LETNO POROČILO

Informacijskega pooblaščenca za leto 2019

'19

UVODNA BESEDA INFORMACIJSKE POOBLAŠČENKE

Spoštovani,

tako v Sloveniji kot širše družbena dogajanja v letu 2019 dokazujejo, kako pomembno je učinkovito varstvo pravice dostopa do informacij javnega značaja in varstva osebnih podatkov. To potrjujejo tudi skrbi in izzivi, glede katerih se posamezniki in organizacije obračajo na Informacijskega pooblaščenca. Ti so zelo raznoliki, skupna točka vseh pa je ugotovitev, da nas kot družbo na obeh področjih kljub napredku čaka še veliko dela. Dobra novica je, da v Sloveniji neodvisne nadzorne institucije, med katerimi je tudi Informacijski pooblaščenec, uživajo izredno veliko zaupanje, višje od evropskega povprečja, saj so prve, na katere bi se ljudje obrnili po pomoč v primeru kršitev. To dokazuje raziskava Eurobarometer, opravljena v letu 2019, ki Slovenijo tudi glede poznavanja Splošne uredbe o varstvu podatkov (Splošna uredba), pravic posameznikov in zavedanja o obstoju nadzornega organa uvršča nad evropsko povprečje, v primerjavi s podatki iz leta 2015 pa se je ta delež celo precej povečal.

Analiza dela Informacijskega pooblaščenca v letu 2019 kaže, da na področju dostopa do informacij javnega značaja med izzivi zlasti izstopa trend rasti pritožb zaradi molka organa (delež teh pritožb znaša kar 44%). Na področju varstva osebnih podatkov in zasebnosti smo v zadnjih dveh letih priča bistvenem porastu števila prijav in števila pritožb v zvezi z uveljavljanjem pravic posameznikov. Hkrati se še vedno soočamo s precejšnjimi izzivi zaradi zamud pri sprejemu nacionalnih predpisov za uporabo Splošne uredbe in za prenos Direktive za organe kazenskega pregona, na kar že več kot tri leta opozarja tudi Informacijski pooblaščenec. Zlasti bo ključno, da zakonodajalec poskrbi, da se Slovenija ne uvrsti na seznam držav, ki nimajo ustrezno urejenih zakonskih pristojnosti nadzornega organa za varstvo podatkov.

Na področju dostopa do informacij javnega značaja je bilo sicer število pritožbenih zadev v letu 2019 na ravni, ki je primerljiva z letom 2018 (leta 2019 je bilo vloženih 540 pritožbenih zadev). Med pritožbami zaradi molka organa zlasti izstopajo organi državne uprave (ministrstva in organi v sestavi), zoper katere je bilo vloženih največ pritožb zaradi molka (29 %). Gre za zavezance, ki bi po 16 letih veljavnosti Zakona o dostopu do informacij javnega značaja (ZDIJZ) vsekakor morali biti sposobni vse zahteve obravnavati pravočasno (v roku 20 delovnih dni). Zmanjšalo pa se je število pritožb zaradi molka občinskih organov. Od vseh prejetih pritožb zaradi molka organa jih je bilo 26 vloženih s strani medijev. Tudi v teh postopkih je Informacijski pooblaščenec največ pritožb prejel zoper organe državne uprave (10 pritožb). Informacijski pooblaščenec je vodil 17 postopkov zoper poslovne subjekte pod prevladujočim vplivom, kar predstavlja le 3 % vseh pritožbenih zadev.

Navedeno kaže, da so zavezanci večinoma v molku, ker k reševanju zahtevkov po ZDIJZ ne pristopijo pravočasno. V prihodnje bo zato treba (še) več napora vložiti v aktivnejše usposabljanje zavezancev, kar je sicer primarno naloga Ministrstva za javno upravo. Informacijski pooblaščenec kot pritožbeni organ lahko organom svetuje le neformalno, na podlagi primerov iz prakse. Leta 2019 je podal 300 pisnih odgovorov na zaprosila zavezancev ter 629-krat svetoval v okviru telefonskega dežurstva, primere iz prakse pa je redno objavljal na svoji spletni strani – vse zato, da bi olajšal delo zavezancem in seznanjal javnost s pomenom te temeljne človekove pravice. S ciljem boljšega poznavanja prakse je Informacijski pooblaščenec izvedel tudi pet praktičnih delavnic za upravne enote. Informacijski pooblaščenec glede na izkušnje iz leta 2019 svetuje, naj zavezanci izjeme od prostega dostopa do informacij javnega značaja razlagajo ozko in pri tem dosledno upoštevajo načelo delnega dostopa ter obstoj absolutno javnih podatkov, kot so npr. podatki, povezani z delom javnih uslužbencev. To se s Splošno uredbo ni v ničemer spremenilo.

Na področju varstva osebnih podatkov je Informacijski pooblaščenec leta 2019 obravnaval 974 prijav oz. pobud za uvedbo inšpekcijskega postopka, kar je največ doslej, in uvedel 139 prekrškovnih postopkov. Poleg tega je prejel 181 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. Na mednarodni ravni je Informacijski pooblaščenec izvedel 148 postopkov čezmejnega sodelovanja po členih 60 in 61 Splošne uredbe, v zvezi z upravljavci, ki izvajajo čezmejno obdelavo osebnih podatkov, pri čemer se je v 77 postopkih opredelil za zadevni nadzorni organ (po členu 56 Splošne uredbe). Informacijski pooblaščenec je leta 2019 prejel tudi devet primerov obvestil o kršitvah podatkov o pacientih na podlagi 46. člena Zakona o pacientovih pravicah ter 137 uradnih obvestil o kršitvi varnosti osebnih podatkov na podlagi člena 33 Splošne uredbe. Najpogosteje so se pojavili izguba ali kraja nosilcev osebnih podatkov (npr. osebnih računalnikov in USB-ključkov), nepooblaščeno dostopanje do osebnih podatkov zaradi programske napake ali zlorabe pooblastil s strani zaposlenih, napad hekerjev na informacijski sistem, onemogočanje dostopa do podatkov zaradi kriptiranja z zlonamerno programsko kodo ter posredovanje osebnih podatkov nepooblaščenim ali napačnim osebam. Pri obravnavi prijav ter izvajanju preventivnih inšpekcijskih nadzorov Informacijski pooblaščenec ugotavlja, da so ugotovljene nepravilnosti ali pomanjkljivosti v veliki meri še vedno posledica nepoznavanja oz. nerazumevanja zakonodaje, kar pa gre pripisati tudi dejstvu, da nov zakon o varstvu osebnih podatkov (ZVOP-2), ki bi jasneje določil posamezna pravila v zvezi z izvajanjem Splošne uredbe, še vedno ni sprejet. Do prijav in kršitev Splošne uredbe pogosto prihaja tudi zato, ker upravljavci posamezniku ob zbiranju osebnih podatkov ne zagotovijo ustreznih oz. popolnih informacij, čemur bo v letu 2020 Informacijski pooblaščenec posvetil dodatno pozornost.

Ker večina zavezancev ne želi kršiti zakonodaje in si želi delovati skladno z zakoni, jim je treba pri tem pomagati in jim ponuditi ustrezna orodja, kot so mnenja, smernice, obrazci, infografike idr. Informacijski pooblaščenec je zato leta 2019 tudi na področju varstva podatkov nadaljeval okrepljeno delovanje za zagotavljanje skladnosti, preventive in pomoči posameznikom. Svetoval je 3.284 posameznikom in pravnim osebam, in sicer je izdal 1.261 pisnih mnenj ter odgovoril na 2.023 telefonskih klicev. Pomembna skupina sogovornikov Informacijskega pooblaščenca so tudi pooblaščene osebe za varstvo osebnih podatkov, ki jih je več kot 2000. Informacijski pooblaščenec uspešno kandidira na razpisih Evropske komisije za projekte iz programa REC (Rights, Equality and Citizenship Programme), prav s ciljem dodatne krepitve vseh teh aktivnosti.

Glede drugih mehanizmov Splošne uredbe iz načela odgovornosti Informacijski pooblaščenec ocenjuje, da se izboljšuje znanje glede izvedb ocen učinkov na varstvo osebnih podatkov, ki so bistvene za zagotavljanje odgovorne uvedbe tveganih oblik obdelave in novih tehnologij pri obdelavi osebnih podatkov. Te bi morale biti tudi ključni element postopka priprav novih predpisov, ki predvidevajo resne posege v zasebnost posameznikov in/ali uvedbo modernih tehnologij.

Izkušnje v letu 2019 so tudi na ravni Evropske unije (EU) in pri sodelovanju v okviru Evropskega odbora za varstvo podatkov (EOVP) pokazale na številne izzive, zlasti glede izvajanja čezmejnih postopkov in razlik v nacionalnih procesnih pravilih v državah članicah EU. Tudi to je eden od razlogov, da so postopki daljši in se prve odločitve pričakuje šele v letu 2020. Odgovore deloma išče EOVP, ki aktivno pristopa k iskanju skupnih opredelitev in interpretacij konceptov v Splošni uredbi, deloma pa k reševanju lahko pristopi tudi evropski zakonodajalec, predvsem v okviru razmislekov o potencialni bodoči reviziji Splošne uredbe.

Izzivi, ki so pred nami na obeh področjih, tudi v letu 2020 niso majhni, a verjamem, da jim bo Informacijski pooblaščenec z dobro ekipo, konstruktivnim sodelovanjem z vsemi deležniki in odprtostjo do posameznikov in organizacij še naprej kos. Vsekakor pa je na področju varstva podatkov velika odgovornost na zakonodajalcu, od katerega je odvisno, kaj bo z varstvom podatkov v Sloveniji v bodoče.

Mojca Prelesnik, informacijska pooblaščenka

STRNJEN PREGLED LETA 2019

DOSTOP DO INFORMACIJ JAVNEGA ZNAČAJA

Informacijski pooblaščenec ugotavlja, da je bilo število pritožbenih zadev na področju dostopa do informacij javnega značaja v letu 2019 na primerljivi ravni kot v letu 2018 (leta 2019 je bilo vloženih 540 pritožbenih zadev). Nadaljuje pa se trend rasti števila pritožb zaradi molka organov (v letu 2018 je Informacijski pooblaščenec obravnaval 213 tovrstnih pritožb, v letu 2019 pa 235), pri čemer zlasti izstopajo organi državne uprave (ministrstva in organi v sestavi).

Podobno kot v letu 2018 se je tudi v letu 2019 povečalo število pritožbenih postopkov glede dostopa do informacij, ki se nanašajo na javne uslužbence in javne funkcionarje (število teh pritožb se je povečalo za 75%). Ker so zavezanci v teh primerih dostop do zahtevanih informacij neutemeljeno zavrnili s sklicevanjem na varovane osebne podatke, Informacijski pooblaščenec opozarja, da so ti podatki tudi po uveljavitvi Splošne uredbe, v skladu s tretjim odstavkom 6. člena ZDIJZ, določeni kot absolutno javni. Takšna je tudi dolgoletna praksa Informacijskega pooblaščenca in Upravnega sodišča.

Tudi v letu 2019 se je povečalo število pritožb, ki se nanašajo na dokumente iz inšpekcijskih postopkov. V teh pritožbenih postopkih je bilo ugotovljeno, da zavezanci pogosto neupravičeno niso uporabili pravila delnega dostopa, ampak so prosilcem dostop zavrnili v celoti, čeprav zahtevane informacije niso v celoti predstavljale zakonskih izjem od prosto dostopnih informacij. Ob tem velja opozoriti, da če dokument ali njegov del le delno vsebuje varovane informacije in je te 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.

Ker morajo zavezanci informacije javnosti posredovati tudi sami, brez zahteve prosilca, jih Informacijski pooblaščenec poziva, naj temu področju namenijo več pozornosti in naj ravnajo proaktivno ter se s tem izognejo morebitnim postopkom po ZDIJZ. V več pritožbenih postopkih so bile namreč predmet zahteve informacije, ki bi jih organi morali že sami javno objavljati po 10. in 10.a členu ZDIJZ.

Podobno kot leta 2018 je tudi za leto 2019 možen zaključek, da zavezanci pri obravnavi zahtev ne namenijo dovolj pozornosti postopkovnim vprašanjem, posledica nepopolnega oz. napačnega ugotovljenega dejanskega stanja s strani zavezanca na prvi stopnji pa je, da se izpodbijane odločbe ne da preizkusiti. V primerih, ko zavezanci 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 odločbe mora biti razvidno, o katerih dokumentih so odločali ter v katerem delu je bila zahteva prosilca zavrnjena. Razlogi, zakaj se dostop do zahtevanih dokumentov zavrne, morajo biti pojasnjeni na način, ki je prosilcem razumljiv in skladen z izrekom odločbe.

Ker se je leta 2019 vnovič povečalo število pritožb zaradi molka pri organih ožje državne uprave, Informacijski pooblaščenec te poziva, naj področju dostopa do informacij javnega značaja namenijo več pozornosti in s tem zagotovijo, da bodo zahteve prosilcev obravnavali v okviru zakonskih rokov.

VARSTVO OSEBNIH PODATKOV

Delo Informacijskega pooblaščenca na področju varstva osebnih podatkov je tudi v letu 2019 v največji meri zaznamovala Splošna uredba, ki je glede na Zakon o varstvu osebnih podatkov (ZVOP-1) obseg nalog in pristojnosti Informacijskega pooblaščenca še razširila. Povečal se je obseg aktivnosti tako pri upravljavcih osebnih podatkov kot tudi pri Informacijskem pooblaščencu. Največji izzivi v letu 2019 so bili na tem področju za vse povezani zlasti z dejstvom, da Slovenija v svoj pravni red še vedno ni sprejela zakona za uporabo Splošne uredbe in prenos Direktive za organe kazenskega pregona.

Z vidika postopkov, za katere je pristojen Informacijski pooblaščenec, so ti izzivi povezani zlasti z vsebinskimi nejasnostmi glede hkratne veljavnosti ZVOP-1 in Splošne uredbe; s procesnimi nedorečenostmi glede vodenja upravnih postopkov reševanja pritožb posameznikov v zvezi z uveljavljanjem njihovih pravic iz členov 13 do 22 Splošne uredbe, kjer Informacijski pooblaščenec nastopa kot pritožbeni organ; ter z odsotnostjo procesnih določb za vodenje prekrškovnih postopkov in izrekanje glob za ugotovljene kršitve. Informacijski pooblaščenec lahko ob odsotnosti ZVOP-2 postopek za prekrške uvede le v primeru, če gre za kršitev tistih členov ZVOP-1, ki še veljajo, ali v primeru kršitev s strani zavezancev po Direktivi za organe kazenskega pregona, za katere do sprejema novih predpisov velja ZVOP-1 v celoti.

Informacijski pooblaščenec torej zaradi odsotnosti novega ZVOP-2 v obravnavanem obdobju ni mogel izrekati sankcij za tiste kršitve, ki so določene zgolj v členu 83 Splošne uredbe. Na težave je Informacijski pooblaščenec večkrat opozoril tudi pristojno ministrstvo. Usklajenost nacionalnih določb s Splošno uredbo pa je pomembna tudi z vidika usklajevanja praks v državah članicah EU prek mehanizma poenotenja izrečenih glob, ki naj bi ga uporabljali vsi nadzorni organi. V primerih čezmejnega sodelovanja pri inšpekcijskem nadzoru to pomeni resno procesno oviro.

Število prijav in pritožb v zvezi z uveljavljanjem pravic posameznikov, ki jih je v obravnavanem obdobju prejel Informacijski pooblaščenec, se je sicer v primerjavi s preteklimi leti nekoliko povečalo (974 prijav in 181 pritožb posameznikov). Poleg tega je Informacijski pooblaščenec v obravnavanem obdobju prejel in obravnaval tudi devet samoprijav glede nedovoljene obdelave osebnih podatkov o pacientih na podlagi Zakona o pacientovih pravicah ter 137 uradnih obvestil o kršitvi varnosti osebnih podatkov na podlagi člena 33 Splošne uredbe. Te prijave so se nanašale zlasti na: izgubo ali krajo nosilcev osebnih podatkov, napad na informacijski sistem ali napad z zlonamerno programsko kodo ter posredovanje osebnih podatkov nepooblaščenim ali napačnim osebam. Do prijav in kršitev Splošne uredbe je pogosto prihajalo zato, ker upravljavci posamezniku ob zbiranju osebnih podatkov niso zagotovili ustreznih oz. popolnih informacij. Te kršitve še vedno spadajo tudi med najpogosteje ugotovljene kršitve. Po uveljavitvi ZVOP-2 bo lahko Informacijski pooblaščenec za takšne kršitve izrekal globo.

Informacijski pooblaščenec na podlagi izvedenih inšpekcijskih pregledov ugotavlja, da so ugotovljene nepravilnosti v veliki meri posledica nepoznavanja oz. nerazumevanja zakonodaje. To gre zlasti pripisati dejstvu, da v Sloveniji še nimamo novih sistemskih predpisov na področju varstva podatkov. Poleg tega so ugotovljene kršitve pogosto posledica malomarnega ali neustreznega zagotavljanja varnosti osebnih podatkov ter namerne nezakonite obdelave osebnih podatkov s strani zaposlenih pri upravljavcih osebnih podatkov, kar se kaže zlasti z nezakonitimi vpogledi v zbirke osebnih podatkov, sporno obdelavo osebnih podatkov za namene neposrednega trženja ter izvajanjem videonadzora delovnih prostorov z namenom nadzora nad zaposlenimi. V obravnavanem obdobju so zaposleni najpogosteje nezakonito vpogledovali v zbirke osebnih podatkov s področja notranjih zadev oz. policije ter v zbirke osebnih podatkov, ki jih vodijo zdravstvene institucije. Informacijski pooblaščenec je v primeru ugotovljenih kršitev vsem kršiteljem z odločbo o prekršku izrekel ustrezno sankcijo. Na področju uveljavljanja pravic posameznikov so pritožbe v 70 primerih zadevale upravljavce iz javnega sektorja (zlasti ministrstva in organe v njihovi sestavi, sodišča, javne zdravstvene zavode in centre za socialno delo), 111 pritožb pa se je nanašalo na upravljavce iz zasebnega sektorja (npr. banke, zavarovalnice, operaterje elektronskih komunikacij, društva, odvetnike in zasebne izvajalce zdravstvene dejavnosti). Le 17 pritožb se je nanašalo na pravico do seznanitve z zdravstveno dokumentacijo.

