zdravstvene dejavnosti).

Le 16 pritožb se je nanašalo na pravico do seznanitve z zdravstveno dokumentacijo, vse preostale so se nanašale na pravico do seznanitve z lastnimi osebnimi podatki.

Pred 25. 5. 2018 je bilo vloženih 40 pritožb, po 25. 5. 2018 pa je bilo vloženih 66 pritožb, pri čemer se jih je del nanašal še na predpise, ki so se uporabljali pred 25. 5. 2018.

Informacijski pooblaščenec je v 106 pritožbenih postopkih, ki se izvajajo po določbah ZUP, izdal 19 upravnih odločb (kar je 73 % več kot leta 2017), v drugih pritožbenih postopkih pa je, po izvedenem ugotovitvenem postopku, izdal 68 sklepov, formalnih pojasnil, pozivov in predlogov za ravnanje. Večina odločb je bila za posameznike ugodilnih.

Zoper zgornje akte ni bil sprožen noben upravni spor pred Upravnim sodiščem RS.

Pravica do seznanitve z lastnimi osebnimi podatki je zagotovljena vsakemu posamezniku v tretjem odstavku 38. člena Ustave RS in v členu 15 Splošne uredbe. Postopkovna pravila so urejena v členu 11 in 12 Splošne uredbe. Za zahteve posameznikov, ki so bile pri upravljavcih vložene pred 25. 5. 2018, in za zahteve, ki se po 25. 5. 2018 nanašajo na področje preprečevanja, odkrivanja, preiskovanja in pregona kaznivih dejanj ter izvrševanja kazenskih sankcij, sta se leta 2018 uporabljala 30. in 31. člen ZVOP-1 – in se uporabljal še vedno. Po členu 15 Splošne uredbe je posameznik na zahtevo upravičen, da mu upravljavec (1) potrdi, ali se v zvezi z njim obdelujejo osebni podatki, (2) omogoči vpogled ali posreduje reprodukcijo teh osebnih podatkov, torej zagotovi dostop do njihove vsebine, in (3) če se osebni podatki posameznika pri upravljavcu res obdelujejo, tudi dodatne informacije o:

- namenu obdelave podatkov,
- vrsti podatkov,
- uporabnikih podatkov,
- obdobju hrambe podatkov,
- obstoju pravic posameznika v zvezi z njegovimi podatki,
- viru podatkov in
- obstoju avtomatiziranega sprejemanja odločitev, vključno z oblikovanjem profilov, ter informacije o razlogih zanj, pa tudi pomen in predvidene posledice take obdelave za posameznika, na katerega se osebni podatki nanašajo.

Po 30. členu ZVOP-1 je bila ureditev nekoliko drugačna, vendar bistvenih razlik v primerjavi s Splošno uredbo ni.

Glede na določbe člena 12 Splošne uredbe mora upravljavec osebnih podatkov o posameznikovi zahtevi odločiti v enem mesecu. Posredovanje osebnih podatkov in dodatnih informacij posamezniku je praviloma brezplačno. Če upravljavec posamezniku ne odgovori v predpisanim roku ali če njegovo zahtevo zavrne, lahko posameznik vloži pritožbo pri Informacijskem pooblaščencu.

Posebne pravice glede seznanitve z zdravstveno dokumentacijo po ZPacP so še:

1. pravica pacienta do seznanitve z lastno zdravstveno dokumentacijo, ki vključuje tudi pravico do pridobitve pojasnil o vsebini dokumentacije in pravico dajanja pripomb na vsebino zdravstvene dokumentacije;
2. pravica svojcev in drugih upravičenih oseb do seznanitve z zdravstveno dokumentacijo umrlega pacienta;
3. pravica določenih drugih oseb do seznanitve z zdravstveno dokumentacijo pacienta.

Tudi o teh se na pritožbeni stopnji odloča pri Informacijskemu pooblaščencu.

Spoštna uredba ureja še nekatere druge pravice posameznikov, ki se uveljavljajo na zahtevo:

1. Pravica do prenosljivosti osebnih podatkov, ki pomeni možnost, da posameznik doseže prenos osebnih podatkov, ki se obdelujejo v avtomatizirani obliki, drugemu upravljavcu na način, da se ti podatki lahko v enaki obliki vključijo oz. uporabljajo pri drugem upravljavcu. Lahko pa te podatke na enak način pridobi tudi sam.
2. Pravica do ugovora, ki pomeni, da lahko posameznik pod določenimi pogoji (npr. če se podatki obdelujejo za neposredno trženje) doseže, da upravljavec določene obdelave ne sme več izvajati.
3. Pravica do ugovora odločitvi o posamezniku (npr. o njegovih pravicah in dolžnostih), če je bila odločitev sprejeta izključno z avtomatizirano obdelavo.
4. Pravica do popravka, ki pomeni možnost, da posameznik doseže, da upravljavec izvede popravek ali dopolnitev netočnih ali nepopolnih podatkov, ki se vodijo pri njem.
5. Pravica do izbrisa, ki pomeni, da mora upravljavec pod določenimi pogoji izbrisati osebne podatke – tipični so neobstoječi pravni podlage za obdelavo podatkov, neobstoječi zakonitega namena za obdelavo podatkov in zahteva področnega predpisa, da se podatki izbrišejo.
6. Pravica do omejitve obdelave, ki omogoča popolno ali delno ter dolgoročno ali začasno blokado določene obdelave osebnih podatkov pod določenimi pogoji.

3.4 PRIPRAVA MNENJ IN POJASNIL

3.4.1 SPLOŠNA POJASNILA

Na podlagi člena 57 Splošne uredbe in 49. člena ZVOP-1 Informacijski pooblaščenec izdaja neobvezna mnenja, pojasnila in stališča o vprašanjih s področja varstva osebnih podatkov, s katerimi prispeva k ozaveščenosti upravljalcev in obdelovalcev ter širše javnosti. Leta 2018 je izdal **2.192 pisnih mnenj in napotitev na mnenja, kar predstavlja 70-odstotni porast glede na leto 2017**, ko je bilo izdanih 1.289 pisnih mnenj in napotitev. Če je posameznik zastavil vprašanje, na katerega je Informacijski pooblaščenec v preteklosti podobno že odgovoril, je prejel le napotitev na mnenje, objavljeno na spletni strani.

POMEMBNO

Na spletni strani <https://www.ip-rs.si/vop/> je objavljenih okrog 4.000 mnenj, ki so razvrščena v 48 vsebinskih področij. Uporabniki lahko brskajo za mnenji, ki so bila izdana pred veljavnostjo Splošne uredbe, ter z ločenim iskalnikom dostopajo do mnenj, ki so bila izdana po 25. 5. 2018. Informacijski pooblaščenec spodbuja svetovanje oz. posredovanje ustnih odgovorov na vprašanja, zato je v uradu vsak dan na voljo dežurni državni nadzornik, ki na vprašanja odgovarja po telefonu. Leta 2018 so državni nadzorniki sprejeli 3.230 klicev. Leta 2017 je bilo klicev 1.998, kar pomeni skoraj 62-odstotni porast števila prejetih klicev v primerjavi z letom prej. Skupno je torej Informacijski pooblaščenec svetoval 5.422 posameznikom in pravnim osebam, ki so se nanj obrnile z vprašanji s področja varstva osebnih podatkov.



2.192 mnenj

+70%



3.230 klicev

+62%

3.4.2 MNENJA NA PREDPISE

Informacijski pooblaščenec podaja mnenja na predpise skladno s točko c člena 57 Splošne uredbe, ki določa, da vsak nadzorni organ na svojem ozemlju v skladu s pravom članice svetuje nacionalnemu parlamentu, vladi ter drugim institucijam in organom o zakonodajnih in upravnih ukrepih v zvezi z varstvom pravic in svoboščin posameznikov pri obdelavi, in 48. členom ZVOP-1, ki določa, da državni nadzorni organ 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 osebne podatke.

POMEMBNO

Leta 2018 je Informacijski pooblaščenec izdal 64 mnenj na predloge sprememb zakonov ter na predloge novih zakonov in drugih predpisov. Pri tem je treba poudariti razveseljivo dejstvo, da se je število predpisov, ki prinašajo posege v zasebnost posameznikov z vidika obdelave osebnih podatkov, prvič po več letih zmanjšalo, in to občutno, saj je Informacijski pooblaščenec leta 2017 izdal skoraj enkrat več mnenj na predloge predpisov.

Informacijski pooblaščenec je leta 2018 podal mnenje, pripombe oz. je sodeloval pri pripravi naslednjih predpisov (v zvezi z nekaterimi je podal več mnenj):

- Predlog Zakona o spremembah in dopolnitvah Zakona o postopku priznavanja poklicnih kvalifikacij za opravljanje reguliranih poklicev,
- Predlog Zakona o spremembah in dopolnitvah Zakona o integriteti in preprečevanju korupcije,
- Predlog Zakona o spremembah in dopolnitvah Zakona o nalogah in pooblastilih policije,
- Predlog novega Zakona o varstvu osebnih podatkov (ZVOP-2) – pet mnenj,
- Predlog Zakona o nekaterih koncesijskih pogodbah,
- Predlog Zakona o dopolnitvah Zakona o letalstvu,
- Predlog Zakona o letalstvu,
- Predlog Pravilnika o Etični komisiji za presuditve,
- Predlog Zakona o spremembah in dopolnitvah Zakona o izvajanju rejniške dejavnosti,
- Predlog Zakona o izvajanju Uredbe (EU) o določitvi splošnega okvira za listinjenje in o vzpostavitvi posebnega okvira za enostavno, pregledno in standardizirano listinjenje,
- Predlog Uredbe o izvajanju Uredbe (EU) o izvedenih finančnih instrumentih OTC, centralnih nasprotnih strankah in rezitorijih sklenjenih poslov,
- Predlog Letnega programa statističnih raziskovanj za leto 2019,
- Predlog Zakona o kazenskem postopku (ZKP-N) (dve mnenji),
- Predlog Pravilnika o obdelavi osebnih podatkov Centra za izobraževanje v pravosodju,

- Predlog Zakona o spremembah in dopolnitvah Zakona o tujcih (dve mnenji),
- Predlog Zakona o poslovnih skrivnostih,
- 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 Pravilnika o evidenci organizacij proizvajalcev, združenj organizacij proizvajalcev in skupin proizvajalcev za skupno trženje,
- Osnutek obrazca izjave na podlagi 113. člena Zakona o urejanju prostora,
- Predlog Uredbe o izvzemu prirediteljev klasičnih iger na srečo iz izvajanja ukrepov za odkrivanje in preprečevanje pranja denarja in financiranja terorizma,
- Predlog Pravilnika o tehničnih pregledih motornih in priklopnih vozil,
- Dopustnost posredovanja podatkov o polnoletnih šolajočih se dijakih staršem,
- Spremembe in dopolnitve Poslovnika Občinskega sveta Mestne občine Koper,
- Predlog Pravilnika o dopolnitvah pravilnika o priznanju organizacij proizvajalcev in združenj organizacij proizvajalcev v sektorjih sadje in zelenjava, oljčno olje in namizne oljke ter hmelj,
- Predlog Uredbe o izvajanju uredbe 2016/1012/EU o zootehniških in genealoških pogojih za rejo, trgovino s čistopasemskimi plemenskimi živalmi, hibridnimi plemenskimi prašiči in njihovim zarodnim materialom ter za njihov vstop v Unijo,
- Predlog Uredbe o podatkih v evidenci vrednotenja,
- Predlog Pravilnika o pripravištvu in strokovnih izpitih zdravstvenih delavcev in zdravstvenih sodelavcev na področju zdravstvene dejavnosti,
- Predlog sprememb Zakona o prevozih v cestnem prometu (dve mnenji),
- Predlog Pravilnika o enotnem informacijskem sistemu na področju javnega naročanja,
- Osnutek Odredbe o določitvi programa strokovnega usposabljanja in programa obdobnega izpopolnjevanja nadzornika na smučišču,
- Predlog Zakona o spremembah in dopolnitvah Zakona o visokem šolstvu,
- Predlog Pravilnika o priznavanju organizacij proizvajalcev in združenj organizacij proizvajalcev v sektorjih sadje in zelenjava, oljčno olje in namizne oljke ter hmelj,
- Osnutek Odredbe o določitvi programa strokovnega usposabljanja za varnostnika nadzornika,
- Predlog Pravilnika o opravljanju overitev v mednarodnem prometu,
- Predlog Zakona o znanstveno-raziskovalni dejavnosti,
- Spremembe Zakona o centralnem kreditnem registru z namenom automatiziranega dostopa članov do sistema SISBON, povezovanja zbirk ter avtomatiziranega odločanja o odobritvi kreditov potrošnikom,
- Dopolnjen predlog novele Zakona o zavarovalništvu,

- Predlog sprememb Zakona o štipendirjanju,
- Predlog Zakona o socialnem vključevanju invalidov,
- Osnutek Zakona o znanstveno-raziskovalni dejavnosti.
- Predlog Uredbe o izvedbi ukrepov kmetijske politike za leto 2018,
- Predlog sprememb Pravil sistema izmenjave informacij o zadolženosti fizičnih oseb – SIS BON na podlagi drugega odstavka 26. člena Zakona o centralnem kreditnem registru,
- Predlog Pravilnika o strokovni komisiji za ukrep Sodelovanje v okviru Programa razvoja podeželja Republike Slovenije za obdobje 2014–2020,
- Predlog Zakona o konzularni zaščiti,
- Predlog Zakona o spremembah in dopolnitvah Zakona o zaščiti prič (ZZPrič-C),
- Mnenje glede podatkov o lokaciji kličočega v povezavi s pripravo Pravilnika o kakovosti storitve za enotno evropsko telefonsko številko za klice v sili 112 in številko policije 113,
- Predlogi za vključitev ureditve zbiranja podatkov o etnični pripadnosti v okviru sprememb Zakona o romski skupnosti,
- Predlog Zakona o spremembah Zakona o upravljavcih alternativnih investicijskih skladov,
- Sporazum o zaposlovanju državljanov Republike Srbije v Republiki Sloveniji,
- Dopolnjen predlog za spremembe in dopolnitve Zakona o zavarovalništvu,
- Predlog Zakona o izvajajujoči Uredbe (EU) o dokumentih s ključnimi informacijami o paketnih naložbenih produktih za male vlagatelje in zavarovalnih naložbenih produktih,
- Predlog Zakona o spremembah Zakona o investicijskih skladih in družbah za upravljanje,
- Predlog novega Zakona o varnosti v železniškem prometu,
- Predlog Uredbe Sveta o pristojnosti, priznavanju in izvrševanju odločb v zakonskih sporih v zvezi s starševsko odgovornostjo ter mednarodni ugrabitvi otrok,
- Predlog novele Zakona o osebni asistenci,
- Osnutek Pravilnika o izvrševanju probacijskih nalog in o izvrševanju dela v splošno korist,
- Pravilnik o poravnavanju v kazenskih zadevah.

3.5 SKLADNOST IN PREVENTIVA

Splošna uredba daje veliko težo novemu načelu odgovornosti (angl. accountability) in predvideva nabor ukrepov in mehanizmov, ki jih morajo izvajati upravljavci in obdelovalci s ciljem zagotavljanja skladnosti. Informacijski pooblaščenec zato vedno več pozornosti namenja preventivnemu delovanju, saj se je treba zavedati, da zgolj inšpekcijski nadzor skladnosti ne zagotavlja, temveč bi moral biti zadnji ukrep za njeno zagotovitev. Zavezancem, ki zakonodaje ne želijo kršiti, morajo biti na razpolago ustrezne informacije, orodja in mehanizmi, s katerimi lahko zagotovijo spoštovanje pravil.

POMEMBNO

Informacijski pooblaščenec je leta 2018 okreplil delovno področje, ki skrbi za področje skladnosti, preventive in informacijskih tehnologij; na tem področju delujejo strokovnjaki s pravnimi, tehnoškimi in komunikološkimi znanji, ki so potrebna za ustrezeno pripravo gradiv in komunikacijo z zavezanci.

3.5.1. OBVEZNOSTI UPRAVLJAVCEV

V sklop mehanizmov za skladnost in upoštevanje načela odgovornosti sodijo naslednji mehanizmi, ki ji določa Splošna uredba:

- upoštevanje načela vgrajenega in privzetega varstva podatkov,
- ustreznost ureditve v primerih skupnega upravljanja,
- ustrezna ureditev pogodbenih razmerij s (pogodbenimi) obdelovalci,
- evidentiranje dejavnosti obdelave,
- zagotavljanje organizacijskih in tehničnih postopkov in ukrepov za varnost,
- obveznost poročanja o kršitvah varnosti podatkov,
- izvajanje ocen učinka glede varstva osebnih podatkov,
- imenovanje pooblaščenih oseb za varstvo osebnih podatkov,
- kodeksi ravnanja in
- certifikacija.

Z namenom ustreznega informiranja zavezancev in učinkovitega izvajanja teh obveznosti je Informacijski pooblaščenec vzpostavil številne postopke ter pripravil gradiva, kot pojasnjuje v nadaljevanju.

3.5.2 POGODBENA OBDELAVA

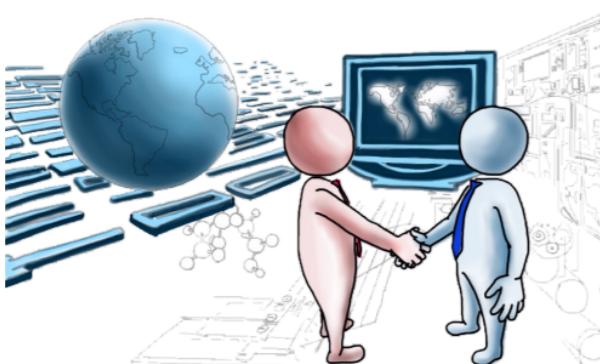
Upravljavci zbirk osebnih podatkov številne obdelave osebnih podatkov zaupajo pogodbenim obdelovalcem, kar velja tudi za največje državne registre in druge velike zbirke osebnih podatkov. Velik izziv predstavljajo tudi nove oblike izvajanja informacijskih storitev, ki so po naravi globalne in veliko bolj fluidne, kot to predvidevajo naši zakonski okviri, npr. računalništvo v oblaku, kjer gre običajno za pogodbeno obdelavo osebnih podatkov, pogodbeni partnerji so velika multinacionalna podjetja, osebni podatki pa se nahajajo na (pogosto) neznanih lokacijah. Med klasične pogodbene obdelovalce sodijo računovodski servisi, IT-vzdrževanje sistemov z osebnimi podatki, oglaševalske storitve in klicni centri, storitve hrambe, arhiviranja in uničenja podatkov. Splošna uredba v členu 28 vsebuje več zahtev glede ustrezne ureditve pogodbene obdelave, med drugim:

- natančnejšo opredelitev vsebine, obsega, namenov in trajanja pogodbene obdelave,
- ureditev pravil glede najemanja storitev podobdelovalcev,
- natančnejšo ureditev vidikov varnosti ter obveznosti in pravic upravljavca.

POMEMBNO

Informacijski pooblaščenec je v pomoč upravljavcem izdal smernice o pogodbeni obdelavi, v katerih z mnogimi praktičnimi primeri pojasnjuje, kaj vse sodi med pogodbeno obdelavo, kakšne so obveznosti upravljavca osebnih podatkov in njegovih pogodbenih obdelovalcev, navaja pasti in priporočila za zakonsko skladno ureditev zunanjega izvajanja storitev, ki vključuje osebne podatke.

Smernice o pogodbeni obdelavi osebnih podatkov



Smernice Informacijskega pooblaščenca

o (pogodbeni) obdelavi osebnih podatkov

3.5.3 EVIDENCE OBDELAV

Splošna uredba ohranja dolžnost vestnega evidentiranja obdelave osebnih podatkov v zbirkah osebnih podatkov. Zavezanci vodijo zbirke osebnih podatkov o zaposlenih, strankah, uporabnikih in drugih kategorijah posameznikov, število zbirk pa v večjih podjetjih in državnih organih presega število 50. Med pogosto spregledanimi zbirkami osebnih podatkov so podatki o zaposlenih, ki nastajajo ob uporabi službenih sredstev (interneta, e-pošte, tiskalnikov ipd.). **Celovit popis zbirk osebnih podatkov je prvi in najpomembnejši korak k zagotavljanju skladnosti, zavezanci pa morajo za vsako zbirko osebnih podatkov natančno opredeliti vsebino, pravne podlage, roke hrambe, namene uporabe podatkov in druge pomembne elemente.** Splošna uredba je ukinila dolžnost prijave zbirk v register zbirk pri Informacijskem pooblaščencu, a je po drugi strani obveznost popisa zbirk razširila tudi na (pogodbene) obdelovalce.

POMEMBNO

Informacijski pooblaščenec je v pomoč zavezancem na spletni strani objavil opis dolžnosti z razlago in navodili. Pripravil je tudi dva vzorca evidenc dejavnosti obdelave (obrazec za upravljavce in obrazec za obdelovalce), s katerim lahko zavezanci enostavno in učinkovito popišejo svoje zbirke.