Informacijski pooblaščenec je zaradi suma kršitev določb ZVOP-1 leta 2019 uvedel 139 postopkov o prekršku, od tega je 83 postopkov uvedel zoper pravne osebe javnega sektorja in njihove odgovorne osebe, 32 zoper pravne osebe zasebnega sektorja in njihove odgovorne osebe, 24 pa zoper posameznike (od tega 19 zoper odgovorne osebe državnih organov in samoupravnih lokalnih skupnosti, pri katerih za prekrške odgovarjajo le njihove odgovorne osebe).

Informacijski pooblaščenec je leta 2019 prejel šest vlog za izdajo dovoljenja za uvedbo biometrijskih ukrepov, 24 vlog za pridobitev dovoljenja za povezovanje zbirk osebnih podatkov in eno vlogo, s katero je vlagatelj zaprosil za odobritev upravnega dogovora, ki se nanaša na prenose osebnih podatkov, pridobljenih pri opravljanju nalog oz. izvajanju pooblastil in odgovornosti med finančnimi nadzornimi organi Evropskega gospodarskega prostora (EGP) in finančnimi nadzornimi organi zunaj EGP. Pridobitev dovoljenja oz. odločba nadzornega organa je v zvezi s prenosom osebnih podatkov v države izven EU in EGP v skladu s Splošno uredbo sicer potrebna le:

- kadar 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));
- kadar 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 zavezujočih poslovnih pravil (člen 47(1)).

Informacijski pooblaščenec je leta 2019 nadaljeval okrepljeno delovanje na področju skladnosti in preventive, in sicer je prek mnenj in v okviru telefonskega dežurstva svetoval 3.284 posameznikom in pravnim osebam, ki so se nanj obrnili z vprašanji s področja varstva osebnih podatkov (izdanih je bilo 1.261 pisnih mnenj in napotitev na mnenja ter opravljenih 2.023 svetovalnih klicev). Vsa mnenja Informacijski pooblaščenec objavlja tudi na svoji spletni strani. Informacijski pooblaščenec ocenjuje, da se je poznavanje določb Splošne uredbe v letu 2019 izboljšalo in da se je med zavezanci izboljšalo razumevanje ključnih konceptov Splošne uredbe, ostajajo pa številne pravne nejasnosti zaradi odsotnosti nacionalnih sistemskih predpisov. Leta 2019 je Informacijski pooblaščenec zaznal splošen trend znatnega povečanja sklepanja pogodb o pogodbeni obdelavi osebnih podatkov med zavezanci. Število mnenj na to temo se je v primerjavi z letom 2018 skoraj potrojilo.

Glede ostalih mehanizmov Splošne uredbe iz načela odgovornosti Informacijski pooblaščenec ocenjuje, da se izboljšuje znanje glede izvedb ocen učinkov na varstvo osebnih podatkov. V okviru postopka predhodnega posvetovanja je Informacijski pooblaščenec v sedmih primerih izdal mnenja glede ocen učinkov. Premalo pa je zavedanja o pomenu ocen učinkov kot ključnega elementa postopka priprav novih predpisov, ki predvidevajo resne posege v zasebnost posameznikov in/ali uvedbo modernih tehnologij. Informacijski pooblaščenec je leta 2019 izdal 73 mnenj na predloge sprememb zakonov ter na predloge novih zakonov in drugih predpisov. Pričakovanja glede Splošne uredbe prav tako niso bila izpolnjena glede kodeksov ravnanja, ki bi lahko združenjem upravljavcev omogočila skladnost. Informacijski pooblaščenec je v mnenje prejel le en primer takega kodeksa, ki pa ga ni predložil ustrezen subjekt. Zaradi odsotnosti nacionalnih izvedbenih predpisov je na ravni Slovenije povsem prezrto tudi področje vzpostavitve mehanizmov certificiranja za varstvo podatkov ter pečatov in označb za varstvo podatkov za izkazovanje, da so dejanja obdelave s strani upravljavcev in obdelovalcev v skladu s Splošno uredbo.

Informacijski pooblaščenec je prav s ciljem krepitve področja preventivnega delovanja uspešno kandidiral na razpisih Evropske komisije za projekte iz programa REC (Rights, Equality and Citizenship Programme). Leta 2019 je tako uspešno nadaljeval izvajanje projekta RAPiD.Si, katerega glavni namen je izobraževanje in ozaveščanje predvsem manjših in srednje velikih podjetij ter posameznikov o reformi zakonodajnega okvira s področja varstva osebnih podatkov, leta 2020 pa bo začel izvajati nov projekt iDECIDE, namenjen povečevanju zavedanja o reformi okvira za varstvo osebnih podatkov predvsem med mladoletniki ter starejšo in delovno populacijo.

Informacijski pooblaščenec je leta 2019 aktivno sodeloval tudi v čezmejnih primerih po načelu »vse na enem mestu« po Splošni uredbi, ki predvideva, da postopek nadzora v čezmejnem primeru obdelave osebnih podatkov vodi t. i. vodilni organ v sodelovanju z drugimi organi za varstvo osebnih podatkov. Informacijski pooblaščenec je leta 2019 izvedel 148 postopkov sodelovanja po členih 60 in 61 Splošne uredbe v zvezi z upravljavci, ki izvajajo čezmejno obdelavo osebnih podatkov, ob tem pa se je v 77 postopkih opredelil za zadevni nadzorni organ (po členu 56 Splošne uredbe). Od tega je sedem postopkov ugotavljanja po členu 56, 14 postopkov sodelovanja po členu 60 in 33 postopkov zagotavljanja medsebojne pomoči po členu 61 Splošne uredbe začel Informacijski pooblaščenec. Pri postopkih v zvezi s čezmejnimi primeri gre zlasti za priljubljene ponudnike komunikacijskih spletnih storitev oz. spletne velikane (Facebook, Google, Amazon, Apple, PayPal, WhatsApp, Twitter, Instagram, Microsoft itd.); Informacijski pooblaščenec v teh primerih 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 inšpekcijskega nadzora, kot ga je uvedla Splošna uredba, je nedvomno ena ključnih novosti in okrepitev, predvsem v smislu enotnega delovanja in skupnega ukrepanja 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, ki jih uporabljajo posamezniki v vseh teh državah. Seveda pa tako sodelovanje za vse nadzorne organe pomeni velik izziv, potrebujejo namreč dodatne vire, tako finančne kot kadrovske. Ob sodelovanju po poglavju 7 Splošne uredbe pa so se leta 2019 pokazali tudi drugi izzivi, ki izvirajo predvsem iz razlik v nacionalnih procesnih pravilih v državah članicah EU – postopki proti velikim multinacionalnim podjetjem so v teh primerih zapleteni in daljši. Prve odločitve v takih primerih bodo znane v letu 2020. Konkreten izziv učinkovitemu vodenju tovrstnih postopkov predstavljajo tudi različne interpretacije konceptov in norm tovrstnega sodelovanja.

Odgovore na izzive deloma išče EOVP, ki izdaja priporočila in smernice, deloma pa bo moral k reševanju pristopiti tudi evropski zakonodajalec, predvsem v okviru razmislekov o potencialni bodoči reviziji Splošne uredbe.

KAZALO

1.1 NASTANEK IN OSEBNA IZKAZNICA INFORMACIJSKEGA POOBLAŠČENCA 2
1.1.1 ORGANIZIRANOST 5
1.2 KLJUČNA PODROČJA DELOVANJA IN PRISTOJNOSTI 8
1.3 FINANČNO POSLOVANJE V LETU 2019 13
2.1 PRAVNA UREDITEV NA PODROČJU DOSTOPA DO INFORMACIJ JAVNEGA ZNAČAJA 18
2.2 ŠTEVILO VLOŽENIH PRITOŽB IN REŠENIH ZADEV 21
2.2.1 PRITOŽBE ZOPER ZAVRNILNE ODLOČBE IN IZDANE ODLOČBE 21
2.2.2 PRITOŽBE ZOPER MOLK 23
2.3 ŠTEVILO VLOŽENIH TOŽB IN PREJETIH SODB 24
2.4 STORJENI PREKRŠKI PO ZDIJZ, ZInfP IN ZMed 24
2.5 IZBRANI PRIMERI NA PODROČJU DOSTOPA DO INFORMACIJ JAVNEGA ZNAČAJA 24
2.6 AKTIVNOSTI IZOBRAŽEVANJA IN OZAVEŠČANJA 33
2.6.1 DAN PRAVICE VEDETI 33
2.6.2 MEDNARODNO SODELOVANJE 34
2.7 SPLOŠNA OCENA IN PRIPOROČILA 34
3.1 KONCEPT VARSTVA OSEBNIH PODATKOV V REPUBLIKI SLOVENIJI 38
3.2 INŠPEKCIJSKI NADZOR V LETU 2019 41
3.2.1 INŠPEKCIJSKI NADZOR V JAVNEM SEKTORJU 43
3.2.2 INŠPEKCIJSKI NADZOR V ZASEBNEM SEKTORJU 44
3.2.3 PRIJAVA KRŠITEV VARNOSTI OSEBNIH PODATKOV 45
3.2.4 SODELOVANJE PRI ČEZMEJNIH INŠPEKCIJSKIH NADZORIH 46
3.2.5 PREKRŠKOVNI POSTOPKI 50
3.2.6 IZBRANI PRIMERI OBDELAVE OSEBNIH PODATKOV 52
3.3 DRUGI UPRAVNI POSTOPKI 59
3.3.1 DOPUSTNOST IZVAJANJA BIOMETRIJSKIH UKREPOV 59
3.3.2 POVEZOVANJE ZBIRK OSEBNIH PODATKOV 60
3.3.3 PRENOS OSEBNIH PODATKOV V TRETJE DRŽAVE 63
3.3.4 PRAVICE POSAMEZNIKOV 64
3.3.5 ZAHTEVA ZA OCENO USTAVNOSTI 66
3.4 PRIPRAVA MNENJ IN POJASNIL 68
3.4.1 SPLOŠNA POJASNILA 68
3.4.2 MNENJA NA PREDPISE 68
3.5 SKLADNOST IN PREVENTIVA 70
3.5.1 OBVEZNOSTI UPRAVLJAVCEV 70
3.5.2 POGODBENA OBDELAVA 71
3.5.3 EVIDENCE OBDELAV 71
3.5.4 OCENE UČINKOV NA VARSTVO OSEBNIH PODATKOV 72
3.5.5 POOBLAŠČENE OSEBE ZA VARSTVO PODATKOV 72
3.5.6 KODEKSI RAVNANJA IN POTRJEVANJE 73
3.5.7 AKTIVNOSTI IZOBRAŽEVANJA IN OZAVEŠČANJA 74
3.5.8 PREVENTIVNE AKTIVNOSTI ZA SKLADNOST 77
3.6 MEDNARODNO SODELOVANJE 77
3.6.1 SODELOVANJE V EVROPSKEM ODBORU ZA VARSTVO PODATKOV 77
3.6.2 SODELOVANJE V DRUGIH NADZORNIH TELESIH EVROPSKE UNIJE 78
3.6.3 SODELOVANJE V DRUGIH MEDNARODNIH TELESIH 79
3.7 SPLOŠNA OCENA STANJA VARSTVA OSEBNIH PODATKOV 81

SEZNAM UPORABLJENIH KRATIC IN OKRAJŠAV 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
ZOIzk-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
ZUstS - Zakon o Ustavnem sodišču
ZGD-1 - Zakon o gospodarskih družbah
ZDavP-2 - Zakon o davčnem postopku
ZJN-3 - Zakon o javnem naročanju
ZPosS - Zakon o poslovni skrivnosti
ZKP - Zakon o kazenskem postopku
ZIN - Zakon o inšpekcijskem nadzoru
ZP-1 - Zakon o prekrških
ZUPJS - Zakon o uveljavljanju pravic iz javnih sredstev

O INFORMACIJSKEM POOBLAŠČENCU

Pod svojo streho združuje dostop do informacij javnega značaja in varstvo osebnih podatkov

1.1 NASTANEK IN OSEBNA IZKAZNICA INFORMACIJSKEGA POOBLAŠČENCA

Informacijski pooblaščenec je samostojen in neodvisen državni organ s pristojnostmi na področju dveh z Ustavo Republike Slovenije zavarovanih temeljnih človekovih pravic, pravico dostopa do informacij javnega značaja in pravico 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.

Obisk predsednika Republike Slovenije, g. Boruta Pahorja, 19. 10. 2019.

LETO 2019 V ŠTEVILKAH

47
zaposlenih

2.232.236,00
EUR proračuna

Varstvo osebnih podatkov

1183
inšpekcijskih postopkov
+11,5%

139
prekrškovni postopek

1261
pisnih mnenj

2023
ustnih mnenj

77
postopkov odločanja o vodilnem nadzornem organu

137
prijav kršitev varnosti

7
mnenj na prejete ocene učinka

2169
imenovanih pooblaščenih oseb za varstvo podatkov

4
preventivne aktivnosti v skladnost

75
mednarodnih sodelovanj “vse na enem mestu”

3
nove smernice

2
obrazca za zavezance

73
postopki vzajemne pomoči drugim nadzornim organom EU

6
infografik

102
predavanji

73
mnenj na predpise

Informacije javnega značaja

540
vloženih pritožb

301
izdana odločba

235
pozivov zaradi molka

42
in camera ogledov

37 dni
povprečen čas reševanja pritožbenih zadev

300
pisnih prošenj za pojasnila

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 sistemizaciji 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 čim učinkovitejšo 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. 2019 je bilo pri Informacijskem pooblaščencu zaposlenih 47 uslužbencev, 46 za nedoločen čas ter eden za določen čas (poslovni sekretar). Izobrazbena struktura zaposlenih je razvidna iz preglednice.

Izobrazbena struktura zaposlenih pri Informacijskem pooblaščencu 31. 12. 2019.

	Srednja strokovna šola	Višja strokovna šola	Visoka strokovna šola, univerzitetni program	Univerzitetna izobrazba	Magisterij	Doktorat	**Skupaj**
Informacijska pooblaščenka				1			**1**
Namestniki informacijske pooblaščenke				2	2		**4**
Vodja mednarodnega sodelovanja in nadzora						1	**1**
Vodja nadzornikov					1		**1**
Generalna sekretarka					1		**1**
Državni nadzorniki za varstvo osebnih podatkov				10	5	1	**16**
Samostojni svetovalec pooblaščenca				1	1		**2**
Svetovalec pooblaščenca za dostop do informacij javnega značaja				5	1		**6**
Svetovalec pooblaščenca za varstvo osebnih podatkov				2	1		**3**
Svetovalec pooblaščenca za preventivo				1			**1**
Asistent svetovalca			1	1			**2**
Raziskovalec			1	1			**2**
Sistemski administrator			1				**1**
Strokovni sodelavec za finančne in kadrovske		1					**1**
Poslovni sekretar			2				**2**
Dokumentalist		1					**1**
Projektni sodelavec	2						**2**
Skupaj	**2**	**2**	**5**	**24**	**12**	**2**	**47**

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

Informacijski pooblaščenec je pristojen tudi za vodenje evidence vseh podeljenih izključnih pravic na področju ponovne uporabe informacij (peti odstavek 36.a člena ZDIJZ).

Na področju dostopa do informacij javnega značaja Informacijskemu pooblaščencu pristojnosti podeljuje tudi Zakon o medijih (ZMed) (45. člen). Po ZMed se zavrnilni odgovor zavezanca na vprašanje, ki ga zastavi predstavnik medija, šteje kot zavrnilna odločba. Molk zavezanca ob takem vprašanju je razlog za pritožbo, o kateri odloča Informacijski pooblaščenec po določbah ZDIJZ.

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

Na delo Informacijskega pooblaščenca **na področju varstva osebnih podatkov** je zelo vplival začetek uporabe **Uredbe (EU) 2016/679 Evropskega parlamenta in Sveta z dne 27. aprila 2016 o varstvu posameznikov pri obdelavi osebnih podatkov in o prostem pretoku takih podatkov ter razveljavitvi Direktive 95/46/ES** (Splošna uredba o varstvu podatkov, Splošna uredba), ki se uporablja neposredno v vseh državah EU od 25. 5. 2018. 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 2019 ni bil sprejet. Zato se poleg Splošne uredbe še vedno uporablja tudi **Zakon o varstvu osebnih podatkov (ZVOP-1)**, in sicer tiste določbe, ki jih uredba ne ureja in ki z njo niso v nasprotju. Tako ima Informacijski pooblaščenec na področju varstva osebnih podatkov naslednje pristojnosti, ki mu jih dajeta **ZVOP-1 in 2. člen ZInfP**:
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 upravljavec osebnih podatkov ne ugodi zahtevi posameznika glede njegove pravice do seznanitve z zahtevanimi podatki, do izpisov, seznamov, vpogledov, potrdil, informacij, pojasnil, prepisovanja ali kopiranja po določbah zakona, ki ureja varstvo osebnih podatkov (pristojnost je določena v 2. členu ZInfP);
3. vodenje postopkov o prekrških s področja varstva osebnih podatkov (hitri postopek);
4. 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);
5. 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);
6. 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;

7. 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;
8. dajanje in objava neobveznih mnenj o skladnosti kodeksov poklicne etike, splošnih pogojev poslovanja oz. njihovih predlogov s predpisi s področja varstva osebnih podatkov;
9. priprava, dajanje in objava neobveznih navodil in priporočil glede varstva osebnih podatkov na posameznem področju;
10. 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 neobvezna mnenja, pojasnila, stališča in priporočila glede varstva osebnih podatkov na posameznih področjih (49. člen ZVOP-1);
11. dajanje izjav za javnost o opravljenih nadzorih in priprava letnega poročila o svojem delu v preteklem letu;
12. 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).