3.5.4 PRIJAVA KRŠITEV VARNOSTI OSEBNIH PODATKOV

Splošna uredba uvaja dolžnost obveščanja nadzornega organa (Informacijskega pooblaščenca) o zaznanih krštvah varnosti osebnih podatkov, če je verjetno, da bi bile s kršitvijo ogrožene pravice in svoboščine posameznikov. **Obvestilo je treba podati takoj po zaznani kršitvi, najkasneje pa v 72 urah.** Kadar je verjetno, da kršitev varnosti osebnih podatkov povzroči veliko tveganje za pravice in svoboščine posameznikov, mora upravljavec kršitev sporočiti tudi posamezniku, na katerega se osebni podatki nanašajo. V primeru hudih kršitev lahko Informacijski pooblaščenec zavezancu naloži, da mora o kršitvi obvestiti tudi prizadete posameznike. Kršitve varnosti osebnih podatkov so v praksi lahko:

- dostop s strani nepooblaščene osebe,
- posredovanje osebnih podatkov nepravemu naslovniku,
- izguba ali kraja računalniške opreme, ki vsebuje osebne podatke,
- nepooblaščeno uničenje baz z osebnimi podatki,
- sprememba osebnih podatkov brez potrebnega dovoljenja,
- izguba dostopa do osebnih podatkov (izguba gesla; izguba opreme, ki omogoča dešifriranje; nepooblaščena namestitev šifrirnega programa, ki onemogoča dostop do podatkov, t. i. izsiljevalski virus).

Prijava kršitev varnosti glede na:

Informacijski pooblaščenec je v pomoč zavezancem na spletni strani opisal njihove dolžnosti glede prijav kršitev varnosti. Priporočljivo je, da imajo vnaprej vzpostavljen (in dokumentiran) učinkovit sistem za zaznavanje in sporočanje kršitev za zagotovitev skladnosti in preprečevanje negativnih posledic za posamezni ter odvrnitev nepotrebnih sankcij zaradi kršitve obveznosti uradnega obveščanja.

POMEMBNO

Informacijski pooblaščenec je zasnoval ustrezен postopek za poročanje ter odprl namenski poštni predal (prijava-krsitev@ip-rs.si). Pripravljena so bila tudi interna navodila za obravnavo prejetih obvestil (vključno s čezmejnimi primeri), na ravni EU pa je bil sprejet vzorec obrazca za poročanje o krštvah varnosti, ki je dostopen na spletni strani Informacijskega pooblaščenca.

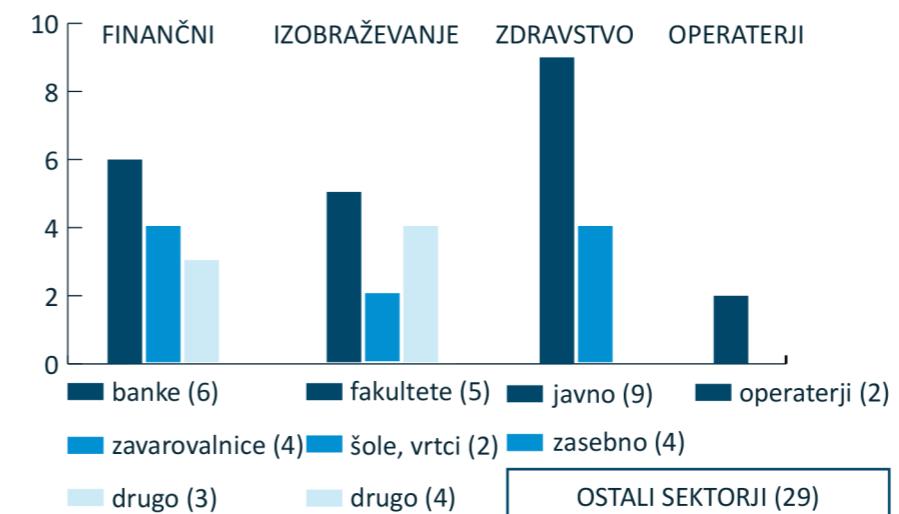
Statistika prijav kršitev varnosti po členu 33 Splošne uredbe

Informacijski pooblaščenec je leta 2018 prejel 68 uradnih obvestil o kršitvi varnosti osebnih podatkov, ki so jih poslali upravljavci osebnih podatkov. Vlaganje takšnih uradnih obvestil o kršitvi varnosti osebnih podatkov, t. i. »samoprijav«, je novost, ki jo upravljavcem in obdelovalcem osebnih podatkov nalaga člen 33 Splošne uredbe.

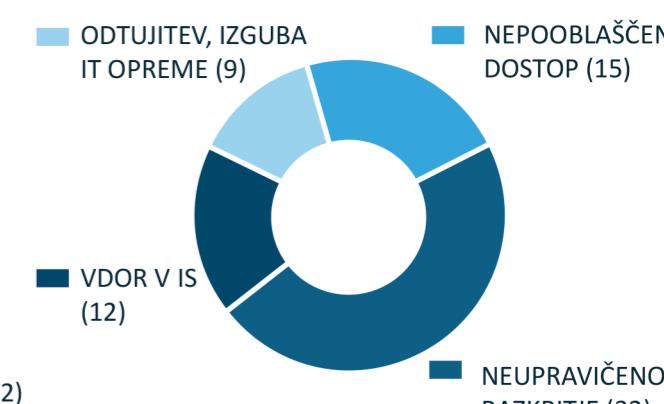


V letu 2018 je bilo prejetih 68 prijav kršitev varnosti (t. i. samoprijav)

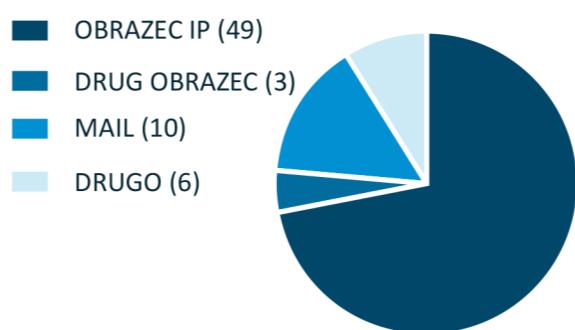
Sektor



Vrsto kršitve



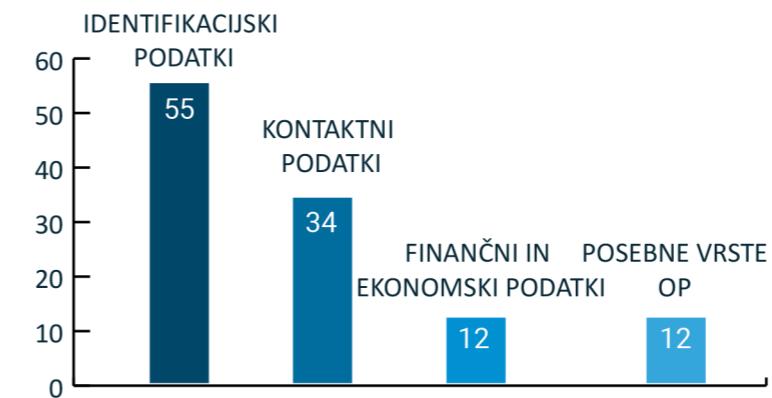
Način prijave



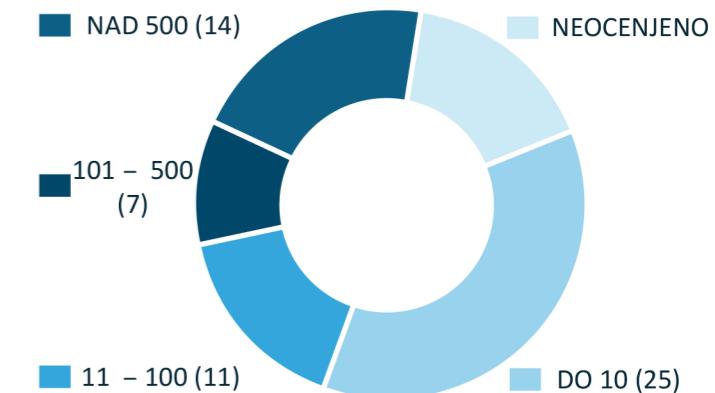
Tip kršitve



Vrste osebnih podatkov



Število prizadetih posameznikov



Prijavljenih je bilo 68 kršitev varnosti, pri čemer je lahko v sklopu ene prijave več vrst in tipov kršitev.

3.5.5 OCENE UČINKOV NA VARSTVO OSEBNIH PODATKOV

Ocene učinkov v zvezi z varstvom podatkov (angl. Data Protection Impact Assessment; DPIA), kot jih opredeljuje člen 35 Splošne uredbe, predstavljajo enega ključnih konceptov v okviru načela odgovornosti. Ocene učinkov v zvezi z varstvom osebnih podatkov so orodje za identifikacijo, analizo in zmanjševanje tveganj glede nezakonitih ravnanj z osebnimi podatki, do katerih lahko pride pri določenem projektu, sistemu ali uporabi tehnologije (npr. uvajanje kluba zvestobe, izvedba velike nagradne akcije, predlog novega policijskega pooblastila za nadzor državljanov). Poenostavljeno povedano gre za **vnaprejšnje ugotavljanje, kaj bi lahko šlo narobe z vidika varstva osebnih podatkov ter za vnaprejšnjo opredelitev ukrepov za zmanjšanje teh tveganj**. Pravočasno in celovito izvedene ocene učinkov lahko zavezancem prihranijo nepotrebne in drage popravljalne ukrepe, stroške zaradi izrečenih kazni in izgubljeno zaupanje posameznikov.

Upravljavci morajo izvesti oceno učinkov, kadar je možno, da bi določena vrsta obdelave povzročila veliko tveganje za pravice in svoboščine posameznikov, ocena učinka pa obsega:

- sistematičen opis dejanj in namenov obdelave, kadar je ustrezno pa tudi zakonitih interesov, za katere si upravljavci prizadevajo;
- oceno potrebnosti in sorazmernosti dejanj obdelave glede na njihov namen;
- oceno tveganj za posameznike, na katere se osebni podatki nanašajo;
- ukrepe za obravnavanje tveganj, vključno z zaščitnimi ukrepi, varnostne ukrepe ter mehanizme za zagotavljanje varstva osebnih podatkov.