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 osebnih podatkov; 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 osebnih podatkov;
(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 ustreznem 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 osebnih 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 v skladu s členom 40(5) odobri take kodekse ravnanja, ki zagotavljajo zadostne zaščitne ukrepe;
(n) spodbuja vzpostavitev mehanizmov potrjevanja za varstvo podatkov ter pečatov in označb za varstvo podatkov v skladu s členom 42(1) in odobri 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-1), 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 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 terminalski opremi naročnika ali uporabnika s pomočjo piškotkov in podobnih tehnologij;
- kot prekrškovni organ v skladu z zakonom, ki ureja prekrške, vodi postopke zaradi kršitev navedenih določb ZEKom-1; globe za kršitve so določene v 232. do 236. členu ZEKom-1.

ZCKR ureja vzpostavitev centralnega kreditnega registra kot osrednje nacionalne zbirke podatkov o zadolženosti fizičnih oseb in poslovnih subjektov. Del tega registra je tudi sistem izmenjave informacij o

zadolženosti posameznih fizičnih oseb, poznan kot SISBON. Tako register kot sistem izmenjave informacij upravlja Banka Slovenije, ki je v skladu s 366. in 400. členom Zakona o 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.

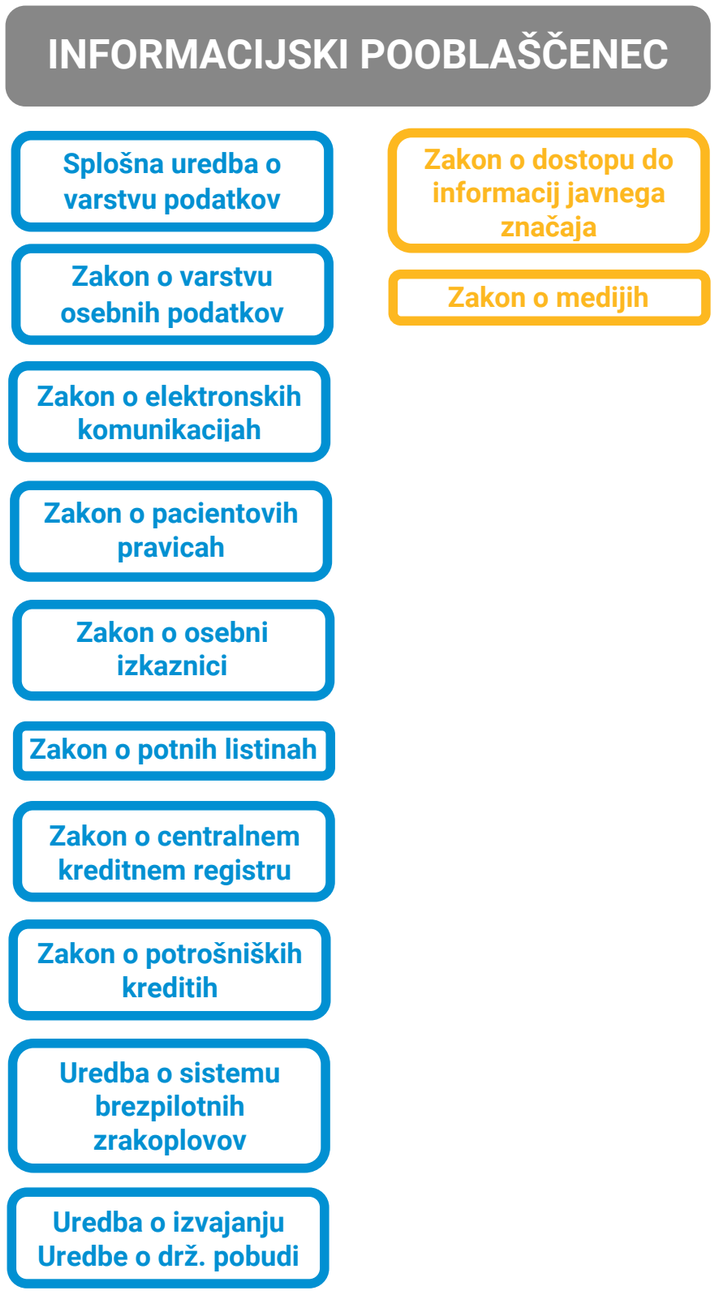
Uredba o sistemih brezpilotnih zrakoplovov v drugem odstavku 21. člena določa, da Informacijski pooblaščenec izvaja nadzor nad izvajanjem petega odstavka 19. člena, ki določa, da mora operater pred izvajanjem letalskih dejavnosti izvesti oceno učinkov v zvezi z varstvom osebnih podatkov na obrazcu iz 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** (ZUstS) 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, ali obdelava in uporaba podatkov, vnesenih v SIS, ne pomeni kršenja pravic oseb, na katere se podatki nanašajo.

Pristojnosti Informacijskega pooblaščenca.



1.3 FINANČNO POSLOVANJE V LETU 2019

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 2019 **veljavni proračun na integralnih postavkah 2.232.236,00 EUR**, od tega na postavki plače 1.871.937,00 EUR, na postavki materialni stroški 346.447,00 EUR in na postavki investicije 13.852,00 EUR. Evidentiranih odredb na integralnih postavkah je bilo na dan 31. 12. 2019 2.229.466,19 EUR, od tega na postavki plače 1.871.932,34 EUR, na postavki materialni stroški 343.682,70 EUR in na postavki investicije 13.851,15 EUR.

Proračun Informacijskega pooblaščenca 2015-2019.

Proračunsko leto	Veljavni proračun
2015	1.243.661,35 EUR
2016	1.335.457,02 EUR
2017	1.459.747,90 EUR
2018	1.833.399,66 EUR
2019	2.232.236,00 EUR

Informacijski pooblaščenec je v letu 2019 razpolagal z namenskimi sredstvi v znesku 7.317,92 EU. Porabe namenskih sredstev v letu 2019 ni bilo.

V proračun leta 2020 bo Informacijski pooblaščenec prenesel skupaj 7.321,05 EUR namenskih sredstev in sredstev donacij, ki so bile financirane s strani Evropske unije (7.317,92 EUR namenskih sredstev, 0,14 EUR donacije – mednarodna spletna stran in 2,99 EUR finančnih sredstev projekta Taiex).

Informacijski pooblaščenec je za pokrivanje tekočih obveznosti novembra prejel 81.700,00 EUR sredstev iz splošne tekoče proračunske rezervacije na podlagi 28. člena Zakona o izvrševanju proračunov Republike Slovenije za leti 2018 in 2019. Z integralnih postavk je bilo decembra 10.000,00 EUR prenesenih na postavko Tekoča proračunska rezerva pri Ministrstvu za finance.

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

Proračun Informacijskega pooblaščenca 2019

	Veljavni proračun v EUR	Prevzete obveznosti v EUR	Razpoložljiv proračun v EUR konec leta
Informacijski pooblaščenec	**2.300.057,05**	**2.289.794,53**	**10.262,52**
Podprogrami			
OPRAVLJANJE DEJAVNOSTI	**2.232.236,00**	**2.229.466,19**	**2.769,81**
PP 1271 Materialni stroški	346.447,00	343.682,70	2.764,30
PP 1273 Investicije	13.852,00	13.851,15	0,85
PP 1267 Plače	1.871.937,00	1.871.932,34	4,66
NAMENSKA SREDSTVA	**7.317,92**	**0,00**	**7.317,92**
7459 Namenska sr. kupnine	7.317,92	0	7.317,92
DONACIJE - EU projekti	**60.503,13**	**60.328,34**	174,79
PP 9958 Mednarodna spl. str.	0,14	0	0,14
PP130134 projekt Taiex	2,99	0,00	2,99
PP 190100 RAPiD.si	60.500,00	60.328,34	171,66

Za materialne stroške je bilo leta 2019 porabljenih 343.682,70 EUR, in sicer za pisarniški in splošni material in storitve 60.789,13 EUR (pisarniški material, čiščenje poslovnih prostorov, storitve varovanja zgradb in prostorov, spremljanje medijev in arhiviranje, stroški prevajalskih storitev, reprezentanca in drugi splošni material in storitve), posebni material in storitve 2.664,66 EUR (nakup drobnega inventarja, zdravniški pregledi zaposlenih in protokolarna darila), energija, voda, komunalne storitve, pošta in komunikacije 39.653,27 EUR (električna energija, ogrevanje, voda in komunalne storitve, odvoz smeti, stroški telefonov ter poštne storitve), prevozni stroški in storitve 9.693,61 EUR (vzdrževanje, popravila, zavarovanje in registracija dveh službenih vozil, gorivo za službeni vozili, najem vozil oz. taksi storitve ter drugi prevozni in transportni stroški), izdatki za službena potovanja 29.584,76 EUR (dnevnice, nočnine, letalske karte, hotelske storitve in stroški prevozov), tekoče vzdrževanje 14.483,81 EUR (najem poslovnih prostorov, zavarovalne premije, vzdrževanje druge opreme ter druge nelicenčne programske opreme – vzdrževanje spletnega mesta ter evidence prisotnosti, tekoče vzdrževanje operativnega informacijskega okolja ter izdatki za tekoče vzdrževanje in zavarovanje), poslovne najemnine in zakupnine 154.875,87 EUR (najemnina in zakupnine za poslovne objekte in parkirne prostore, najem programske računalniške opreme – IUS-INFO in prekrškovni portal), drugi operativni odhodki 31.937,59 EUR (stroški konferenc, seminarjev in simpozijev doma in v tujini, plačila avtorskih honorarjev, izdatki za strokovno izobraževanje zaposlenih, sodni stroški, prispevki za spodbujanje zaposlovanja invalidov - kvote Javnemu jamstvenemu, preživninskemu in invalidskemu skladu). Informacijski pooblaščenec je z naslova refundacij potnih stroškov (letalske karte) od Evropske komisije na postavko prejel 25.570,64 EUR. S postavke materialni stroški je Informacijski pooblaščenec leta 2019 prerazporedil 4.053,00 EUR prostih pravic porabe v Tekočo proračunsko rezervo pri Ministrstvu za finance.

Za investicije je bilo do konca leta 2019 porabljenih 13.851,15 EUR. Sredstva so bila porabljena za nakup pisarniškega pohištva in pisarniške opreme (pisarniški stoli), strojne računalniške opreme (osem monitorjev, tiskalnik in skener), avdiovizualne opreme, opreme za evidenco in kontrolo prisotnosti ter za nakup nematerialnega premoženja (licenca Amebis Besana). Informacijski pooblaščenec je s postavke investicije leta 2019 prerazporedil 2.648,00 EUR prostih pravic porabe v Tekočo proračunsko rezervo pri Ministrstvu za finance.

Za plače zaposlenih je bilo porabljenih 1.871.932,34 EUR oz. 99,99 % glede na veljavni proračun za leto 2019. Glede na predhodna leta se je poraba sredstev povečala zaradi sprostitve napredovanj, realizacije dogovora o plačah in zaradi drugih stroškov dela v javnem sektorju ter aneksov h kolektivnim pogodbam dejavnosti in poklicev, višjega regresa za letni dopust ter dodatnih zaposlitev v skladu s kadrovskim načrtom in novimi pristojnostmi Informacijskega pooblaščenca na področju uveljavitev Splošne uredbe ter 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 uredbe v Republiki Sloveniji je za Informacijskega pooblaščenca pomenila prevzem številnih novih nalog in zadolžitev, ki zahtevajo dodatne zaposlitve. 1.871.932,34 EUR je bilo porabljenih za osnovne plače in dodatke v znesku 1.487.351,17 EUR, regres za letni dopust 40.745,83 EUR, povračila in nadomestila 65.030,24 EUR, sredstva za delovno uspešnost z naslova povečanega obsega dela zaradi povečanega pripada zadev in z naslova EU projekta RAPiD.Si 18.815,90 EUR, druge izdatke zaposlenim 1.155,02 EUR, prispevke delodajalcev za pokojninsko in invalidsko zavarovanje 133.450,29 EUR, prispevke za zdravstveno zavarovanje 106.910,99 EUR, prispevke za zaposlovanje 829,78 EUR, prispevek za starševsko varstvo 1.507,90 EUR ter premije kolektivnega dodatnega pokojninskega zavarovanja na podlagi Zakona o dodatnem pokojninskem zavarovanju javnih uslužbencev 16.135,22 EUR. Informacijski pooblaščenec je leta 2019 od Zavoda za zdravstveno zavarovanje Slovenije z naslova refundacij boleznin in invalidnin prejel sredstva na postavko za plače v višini 27.237,70 EUR. S postavke plače je Informacijski pooblaščenec leta 2019 prerazporedil 3.299,00 EUR prostih pravic porabe v Tekočo proračunsko rezervo pri Ministrstvu za finance.

Namenska sredstva kupnine – v leto 2019 je bilo prenesenih 7.317,92 EUR finančnih sredstev kupnin. Leta 2019 na postavki ni bilo niti prilivov niti porabe. Preostanek finančnih sredstev v višini 7.317,92 EUR se prenese v leto 2020.

Mednarodna spletna stran info-commissioners.org – iz leta 2018 je bilo prenesenih 0,14 EUR finančnih sredstev. Leta 2019 na tej postavki ni bilo porabe. Projekt se leta 2020 zaključi, preostanek sredstev bo nakazan na podračun izvrševanja proračuna.

Projekt Taiex – iz leta 2018 je v bilo v leto 2019 prenesenih 2,99 EUR. Za Taiex projekt leta 2019 ni bilo niti prilivov niti porabe. Projekt se leta 2020 zaključi, preostanek sredstev bo nakazan na podračun izvrševanja proračuna.

Projekt RAPiD.Si – Informacijski pooblaščenec v letih 2019, 2020 in 2021 kot vodilni in edini partner izvaja projekt RAPiD.Si — REC-AG-2017/REC-RDAT-TRAI-AG-2017 – »Raising Awareness on Data Protection and the GDPR in Slovenia — RAPiD.Si«, št. pogodbe 814738. Projekt financira Evropska komisija v okviru Programa za pravice, enakost in državljanstvo 2014–2020. Projekt traja 36 mesecev, osredotoča pa se na aktivnosti izobraževanja in ozaveščanja predvsem malih in srednje velikih slovenskih podjetij ter na dejavnosti ozaveščanja splošne slovenske javnosti o novih pravilih EU glede varstva osebnih podatkov, ki jih prinaša uveljavitev Splošne uredbe in novega ZVOP-2. Za sodelovanje v projektu bo Informacijski pooblaščenec prejel evropska namenska sredstva v načrtovani skupni višini 84.539,00 EUR, sam pa bo v okviru svojih aktivnosti za izvajanje projekta z integralnih proračunskih sredstev zagotovil 21.130,00 EUR. Sredstva bodo porabljena za pokrivanje stroškov, povezanih z delom zaposlenih, za pokrivanje povečanega obsega dela zaposlenih, za stroške izvedbe seminarjev, poti do krajev izvedbe predavanj, za zakup spletne domene in zakup spletnega gostovanja, za telefonske linije 080, za storitve Zveze potrošnikov Slovenije kot podizvajalca v projektu ter za druge stroške v zvezi s pripravo in izvedbo navedenih aktivnosti ter materialnih stroškov, ki jih bo s tem imel Informacijski pooblaščenec.

Dne 29. 9. 2018 je bilo s strani Evropske komisije nakazanih 67.631,20 EUR. Znesek je bil nakazan na poseben račun, odprt pri Upravi za javna plačila. Z rebalansom proračuna za leto 2019 je bil uvrščen nov projekt NRP 1215-19-0001, s katerim so bile povečane pravice porabe za leto 2019, in sicer v znesku 60.500,00 EUR. Za izvajanje projekta je bilo leta 2019 porabljenih 60.328,34 EUR. Poraba leta 2019 za potrebe projekta je na postavkah integralna sredstva, materialni stroški in plače znašala 17.314,66 EUR.

Dne 29. 9. 2018 je bilo s strani Evropske komisije nakazanih 67.631,20 EUR. Znesek je bil nakazan na poseben račun, odprt pri Upravi za javna plačila. Z rebalansom proračuna za leto 2019 je bil uvrščen nov projekt NRP 1215-19-0001, s katerim so bile povečane pravice porabe za leto 2019, in sicer v znesku 60.500,00 EUR. Za izvajanje projekta je bilo leta 2019 porabljenih 60.328,34 EUR. Poraba leta 2019 za potrebe projekta je na postavkah integralna sredstva, materialni stroški in plače znašala 17.314,66 EUR.

Projekt IP-CRISP – Informacijski pooblaščenec je leta 2014 začel sodelovati v projektu v okviru Sedmega okvirnega programa THEME [SEC-2013.5.4-1] – »Evaluation and Certification Schemes for Security Products – Capability«, št. pogodbe 607941. Projekt je bil financiran s strani Evropske komisije, ki jo zastopa Izvajalska agencija za raziskave. Projekt je trajal 36 mesecev. Osredotočen je bil na izboljšanje metodologije za certificiranje varnostnih izdelkov, med drugim upoštevajoč vidike varstva osebnih podatkov. Sodelovanje Informacijskega pooblaščenca kot enega izmed partnerjev projekta je vključevalo sodelovanje zaposlenih pri pripravi posameznih gradiv, analiz, raziskav in drugih aktivnosti ter napotitev zaposlenih na misije in sestanke, na katerih so se izvajale posamezne naloge s področja varstva osebnih podatkov, ki jih je pokrival projekt, med drugim predstavitve, seminarji in delavnice za posamezne ciljne skupine. Zaključno finančno poročilo je bilo po koncu projekta sicer v roku oddano že maja 2017, vendar je Evropska komisija od vseh sedmih partnerjev v projektu zahtevala več dodatnih pojasnil, tako da je bilo finančno poročilo s strani Evropske komisije sprejeto šele decembra 2017. Za sodelovanje v projektu je Informacijski pooblaščenec prejel namenska finančna sredstva v višini 132.400,00 EUR.