Za oceno tveganj je treba ugotoviti tako verjetnost kot resnost tveganj za pravice in svoboščine posameznika. V pripravo ocen učinka je priporočljivo vključiti tudi pooblaščeno osebo za varstvo podatkov in, če se oceni kot primerno, se za mnenje zaprosi tudi relevantna strokovna združenja, zbornice, strokovnjake itd.

POMEMBNO

Informacijski pooblaščenec je za zavezance na spletni strani objavil **podrobna pojasnila in praktične smernice, kako izvesti oceno učinka**, in sicer s primerom metodologije, priporočili in številnimi primeri. Informacijski pooblaščenec je sprejel **seznam vrst obdelav osebnih podatkov, ki terjajo izvedbo ocene učinka**, ter jih potrdil pri Evropskem odboru za varstvo podatkov.

Smernice Ocene učinkov na varstvo podatkov



OCENE UČINKOV NA VARSTVO PODATKOV

Smernice Informacijskega pooblaščenca



V primeru, da izvedena ocena učinkov glede varstva osebnih podatkov identificira nesprejemljivo visoka tveganja, mora zavezanci opraviti predhodno posvetovanje z nadzornim organom. Po Splošni uredbi nadzorni organ v osmih tednih po prejemu zahteve za posvetovanje pisno svetuje upravljavcu, kadar je ustrezno, pa tudi obdelovalcu, in lahko uporabi katero koli pooblastilo iz člena 58 Splošne uredbe. To obdobje se lahko ob upoštevanju kompleksnosti predvidene obdelave podaljša za nadaljnjih šest tednov.

Informacijski pooblaščenec je kmalu po začetku veljave Splošne uredbe pričel prejemati zahteve zavezancev za predhodno posvetovanje. Nanašale so se na:

- vzpostavitev imenika uporabnikov sistema takojšnjih plačil,
- skladnost informacijskega sistema inšpektorata s predpisi o varovanju osebnih podatkov,
- sistem za slednje poštnih pošiljk,
- sistem za slednje zaposlenim s pomočjo naprav GPS,
- obdelave osebnih podatkov na področju distribucije električne energije,
- razširitev obdelave podatkov v klubu zvestobe.

V prejetih ocenah učinka so bile pogosto zapostavljene zlasti pravice posameznika in dolžnosti upravljalca po Splošni uredbi (npr. tveganja v zvezi z najemanjem pogodbenih obdelovalcev), pogosto je bilo tudi podcenjevanje resnosti uresničitve določenih tveganj.

POMEMBNO

Informacijski pooblaščenec je leta 2018 podal šest mnenj na prejete ocene učinka v zvezi z varstvom podatkov.

3.5.6 POOBLAŠČENE OSEBE ZA VARSTVO PODATKOV

Določitev pooblaščenih oseb za varstvo osebnih podatkov (angl. Data Protection Officer; DPO) je prav gotovo ena najodmevnnejših novosti, ki jih je prinesla Splošna uredba. Pooblaščena oseba naj bi izvajala svetovalne in nadzorne naloge na področju varstva osebnih podatkov. Obveznost imenovanja pooblaščene osebe ni vezana na število zaposlenih v podjetju – Splošna uredba določa, da morajo pooblaščeno osebo imenovati organi v javnem sektorju ter zavezanci, katerih temeljne dejavnosti 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 (npr. banke, zavarovalnice, trgovci s klubni zvestobo in operatorji elektronskih komunikacij), ali če temeljne dejavnosti upravljalca ali obdelovalca zajemajo obsežno obdelavo posebnih vrst podatkov ter osebnih podatkov v zvezi s kazenskimi obsodbami in prekrški iz člena 10 (npr. zdravstvene institucije in prekrškovni organi). **Pooblaščena oseba deluje kot notranji revizor za varstvo osebnih podatkov, njene glavne naloge so spremljanje skladnosti, svetovanje upravljavcem in obdelovalcem o njihovih obveznostih, izobraževanje in ozaveščanje zaposlenih ter svetovanje glede izvedbe ocene učinka v zvezi z varstvom podatkov.** Pooblaščena oseba je kontaktna točka za nadzorni organ in mora biti dostopna posameznikom. Pooblaščena oseba mora biti neodvisna, pravočasno vključena v vse zadeve v zvezi z varstvom osebnih podatkov, aktivno jo mora podpirati višje vodstvo, imeti mora strokovno znanje o nacionalni in evropski zakonodaji in praksi na področju varstva podatkov, poznati pa mora tudi poslovne procese v podjetju oz. organizaciji.

Informacijski pooblaščenec je leta 2018 izvedel številne aktivnosti v zvezi s pooblaščenimi osebami:

- pripravil je [podrobna pojasnila](#) s povezavami na uporabna gradiva na svoji spletni strani,
- pripravil in objavil [obrazec za imenovanje pooblaščenih oseb](#),
- vzpostavil interni postopek za obravnavo in vodenje prejetih imenovanj s potrdilom o imenovanju ter opozorilom v primeru očitnega konflikta interesov,
- izdal [priporočila glede delovanja pooblaščene osebe](#) za varstvo podatkov z vzorčnim primerom letnega delovnega načrta pooblaščene osebe.

POMEMBNO

Do konca leta 2018 je pooblaščeno osebo prijavilo 1920 zavezancev, predstavniki Informacijskega pooblaščenca pa so o njihovih dolžnostih, položaju in imenovanju večkrat predaval na javnih dogodkih. Informacijski pooblaščenec je kot zavezanc tudi sam imenoval pooblaščeno osebo ter vzpostavil namenski elektronski predal dpo@ip-rs.si.

3.5.7 KODEKSI RAVNANJA IN POTRJEVANJE

Splošna uredba vsebuje tudi nekatere prostovoljne mehanizme, kot sta potrjevanje kodeksov ravnanja in certifikacija.

Združenja, zbornice, zveze in druga telesa, ki predstavljajo vrste upravljalcev ali obdelovalcev, lahko pripravijo kodekse ravnanja oz. takšne kodekse spremenijo ali razširijo z namenom podrobnejše obrazložiti uporabo Splošne uredbe (na primer glede zbiranja osebnih podatkov, ustreznih načinov informiranja in pridobivanja privolitve itd.). Združenja, ki nameravajo pripraviti kodeks ravnanja oz. spremeniti ali razširiti veljavni kodeks, Informacijskemu pooblaščencu predložijo osnutek kodeksa, spremembo ali razširitev. Informacijski pooblaščenec poda mnenje, ali je osnutek kodeksa, sprememba ali razširitev skladna s Splošno uredbo, in osnutek potrdi, če oceni, da zagotavlja zadostne in ustrezne zaščitne ukrepe.

POMEMBNO

Leta 2018 je Informacijski pooblaščenec prejel samo en osnutek kodeksa, ki še ni bil primeren za potrditev. Informacijski pooblaščenec ugotavlja, da bi združenja, zbornice, zveze in podobna telesa v pripravo kodeksov lahko vložila več energije, saj bi tako razbremenila svoje člane in zagotovila enotno, predvsem pa s strani nadzornega organa potrjeno zakonito prakso, postopke oz. delovanje. Zagotavljanje skladnosti je učinkovitejše na ravni zvez kot takrat, kadar je odvisno od angažiranosti vsakega posameznega člana ali članice, zato Informacijski pooblaščenec upa, da bodo zavezanci v bodoče prepoznali koristi kodeksov.

Spološna uredba prinaša tudi možnost certifikacije, ki pa bo predhodno terjala razvoj ustreznih sistemov za akreditacijo in certifikacijo; aktivnosti še potekajo na evropskem nivoju, zato certifikacija leta 2018 še ni bila mogoča v nobeni državi članici. Po sprejemu akreditacijskih in certifikacijskih shem bodo zavezanci svoje dejavnosti obdelave lahko predložili v presojo ustreznemu certifikacijskemu organu, ki jim bo po uspešno prestani presoji izdal certifikat za obdobje treh let z možnostjo podaljšanja. Certifikacija naj bi bila namenjena dvigu zaupanja pri strankah. Udeležba bo prostovoljna, finančne vidike certifikacije pa naj bi določal trg glede na povpraševanje in ponudbo.

3.5.8 AKTIVNOSTI IZOBRAŽEVANJA IN OZAVEŠČANJA

Informacijski pooblaščenec je leta 2018 bistveno okreplil aktivnosti na področju izobraževanja in ozaveščanja. V ta namen uporablja širok instrumentarij glede na tematsko področje, ciljne javnosti in komunikacijske pristope, vanj pa poleg splošne komunikacije z novinarji sodijo:

- spletno mesto Informacijskega pooblaščenca (www.ip-rs.si),
- priprava gradiv,
- organizacija in izvedba dogodkov,
- sodelovanje z drugimi organizacijami,
- sodelovanje v različnih projektih,
- prisotnost na družbenih omrežjih.

Informacijski pooblaščenec je leta 2018 korenito posodobil [svoje spletno mesto](#), ki predstavlja ključno točko za komunikacijo z javnostmi. Ažurno so bile objavljene novosti ob sprejemu Splošne uredbe, opisana ključna področja uredbe, izvedena sta bila vsebinski pregled in prenova vsebinskih področij zaradi sprejema Splošne uredbe. Na spletnem mestu je Pooblaščenec sproti objavljal novosti, nova gradiva, obiskovalci strani se lahko prijavijo na e-novice.

Pooblaščenec je leta 2018 izdal več različnih gradiv. Poleg mnenj med najpomembnejše sodijo smernice – izdane so bile naslednje:

- [smernice o pogodbni obdelavi](#),
- [smernice o ocenah učinkov na varstvo osebnih podatkov](#),
- [smernice o prenosu osebnih podatkov v tretje države in mednarodne organizacije](#),
- [smernice Informacijskega pooblaščenca za oblikovanje izjave o varstvu osebnih podatkov na spletnih straneh](#),
- [kodeks obnašanja pri zbiranju osebnih podatkov](#),
- [smernice Informirani potrošniki – komu dajemo katere osebne podatke in zakaj](#).

Pripravljeni so bili obrazci v pomoč zavezancem, in sicer:

- [Vzorec obrazca za evidentiranje dejavnosti obdelave po členu 30 Splošne uredbe o varstvu podatkov za upravljavce](#),
- [Vzorec obrazca za evidentiranje dejavnosti obdelave po členu 30 Splošne uredbe o varstvu podatkov za obdelovalce](#),
- [Obrazec za informiranje posameznikov po členu 13 Splošne uredbe o varstvu podatkov](#),
- [Obrazec za informiranje posameznikov po členu 14 Splošne uredbe o varstvu podatkov](#),
- [priporočila informacijskega pooblaščenca glede delovanja pooblaščene osebe za varstvo osebnih podatkov z vzorčnim primerov letnega delovnega načrta pooblaščene osebe](#),
- [Obrazec za imenovanje pooblaščene osebe za varstvo osebnih podatkov \(člen 37 Splošne uredbe o varstvu podatkov\)](#),
- [Obrazec za uradno obvestilo o kršitvi varnosti osebnih podatkov \(člen 33 Splošne uredbe o varstvu podatkov\)](#).