Leta 2014 je Evropska komisija nakazala 82.076,50 EUR na poseben račun, odprt pri Upravi za javna plačila. S sklepom Vlade RS so bile povečane pravice porabe za leto 2014 v znesku 9.549,00 EUR. Leta 2014 je bilo za izvajanje projekta porabljenih 9.236,60 EUR ter na postavki integralna sredstva materialni stroški in plače 2.241,72 EUR. Leta 2015 so bile s sklepom Vlade povečane pravice porabe za 22.101,00 EUR. Za izvajanje projekta je bilo porabljenih 22.099,25 EUR. Leta 2016 je bilo s strani Evropske komisije nakazanih 20.802,98 EUR. S sklepom Vlade so bile povečane pravice porabe za leto 2016 v znesku 12.300,00 EUR, s 50.720 EUR na 63,020,00 EUR. Za izvajanje projekta je bilo porabljenih 62.850,63 EUR. Leta 2018 je veljavni proračun znašal 13.441,00 EUR (dovoljena poraba je bila samo 8.209,48,00 EUR, glede na sredstva, prejeta v vseh letih), porabljena so bila finančna sredstva v znesku 8.126,28 EUR, in sicer za pokrivanje stroškov zaposlenih ter stroškov za službene poti. Informacijski pooblaščenec je zadnje nakazilo sredstev v višini 29.520,86 prejel decembra 2018. Projekt se je leta 2018 zaključil, preostanek sredstev bo v letu 2020 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 taka tudi zaščitena na ustavni ravni, se je začela uveljavljati šele 11 let po sprejetju Ustave RS, in sicer s sprejetjem Zakona o dostopu do informacij javnega značaja. 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 razveljavitvi Direktive 90/313/EGS, ki je začela veljati 28. 1. 2003, ter Direktiva 2003/98/ES Evropskega parlamenta in Sveta o ponovni uporabi informacij javnega sektorja, ki je začela veljati 17. 11. 2003, spremenjena z Direktivo 2013/37/EU Evropskega parlamenta in Sveta z dne 26. junija 2013 o spremembi Direktive 2003/98/ES o ponovni uporabi informacij javnega sektorja (UL L št. 175 z dne 27. 6. 2013, str. 1).

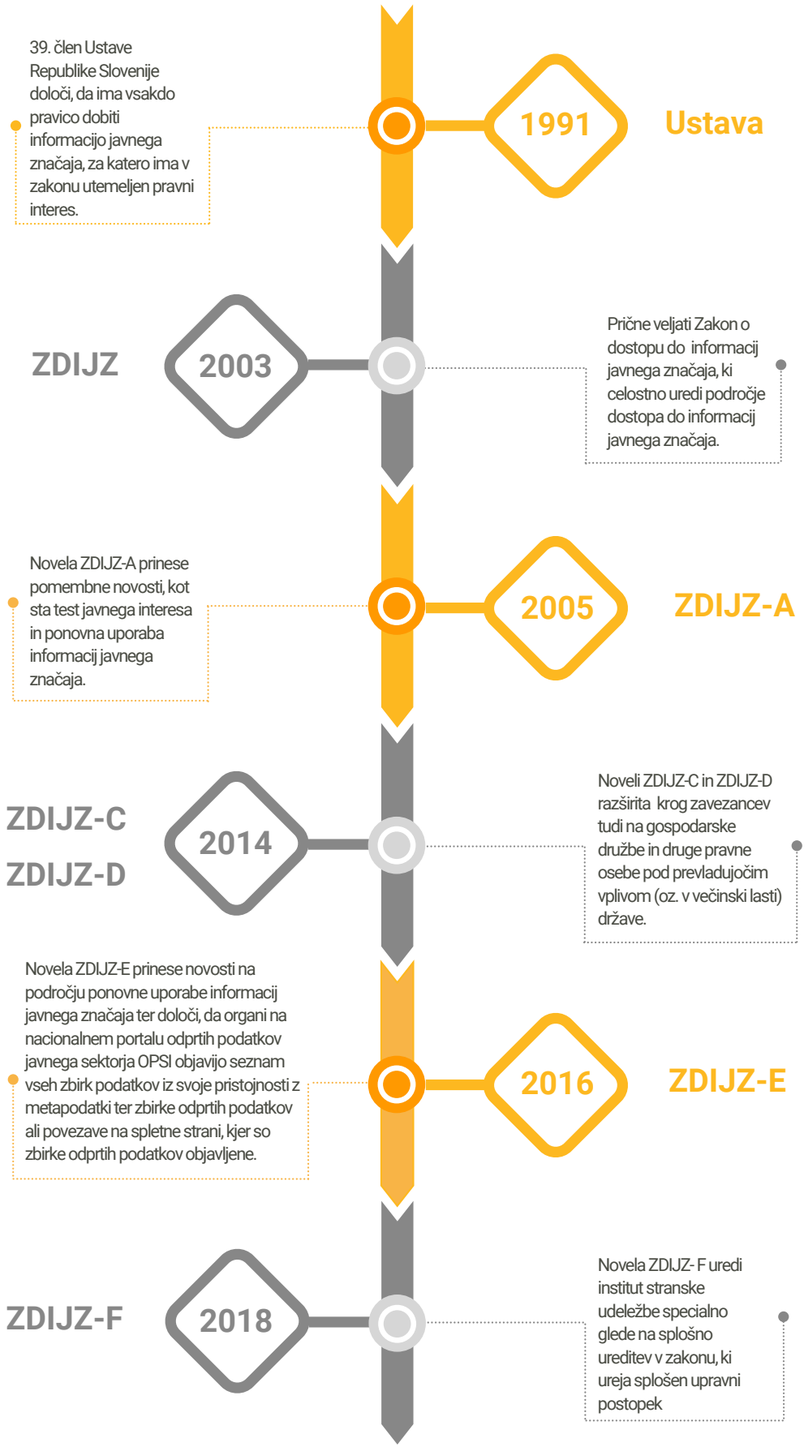
Leta 2005 je bil z novelo ZDIJZ-A narejen še korak naprej. Novela je namreč zožila možnost neupravičenega zapiranja dostopa do informacij in uvedla številne novosti, kot so ponovna uporaba informacij javnega značaja in pristojnosti upravne inšpekcije na področju izvajanja tega zakona. Najpomembnejša 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 finančnih sredstev 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 spletne 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 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.

Časovnica razvoja Zakona o dostopu do informacij javnega značaja.



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) definiran drugače; pri zavezancih iz druge skupine je ožji. Medtem ko **za organe na splošno velja, 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 pa velja ravno obraten miselni proces: informacije javnega značaja so le tisti dokumenti, zadeve, dosjeji, registri, evidence in dokumentarno gradivo, ki jih kot take določa ZDIJZ** (npr. informacije, povezane s sklenjenimi pravnimi posli, ter informacije o članih poslovodnega organa, organa upravljanja in organa nadzora). Za te zavezance velja tudi časovna omejitev, saj se dolžnost posredovanja nanaša le na informacije, nastale v času pod prevladujočim vplivom. Zavezanci, ki izpolnjujejo kriterije za umestitev v obe skupini (npr. gospodarske družbe v 100-odstotni lasti občine, ki so hkrati tudi izvajalke javne službe), so zavezani posredovati obe vrsti informacij javnega značaja. Tisti poslovni subjekti pod prevladujočim vplivom oseb javnega prava, ki hkrati ne sodijo med organe, lahko uporabijo t. i. poenostavljen postopek odločanja o zahtevah (npr. ne izdajo zavrnilne odločbe, ampak vlagatelja pisno obvestijo o razlogih, zaradi katerih informacije ne bodo posredovali). Ostali zavezanci (npr. nosilci javnih pooblastil, ki so hkrati pod prevladujočim vplivom pravnih oseb javnega prava) so dolžni voditi upravni postopek, kot je določen za organe.

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 dobi njen prepis, fotokopijo ali elektronski zapis**. Zavezanec mora o zahtevi odločiti v 20 delovnih dneh, organi lahko v izjemnih okoliščinah podaljšajo rok za največ 30 delovnih dni. **Vpogled v zahtevano informacijo je brezplačen, kadar ne terja izvedbe delnega dostopa**. Za posredovanje prepisa, fotokopije ali elektronskega zapisa zahtevane informacije lahko zavezanec prosilcu zaračuna materialne stroške. Če zavezanec prosilcu zahtevane informacije javnega značaja ne posreduje, ima prosilec v 15 dneh pravico vložiti pritožbo zoper zavrnilno odločbo ali obvestilo, s katerim je zavezanec zahtevo zavrnil. O pritožbi odloča Informacijski pooblaščenec. Prav tako ima prosilec pravico do pritožbe, če mu zavezanec na zahtevo v zakonskem roku ni odgovoril (oz. je v molku) ali če informacije ni dobil v obliki, v kateri jo je zahteval.

Kje so izjeme?

Zavezanec lahko prosilcu dostop do zahtevane informacije zavrne, če se zahteva nanaša na eno izmed izjem, **določenih v prvem odstavku 6. člena ZDIJZ in 5.a členu ZDIJZ** (tajni podatek, poslovna skrivnost, osebni podatek, davčna tajnost, sodni postopek, upravni postopek, statistična zaupnost, dokument v izdelavi, notranje delovanje organa, varovanje naravne 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. Zavezanec pod prevladujočim vplivom prosilcu praviloma ne sme zavrniti dostopa, če gre za absolutno javne informacije (osnovni podatki o poslih, ki se nanašajo na izdatke); razkritju teh podatkov se lahko poslovni subjekt izogne le, če izkaže, da bi to huje škodovalo njegovemu konkurenčnemu položaju na trgu.

Če dokument, ki ga zahteva prosilec, delno vsebuje informacije iz 5.a ali 6. člena ZDIJZ, to ni razlog, da bi

zavezanec zavrnil dostop do celotnega dokumenta. Če je te informacije mogoče iz dokumenta izločiti, ne da bi to ogrozilo njihovo zaupnost, se jih prekrije, prosilcu pa se posreduje preostali del informacij javnega značaja. Zavezanec mora namreč v skladu z 19. členom Uredbe o posredovanju in ponovni uporabi informacij javnega 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), zavezanec pa ga mora o zavrnitvi ali delni zavrnitvi pisno obvestiti do konca naslednjega delovnega dne. V nasprotnem primeru mora zavezanec odgovor na vprašanje poslati najpozneje **v sedmih delovnih dneh** od prejema vprašanja, pri čemer sme odgovor zavrniti le, če so zahtevane informacije izvzete iz prostega dostopa po ZDIJZ. Medij lahko po prejemu odgovora zahteva dodatna pojasnila, ki mu jih mora zavezanec posredovati najpozneje v treh dneh. Če zavezanec z informacijo, ki predstavlja odgovor na vprašanje, ne razpolaga v materializirani obliki, se medij ne more pritožiti zoper obvestilo o zavrnitvi ali delni zavrnitvi odgovora. Pritožba pa je dovoljena, kadar odgovor na vprašanje izhaja iz dokumenta.

2.2 ŠTEVILO VLOŽENIH PRITOŽB IN REŠENIH ZADEV

Leta 2019 je Informacijski pooblaščenec vodil 540 pritožbenih postopkov, od tega 305 postopkov zaradi zavrnitve dostopa do zahtevane informacije (med njimi je bilo 17 pritožbenih postopkov zoper poslovne subjekte pod prevladujočim vplivom oseb javnega prava) in 235 postopkov zaradi t. i. molka organa (neodzivnosti).

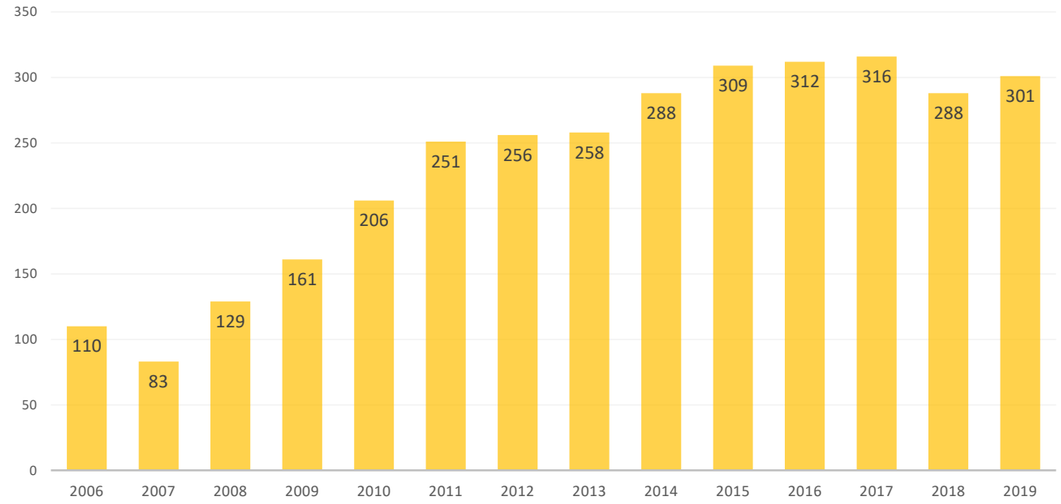
Leta 2019 je Informacijski pooblaščenec odgovoril tudi na 300 pisnih prošenj za neformalno pomoč ali mnenje, ki jih je prejel od zavezancev prve stopnje in prosilcev, odgovoril pa je tudi na 629 zaprosil v okviru telefonskega dežurstva. Vsem je odgovoril v okviru svojih pristojnosti, največkrat jih je 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.

2.2.1 PRITOŽBE ZOPER ZAVRNILNE ODLOČBE IN IZDANE ODLOČBE

V okviru pritožbenih postopkov zoper odločbe, s katerimi so zavezanci v letu 2019 zavrnili zahteve po dostopu do informacij javnega značaja ali zahteve po njihovi ponovni uporabi, je Informacijski pooblaščenec izdal 243 odločb, štiri pritožbe prosilcev pa je s sklepom zavrgel, in sicer dve, ker sta bili prepozni, in dve, ker sta bili nedovoljeni (pritožba zoper sklep, zoper katerega po zakonu ni pritožbe; pritožba zoper odgovor na neformalno vlogo). Informacijski pooblaščenec je poleg omenjenih 243 odločb izdal še 58 odločb, ki so se nanašale na postopke, začete pred letom 2019, skupaj je torej izdal 301 odločbo. Med reševanjem pritožb je opravil 42 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 izdanih odločbah (301):
- pritožbo zavrnil – 136,
- pritožbi delno ali v celoti ugodil oz. rešil zadevo v korist prosilca – 114,
- pritožbi ugodil in zadevo vrnil v ponovno odločanje prvostopenjskemu organu – 48,
- pritožbo zavrgel – 2,
- odločbo prvostopenjskega organa razglasil za nično – 1.

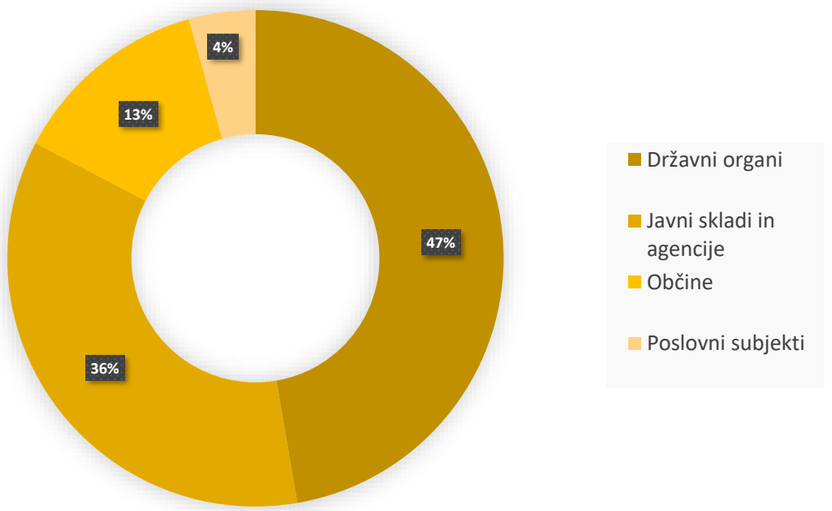
Število izdanih odločb na področju dostopa do informacij javnega značaja med letoma 2006 in 2019.



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

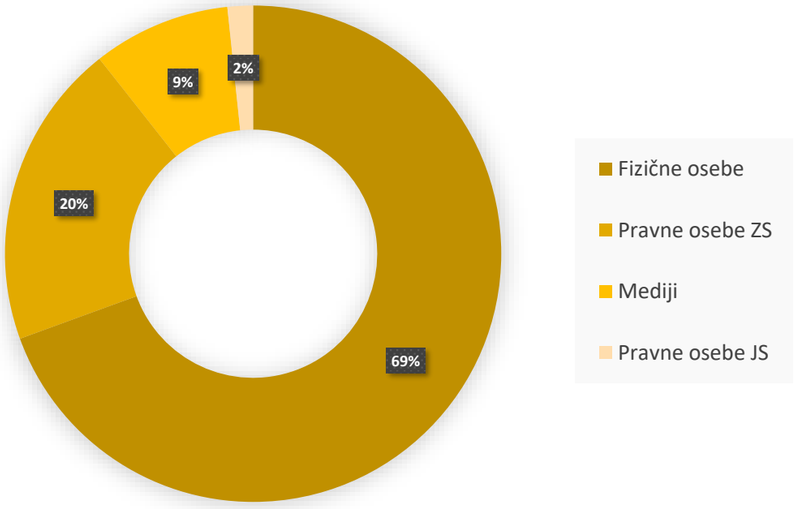
- državni organi – 155, od tega ministrstva in organi v sestavi ter upravne enote 110, sodišča, vrhovno državno tožilstvo in državno odvetništvo pa 33,
- javni skladi, zavodi, agencije, izvajalci javnih služb, nosilci javnih pooblastil in druge pravne osebe javnega prava – 98,
- občine – 36,
- poslovni subjekti pod prevladujočim vplivom države, občin ali drugih oseb javnega prava – 12.

Zoper katere zavezance so bile vložene pritožbe?



V 209 primerih so bili prosilci fizične osebe, v 60 primerih so se pritožile pravne osebe zasebnega sektorja, novinarji in medijske hiše so se pritožili 27-krat, pravne osebe javnega sektorja pa petkrat.