Novost preteklega leta so infografike, ki posamezna tematska področja, kljub temu da gre za kompleksne teme, predstavijo na enostaven in učinkovit način:

- [pravne podlage za javni sektor](#),
- [pravne podlage za zasebni sektor z veljavno privolitvijo](#),
- [neposredno trženje](#).

Informacijski pooblaščenec je ob evropskem dnevu varstva osebnih podatkov organiziral poseben dogodek na temo novosti Splošne uredbe, na katerem so bila izvedena tematska predavanja o najbolj perečih temah. Že tradicionalno je bila podeljena posebna nagrada za ambasadorja zasebnosti, podeljena so bila tudi priznanja prejemnikom mednarodnega certifikata za informacijsko varnost po standardu ISO/EIC 27001:2013.



Nagrado za ambasadorja zasebnosti za leto 2017 je prejel ICS – Inštitut za korporativne varnostne študije, in sicer za izvedbo številnih aktivnosti na področju informacijske varnosti, ki predstavlja enega od temeljev ustreznega varstva osebnih podatkov. Nagrjenec že vrsto let združuje priznane varnostne strokovnjake na področju informacijske in korporativne varnosti ter skrbi za njihova redna srečanja, dodatna izobraževanja, izmenjavo izkušenj in znanj.

POMEMBNO

Informacijski pooblaščenec je leta 2018 o novostih Splošne uredbe izvedel 109 pro bono predavanj različnim zbornicam in združenjem v javnem in zasebnem sektorju ter na konferencah in seminarjih.

Informacijski pooblaščenec je konec leta 2018 javnosti predstavil evropski projekt RAPiD.Si (Raising Awareness on Data Protection and the GDPR in Slovenia), katerega glavni namen je izobraževanje in ozaveščanje manjših in srednje velikih podjetij ter posameznikov o reformi zakonodajnega okvira s področja varstva osebnih podatkov. Projekt RAPiD.Si je sofinanciran s strani Evropske unije v okviru Splošnega programa za pravice, enakost in državljanstvo 2014–2020 in bo trajal do septembra 2020.

POMEMBNO

Glavni cilji evropskega projekta RAPiD.Si so: podjetjem omogočiti dostop do informacij in uporabnih orodij, ki pripomorejo k prenosu zakonskih zahtev v prakso, ter opolnomočiti posamezni, da uresničujejo svoje pravice s področja varstva osebnih podatkov, ki jih daje zakonodaja.

V sklopu projekta je bila postavljena nova spletna stran www.upravlavec.si, ki odgovarja na najpogostejsa vprašanja, s katerimi se v praksi srečujejo predvsem obrtniki in majhna podjetja. Na spletni strani so na voljo pojasnila in konkretni napotki, kako zadostiti zakonskim zahtevam s področja varstva osebnih podatkov, pa tudi neobvezujoči obrazci, ki so podjetjem lahko v pomoč. Ena izmed projektnih aktivnosti, namenjena majhnim podjetjem, je tudi **telefonsko svetovanje na brezplačni številki 080 29 00**. Vsak delovni dan do novembra 2019 bodo podjetjem svetovali strokovni sodelavci Informacijskega pooblaščenca. V naslednjih dveh letih bo Informacijski pooblaščenec v sodelovanju z Obrtno-podjetniško zbornico Slovenije in Gospodarsko zbornico Slovenije izvedel **20 brezplačnih predavanj**.

Aktivnosti projekta RAPiD.Si za majhna in srednje velika podjetja

Aktivnosti projekta RAPiD.Si za posamezni

WWW.UPRAVLJAVEC.SI

**VARSTVO OSEBNIH PODATKOV
ZA MAJHNA PODJETJA**

Kaj zahteva Splošna uredba o varstvu podatkov od majhnih in srednje velikih podjetij? Razlage, obrazci, akcijski načrt na strani www.upravlavec.si

080 29 00

Brezplačno telefonsko svetovanje za majhna podjetja vsak delovnik od 8.30 do 12.30.

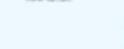
Mesečne e-novičke: nasveti o neposrednem trženju, pogodbeni obdelavi, obveščanju posameznikov itd.

20 brezplačnih predavanj po Sloveniji. Lokacije in datumi bodo objavljeni na strani www.upravlavec.si

Aktivnosti ozaveščanja malih in srednjih velikih podjetij o reformi zakonodajnega okvira s področja varstva osebnih podatkov so nastale v sklopu projekta RAPiD.Si.



Projekt sofinanira Evropska unija.



Projekt izvaja Informacijski pooblaščenec.

TI ODLOČAŠ O SVOJIH OSEBNIH PODATKIH!

Posamezniki imamo pravico do dostopa, popravka, izbrisala, omejitve obdelave, ugovora in prenosljivosti osebnih podatkov.

1 WWW.TIODLOCAS.SI

Na spletni strani najdete **podrobne razlage**, konkretné primere in navodila, kako uveljavljate svoje pravice. Rešite tudi kviz in preverite, kako dobro poznate svoje pravice.

2 FACEBOOK STRAN
[INFORMACIJSKI POOBLAŠČENEC](http://INFORMACIJSKI.POOBLAŠČENEC)

Na Facebook strani Informacijskega pooblaščenca (@informacijski.pooblaščenec) spremljajte nasvete, kako zaščitite svojo zasebnost in uveljavljate svoje pravice.

3 REVIIA ZPTEST

V sodelovanju z Zvezo potrošnikov Slovenije bo v reviji ZPTest občasna posebna rubrika namenjena pravicam s področja varstva osebnih podatkov posameznikov.

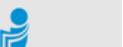


ZVEZA
POTROŠNIKOV
SLOVENIJE

Aktivnosti ozaveščanja posameznikov o njihovih pravicah s področja varstva osebnih podatkov so nastale v sklopu projekta RAPiD.Si.



Projekt sofinanira Evropska unija.



Projekt izvaja Informacijski pooblaščenec.



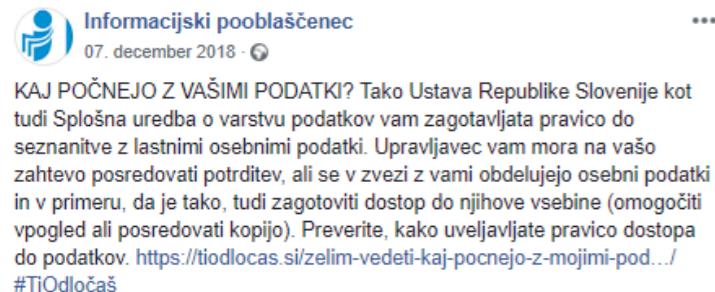
Projekt RAPiD.Si je namenjen ozaveščanju majhnih in srednje velikih podjetij o reformi zakonodajnega okvira s področja varstva osebnih podatkov kot tudi izobraževanja posameznikov glede uveljavljanja njihov pravic. Projekt je sofinanciran s strani Evropske unije v okviru Splošnega programa za pravice, enakost in državljanstvo 2014–2020.

Drugi sklop projektnih aktivnosti je namenjen izobraževanju posameznikov o pomenu zasebnosti in njihovih temeljnih pravicah s področja varstva osebnih podatkov. Na novo postavljeni spletni strani www.tiodlocas.si je Informacijski pooblaščenec podrobno pojasnil pravice posameznikov in podal konkretnne napotke, kako jih uresničiti. Leta 2019 bo Informacijski pooblaščenec nadgradil spletne aktivnosti s sodelovanjem z **Zvezo potrošnikov Slovenije: v reviji ZPStest bo imel občasno rubriko**, izdana pa bo tudi **skupna brošura** o varstvu osebnih podatkov potrošnikov.

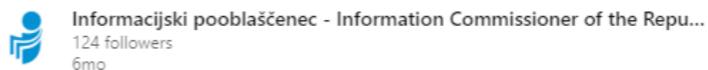
POMEMBNO

Informacijski pooblaščenec je z namenom zagotavljanja transparentne in proaktivne komunikacije leta 2018 vzpostavil prisotnost na profesionalnem omrežju LinkedIn, kjer želi doseči predvsem majhna in srednje velika podjetja. Prav tako je okrepil komunikacijo na Facebook strani, kjer z objavami, prilagojenimi splošni javnosti, skrbi za dvig ozaveščenosti glede varstva zasebnosti, predvsem pri uporabi spletnih storitev. Informacijski pooblaščenec še naprej aktivno sodeluje v Svetu projekta SAFE-SI in Spletno oko, ki izvajata pomembno preventivno dejavnost na področju izobraževanja o varni rabi interneta za šolarje, učitelje in starše.

Primer objave na Facebook strani Informacijskega pooblaščenca



Primer objave na LinkedIn poslovni strani Informacijskega pooblaščenca



Tako upravljavec kot obdelovalec se morata zavedati svojih pravic in obveznosti v zvezi z obdelavo osebnih podatkov, ki naj bodo jasno opredeljene v pogodbi. Splošna uredba o varstvu podatkov zahteva, da so pogodbe v pisni obliki, določen pa je tudi minimalni obseg sestavin pogodbe. Posodobili smo smernice o pogodbeni obdelavi in odgovorili na nekatera najpogostejsa vprašanja, ki se zastavlajo. <https://lnkd.in/g-abgFK>

[See translation](#)



[Like](#) [Comment](#)

3.6 MEDNARODNO SODELOVANJE

3.6.1 SODELOVANJE V EVROPSKEM ODBORU ZA VARSTVO PODATKOV

Informacijski pooblaščenec je kot nacionalni nadzorni organ za varstvo osebnih podatkov do maja 2018 na ravni EU aktivno sodeloval na plenarnih sestankih ter pri delu številnih podskupin Delovne skupine za varstvo podatkov iz 29. člena Direktive 95/46/ES (Article 29 Data Protection Working Party – WP29), ki je Evropski komisiji dajala strokovna mnenja s področja varstva osebnih podatkov. Leta 2018 je bila Delovna skupina osredotočena predvsem na priprave na uporabo Splošne uredbe o varstvu podatkov in priprave na vzpostavitev Evropskega organa za varstvo podatkov.