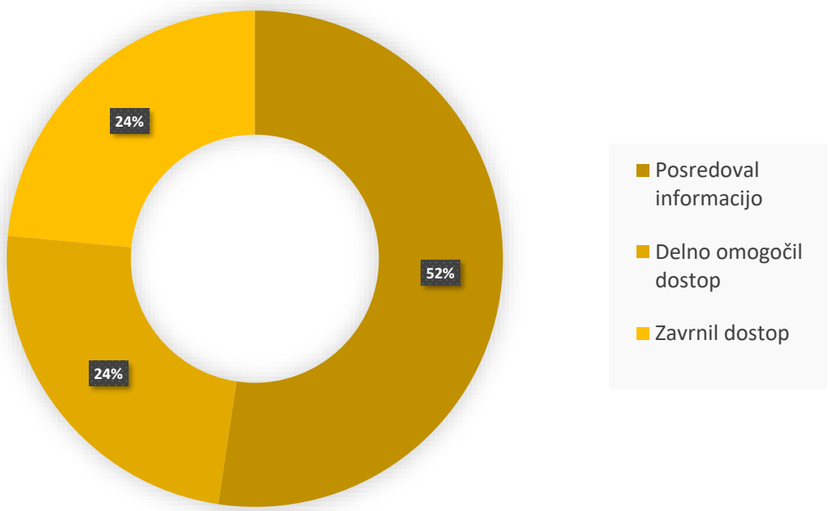
Pritožbe zoper zavrnitev dostopa do informacij.



2.2.2 PRITOŽBE ZOPER MOLK

Informacijski pooblaščenec je v letu 2019 vodil 235 postopkov zaradi molka organa. Po podatkih je bilo največ molka med organi državne uprave (ministrstva, organi v sestavi itd.), občinami ter javnimi zavodi. V pritožbenih postopkih je Informacijski pooblaščenec zaradi molka v 172 primerih zavezance pozval, naj o zahtevi prosilca čim prej odločijo. Po pozivu Informacijskega pooblaščenca so v 89 primerih zavezanci prosilcu informacijo posredovali, v 41 primerih so prosilcu delno omogočili dostop (določene podatke so zakrili oz. omogočili dostop le do določenih informacij, dostop do ostalih pa so z odločbo zavrnili), v 40 primerih so prosilcu dostop zavrnili in mu izdali zavrnilno odločbo, v dveh primerih pa sta zavezanca s sklepom zahtevo prosilca zavrgla.

Kako so ravnali zavezanci po pozivu Informacijskega pooblaščenca zaradi molka?



V 28 primerih je Informacijski pooblaščenec pritožbo s sklepom zavrgel, in sicer v 23 primerih zaradi preuranjenosti, v petih primerih pa zaradi pomanjkljive vloge, ki je prosilec kljub pozivu k dopolnitvi ni dopolnil. V 19 primerih je prosilec tekom postopka pritožbo umaknil, saj je od zavezanca že prejel zahtevano informacijo.

V 15 primerih je Informacijski pooblaščenec postopek z molkom zaključil tako, da je prosilcu pojasnil:
- da za reševanje njegove vloge ni pristojen, in mu svetoval, kako ravnati v zvezi z njegovo zahtevo,
- da vloga, ki jo je prosilec vložil pri zavezancu, ni formalna v skladu z ZDIJZ,
- da zavezanec njegove vloge utemeljeno ni obravnaval po ZDIJZ, temveč na drugi pravni podlagi,
- da je zavezanec njegovo vlogo odstopil v reševanje drugemu zavezancu.

V dveh primerih je Informacijski pooblaščenec prevzel pritožbo v odločanje in sam meritorno odločil.

Izmed vseh 235 molkov je bilo 26 molkov v povezavi z ZMed, največ med organi državne uprave (10), občinami (6) in javnimi zavodi (4).

2.3 ŠTEVILO VLOŽENIH TOŽB IN PREJETIH SODB

Pritožba zoper odločbo Informacijskega pooblaščenca ni dopustna, mogoče pa je sprožiti upravni spor. Leta 2019 je bilo na Upravnem sodišču RS vloženih 34 tožb zoper odločbe Informacijskega pooblaščenca (zoper 11,3 % izdanih odločb) in ena tožba zoper sklep, s katerim je Informacijski pooblaščenec zavrgel predlog za obnovo postopka. 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 2019 odločilo o 52 tožbah, ki so bile vložene zoper odločbe Informacijskega pooblaščenca, in:
- tožbo zavrnilo – 23,
- tožbi ugodilo, izpodbijano odločbo oz. del odločbe odpravilo in zadevo vrnilo Informacijskemu pooblaščencu v ponovno odločanje – 20,
- tožbo zavrglo – 5,
- postopek ustavilo zaradi umika tožbe – 3,
- tožbi delno ugodilo tako, da je v enem delu spremenilo izrek izpodbijane odločbe, v preostalem delu pa je tožbo zavrnilo – 1.

Leta 2019 je en zavezanec na Vrhovno sodišče RS vložil revizijo zoper sodbo Upravnega sodišča.

2.4 STORJENI PREKRŠKI PO ZDIJZ, ZINFP IN ZMED

Leta 2019 Informacijski pooblaščenec ni izdal nobene odločbe o prekršku zaradi kršitev določb ZDIJZ, ZInfP ali ZMed.

2.5 IZBRANI PRIMERI NA PODROČJU DOSTOPA DO INFORMACIJ JAVNEGA ZNAČAJA

Imena in priimki imetnikov diplomatskih potnih listov niso varovani osebni podatki

Prosilec je od Ministrstva RS za zunanje zadeve zahteval vse dokumente, ki se nanašajo na diplomatske potne liste štirih predstavnikov katoliške cerkve. Organ je zahtevo delno zavrnil s sklicevanjem na varstvo osebnih podatkov po 3. točki prvega odstavka 6. člena ZDIJZ. Prosilcu je posredoval zahtevane dokumente, pri čemer je prekril imena in priimke, rojstne datume, nazive, naslove bivanja, elektronske naslove, telefonske številke, lastnoročne podpise in druge podatke, iz katerih bi bilo mogoče sklepati o identiteti imetnikov diplomatskih potnih listin. Obstoja javnega interesa ni ugotovil. V pritožbenem postopku je Informacijski pooblaščenec, skladno z določbo 44. člena Zakona o splošnem upravnem postopku (ZUP), v postopek kot stranske udeležence pozval vse štiri osebe, na katere se je nanašala zahteva za posredovanje informacij javnega značaja. Do izdaje odločbe nihče od pozvanih posameznikov ni priglasil stranske udeležbe. Ker osebni podatek pomeni katero koli informacijo v zvezi z določenim ali določljivim posameznikom, pri čemer je določljiv posameznik

tisti, ki ga je mogoče neposredno ali posredno določiti, je bilo v obravnavani zadevi nesporno, da vsi zahtevani dokumenti vsebujejo osebne podatke konkretnih štirih posameznikov in izpolnjujejo kriterije za izjemo od prostega dostopa po 3. točki prvega odstavka 6. člena ZDIJZ. Iz člena 6(1) Splošne uredbe kot splošno pravilo izhaja, da je obdelava osebnih podatkov (torej tudi razkritje podatkov javnosti) zakonita (dopustna) med drugim takrat, če je obdelava potrebna za izpolnitev zakonske obveznosti, ki velja za upravljavca (točka c), ali pri izvajanju javne oblasti, dodeljene upravljavcu (točka e). Tako zakonsko podlago za obdelavo osebnih podatkov v postopku z zahtevo po ZDIJZ, upoštevajoč točko (c) člena 6(1) Splošne uredbe, lahko predstavlja tudi določba drugega odstavka 6. člena ZDIJZ. Ta določa, da se, ne glede na določbe prejšnjega odstavka (izjeme od prostega dostopa do informacij javnega značaja, op. Informacijskega pooblaščenca), dostop do zahtevane informacije dovoli, če je javni interes glede razkritja močnejši od javnega interesa ali interesa drugih oseb za omejitev dostopa do zahtevane informacije, razen v tam taksativno naštetih primerih, med katerimi pa ni izjeme varstva osebnih podatkov. Pri opravi testa prevladujočega interesa javnosti je Informacijski pooblaščenec izhajal iz ugotovitve, da je prosilec zahteval dokumente, ki so nastali v postopkih izdaje diplomatskih potnih listin, izdanih na podlagi nacionalnega interesa, po vložitvi vloge (prošnje) za izdajo takšnih potnih listih s strani konkretnih štirih posameznikov. Ta nacionalni interes se presoja skladno z Uredbo, ki podrobneje določa merila za ugotavljanje interesa Republike Slovenije, na podlagi katerih se izda diplomatski potni list, ugotavlja pa jih minister za zunanje zadeve. Kot izhaja iz Uredbe, »se pri presoji o izdaji diplomatskega potnega lista, kadar gre za predstavljanje Slovenije v tujini, zlasti upošteva, ali oseba /…/ v kateri od mednarodno široko priznanih in s slovenskim narodom zgodovinsko povezanih verskih skupnosti uživa poseben ugled ali ima v njej visok položaj«. Informacijski pooblaščenec je zato javni interes za razkritje določenih osebnih podatkov konkretnih štirih posameznikov prepoznal v upravičenem interesu javnosti izvedeti, na kakšen način država izvaja politiko izdajanja diplomatskih potnih listin na podlagi nacionalnega interesa, kaj oz. koga šteje za upravičenega imetnika diplomatskega potnega lista, izdanega na podlagi nacionalnega interesa, kadar ga ta potrebuje za predstavljanje Slovenije v tujini, in kdo je oseba, ki uživa poseben ugled v mednarodno široko priznani in s slovenskim narodom zgodovinsko povezani verski skupnosti, ali ima v njej visok položaj. Pri podelitvi diplomatskega potnega lista na podlagi nacionalnega interesa posameznik takšen potni list pridobi v postopku ugotavljanja le-tega, odločanje o njegovem obstoju pa je v diskrecijski pravici ministra za zunanje zadeve. Prav v takšnih primerih je po oceni Informacijskega pooblaščenca pomembna odprtost konkretnih informacij tudi z vidika razumevanja posledic odločitev javnega sektorja. Tako lahko državljani razumejo posledice odločitev javnih organov oz. izrazijo morebitne (bistvene) pomisleke glede takih odločitev. S preglednostjo dela funkcionarjev in uradnikov se zmanjšuje tudi možnost neodgovornega sprejemanja političnih in strokovnih odločitev. Preglednost njihovega dela prispeva k bolj premišljenim odločitvam in s tem k dvigu kakovosti uradništva samega oz. določenih postopkov pri organu ter zmanjševanju korupcijskih tveganj. Ker iz zakonske definicije (prvi odstavek 9. člena ZPLD-1) izhaja, da mora biti izdaja diplomatskih potnih listov konkretnim posameznikom v interesu Republike Slovenije (in ne v njihovem osebnem interesu), se mora po oceni Informacijskega pooblaščenca njihova pravica do varstva osebnih podatkov v delu, ki se nanaša na njihova imena in priimke, umakniti javnemu interesu, ki v tem primeru prevlada. Zaradi upoštevanja načela najmanjšega obsega podatkov (točka (c) člena 5 Splošne uredbe) niso prosto dostopni tisti osebni podatki, ki s samo podelitvijo diplomatskega potnega lista niso v bistveni zvezi, tj. datum in kraj rojstva, bivališče in elektronski naslov.

KLJUČNE BESEDE: osebni podatki, odločba številka 090-285/2018.

Postopki dodeljevanja javnih sredstev morajo biti še posebej transparentni in pregledni

Prosilec je Ministrstvo RS za gospodarski razvoj in tehnologijo zaprosil za ocenjevalni list projekta, ki je nastal v postopku izvedbe javnega razpisa za dodeljevanje spodbud v okviru iniciative EUREKA 2018. Organ je zahtevo delno zavrnil s sklicevanjem na varstvo osebnih podatkov po 3. točki prvega odstavka 6. člena ZDIJZ. Na ocenjevalnem listu je prekril ime in priimek ocenjevalca. Hkrati se je skliceval tudi na izjemo notranjega delovanja po 11. točki prvega odstavka 6. člena ZDIJZ in navedel, da bi mu z razkritjem imena in priimka ocenjevalca nastala škoda. Javnost imen bi lahko imela za posledico nesodelovanje ocenjevalcev, kar bi povzročilo motnje pri dejavnosti oz. delu organa. Razlog za ohranjanje anonimnosti ocenjevalcev, ki niso v delovnem razmerju z organom, temveč sodelujejo z organom na podlagi pogodbe, je tudi zagotavljanje nepristranskega ocenjevanja ter avtonomnosti in neodvisnosti ocenjevalcev. Informacijski pooblaščenec je v pritožbenem postopku ugotovil, da ime in priimek ocenjevalca, ki pogodbeno sodeluje z organom, ni varovan osebni podatek, saj obstaja ena izmed pravnih podlag, naštetih v prvem odstavku člena 6(1) Splošne uredbe, zaradi katere je razkritje podatka zakonito. Ocenjevalec je naveden v bazi ocenjevalcev, ki se vodi pri Javni agenciji RS za spodbujanje podjetništva, internacionalizacije, tujih investicij in tehnologije, in sicer na podlagi

javnega poziva recenzentom tehnološko razvojnih projektov. Organ je z ocenjevalcem v pogodbenem razmerju na podlagi dogovora o sodelovanju, ocenjevalec pa za svoje delo od organa prejme plačilo, in sicer javna sredstva. Za razkritje podatkov o porabi javnih sredstev in za razkritje podatkov, povezanih z opravljanjem javne funkcije, obstaja neposredna podlaga v 1. alineji tretjega odstavka ZDIJZ, ki določa, da se podatki o porabi javnih sredstev in podatki o opravljanju javne funkcije razkrijejo tudi, kadar je podana izjema varstva osebnih podatkov. Ocenjevalec je na zahtevanem dokumentu naveden v okviru funkcije, ki jo opravlja, in za katero je prejel plačilo iz javnih sredstev. Svojo oceno je podal v okviru postopka javnega razpisa, za kar ga je pooblastil organ, kar hkrati pomeni, da gre za informacije, ki so povezane z delom organa. Projekt EUREKA je mednarodna tehnološka pobuda, katere namen je narediti gospodarstva EU konkurenčnejša. V okviru projekta organ nastopa v vlogi posredniškega organa in zagotavlja finančna sredstva za izvedbo javnega razpisa; kot izhaja iz samega razpisa, sredstva delno zagotavlja EU in delno Slovenija. Ker je organ prenesel svojo javno funkcijo na tretje osebe, so te prevzele nase določene naloge, ki sicer primarno sodijo v izvajanje javne funkcije organa. Posledično je ocenjevalčevo delo podvrženo enakemu režimu, kot če bi to oceno izvedel organ sam. Ocenjevalčevo delo zahteva visoko strokovnost in nepristranskost; ocenjevalec ne more biti kdor koli, temveč gre za zunanje strokovnjake, ki so izbrani za vsako področje posebej. Podatek o tem, kako je ocenjevalec posamezen projekt ocenil, ne more predstavljati osebnega podatka ocenjevalca, ker slednje ne sodi v njegovo osebno sfero in ne razkriva nobenih informacij o ocenjevalcu kot posamezniku. Podatek o imenu in priimku ocenjevalca pa ne more ustrezati niti definiciji izjeme »notranjega delovanja organa«, saj je ta namenjena temu, da varuje »notranje razmišljanje organa«, ne pa zunanje subjekte, ki sodelujejo z organom zaradi svoje strokovnosti na določenem področju. Postopek javnega razpisa je praviloma javen, torej ne gre za »notranje razmišljanje organa«, pri ocenjevanju prijav, prispelih na javni razpis, pa tudi ne gre za »notranje delovanje organa«, saj je od ocen odvisna podelitev spodbud organa. Pristojnost organa, vezana na odločanje v postopkih javnega razpisa, predstavlja tipičen primer »zunanjega delovanja«, saj gre za javni razpis, s katerim se pri različnih projektih praviloma javno odloča o zunanjih prijaviteljih. Zmotno je bilo tudi izhodišče organa, da je le z anonimnostjo mogoče doseči nepristransko in avtonomno ocenjevanje projektov. Posameznika, ki ocenjuje, morajo odlikovati strokovna avtoriteta, integriteta in visoka moralna drža; nepristranskost in neodvisnost ocenjevalcev se doseže s strokovnim delom, pravilnim pristopom in odnosom, preglednimi zaključki in kakovostnim delom. Javnost ocenjevalcev je nujna zaradi preglednosti delovanja organa, preglednosti dodeljevanja javnih sredstev, možnosti preverbe, ali so bili ocenjevalci kompetentni in strokovni na področju, ki so ga ocenjevali, ter možnosti, da prijavitelji preverijo (ne)obstoj razlogov, zaradi katerih bi jih konkretni ocenjevalec lahko ocenil pristransko in nepošteno. Informacijski pooblaščenec je organu odredil, da prosilcu posreduje tudi ime in priimek ocenjevalca.

KLJUČNE BESEDE: osebni podatki, notranje delovanje, odločba številka 090-110/2019/5

Predhodno opozorilo na plačilo stroškov posredovanja informacij je obvezno

Prosilec je od Občine Oplotnica zahteval kopije plačanih računov stroškov, ki jih je plačal najemnik poslovnega prostora v športni dvorani. Organ je prosilcu posredoval fotokopije računov s prilogami ter izdal sklep o plačilu materialnih stroškov posredovanja informacij. V pritožbi je prosilec izpostavil, da je zahteval zgolj račune, ki jih plačuje najemnik poslovnega prostora, in ne vseh računov, ki jih plačuje organ. Ker je menil, da mu je bil kup papirja, ki ga ni zahteval, posredovan z določenim namenom, je oporekal plačilu stroškov v celoti. Predmet pritožbe v obravnavani zadevi je bilo vprašanje pravilnosti in utemeljenosti zaračunanih stroškov dostopa do informacij javnega značaja. Glede na ZDIJZ in Uredbo o posredovanju in ponovni uporabi informacij javnega značaja ni dvoma, da organ prosilcu lahko zaračuna stroške posredovanja zahtevanih informacij. Pri tem pa mora izpolniti vse zakonske določbe, ki urejajo zaračunavanje stroškov posredovanja informacij. Predvsem je organ dolžan prosilca opozoriti na plačilo stroškov in, če prosilec to zahteva, prosilcu vnaprej sporočiti višino stroškov, ki mu jih bo zaračunal za posredovanje informacij. V pritožbenem postopku se utemeljenost same višine stroškov ugotavlja šele po ugotovitvi, ali je organ zadostil zahtevam glede objave stroškovnika ter ali je prosilca opozoril na plačilo stroškov. Glede na to, da je enotni stroškovnik objavljen v Uredbi o posredovanju in ponovni uporabi informacij javnega značaja, ki je javno objavljena v uradnem listu, je Informacijski pooblaščenec štel, da tega stroškovnika organu ni treba objaviti tudi v njegovem katalogu informacij javnega značaja, nedvomno pa organu še vedno ostane obveznost, da prosilca vnaprej obvesti o tem, da mu namerava zaračunati stroške. Takšno obvestilo prosilcu omogoča, da si glede posredovanja zahtevanih informacij lahko premisli, še preden mu organ posreduje zahtevane informacije. V pritožbenem postopku je organ na izrecni poziv Informacijskega pooblaščenca pojasnil, da prosilca ni predhodno obvestil o tem, da bo potrebno plačilo stroškov. Informacijski pooblaščenec je tako ugotovil, da organ v obravnavanem primeru ni zadostil zakonski predpostavki iz tretjega odstavka 36. člena ZDIJZ, zato je pritožbi ugodil in sklep

o plačilu materialnih stroškov posredovanja informacij odpravil.

KLJUČNE BESEDE: stroški, odločba številka 090-112/2019

Priklic obstoječih podatkov iz računalniške baze ne pomeni ustvarjanja novega dokumenta

Prosilec je od Agencije RS za okolje zahteval podatek o številu in vrsti upravnih postopkov, v katerih je stranka določena gospodarska družba oz. v katerih stranko zastopa določen odvetnik. Organ je zahtevo zavrnil s sklicevanjem na četrto točko 5. člena ZDIJZ, ki določa, da organ ni dolžan zagotavljati pretvorbe iz ene oblike v drugo ali zagotoviti izvlečkov iz dokumentov, kadar bi to pomenilo nesorazmeren napor izven preprostega postopka, ter tudi ne nadaljevati z ustvarjanjem določenih informacij samo zaradi ponovne uporabe s strani drugih organov ali oseb. Prosilec je odločitev organa ugovarjal, saj ni bilo dvoma, da je zahteval informacije, kakršne naslovni organ hrani v svoji računalniški bazi podatkov. Ob odstopu pritožbe je organ navedel, da je prosilec zahteval podatke, ki niso informacije javnega značaja v smislu prvega odstavka 4. člena ZDIJZ, saj ni zahteval podatkov glede emisij v okolje, odpadkov, nevarnih snovi v obratu ali podatkov iz varnostnega poročila in drugih podatkov, za katere tako določa zakon, ki ureja varstvo okolja. V pritožbenem postopku je Informacijski pooblaščenec ugotovil, da po določbah ZDIJZ celotno delovno področje organa zajema vse javnopravne naloge, ki jih opravlja organ, in tudi vse dejavnosti, ki se opravljajo v zvezi s temi nalogami, zato so bile navedbe, da prosilec ni zahteval informacij javnega značaja, neutemeljene. Ker je organ v izpodbijani odločbi navedel, da z zahtevanimi informacijami ne razpolaga, je Informacijski pooblaščenec ugotavljal tudi, ali je pri zahtevanih informacijah izpolnjen t. i. kriterij materializirane oblike. Informacijski pooblaščenec je izvedel t. i. ogled in camera, pri katerem je ugotovil, da se v elektronski bazi Lotus Notes v povezavi z gospodarsko družbo kot odvetnikom pojavijo zadetki tako med rešenimi zadevami kot med zadevami v reševanju. Z vpogledom v omenjeni sistem je Informacijski pooblaščenec zaključil, da so v njem zavedene praktično vse zahtevane informacije in da jih je mogoče pridobiti na enostaven način. Tako je Informacijski pooblaščenec izpodbijano odločbo odpravil in organu odredil posredovanje izpisov iz elektronske evidence upravnih zadev organa.

KLJUČNE BESEDE: ali dokument obstaja, odločba številka 090-34/2019

Deli dokumenta, ki se nanašajo na porabo javnih sredstev, niso poslovna skrivnost

Prosilec (novinar) je od Slovenskega državnega holdinga zahteval Sporazum o prekinitvi delovnega razmerja s predsednico uprave. Organ je zahtevo prosilca zavrnil s sklicevanjem na izjemo varstva poslovne skrivnosti po 2. točki prvega odstavka 6. člena ZDIJZ. Prosilec se je na odločitev pritožil, saj je menil, da so podatki, koliko sredstev oz. kaj vse je pripadlo predsednici uprave na podlagi sporazuma o predčasni prekinitvi delovnega razmerja, v absolutnem interesu javnosti. V pritožbenem postopku je Informacijski pooblaščenec ugotovil, da je glede zahtevanega sporazuma izpolnjen kriterij za poslovno skrivnost po prvem odstavku 39. člena Zakona o gospodarskih družbah (ZGD-1). Ta določa, da se za poslovno skrivnost štejejo podatki, za katere tako določi družba s pisnim sklepom; s tem sklepom morajo biti seznanjeni družbeniki, delavci, člani organov in druge osebe, ki morajo varovati poslovno skrivnost. Toda čeprav je zahtevani sporazum predstavljal poslovno skrivnost po subjektivnem kriteriju, je Informacijski pooblaščenec ugotovil, da zahtevane informacije predstavljajo podatke, ki skladno s tretjim odstavkom 39. člena ZGD-1 ne morejo biti določeni za poslovno skrivnost. Sporazum je namreč vseboval podatke, ki so po zakonu javni, in sicer po 1. alineji tretjega odstavka 6. člena ZDIJZ. Ta določa, da se ne glede na določbe prvega odstavka 6. člena ZDIJZ (tj. ne glede na podano izjemo poslovne skrivnosti) dostop do zahtevane informacije dovoli, če gre za podatke o porabi javnih sredstev, razen v primerih iz 1. in 5. do 8. točke prvega odstavka 6. člena ZDIJZ ali v primerih, ko zakon, ki ureja javne finance, ali zakon, ki ureja javna naročila, določa drugače. Čeprav ZDIJZ ne vsebuje definicije javnih sredstev, se je ta za potrebe postopkov dostopa do informacij javnega značaja izoblikovala s prakso Informacijskega pooblaščenca in sodišč. Pojem porabe javni sredstev (tako npr. sodba Upravnega sodišča I U 764/2015-27 z dne 24. 8. 2016) pomeni vsako odplačno ali neodplačno razpolaganje s premoženjem, tudi sprememba ali pretvorba premoženja iz ene oblike v drugo; tako poraba javnih sredstev niso le odlivi z računa neke javne inštitucije, ampak tudi vse druge odplačne ali neodplačne oblike razpolaganja z javnimi sredstvi. Iz javnopravne narave in predvsem iz nalog, za izpolnjevanje katerih je bil organ ustanovljen, ter izvora oz. svojstva premoženja, s katerim organ upravlja, je nesporno, da razpolaga in upravlja z javnimi sredstvi ter da je vsakršno razpolaganje z javnimi sredstvi (tudi v primeru izplačil oz. zavez k izplačilom javnih sredstev) javno. Informacijski pooblaščenec je zato odredil, da organ prosilcu posreduje tiste dele zahtevanega dokumenta, iz katerih izhajajo razlogi, pogoji in višina izplačil javnih sredstev.

KLJUČNE BESEDE: poslovna skrivnost, mediji, odločba številka 090-130/2019

Dostop do osebnih podatkov absolutno javnih oseb je prost skozi prizmo javnega interesa

Prosilec je od Vrhovnega državnega tožilstva zahteval dostop do kazenskih ovadb proti nekdanjemu mariborskemu županu in do dokumentov, ki kažejo, kako so se ti postopki zaključili. Organ je zahtevo zavrnil s sklicevanjem na izjemo varstva osebnih podatkov. Prosilec se je na odločitev organa pritožil, saj obstoječa praksa na tem področju – konkretno javna objava sodb – kaže, da se prednost daje vrednoti dostopa do informacij. Vrhovno sodišče javno objavlja tako obsodilne kot oprostilne sodbe oz. so te dostopne z zahtevo po ZDIJZ. Čeprav skladno z ZDIJZ prosilcu ni treba pojasnjevati razloga, zakaj želi imeti dostop do zahtevane informacije, je navedel, da je zahtevo vložil izključno z namenom nadzora nad delom tožilstva. V pritožbenem postopku je Informacijski pooblaščenec, skladno z določbo 44. člena ZUP, v postopek pozval tudi nekdanjega mariborskega župana, ki je udeležbo tudi priglasil. Informacijski pooblaščenec je stališče organa, da podatki iz sklepov o zavrženju ovadb niso prosto dostopne informacije javnega značaja, ker bi razkritje lahko vplivalo na pridobivanje dokazov v morebitnem novem postopku, ocenil kot napačno. Razkritje teh podatkov že pojmovno ne more škodovati njihovi izvedbi, saj so bile ovadbe zavržene in so bili s tem postopki zaključeni. Iz besedila določila 6. točke prvega odstavka 6. člena ZDIJZ izhaja, da se sme dostop zavrniti le v primeru, če se podatek nanaša na konkretne kazenske postopke, ki pa so v obravnavanem primeru (že) zaključeni z zavrženjem ovadb. V zvezi z varstvom osebnih podatkov je Informacijski pooblaščenec ugotovil, da je za razkritje nekaterih zahtevanih informacij podan javni interes, saj je nekdanji mariborski župan absolutna javna oseba par excellence, za katero velja, da mora na račun svoje zasebnosti trpeti večje omejitve, kot bi jih bila dolžna trpeti sicer. Čeprav se organ in stranski udeleženec do obstoja javnega interesa nista opredelila, je Informacijski pooblaščenec javni interes prepoznal zlasti v tem: (a) da je stranski udeleženec kot nosilec uradnih (političnih) funkcij absolutna javna oseba par excellence, (b) da se tematika zahtevanih dokumentov nanaša na informacije, ki so neposredno povezane z družbeno vlogo in funkcijo stranskega udeleženca in z njegovimi ravnanji v okviru ali v neposredni povezavi s to družbeno vlogo (vsebina dokumentov je močno povezana z opravljanjem javne funkcije stranskega udeleženca), (c) da so zahtevane informacije pomembne za javno razpravo o relevantnih vprašanjih oz. zadevah v demokratični družbi (ocena pravilnosti in zakonitosti dela organov odkrivanja in pregona kaznivih dejanj, ki so jih v kazenskih postopkih podala sodišča), (d) da se z delnim dostopom do zahtevanih dokumentov omogoča pregled ravnanja tožilstva in policije pri odločanju v pomembnih javnih zadevah. Tako je Informacijski pooblaščenec pritožbi ugodil in odredil delni dostop do dokumentov, ki so izkazovali, kako so se zaključili (pred)kazenski postopki zoper nekdanjega župana Mestne občine Maribor. Podatki, do katerih je Informacijski pooblaščenec dostop odobril, so obsegali zakonske označbe kaznivega dejanja z navedbami določb kazenskega zakona, ki naj se po predlogu tožilca uporabijo, sodišče, pred katerim je tekel kazenski postopek, tiste dele posameznih obrazložitev, ki vsebujejo pravno podlago za posamezno ravnanje pristojnih organov, splošni opis očitanega kaznivega dejanja, pravni pouk, odločitev o stroških.

KLJUČNE BESEDE: osebni podatek, test interesa javnosti, številka odločbe 090-276/2018

Podatki o enolični identifikacijski številki državnega tožilca so podatki, povezani z opravljanjem javne funkcije

Prosilec je od Vrhovnega državnega tožilstva zahteval posredovanje elektronskih zapisov vseh posebnih statističnih delov letnih poročil vseh državnih tožilstev, ki so bili do vložitve zahteve izdelani in posredovani skladno s Pravilnikom o obliki letnega poročila o poslovanju državnega tožilstva. Organ je prosilcu zavrnil dostop do »enolične identifikacijske (ID) številke državnega tožilca« in »enolične (ID) številke kaznivega dejanja« s sklicevanjem na izjemo varstva osebnih podatkov in varstva kazenskega postopka. Pri tem je navedel, da je prek povezave ID tožilca in ID kaznivega dejanja omogočeno lociranje osebnih podatkov v zvezi s konkretnim posameznikom ter se lahko tako neposredno ali posredno identificira posameznega državnega tožilca. S povezavo med obema ID-podatkoma lahko pride do razkritja identitete pristojnega tožilca, ki obravnava konkretno kaznivo dejanje, v fazi, v kateri bi razkritje škodovalo interesom kazenskega postopka, saj zahtevana informacija ob dodatnem raziskovanju, a brez večjega napora omogoča tudi identifikacijo posamezne kazenske zadeve. Prosilec se je na odločitev organa pritožil, saj je menil, da šifra državnega tožilca ne predstavlja njegovega varovanega osebnega podatka, ampak zgolj podatek o izvrševanju javne funkcije, ki razkriva, da je določeni državni tožilec opravil nekatera procesna dejanja oz. kakšen je bil obseg njegovega dela. Informacijski pooblaščenec je v pritožbenem postopku ugotovil, da je obdelava osebnih podatkov zakonita, če je podana ena od pravnih podlag, ki jih določa Splošna uredba v prvem odstavku člena

6. Iz tega člena kot splošno pravilo izhaja, da je obdelava osebnih podatkov (torej tudi razkritje podatkov javnosti) zakonita (dopustna), med drugim v primeru, če je obdelava potrebna za izpolnitev zakonske obveznosti, ki velja za upravljavca (točka c), ali pri izvajanju javne oblasti, dodeljene upravljavcu (točka e). Tako zakonsko podlago za obdelavo osebnih podatkov v postopku z zahtevo po ZDIJZ, upoštevajoč točko c člena 6(1) Splošne uredbe, predstavlja 1. alineja tretjega odstavka 6. člena ZDIJZ. Ta določa, da se dostop do zahtevane informacije dovoli, če gre za podatke o porabi javnih sredstev ali za podatke, povezane z opravljanjem javne funkcije ali delovnega razmerja javnega uslužbenca, razen v primerih iz 1. in 5. do 8. točke prvega odstavka ter v primerih, ko zakon, ki ureja javne finance, ali zakon, ki ureja javna naročila, določa drugače. Nesporno je torej, da primer iz 3. točke prvega odstavka 6. člena ZDIJZ (varstvo osebnih podatkov) ne sodi med tiste zakonske izjeme, ki bi bile izvzete iz dolžnosti organa do posredovanja zahtevanih informacij, če so povezane z opravljanjem javne funkcije ali delovnega razmerja javnega uslužbenca. Podatek o enolični identifikacijski (ID) številki državnega tožilca se nanaša na posameznega državnega tožilca in predstavlja njegovo anonimizirano šifro (13. člen Pravilnika), ki mu je dodeljena za potrebe opravljanja nalog iz njegove pristojnosti, zato je Informacijski pooblaščenec menil, da gre za podatek, ki je povezan z opravljanem njegove javne funkcije. Podatek o enolični identifikacijski številki (ID) kaznivega dejanja pojmovno ne more predstavljati osebnega podatka, saj gre za enolično oznako kaznivega dejanja. Organ tudi ni uspel izkazati obstoja izjeme po 6. točki prvega odstavka 6. člena ZDIJZ. Za uspešno sklicevanje na izjemo varstva kazenskega postopka morata biti kumulativno izpolnjena dva pogoja: (1) zahtevan podatek je bil pridobljen ali sestavljen zaradi konkretnega kazenskega pregona ali v zvezi z njim in (2) razkritje zahtevanega podatka bi škodovalo izvedbi konkretnega postopka. Iz besedila določila točke 6 prvega odstavka 6. člena ZDIJZ izhaja, da se sme dostop zavrniti le v primeru, če se podatek nanaša na konkretne kazenske postopke, ki so še v teku. Tega določila ni mogoče razlagati tako široko, da bi se lahko to izjemo uveljavljalo tudi v primeru bodočih (»ponovno odprtih«) kazenskih pregonov, pri čemer se je Informacijski pooblaščenec strinjal s stališčem prosilca, da bi s tako široko razlago organ lahko vse informacije o pregonu prikrival vse do zastaranja kazenskega pregona. Ker ID številka državnega tožilca ni varovan osebni podatek, za prekritje ID številke kaznivega dejanja pa organ ni izkazal pogoja nastanka škode za postopek, je Informacijski pooblaščenec organu odredil posredovanje zahtevanih podatkov.