Od maja 2018 je Informacijski pooblaščenec član Evropskega odbora za varstvo podatkov (EOVP), ki je neodvisni evropski organ za zagotavljanje dosledne uporabe pravil o varstvu podatkov v Evropski uniji in za spodbujanje sodelovanja med organi EU za varstvo podatkov. V odboru sodelujejo predstavniki vseh 28 neodvisnih nadzornih organov EU in EGS (Islandija, Norveška in Lihtenštajn), Evropske komisije in Evropskega nadzornika za varstvo podatkov; odbor nadomešča Delovno skupino za varstvo podatkov iz člena 29 (Article 29 Working Party). Evropski odbor za varstvo podatkov je bil ustanovljen maja 2018 na podlagi Splošne uredbe in ima sedež v Bruslju. Deluje v skladu s svojim pravilnikom in vodilnimi načeli.



European Data Protection Board

Ključne pristojnosti odbora v okviru postopkov sodelovanja nadzornih organov so:

- **sprejemanje pravno zavezujočih odločitev odbora** v okviru mehanizma za skladnost v zvezi z nacionalnimi nadzornimi organi, da zagotovi dosledno uporabo Splošne uredbe;
- **sprejemanje splošnih smernic** za podrobnejšo opredelitev pogojev evropske zakonodaje o varstvu podatkov, s čimer svojim deležnikom zagotavlja dosledno razlagu njihovih pravic in obveznosti;
- **svetovanje Evropski komisiji** v zvezi z vprašanji varstva podatkov in pripravo evropskih predpisov s področja varstva podatkov;
- **promocija sodelovanja in izmenjave izkušenj** med nacionalnimi nadzornimi organi za varstvo podatkov.

Mehanizem za skladnost, kot je opredeljen v Splošni uredbi, poteka prek:

- **Izdaje mnenj odbora za zagotavljanje dosledne uporabe evropske zakonodaje o varstvu podatkov** (po členu 64 Splošne uredbe), med drugim v določenih primerih glede sprejema seznama dejanj obdelave, za katere velja zahteva po oceni učinka v zvezi z varstvom podatkov; v zvezi kodeksom ravnanja s čezmejnim vplivom ter v določenih primerih glede odobritve merit za pooblastitev organa za spremljanje skladnosti s kodeksom ravnanja; v zvezi z določitvijo standardnih določil o varstvu podatkov v zvezi s prenosi podatkov v tretje države; v zvezi z odobritvijo pogodbenih določil ali zavezujočih poslovnih pravil.
- **Reševanja sporov med nadzornimi organi** (po členu 65 Splošne uredbe), na primer glede nasprotujočih si stališč o vsebini odločitve v čezmejnih primerih; o tem, kateri nadzorni organ je vodilni v določenem čezmejnem postopku; ter v primeru nespoštovanja mnenja odbora s strani posameznega nadzornega organa.
- **Reševanja nujnih postopkov** (po členu 66 Splošne uredbe) s sprejemom začasnih ukrepov v izjemnih primerih, ko je ukrepanje potrebno zaradi varstva pravic in svoboščin posameznikov.

Delo odbora, ki se vsak mesec sestaja na plenarni ravni, poteka v 12 podskupinah strokovnjakov. Te obravnavajo različna področja dela odbora, v njih pa sodelujejo predstavniki vseh nadzornih organov. Predstavniki Informacijskega pooblaščenca med drugim aktivno sodelujejo v podskupinah za: tehnološka vprašanja, prenose podatkov v tretje države, področje varstva podatkov v okviru dela organov pregona, družbene medije, finančne zadeve, vprašanja usklajevanja sistema izrekanja upravnih glob, sodelovanje med nadzornimi organi in usklajevanje dela na področju nadzora. Posamezne podskupine glede na področja dela pripravljajo smernice in mnenja odbora ter obravnavajo aktualne izzive, s katerimi se srečujejo posamezni nadzorni organi ter so pomembni v širšem evropskem prostoru, bodisi zaradi čezmejne obdelave podatkov bodisi zaradi pomembnih vprašanj enotnega tolmačenja evropskih predpisov.

Leta 2018 so se nadzorni organi v okviru odbora med drugim ukvarjali z vprašanji enotnega tolmačenja Splošne uredbe glede postopkov čezmejnega sodelovanja, izvedena je bila druga revizija delovanja mehanizma Ščita zasebnosti v zvezi z zagotavljanjem varstva podatkov po prenosu v Združene države Amerike, obravnavala so se vprašanja in izzivi glede delovanja in prenosov podatkov v zvezi z davčnimi postopki po sporazumih FATCA, ki so jih sklenile posamezne države članice EU z Združenimi državami Amerike, v sklepni fazi pa je med drugim tudi priprava mnenja odbora glede tolmačenja pravne podlage po točki b člena 6(1) Splošne uredbe v zvezi s pogodbami o zagotavljanju spletnih storitev potrošnikom.

Leta 2018 je odbor sprejel naslednje smernice:

- Smernice 4/2018 o akreditaciji teles za certificiranje na podlagi člena 43 Splošne uredbe (2016/679),
- Smernice 3/2018 o ozemeljski veljavnosti Splošne uredbe (člen 3),
- Smernice št. 2/2018 o odstopanjih iz člena 49 v skladu z Uredbo (EU) 2016/679.

Poleg tega je odbor leta 2018 sprejel 27 mnenj v zvezi s seznammi dejanj obdelave, za katere velja zahteva po oceni učinka v zvezi z varstvom podatkov, in ki so jih sprejeli posamezni nacionalni nadzorni organi držav članic EU.

Odbor je ob vzpostavitvi maja sprejel tudi naslednje pomembne smernice in mnenja dotedanje delovne skupine WP 29:

- Smernice o privolitvi po Uredbi 2016/679 (WP 259),
- Smernice o transparentnosti v skladu z Uredbo 2016/679 (WP 260),
- Smernice o avtomatiziranem posameznem sprejemanju odločitev in oblikovanju profilov za namene Uredbe 2016/679 (WP 251),
- Smernice o uradnem obvestilu nadzornemu organu o kršitvi varstva osebnih podatkov po Uredbi 2016/679 (WP 250),
- Smernice o pravici do prenosljivosti podatkov (WP 242),
- Smernice o oceni učinka na varstvo podatkov (DPIA) (WP 248),
- Smernice o pooblaščenih osebah za varstvo osebnih podatkov ("DPO") (WP 243),
- Smernice o vodilnem nadzornem organu (WP 244),
- Stališče o tolmačenju člena 30(5) Splošne uredbe,
- Delovni dokument o sodelovanju v postopku odobritve zavezujočih poslovnih pravil (WP 263),
- Delovni dokument o elementih in načelih zavezujočih poslovnih pravil za upravljavce osebnih podatkov (WP 256),
- Delovni dokument o elementih in načelih zavezujočih poslovnih pravil za obdelovalce osebnih podatkov (WP 257),
- Delovni dokument o kriteriju skladnosti (WP 254),
- Smernice o uporabi in določanju upravnih glob za namene Uredbe 2016/679 (WP 253).

3.6.2 SODELOVANJE V DRUGIH NADZORNIH TELESIH EVROPSKE UNIJE

Informacijski pooblaščenec je leta 2018 na ravni EU aktivno sodeloval v petih delovnih telesih, ki se ukvarjajo z nadzorom nad izvajanjem varstva osebnih podatkov v okviru velikih informacijskih sistemov EU, in sicer:

- 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 Europola je po Uredbi o Europolu primarno pristojen Evropski nadzornik 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.

V okviru nadzora nad SIS II, CIS in Eurodac so bila sprejeta poročila o aktivnosti za obdobje 2016–2017. Europolov odbor za sodelovanje je posodobil seznam pristojnih organov držav članic za zagotavljanje pravice posameznikov do dostopa do osebnih podatkov. V okviru nadzora nad SIS II je bilo sprejeto poročilo o beleženju dostopov in obdelav podatkov v SIS II na nacionalni ravni. V okviru nadzora nad VIS je bil sprejet dokument s stališčem nadzorne skupine glede predloga Evropske komisije (COM/2018/302) o spremembji Uredbe o vizumskem informacijskem sistemu in izmenjavi podatkov med državami članicami o vizumih za kratkoročno prebivanje. Sprejeto in poslano Evropskemu parlamentu, Svetu in Komisiji je bilo tudi skupno pismo nadzornih skupin SIS II, VIS in Eurodac o predlogu Evropske komisije za vzpostavitev pravnega okvira za interoperabilnost med obsežnimi informacijskimi sistemi EU.

3.6.3 SODELOVANJE V DRUGIH MEDNARODNIH TELESIH

POSVETOVALNI ODBOR T-PD

V okviru Sveta Evrope je predstavnik Informacijskega pooblaščenca tudi leta 2018 sodeloval v Posvetovalnem odboru (T-PD), ustanovljenem s Konvencijo 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 pridruževanja 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 2018 aktivno pripravljal Priporočilo glede zaščite zdravstvenih podatkov ter Smernice o umetni inteligenci in varstvu osebnih podatkov, izdal pa je Vodič glede uporabe osebnih podatkov v policijskem sektorju, Vodič glede zasebnosti in varstva osebnih podatkov na področju ICANN (Internet Corporation for Assigned Names and Numbers), Poročilo o umetni inteligenci ter Smernice glede varovanja zasebnosti v medijih. Odbor je sodeloval tudi pri izdaji novega Evropskega priročnika o varstvu osebnih podatkov ter vzpostavil nagrado Stefano Rodotà, ki bo prvič podeljena leta 2019. Nagrada bo namenjena priznanju inovativnih in izvirnih akademskih raziskovalnih projektov na področju varstva podatkov.

MEDNARODNA DELOVNA SKUPINA ZA VARSTVO OSEBNIH PODATKOV V TELEKOMUNIKACIJAH (IWGDP)

Informacijski pooblaščenec je tudi leta 2018 aktivno deloval v Mednarodni delovni skupini za varstvo osebnih podatkov v telekomunikacijah (IWGDPT – International Working Group on Data Protection in Telecommunications), v okviru katere se srečujejo predstavniki informacijskih pooblaščencev in organov za varstvo osebnih podatkov in zasebnosti s celega sveta. Delovna skupina je na zasedanjih v Budimpešti in v Queenstownu sprejela nove delovne dokumente, ki so pomemben znak konzenza glede določenih vprašanj varstva osebnih podatkov na mednarodni ravni, predvsem glede izzivov, ki jih prinašajo nove tehnologije.