KLJUČNE BESEDE: kazenski postopek, osebni podatek, odločba številka 090-3/2019

Podatki, ki jih FURS potrebuje za izračun davka, so davčna tajnost

Prosilka je od Javnega zavoda Lekarne Ljubljana zahtevala dostop do davčnih obračunov za leti 2016 in 2017, kot ju je organ posredoval Finančni upravi RS (FURS). Organ je zahtevo zavrnil, ker sta zahtevana davčna obračuna predstavljala in vsebovala podatke, ki so bili po pravilniku in sklepu o določitvi poslovne skrivnosti opredeljeni kot poslovna skrivnost. Prosilka je v pritožbi navedla, da organ opravlja gospodarsko dejavnost lekarništva, ki je predmet konkurenčnih pravil EU, in da pri svojem poslovanju ustvarja velike dobičke, zato je ugotovitev, ali so pri davčni obremenitvi različni izvajalci lekarniške dejavnosti obravnavani enako, v javnem interesu. Prosilka je še dodala, da sta v interesu javnosti tudi ugotovitvi, ali se na lekarniškem trgu na podlagi davčne neenakosti izkrivlja konkurenca oz. prihaja do dejanj nelojalne konkurence ter kolikšne so razsežnosti te težave, ki vpliva tudi na maloprodajne cene lekarniških izdelkov. V pritožbenem postopku ni bilo moč pritrditi navedbam prosilke, da organ opravlja gospodarsko dejavnost lekarništva, ki je predmet konkurenčnih pravil EU. Kot izhaja iz Zakona o lekarniški dejavnosti, je lekarniška dejavnost v Sloveniji urejena kot javna zdravstvena služba, zato mora organ kot javni zavod delovati v javnem interesu in porabljati javna sredstva za namen izvajanja javne službe oz. v okviru omejitev, ki mu jih nalaga zakon. Organ je dostop do zahtevanih davčnih obračunov zavrnil na podlagi izjeme varstva poslovne skrivnosti po 2. točki prvega odstavka 6. člena ZDIJZ, vendar je Informacijski pooblaščenec ugotovil, da gre v obravnavanem primeru za podatke, ki predstavljajo davčno tajnost po Zakonu o davčnem postopku (ZDavP-2). Skladno s 5. točko prvega odstavka 6. člena ZDIJZ organ zavrne dostop do zahtevane informacije, če se zahteva nanaša na podatek, katerega razkritje bi pomenilo kršitev zaupnosti davčnega postopka ali davčne tajnosti, skladno z zakonom, ki ureja davčni postopek. V pritožbenem postopku je Informacijski pooblaščenec ugotovil, da bi razkritje zahtevanih dokumentov, ki se nanašajo na ugotavljanje davčne obveznosti, pomenilo kršitev zaupnosti davčnega postopka ali davčne tajnosti. ZDavP-2 v 8. členu določa, da se podatki zavezancev za davek obravnavajo kot davčna tajnost v skladu s tem zakonom in zakonom o obdavčenju in drugimi splošnimi akti, ki urejajo pobiranje davkov. Z omenjeno določbo je zakonodajalec tako začrtal zelo široko pojmovanje davčne tajnosti. Zahtevane podatke je organ posredoval FURS na predpisanem obrazcu za obračun davka od dohodkov pravnih oseb, ki ga določa Pravilnik o davčnem obračunu od dohodkov pravnih oseb, podatki

se nanašajo na organ kot davčnega zavezanca in so v neposredni zvezi s samo davčno obveznostjo. Vsi pogoji za predmetno izjemo so bili v obravnavani zadevi nedvomno izpolnjeni. V obravnavani zadevi prosilka ni z ničimer konkretno utemeljila, da bi javni interes po razkritju zahtevanih davčnih obračunov pretehtal nad javnim interesom, da se zahtevani podatki prekrijejo. Navedbe prosilke so bile pavšalne in so se nanašale na nadzor lekarniškega trga na splošno. Tudi Informacijski pooblaščenec ni prepoznal nobenega razloga, ki bi bil v prid razkritju zahtevanih podatkov. Ker je bistvo presoje pri testu javnega interesa v možnosti relativizacije določene izjeme, mora biti le-ta omejen zgolj na tiste primere, ko je interes javnosti za razkritje določene izjeme močnejši od interesa, zaradi katerega je določena informacija zavarovana kot izjema. Pri tem je Informacijski pooblaščenec izpostavil stališče sodne prakse, da je javni interes glede razkritja podan, »če bi bile ogrožene take vrednote, kot je npr. življenje, zdravje ali varnost ljudi in podobno« (npr. sodbi št. I U 1488/2011-95 in št. I U 199272010-28). Informacijski pooblaščenec je tako navedel pravilne razloge za zavrnitev dostopa (izjema davčne tajnosti) in pritožbo zavrnil kot neutemeljeno.

KLJUČNE BESEDE: davčna tajnost, številka odločbe 090-161/2019

Podatki o tem, kateri izdelki so bili dobavljeni in po kakšni ceni, predstavljajo informacijo o porabi javnih sredstev

Prosilka je od Medicinske fakultete v Ljubljani zahtevala fotokopijo ponudbenega predračuna, ki ga je izbrani ponudnik priložil v postopku javnega naročila. Organ je zahtevo prosilke zavrnil v delu, ki se nanaša na stolpec »Naziv ponujenega blaga in proizvajalec oz. blagovna znamka«, s sklicevanjem na izjemo poslovne skrivnosti. To je zatrjeval tudi stranski udeleženec, ki ga je organ pozval v postopek. Prosilka se je na odločitev pritožila, ker do trenutka, ko je organ pozval stranskega udeleženca v postopek, noben del ponudbe ni bil označen z oznako poslovna skrivnost in ponudbi o tem ni bil predložen nikakršen sklep. Poleg tega je te podatke treba razkriti na podlagi tretjega odstavka 6. člena ZDIJZ (poraba javnih sredstev), podatek o nazivu ponujenega blaga pa je javen tudi na podlagi drugega odstavka 35. člena Zakona o javnem naročanju (ZJN-3). V pritožbenem postopku je Informacijski pooblaščenec ugotavljal, ali so zahtevane informacije dejansko predstavljale izjemo po 2. točki prvega odstavka 6. člena ZDIJZ, ki jo je v postopku na prvi stopnji zatrjeval stranski udeleženec. Ker se je zahteva nanašala na dokument, ki ga je stranski udeleženec organu v postopku javnega naročanja predložil v ponudbi z dne 25. 5. 2018, tj. pred uveljavitvijo Zakona o poslovni skrivnosti (ZPosS), je Informacijski pooblaščenec upošteval določbe 39. in 40. člena ZGD-1, ki sta veljala pred uveljavitvijo ZPosS. ZGD-1 razlikuje dva kriterija za določitev poslovne skrivnosti, in sicer subjektivnega (prvi odstavek 39. člena ZGD-1) ter objektivnega (drugi odstavek 39. člena ZGD-1), odvisno od tega, na kakšni podlagi se podatki štejejo za poslovno skrivnost. Za poslovno skrivnost se ne morejo določiti podatki, ki so po zakonu javni, ali podatki o kršitvi zakona ali dobrih poslovnih običajev (tretji odstavek 39. člena ZGD-1). Pri subjektivnem kriteriju družba sama, s splošnim ali posamičnim aktom, odredbo ipd., označi določen podatek za zaupen, ne glede na to, kakšnega pomena je za njeno konkurenčno prednost (lahko gre tudi za manj pomemben podatek), kakšna oz. ali sploh kakšna škoda bi z razkritjem nastala ipd. Odločitev o tem, ali se bo določen podatek štel za poslovno skrivnost po prvem odstavku 39. člena ZGD-1, je torej v celoti prepuščena družbi. Ker je stališče sodne prakse glede pravočasnosti izdaje sklepa o poslovni skrivnosti jasno, predloženi Sklep o določitvi poslovne skrivnosti z dne 31. 5. 2019 ni bil pravočasen in za obravnavo konkretnega pritožbenega postopka ni bil relevanten. S sklepom se lahko označi informacije za poslovno skrivnost tudi za nazaj, vendar se takšen sklep šteje za pravočasnega le, če je izdan še pred prejemom zahteve za dostop do informacije javnega značaja (glej sodbe št. U 1976/2008 z dne 26. 5. 2010, št. I U 599/2014 z dne 3. 11. 2015, št. I U 1573/2014 z dne 18. 11. 2015). Za odločitev o tem, ali se bo določen podatek štel za poslovno skrivnost po drugem odstavku 39. člena ZGD-1, je odločilna vsebina podatka oz. očitne hude posledice njegovega razkritja. Ker ima družba oz. podjetje praviloma vsa ustrezna znanja in izkušnje na trgu, na katerem deluje, ter natančno ve, kaj, kako in zakaj bi lahko vplivalo na njen konkurenčni položaj, zgolj splošno, abstraktno in neobrazloženo sklicevanje na poslovno skrivnost ne zadošča (glej sodbe št. U 284/2008 z dne 27. 5. 2009, U 1276/2008 z dne 11. 2. 2010, I U 1132/2015 z dne 27. 1. 2016). Ker stranski udeleženec ni pojasnil, zakaj zahtevane informacije pomenijo konkurenčno prednost, ki jo je treba varovati kot poslovno skrivnost, v obravnavanem primeru tudi objektivni kriterij poslovne skrivnosti ni bil podan. Ker tretji odstavek 39. člena ZGD-1 določa, da se kot poslovna skrivnost ne morejo določiti podatki, ki so po zakonu javni, se morajo ponudniki in naročniki že na podlagi samega zakona zavedati, da ni mogoče pričakovati popolnega varstva poslovne skrivnosti v dokumentih, ki so bili pridobljeni oz. so nastali na podlagi postopka javnega naročanja. Temeljna načela ZJN-3 (3. do 8. člen) zagotavljajo javnost javnih naročil tako splošni kot tudi posebnim javnostim (npr. na javnem razpisu neuspelim ponudnikom) ter nadzor nad pravilnostjo dela javnega sektorja, kar preprečuje slabo upravljanje, zlorabo oblasti in korupcijo. Informacijski pooblaščenec je ugotovil, da načelo publicitete

pokriva tudi podatka »naziv ponujenega blaga« in »proizvajalec oz. blagovna znamka«. Podatek o nazivu ponujenega blaga sodi v okvir »specifikacije ponujenega blaga«, ki je po drugem odstavku 35. člena ZJN-3 javni podatek. Pojem »specifikacija« je povsem jasen. Po jezikovni razlagi »specifikacija« pomeni »podroben opis, oznaka česa glede na posebne, določene značilnosti«, kar jasno kaže, da se s specifikacijo pričakuje, da se predmet naročila ne opredeli zgolj z »osnovnimi« podatki, temveč z vsemi podatki o predmetu naročila, ki so za naročnika tako pomembni, da jih je v razpisni dokumentaciji posebej opredelil. To pomeni, da je obseg informacij, ki sodijo v okvir »specifikacije ponujenega predmeta«, vselej odvisen od zahtev naročnika – ta jih opredeli v razpisni dokumentaciji. Posledično mora ponudnik v svoji ponudbi izkazati, da ponujeni predmet ustreza vsem (ne zgolj določenim) zahtevam iz specifikacije, sicer je iz postopka izključen. Podatki o proizvajalcu blaga oz. blagovni znamki izkazujejo informacije o predmetu naročila, kar pomeni, da gre za podatke o porabi javnih sredstev skladno s 1. alinejo tretjega odstavka 6. člena ZDIJZ. Gre namreč za informacije o tem, kaj (katere izdelke) je organ kupil z javnimi sredstvi. Informacijski pooblaščenec je tako izpodbijano odločbo odpravil in organu naložil posredovanje zahtevanih podatkov.

KLJUČNE BESEDE: javna naročila, odločba številka 090-153/2019

Celovitost seznanitve z informacijo o nameravani strateški državni naložbi v turizmu je v javnem interesu

Prosilka (novinarka) je od Ministrstva za gospodarski razvoj in tehnologijo zahtevala dostop do dokumenta »Naložbeni dokument za naložbo Istrabenz Turizem d.d.«, ki ga je Vlada RS sprejela na seji 30. 5. 2019. Organ je v postopek povabil Slovenski državni holding kot pripravljavca dokumenta, ki je nasprotoval razkritju zahtevanega dokumenta, pri čemer se je skliceval na izjemo poslovne skrivnosti po 2. točki prvega odstavka 6. člena ZDIJZ. Organ se je strinjal s stranskim udeležencem o obstoju poslovne skrivnosti po ZPosS. Ob upoštevanju določbe tretjega odstavka 2. člena ZPosS je zaključil, da se predmetni dokument ne nanaša na podatke o porabi javnih sredstev niti za njegovo razkritje ne obstaja javni interes, ki bi bil večji od interesa do varstva poslovne skrivnosti. V pritožbenem postopku je Informacijski pooblaščenec pozval Družbo za upravljanje terjatev bank (DUTB) in Istrabenz turizem, d. d. k priglasitvi stranske udeležbe. V obravnavani zadevi ni bilo sporno, da je bil zahtevani dokument označen kot poslovna skrivnost, nanjo pa sta se sklicevali tudi stranski udeleženki. Ker je zahtevani dokument nastal pred uveljavitvijo ZPosS, je Informacijski pooblaščenec utemeljevanje izjeme poslovne skrivnosti presojal v obsegu takrat veljavne določbe 39. člena ZGD-1 in ugotovil, da so bili kriteriji za določitev poslovne skrivnosti po subjektivnem kriteriju izpolnjeni. Dokument je bil namreč skladno s Pravilnikom o varovanju poslovne skrivnosti označen kot poslovna skrivnost. V obravnavani zadevi je Informacijski pooblaščenec ugotovil tudi, da zahtevani dokument ne vsebuje podatkov, ki bi izkazovali neposredno porabo javnih sredstev po 1. alineji tretjega odstavka 6. člena ZDIJZ, saj dokument predstavlja analitični dokument in ne pomeni samega prenosa kakršnega koli državnega premoženja oz. javnih sredstev. Nasprotno pa je Informacijski pooblaščenec menil, da bi bilo treba zahtevani dokument razkriti na podlagi drugega odstavka 6. člena ZDIJZ, tj. testa javnega interesa. Pri izvedbi testa javnega interesa v obravnavani zadevi je bilo ključno vprašanje, ali bi se z razkritjem zahtevanega dokumenta dejansko pripomoglo k širši razpravi in razumevanju nečesa pomembnega za širšo javnost, kot so to omogočali že javno objavljeni podatki v zvezi s sprejetjem zahtevanega dokumenta. Informacijski pooblaščenec je javni interes za razkritje zahtevanega dokumenta prepoznal v dejstvu, da ta predstavlja analitični dokument, ki je nastal na podlagi odločitve političnega organa (tj. s sklepom Vlade RS v vlogi skupščine SDH z dne 14. 2. 2019), in je bil potrjen s strani istega organa s sklepom z dne 30. 5. 2019. Zahtevani dokument je nastal kot posledica politične odločitve državnega organa, da bo sledil usmeritvam Strategije trajnostne rasti slovenskega turizma 2017–2021. Poleg tega je zahtevani dokument izkazoval ekonomske učinke kot posledico naložb v namensko družbo, ki naj bi jo ustanovil DUTB in na katero se bodo prenesle delnice Istrabenz turizma, d. d. S prikazovanjem namere o prenosu državne naložbe je bil po mnenju Informacijskega pooblaščenca nedvomno podan javni interes za seznanitev s tem dokumentom, tako z vidika transparentnosti samega postopka izvedbe prenosa kot tudi z vidika možnosti in potrebe sodelovanja javnosti pri razpravi o tej temi že v samem začetku postopka. Organ je pri zavrnitvi dostopa do zahtevanega dokumenta zavzel tudi stališče, da bi z razkritjem posegel v pravico do svobodne gospodarske pobude iz 74. člena Ustave RS. Informacijski pooblaščenec je argument zavrnil, saj svobodna gospodarska pobuda subjektov, ki jih obvladujejo osebe javnega prava (stranski udeleženki Istrabenz turizem in SDH sta v 100-odstotni lasti Republike Slovenije), že v temelju ne more imeti enake teže in pomena, kot ju ima svobodna gospodarska pobuda subjektov, ki jih obvladujejo zasebniki. Ker pravice prosilke oz. javnosti, da se celovito seznani z informacijami o nameravani strateški državni naložbi na tako pomembnem področju, kot je turizem, o naložbi, ki bo imela pomembne gospodarske učinke, ni bilo mogoče zagotoviti z drugimi ukrepi, je Informacijski pooblaščenec pritožbi ugodil in organu naložil posredovanje zahtevanega dokumenta.

KLJUČNE BESEDE: poslovna skrivnost, test javnega interesa, odločba številka 090-194/2019

Pri dostopu do dokumentov Evropskega parlamenta, Sveta in Komisije je treba neposredno upoštevati evropsko pravo

Prosilec je od Ministrstva RS za pravosodje zahteval dostop do mnenja odbora iz člena 255 Pogodbe o delovanju EU glede ustreznosti slovenskega kandidata za sodnika na Splošnem sodišču EU. Organ je zahtevi delno ugodil in prosilcu posredoval dokument, na katerem je prekril ime kandidata in posamezne odstavke besedila. Pri svoji odločitvi se je skliceval na neposredno uporabo evropskega prava, tj. Uredbo Evropskega parlamenta in Sveta (ES) št. 1049/2001 z dne 30. 5. 2001, o dostopu javnosti do dokumentov Evropskega parlamenta, Sveta in Komisije. V postopek na prvi stopnji je pritegnil tudi kandidata za sodnika, ki stranske udeležbe ni prijavil, ter pridobil mnenje Sveta EU o sami zahtevi. Svet EU je ocenil, da zahtevani dokument spada v okvir izjem, kar zadeva zasebnost in integriteto posameznika (člen 4(1(b)) Uredbe (ES) št. 1049/2001), varstvo postopka odločanja (člen 4(3(1)) Uredbe (ES) št. 1049/2001) in varstvo poslovnih interesov (prva alineja člena 4(2) Uredbe (ES) št. 1049/2001). Organ je še navedel, da je v zvezi s podobno zahtevo odločala tudi evropska varuhinja človekovih pravic (odločba z dne 23. 5. 2019). Iz povzetka odločitve v zadevi št. 1955/2017/THH je razvidno, da se je zadeva nanašala na odločitev Sveta EU, s katero je nevladni organizaciji zavrnil dostop do mnenj, ki presojajo primernost kandidatov za položaje sodnikov in generalnih pravobranilcev na Sodišču EU in Splošnem sodišču EU. Svet EU je zavrnil zahtevek za polni javni dostop do mnenja, pri svoji odločitvi se je oprl na nujnost varovanja postopka odločanja odbora, postopkov sodišč, zasebnosti in integritete kandidatov ter poslovnih interesov kandidatov. Varuhinja človekovih pravic je ugotovila, da je bila odločitev Sveta EU glede zavrnitve polnega javnega dostopa do mnenj utemeljena, saj je bil njen namen zagotoviti, da bo odbor lahko še naprej nepristransko dajal iskrena in preudarna mnenja glede primernosti kandidatov. Kljub temu je pozdravila javni interes, ki se je odražal v vložitvi pritožbe, saj je to omogočilo neodvisno preiskavo zadeve, ki je zelo pomembna za državljane EU. Organ je pojasnil, da je dolžan spoštovati načelo lojalnega sodelovanja z evropskimi institucijami in ne ovirati primarne uporabe Uredbe, kadar gre za dokument evropske institucije, ki bi ga lahko prosilec zahteval od organov EU. Tako je organ vsake države članice, ki bi moral po svojih nacionalnih predpisih (npr. po ZDIJZ) dokument razkriti, a mu to prepovedujejo evropski predpisi ali izrecna odločitev evropske institucije, dolžan upoštevati evropsko pravo, ki je nacionalnemu nadrejeno. Tako je moral tudi Informacijski pooblaščenec v pritožbenem postopku neposredno uporabiti evropsko pravo (Uredbo (ES) št. 1049/2001), saj je šlo za dokument, ki ga je ustvaril odbor iz člena 255 Pogodbe o delovanju Evropske unije in je izviral iz pristojnosti Sveta EU. Hkrati je bil Informacijski pooblaščenec vezan tudi na mnenje Sveta EU o sami zahtevi, iz katerega je izhajalo, da se prosilcu lahko omogoči delni dostop do zahtevanega dokumenta. Ker je organ pri izvedbi delnega dostopa popolnoma upošteval mnenje Sveta EU o sami zahtevi, je Informacijski pooblaščenec pritožbo prosilca zavrnil.