Delovni dokument o vprašanjih zasebnosti pri sodobnih povezanih vozilih naslavlja vprašanja zbiranja, posredovanja in izmenjave podatkov, ki nastajajo ob uporabi sodobnih avtomobilov, kjer številni senzorji in sistemi beležijo lokacijo, hitrost, telematske in druge podatke (https://www.datenschutz-berlin.de/fileadmin/user_upload/pdf/publikationen/working-paper/2018/2018-IWGDP-Working_Paper_Connected_Vehicles.pdf).

Drugi sprejeti delovni dokument se nanaša na standarde za zagotovitev varstva osebnih podatkov pri čezmejni izmenjavi osebnih podatkov za potrebe pregona kaznivih dejanj (https://www.datenschutz-berlin.de/fileadmin/user_upload/pdf/publikationen/working-paper/2018/2018-IWGDP-Working_Paper_Cross-border_data_requests.pdf).

Na zadnjem srečanju skupine je bil sprejet delovni dokument o sledenju na javnih površinah, kjer se v okviru uvajanja pametnih mest in nadzora kriminala na javnih lokacijah zbirajo podatki o uporabnikih pametnih telefonov, predvsem na podlagi uporabe brezžičnih omrežij. Sprejeto je bilo tudi mnenje skupine na temo umetne inteligence, ki se vse bolj uporablja v vseh segmentih družbe in prinaša določene nevarnosti z vidika avtomatiziranega odločanja o naših usodah. Dokumenta bosta po pregledu javno objavljena na spletni strani delovne skupine (<https://www.datenschutz-berlin.de/working-paper.html>).

MEDNARODNA KONFERENCA POOBLAŠČENCEV ZA VARSTVO PODATKOV IN ZASEBNOST (ICDPCC)

Mednarodna konferenca pooblaščencev za varstvo podatkov in zasebnost (ang. International Conference of Data Protection and Privacy Commissioners – ICDPPC) že štiri desetletja predstavlja vodilni svetovni forum na področju varstva podatkov in zasebnosti, ki povezuje prizadevanja 122 nadzornih organov za varstvo zasebnosti in podatkov z vsega sveta. Delo konference vodi izvršni odbor, ki mu trenutno predseduje britanska pooblaščenka Elizabeth Denham. Med pomembnejšimi resolucijami, sprejetimi na zadnji konferenci v Bruslju leta 2018, sta resolucija o etiki in varstvu podatkov v umetni inteligenci ter resolucija o sodelovanju med nadzornimi organi za varstvo podatkov in organi za varstvo potrošnikov za boljšo zaščito državljanov in potrošnikov v digitalnem gospodarstvu. Pomemben cilj konference je poglobiti sodelovanje nadzornih organov in s tem dvigniti raven varstva osebnih podatkov v svetu. Osrednje razprave na konferenci leta 2018 so bile posvečene izzivom učinkovitega uveljavljanja varstva osebnih podatkov v digitalnem svetu modernih tehnologij - nevarnosti, ki jih prinašajo posegi v zasebnost, se namreč z razvojem modernih tehnologij nenehno spreminja, njihov celotni obseg pa pogosto spoznamo šele ob pojavu resnih kršitev.



INITIATIVE 20i7

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 izvivi. Ker številna podjetja in organizacije javnega sektorja v regiji čezmejno zbirajo in izmenjujejo osebne podatke, je zagotavljanje ustrezne in čim enotnejše ravni varstva osebnih podatkov pomembno tudi 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 k krepitvi dobrih odnosov med državami.

Na drugem srečanju Iniciative 20i7, ki je aprila 2018 potekalo v Makedoniji, so predstojniki nadzornih organov za varstvo osebnih podatkov iz Hrvaške, Srbije, Bosne in Hercegovine, Črne gore, Kosova, Makedonije in Slovenije razpravljali o izvivih, ki se na nacionalni ravni pojavlja ob implementaciji novih evropskih standardov varstva osebnih podatkov.

3.7 SPLOŠNA OCENA STANJA VARSTVA OSEBNIH PODATKOV

Delo Informacijskega pooblaščenca na področju varstva osebnih podatkov je leta 2018 v največji meri zaznamovala Splošna uredba, ki se je v vseh državah članicah EU začela neposredno uporabljati 25. maja 2018 ter je še razširila naloge in pristojnosti Informacijskega pooblaščenca glede na obstoječi ZVOP-1. Zaradi zahtev po prilagoditvi področja obdelave osebnih podatkov se je precej povečal obseg aktivnosti tako pri upravljavcih kot pri Informacijskem pooblaščencu.

Začetek uporabe Splošne uredbe terja sprejetje novega Zakona o varstvu osebnih podatkov (ZVOP-2), s katerim bi se v Republiki Sloveniji v celoti zagotovilo izvajanje omenjene uredbe. Zakon do konca leta 2018 ni bil sprejet, kar je povzročilo precej odprtih vprašanj tako pri upravljavcih in obdelovalcih osebnih podatkov kot pri Informacijskem pooblaščencu. Nesprejetje ZVOP-2 na samo izvajanje inšpekcijskega nadzora sicer ni bistveno vplivalo, je pa zelo vplivalo na vodenje prekrškovnih postopkov in izrekanje glob za ugotovljene kršitve. Informacijski pooblaščenec je lahko zaradi odsotnosti ZVOP-2 v primeru ugotovljenih kršitev določb Splošne uredbe ali določb ZVOP-1 zavezancu v postopku inšpekcijskega nadzora odredil odpravo ugotovljenih nepravilnosti ter prepovedal obdelavo osebnih podatkov ali njihovo blokiranje, postopek za prekrške pa je lahko uvedel le v tistih primerih, kjer je šlo za kršitev tistih nekaj členov ZVOP-1, ki še veljajo. Informacijski pooblaščenec tako zaradi nesprejetja novega ZVOP-2 v letu 2018 ni mogel izrekati sankcij za kršitve, ki so določene v členu 83 Splošne uredbe, pač pa je lahko v okviru prekrškovnih postopkov sankcioniral samo kršitev tistih določb veljavnega ZVOP-1, ki jih ni nadomestila Splošna uredba.

Informacijski pooblaščenec je podobno kot v preteklih letih tudi leta 2018 prejel veliko število prijav posameznikov, število teh pa se je po začetku uporabe Splošne uredbe bistveno povečalo. Od 25. 5. 2018 do 31. 12. 2018 je Informacijski pooblaščenec tako prejel 598 prijav zaradi kršitve varstva osebnih podatkov, medtem ko jih je v enakem obdobju leta 2017 prejel 290. Občutno povečanje števila prijav je nedvomno rezultat večje ozaveščenosti posameznikov v zvezi z obdelavo njihovih osebnih podatkov in pravicami, ki jim jih daje Splošna uredba, saj se je o slednji v obravnavanem obdobju v medijih veliko govorilo in pisalo. Ozaveščenost se je povečala tudi na strani upravljavcev in obdelovalcev, kar se je pokazalo v povečanju števila zaprosil za ustna in pisna mnenja. Informacijski pooblaščenec je pri obravnavi prijav, ki jih je prejel s strani posameznikov, ugotovil, da so bile v mnogih primerih vložene zaradi nerazumevanja določb Splošne uredbe, kar velja zlasti v primeru obdelave osebnih podatkov na podlagi privolitve posameznika, na katerega se nanašajo osebni podatki. Splošna uredba sicer res določa strožje pogoje, ki morajo biti izpolnjeni, da se privolitev šteje za veljavno, vendar je ob tem treba opozoriti, da je privolitev posameznika le ena od šestih pravnih podlag, ki jih v zvezi z zakonitostjo obdelave osebnih podatkov določa člen 6 Splošne uredbe. Upravljavci so zaradi takšnega nerazumevanja v praksi pogosto pridobivali privolitve posameznikov tudi v primerih, ko je bila obdelava osebnih podatkov sicer že določena v zakonu, ko je bila obdelava

potrebna za izvajanje pogodbe ali pa je bil izpolnjen kakšen drug pogoj iz člena 6 Splošne uredbe, zaradi česar pridobivanje privolitve posameznika sploh ne bi bilo potrebno.

Glede prejetih prijav je treba poudariti, da je do njih pogosto prihajalo tudi zato, ker upravljavci posamezniku ob zbiranju osebnih podatkov niso zagotovili ustreznih oz. popolnih informacij. Upravljavci so namreč dolžni sprejeti ustreerne ukrepe, s katerimi posamezniku zahtevane informacije zagotovijo v jedrnati, pregledni, razumljivi in lahko dostopni obliku ter v jasnom in preprostem jeziku. Vrste informacij, ki jih morajo upravljavci zagotoviti posamezniku, so določene v členih 13 in 14 Splošne uredbe, posameznik pa na podlagi takšnih informacij izve, kdo je upravljavec osebnih podatkov, za kakšne namene in na kakšni pravni podlagi se osebni podatki obdelujejo, kdo so uporabniki osebnih podatkov, koliko časa se podatki hranijo itd. Kršitve določb členov 13 in 14 Splošne uredbe spadajo med pogosteje ugotovljene kršitve v letu 2018, zaradi česar je Informacijski pooblaščenec pripravil in na svojih spletnih straneh objavil vzorce takšnih obvestil.

Tipični primer nezagotavljanja ustreznih informacij so bile npr. pošta in banke, ki so zbirale osebne podatke na podlagi Uredbe EU o informacijah, ki spremljajo prenose sredstev oz. Zakona o preprečevanju pranja denarja in financiranja terorizma, vendar pa posameznikom ob zbiranju osebnih podatkov niso posredovale informacij iz člena 13 Splošne uredbe, zlasti ne podatkov o namenih in pravni podlagi za obdelavo zahtevanih osebnih podatkov, zaradi česar so posamezniki menili, da gre za nezakonito ali vsaj prekomerno zbiranje osebnih podatkov in so zaradi tega vlagali prijave. Neposredovanje takšnih informacij pomeni kršitev pravic posameznika iz člena 13 Splošne uredbe, zato lahko Informacijski pooblaščenec odredi odpravo ugotovljenih nepravilnosti, po uveljavitvi ZVOP-2 pa bo za takšne kršitve lahko oz. bo moral izrekati tudi globe, določene v 4. odstavku člena 83 Splošne uredbe.

Informacijski pooblaščenec je od 25. 5. 2018 do 31. 12. 2018 prejel tudi 68 uradnih obvestil o kršitvi varnosti osebnih podatkov, ki so jih poslali upravljavci osebnih podatkov. Vlaganje takšnih uradnih obvestil o kršitvi varnosti osebnih podatkov, t. i. »samoprijav«, je novost, ki jo upravljavcem in obdelovalcem osebnih podatkov nalaga člen 33 Splošne uredbe, in kot kažejo dosedanje ugotovitve, podjetja oz. upravljavci s posredovanjem takšnih uradnih obvestil o kršitvi varnosti osebnih podatkov Informacijskemu pooblaščencu precej vestno prijavljajo varnostne incidente. Upravljavci osebnih podatkov so uradna obvestila o kršitvi varnosti osebnih podatkov najpogosteje pošiljali zaradi neupravičenega razkritja osebnih podatkov (posredovanja osebnih podatkov nepooblaščenim ali napačnim osebam), nepooblaščenega dostopanja do osebnih podatkov (zaradi programske napake ali zlorabe pooblastil s strani zaposlenih), vdora v informacijski sistem ter izgube ali kraje nosilcev osebnih podatkov (npr. osebnih računalnikov in službenih mobilnih telefonov).

Informacijski pooblaščenec je tudi leta 2018 povečeval obseg izvajanja t. i. preventivnih inšpekcijskih nadzorov pri zavezancih na področjih, na katerih glede na oceno tveganja obstaja bodisi večja verjetnost kršitve predpisov s področja varstva osebnih podatkov bodisi zaradi občutljivosti obdelave osebnih podatkov v primeru kršitev obstaja nevarnost večjih škodljivih posledic za posameznike. Pri opravljanju obsežnejših oz. temeljitejših inšpekcijskih nadzorov je Informacijski pooblaščenec posebno pozornost namenil zlasti preverjanju usklajenosti obdelave osebnih podatkov z določbami Splošne uredbe ter zagotavljanju informacijske varnosti, katere namen je preprečevanje nepooblaščene obdelave osebnih podatkov ter slučajnega ali nepooblaščenega uničevanja ali izgube le-teh.

Pri obravnavi prijav ter izvajaju preventivnih inšpekcijskih nadzorov lahko ugotovimo, da so nepravilnosti ali pomanjkljivosti v pretežni meri posledica nepoznavanja oz. nerazumevanja zakonodaje, saj se je leta 2018 začela uporabljati nova Splošna uredba, ZVOP-2, ki bi v celoti zagotovil neno izvajanje in jasneje določil posamezna pravila izvajanja, pa še ni bil sprejet. Izjema so kršitve, ki se v zvezi z zagotavljanjem varnosti osebnih podatkov pojavljajo zaradi malomarnosti upravljavcev ali obdelovalcev osebnih podatkov, ter nezakoniti vpogledi v zbirke osebnih podatkov s strani zaposlenih, ki takšne vpoglede izvajajo bodisi zaradi radovednosti bodisi zaradi pridobivanja osebnih podatkov za lastne namene. Informacijski pooblaščenec ugotavlja, da zaposleni najpogosteje nezakonito vpogledujejo v zbirke osebnih podatkov s področja notranjih zadev oz. policije, v zbirke osebnih podatkov, ki jih vodijo zdravstvene institucije, precej pogosti so tudi nezakoniti vpogledi v centralni register psov. Večina navedenih zbirk osebnih podatkov ima zagotovljeno sledljivost obdelave osebnih podatkov, ki zagotavlja tudi možnost naknadnega ugotavljanja, katere osebe so v določenem času vpogledovale v osebne podatke določenega posameznika, s čimer so zaposleni, ki jim je zaradi narave dela omogočen dostop do osebnih podatkov v zbirki, sicer seznanjeni, vendar pa nezakonite vpoglede kljub temu opravijo v upanju, da jih ne bodo odkrili. V primeru, ko upravljavec in Informacijski pooblaščenec ugotovita nezakonite vpoglede v osebne podatke s strani posameznega zaposlenega, ti pogosto navajajo, da vpogledov niso opravili oni, temveč je do vpogleda prišlo zaradi zlorabe njihovega uporabniškega imena in gesla s strani neznane osebe. To pa oseb, katerih uporabniško ime in geslo je bilo uporabljen, ne odvezuje prekrškovne odgovornosti, saj so dolžne poskrbeti za varnost osebnih podatkov, ki se vodijo v posamezni zbirki, in sicer tako, da zavarujejo svoje uporabniško ime in geslo ter se takoj po prenehanju dela v zbirki ali ob zapustitvi delovne postaje odjavijo iz zbirke.

Informacijski pooblaščenec je leta 2018 okrepil delovanje na področju skladnosti in preventive. Ob začetku uporabe Splošne uredbe se je pokazalo, da veliko malih upravljavcev osebnih podatkov slabo pozna zakonodajo o varstvu osebnih podatkov, čemur so po oceni Informacijskega pooblaščanca botrovale predvsem izjeme glede dolžnosti evidentiranja zbirk (»katalogi«). Opazno je bilo tudi slabo poznavanje razlik v možnih pravnih podlagah, zlasti v obdelavi na podlagi privolitve posameznika

in pogodbe s posameznikom ter poznavanja pravil o izvajanju neposrednega trženja. Ozaveščanju malih podjetij, ki vendarle predstavljajo večino slovenskega gospodarstva, bo zato tudi v prihodnosti treba nameniti veliko pozornosti in jim ponuditi orodja, s katerimi bodo lahko zagotovila skladnost (mnenja, smernice, obrazce, vzorce, infografike, telefonsko pomoč in druge vsebine na spletnih straneh). Informacijski pooblaščenec bo okviru projekta RAPiD. Si še naprej izvajal številne aktivnosti na tem področju, v sodelovanju z Gospodarsko, Obrtno in Trgovinsko zbornico Slovenije bo z izobraževalnimi vsebinami in uporabnimi orodji poskušal doseči čim več malih podjetij.

Splošna uredba je prinesla pomembne novosti glede sodelovanja nadzornih organov za varstvo osebnih podatkov v državah članicah EU in EGS (Islandija, Norveška in Lichtenštajn) pri čezmejnih primerih. Omogočila in formalizirala je postopek sodelovanja po načelu »vse na enem mestu«, ki predvideva, da postopek nadzora v čezmejnem primeru obdelave osebnih podatkov vodi t. i. vodilni organ in pri tem sodeluje z drugimi organi za varstvo osebnih podatkov, uvedla mehanizme vzajemne pomoči in skupnega ukrepanja organov za varstvo osebnih podatkov v državah članicah EU. Informacijski pooblaščenec je tako leta 2018, od uveljavitve Splošne uredbe, sodeloval v šestih postopkih vzajemne pomoči med organi za varstvo osebnih podatkov. V 81 postopkih ugotavljanja vodilnega organa se je opredelil za zadevni organ, ki sodeluje v postopku čezmejnega postopka nadzora pri zavezancu. Na temelju teh postopkov je bilo začetih 30 postopkov čezmejnega sodelovanja pri inšpeksijskem nadzoru nad podjetji, ki poslujejo čezmejno, po mehanizmu »vse na enem mestu«. Največkrat gre v teh primerih za priljubljene ponudnike komunikacijskih spletnih storitev oz. spletnne velikane, Facebook, Google, Amazon, Apple, PayPal, WhatsApp, Twitter, Instagram, Microsoft itd.; Informacijski pooblaščenec v teh postopkih sodeluje kot zadevni organ. Postopki zadevajo skladnost njihovih praks s Splošno uredbo, tako v smislu zakonitosti obdelave osebnih podatkov kot tudi ustreznosti njihovih politik zasebnosti in obveščanja posameznikov o obdelavi osebnih podatkov, izvrševanja pravic posameznikov ter kršitev varstva osebnih podatkov zaradi vdorov v informacijske sisteme in pomanjkljivega zavarovanja osebnih podatkov.

Sodelovanje v čezmejnih primerih inšpeksijskega nadzora, kot ga je uvedla Splošna uredba, je nedvomno ena ključnih novosti in okrepitev, predvsem v smislu enotnega delovanja nadzornih organov v različnih državah članicah EU in EGS. Le z enotnim pristopom lahko namreč nadzorni organi na ravni EU vplivajo na aktivnosti multinacionalnih ponudnikov sodobnih spletnih storitev, komunikacijskih platform in družbenih omrežij, katerih poslovni model najpogosteje temelji na monetizaciji s pomočjo personaliziranega in ciljanega oglaševanja, ta pa na obdelavi in analizi ogromnih količin podatkov o posameznemu uporabniku. Te storitve uporablja posamezniki v vseh državah članicah EU in EGS, nadzorni organi za varstvo osebnih podatkov pa imajo zdaj na voljo robustne mehanizme in orodja tesnega sodelovanja, s katerimi imajo možnost nastopiti proti spornim praksam, ki so na škodo pravicam posameznikov, z enim glasom. Seveda pa tako

sodelovanje za Informacijskega pooblaščenca, kot tudi za ostale nadzorne organe, pomeni velik izliv v smislu dodatnih potrebnih resursov, tako finančnih kot kadrovskih – znanja, ki so potrebna za obravnavo takih primerov so namreč specifična, predvsem pa vključujejo zelo različne discipline, od prava, poznavanja informacijskih tehnologij in ekonomije do poznavanja sodobne oglaševalske industrije in družbenih medijev. Ključno je odlično poznavanje angleškega jezika, saj je angleščina v omenjenih čezmejnih postopkih operativni jezik. Nenazadnje pa zahteva dodatne resurse tudi administriranje sodelovanja prek nove informacijske platforme, ki je postopke institucionalizirala.

Odgovorna urednica:

Mojca Prelesnik, informacijska pooblaščenka

Avtorji besedil:

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

Jože Bogataj, namestnik informacijske pooblaščenke

Alenka Jerše, namestnica informacijske pooblaščenke

mag. Andrej Tomšič, namestnik informacijske pooblaščenke

Jelena Burnik, MSc, vodja mednaravnega sodelovanja in nadzora

mag. Kristina Kotnik Šumah, namestnica informacijske pooblaščenke

Karolina Kušević, svetovalka Pooblaščenca II

Matej Sironič, svetovalec Pooblaščenca za varstvo osebnih podatkov

Jasmina Mešić, svetovalka Pooblaščenca za preventivo

Tina Ivanc, svetovalka Pooblaščenca za varstvo osebnih podatkov

mag. Nuša Kavšek, svetovalka Pooblaščenca za varstvo osebnih podatkov

Neja Domnik, raziskovalka Pooblaščenca

mag. Urban Brulc, samostojni svetovalec Pooblaščenca

Oblikovanje:

Darko Mohar

Tomaž Brodgesell

Anže Novak

Lektorirala:

Katja Klopčič Lavrenčič

Informacijski pooblaščenec Republike Slovenije

Dunajska cesta 22

1000 Ljubljana

www.ip-rs.si

gp.ip@ip-rs.si

Ljubljana, maj 2019