KLJUČNE BESEDE: pravo EU, številka odločbe 090-204/2019

Izplačila javnega zavoda izkazujejo podatke o porabi javnih sredstev

Prosilka (novinarka) je od Ekonomske fakultete v Ljubljani želela dostop do »vseh« izplačil organa »vsem« osebam za obdobje treh let. Organ je zahtevo prosilke zavrnil s sklicevanjem na zlorabo pravice. Organ je prosilki očital, da njena zahteva ni v ničemer stremela k zagotavljanju odprtosti delovanja države v najširšem smislu, saj je vse podatke, ki jih je želela pridobiti, že prejela na podlagi predhodne zahteve. Tako je bil mnenja, da je namen njene druge zahteve prvenstveno izhajal iz želje po obračunavanju z organom. Pri tem je poudaril, da so morali javni uslužbenci za pripravo podatkov v zvezi s prvotno zahtevo opraviti ogromno dela, za katerega organ ni imel kritja v javnih virih. V zaključku je organ še navedel, da je ravnanje novinarjev in njihovo domnevno raziskovalno novinarstvo na področju izplačil avtorskih honorarjev in plač javnih uslužbencev v visokem šolstvu predvsem s strani medijske hiše POP TV že od prvih objav spletne aplikacije SUPERVIZOR temeljilo zgolj in samo na enostranskem in neobjektivnem poročanju. Škode, ki je bila ustvarjena vsem tistim, ki so bili žrtve te gonje, ni povrnil nihče, ob tem pa javnosti tudi ni bilo nikoli jasno sporočeno, koliko raznovrstnega dela je bilo dejansko opravljenega in kako velik delež le-tega je bil financiran iz absolutno neproračunskih sredstev. V pritožbenem postopku je Informacijski pooblaščenec ugotovil, da organ ni oporekal dejstvu, da zahtevane informacije skladno s 1. alinejo tretjega odstavka 6. člena ZDIJZ predstavljajo prosto dostopne informacije javnega značaja, saj gre za podatke, ki izkazujejo porabo javnih sredstev. Tudi po praksi Informacijskega pooblaščenca in sodišča je nesporno, da organ kot javni zavod razpolaga z javnimi sredstvi, zato zahtevana izplačila organa izkazujejo podatke o porabi javnih sredstev.

Informacijski pooblaščenec je tudi ocenil, da prosilka s tem, ko je vložila zahtevo po dostopu do »vseh« izplačil »vsem« osebam za obdobje treh let, kljub temu da ji je organ na podlagi zahteve z dne 1. 8. 2019 že posredoval določen del podatkov (za prvih petnajst najvišjih izplačil), ni zlorabila pravice dostopa do informacij javnega značaja. Kot izhaja iz Predloga zakona o spremembah in dopolnitvah Zakona o dostopu do informacij javnega značaja (ZDIJZ-C), so elementi oz. kriteriji, ki lahko (skupaj) kažejo na zlorabo pravice, npr. pogostost vlaganja zahtev, obsežnost zahtev, nesorazmerna obremenitev organa, prosilec ne sledi lastnim upravičenim interesom, nagajanje, šikaniranje ipd. Po mnenju Informacijskega pooblaščenca ni šlo za ponavljajočo se zahtevo za isto zadevo, ampak je bila zahteva prosilke povezana z željo pridobiti vsa izplačila organa z imeni in priimki v elektronski obliki, česar ji organ do tedaj še ni posredoval. Predvidevanja in vrednostne ocene organa, ki nimajo osnove v sami zahtevi oz. iz same zahteve niso izhajala, niso bila pravno upoštevna. Zahteva tudi ni bila očitno nedovoljena in neutemeljena, saj je bila usmerjena izključno v informacije, ki so javnega značaja in so lahko prosto dostopne. Objektivno je bilo nemogoče zaključiti, da bi izpolnitev predmetne zahteve ovirala izpolnjevanje temeljnih nalog organa, organ pa se do tega tudi ni konkretno opredelil. Zgolj večji obseg zahtevanih informacij in s tem povezano dodatno delo za organ še ne pomenita zlorabe pravice. Za utemeljitev obstoja zlorabe pravice je treba zadostiti dokaznemu standardu »onkraj dvoma«, ne pa zgolj dokaznemu standardu »verjetnosti«, poleg tega ni dovolj, da gre zgolj za neprijetnost, ampak mora biti delo organa resno ohromljeno zaradi upravnega bremena, ki bi bilo posledica obravnave zahteve po ZDIJZ. V praksi to pomeni, da mora biti izkazana stvarna, resnična grožnja za celotno delo organa. Upoštevati je namreč treba, da je tudi posredovanje informacij javnega značaja ena izmed zakonsko določenih nalog organa, zato je organ dolžan zagotoviti ustrezna sredstva in kader, ki takšne zahteve rešuje. Informacijski pooblaščenec v zahtevi prosilke in v predloženi dokumentaciji ni zaznal okoliščin, ki bi vzbujale pomisleke o slabih namerah prosilke. Informacijski pooblaščenec in sodišče sta že večkrat poudarila, da imajo mediji v družbenem prostoru pomembno vlogo, da kot »javni čuvaji« oz. »četrta veja oblasti« zbirajo informacije, ki so splošnega pomena, zato da bi bile te posredovane javnosti zaradi demokratičnega diskurza. Informacijski pooblaščenec je pritožbi prosilke ugodil in organu naložil posredovanje zahtevanih dokumentov.

KLJUČNE BESEDE: mediji, zloraba pravice, javni uslužbenci, številka odločbe 090-239/2019

2.6 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.

2.6.1 DAN PRAVICE VEDETI

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.

V okviru dogodkov ob svetovnem dnevu pravice vedeti je Informacijski pooblaščenec organiziral posvet z naslovom *Zapleti in razpleti postopkov dostopa do informacij javnega značaja*, na katerem je beseda tekla o procesnih in vsebinskih dilemah pri izvajanju ZDIJZ ter o reševanju izzivov, s katerimi se zavezanci in prosilci srečujejo v praksi. Udeležence posveta sta uvodoma nagovorila minister za javno upravo Rudi Medved in informacijska pooblaščenka Mojca Prelesnik, ki je poudarila, da so zavezanci z določbami ZDIJZ v splošnem dobro seznanjeni in da vse več zaprošajo za pojasnila, iz česar izhaja, da so aktivni in odzivni. Enako velja tudi za prosilce, na kar kaže nenehen trend rasti pritožbenih zadev.

Informacijski pooblaščenec je ob svetovnem dnevu pravice vedeti poudaril, da je svoboden pretok informacij v interesu vseh. Zavezanci in prosilci naj bodo zato pri razvoju dobrih praks dostopa do informacij javnega značaja čim bolj aktivni.

Dogodek "Dan pravice vedeti 2019".

2.6.2 MEDNARODNO SODELOVANJE

Oktobra 2019 se je Informacijski pooblaščenec na povabilo brandenburške informacijske pooblaščenke udeležil mednarodnega simpozija z naslovom *Dostop do informacij javnega značaja in novinarstvo – učinkovito orodje za raziskovanje v praksi?*, ki je potekal v Potsdamu. V okviru dogodka so zastopniki informacijskih pooblaščencev, novinarji in predstavniki nevladnih organizacij iz različnih evropskih držav predstavili dileme pri dostopu do informacij v praksi.

Na povabilo slovenske nevladne organizacije PiNA je Informacijski pooblaščenec v okviru projekta YOU4EU novembra 2019 sodeloval na mednarodni konferenci v Podgorici. Tema konference je bilo vključevanje državljanov v različne procese v EU. Namestnica informacijske pooblaščenke je bila gostja okrogle mize o načrtovanih spremembah zakona o dostopu do informacij javnega značaja v Črni gori. Predstavila je izkušnje Slovenije z izvajanjem ZDIJZ, trenutno stanje ter glavne izzive, s katerimi se Informacijski pooblaščenec srečuje v praksi.

Informacijski pooblaščenec se je decembra 2019 udeležil delavnice *Freedom of Information & Access to Information* v Gibraltarju. To je bila že druga mednarodna delavnica o reševanju konkretnih primerov iz prakse organov, pristojnih za nadzor nad dostopom do informacij javnega značaja. Predstavljene so bile različne nacionalne ureditve postopkov dostopa do informacij javnega značaja, predvsem konkretni primeri 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. Posebna pozornost je bila namenjena izkušnjam s področja proaktivne objave podatkov, mednarodnim standardom v pritožbenih postopkih, dilemi, ali so pravila dostopa do informacij javnega značaja *lex specialis* ali *lex generalis*, vprašanje stroškov dostopa do informacij in druge. Informacijski pooblaščenec je na delavnici sodeloval z dvema prispevkoma: *Exceptions to the duty to disclose information in Slovenia* in *The Public Interest Test in relation to information*.

2.7 SPLOŠNA OCENA IN PRIPOROČILA

Informacijski pooblaščenec ugotavlja, da je bilo število pritožbenih zadev na področju dostopa do informacij javnega značaja v letu 2019 na primerljivi ravni kot v letu 2018 (leta 2019 je bilo vloženih 540 pritožbenih zadev). Povečalo se je število pritožb zoper molk državnih organov (v letu 2018 je Informacijski pooblaščenec

obravnaval 213 tovrstnih pritožb, v letu 2019 pa 222), zmanjšalo pa se je število pritožb zoper molk občin (v letu 2018 je Informacijski pooblaščenec obravnaval 123 tovrstnih pritožb, v letu 2019 pa 106).

Ker se število pritožb zaradi molka organa v zadnjih letih povečuje, je Informacijski pooblaščenec podrobneje analiziral te pritožbene postopke in ugotovil, da je le v 172 primerih od 235 prejetih pritožb zaradi molka dejansko uvedel postopek, v preostalih zadevah pa je bila pritožba prosilca preuranjena, nepopolna oz. ni šlo za molk zavezanca po ZDIJZ, ker zahteva ni bila podana po tem zakonu. V 172 zadevah, v katerih je Informacijski pooblaščenec zoper zavezance uvedel postopek, je velika večina zavezancev molk v dodatnem roku odpravila in prosilcem dostop do zahtevane informacije v celoti oz. delno omogočila (v 130 primerih), v 42 primerih pa so zavezanci izdali zavrnilno odločitev oz. so zahteve zavrgli. Od vseh prejetih pritožb zoper molk organa jih je bilo 26 vloženih s strani medijev, ker ti v zakonskem roku sedmih delovnih dni niso prejeli zahtevanih informacij v skladu s 45. členom ZMed. Tudi v teh postopkih je Informacijski pooblaščenec največ pritožb prejel zoper organe državne uprave (10 pritožb).

Navedeno kaže, da zavezanci večinoma niso molku, ker zahtevanih informacij ne želijo posredovati, ampak po oceni Informacijskega pooblaščenca k reševanju zahtevkov po ZDIJZ ne pristopijo pravočasno in posledično zamudijo skrajni zakonski rok za odločitev. Izhajajoč iz statistike lahko sicer ugotovimo, da je cca. 30 % vloženih pritožb zaradi molka neutemeljenih, še vedno pa je skrb vzbujajoče dejstvo, da narašča število prejetih pritožb zoper organe državne uprave (ministrstva in organi v sestavi). Zoper to skupino zavezancev je bil vložen tudi največji delež vseh pritožb zaradi molka (29 %), pri čemer gre za zavezance iz t. i. kroga ožje državne uprave, ki bi po 16 letih veljavnosti ZDIJZ vsekakor morali biti sposobni vse zahteve za dostop do informacij javnega značaja obravnavati pravočasno, torej v zakonsko določenem roku 20 delovnih dni.

Glede na visok delež pritožb zaradi molka v skupnem deležu vseh pritožb (44 %) Informacijski pooblaščenec ocenjuje, da bo v prihodnje treba (še) več napora vložiti v aktivnejše usposabljanje zavezancev za uporabo zakona v praksi, kar je sicer primarno naloga Ministrstva za javno upravo, ki po 32. členu ZDIJZ med drugim svetuje zavezancem v zvezi z uporabo tega zakona ter opravlja spodbujevalne in razvojne naloge. Informacijski pooblaščenec kot pritožbeni organ lahko organom svetuje le v okviru neformalnega svetovanja, na podlagi primerov iz prakse, ki jih je že obravnaval. Informacijski pooblaščenec je tako v letu 2019 podal 300 pisnih odgovorov na zaprosila zavezancev ter 629-krat svetoval v okviru telefonskega dežurstva. Z namenom predstavitve svoje prakse je izvedel tudi pet praktičnih delavnic za upravne enote: udeležilo se jih je 134 udeležencev iz 51 upravnih enot. Primere svoje prakse Informacijski pooblaščenec redno objavlja na svoji spletni strani, pri čemer se trudi, da je ta ažurna in da so objave pregledno dostopne, vse z namenom olajšati delo zavezancev in seznanjati javnost s pomenom te temeljne človekove pravice.

V letu 2019 je Informacijski pooblaščenec vodil 17 postopkov zoper poslovne subjekte pod prevladujočim vplivom, kar predstavlja le 3 % vseh pritožbenih zadev. Informacijski pooblaščenec ugotavlja, da število teh pritožb že vsa leta ostaja nizko.

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

- Podobno kot v letu 2018 je tudi v letu 2019 Informacijski pooblaščenec zaznal povečanje števila pritožbenih postopkov glede dostopa do informacij, ki se nanašajo na javne uslužbence in javne funkcionarje (število prejetih pritožb se je povečalo za 75 %). Ker so zavezanci v teh primerih dostop do zahtevanih informacij neutemeljeno zavrnili s sklicevanjem na varovane osebne podatke, Informacijski pooblaščenec opozarja, da so tudi po uveljavitvi Splošne uredbe ti podatki, v skladu s tretjim odstavkom 6. člena ZDIJZ, določeni kot absolutno javni. Takšna je tudi dolgoletna praksa Informacijskega pooblaščenca in Upravnega sodišča.
- Tudi v letu 2019 je Informacijski pooblaščenec zaznal povečanje števila pritožb, ki se nanašajo na dokumente iz inšpekcijskih postopkov. V teh pritožbenih postopkih je bilo ugotovljeno, da zavezanci pogosto neupravičeno niso uporabili pravila delnega dostopa, ampak so prosilcem dostop zavrnili v celoti, čeprav zahtevane informacije niso v celoti predstavljale zakonskih izjem od prosto dostopnih informacij. Ob tem velja opozoriti, da če dokument ali njegov del le delno vsebuje varovane informacije in je mogoče slednje izločiti iz dokumenta, ne da bi to ogrozilo njihovo zaupnost, mora organ slediti pravilu delnega dostopa in prosilca seznaniti z vsebino preostalega, nevarovanega dela dokumenta.
- Ker morajo zavezanci informacije javnosti posredovati tudi sami, brez zahteve prosilca, jih Informacijski pooblaščenec poziva, naj temu področju namenijo več pozornosti in naj ravnajo proaktivno ter se s tem izognejo morebitnim postopkom po ZDIJZ. Informacijski pooblaščenec je v več pritožbenih postopkih v letu 2019 namreč ugotovil, da so bile predmet zahteve informacije, ki bi jih morali organi že sami javno objavljati po 10. in 10.a členu ZDIJZ.
- Podobno kot v letu 2018 je tudi v 2019 Informacijski pooblaščenec ugotovil, da zavezanci pri obravnavi zahtev ne namenijo dovolj pozornosti postopkovnim vprašanjem, posledica nepopolno oz. napačno ugotovljenega dejanskega stanja s strani zavezanca na prvi stopnji pa je, da se izpodbijane odločbe ne da preizkusiti. V primerih, ko zavezanci 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 se dostop do zahtevanih dokumentov zavrne, morajo biti pojasnjeni na način, da so prosilcem razumljivi in skladni z izrekom odločbe.
- Ker je Informacijski pooblaščenec v letu 2019 zaznal povečanje števila pritožb zaradi molka pri organih ožje državne uprave, jih poziva, naj področju dostopa do informacij javnega značaja namenijo več pozornosti in s tem zagotovijo, da bodo zahteve prosilcev obravnavali v okviru zakonskih rokov.

VARSTVO OSEBNIH PODATKOV

Varstvo temeljne človekove pravice do zasebnosti

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 izrecno dovoljeno. Vsaka obdelava osebnih podatkov namreč pomeni poseg v z ustavo varovano človekovo pravico. Zato je tak poseg dopusten, če je v zakonu določno opredeljeno, kateri osebni podatki se smejo obdelovati, namen njihove obdelave, zagotovljeno pa mora biti tudi ustrezno varstvo in zavarovanje osebnih podatkov. Namen obdelave osebnih podatkov mora biti ustavno dopusten, obdelovati pa se smejo le tisti osebni podatki, ki so primerni in za uresničitev namena nujno potrebni.

Ureditev varstva osebnih podatkov v sistemskem zakonu je potrebna zaradi enotne določitve načel, pravil in obveznosti ter zaradi zapolnitve pravnih praznin, ki bi lahko nastale v področnih zakonih. Ključni sistemski zakon glede varstva osebnih podatkov je bil do 25. 5. 2018 Zakon o varstvu osebnih podatkov.

V okviru reforme varstva osebnih podatkov na ravni EU pa sta bila 4. 5. 2016 v Uradnem listu EU objavljena ključna gradnika 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) in
- 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 2016/680, t. i. Direktiva za organe pregona kaznivih dejanj).

Splošna uredba o varstvu podatkov (Splošna uredba; angl. General Data Protection Regulation (GDPR)) je začela veljati 25. 5. 2016, uporablja pa se neposredno od 25. 5. 2018. Rok za prenos določb Direktive (EU) 2016/680 v nacionalno zakonodajo je bil dve leti, a Slovenija Direktive za organe pregona kaznivih dejanj do konca aprila 2020 še ni prenesla v svoj pravni red. V Sloveniji tako za zavezance po Direktivi za organe pregona kaznivih dejanj kot sistemski predpis za varstvo osebnih podatkov še vedno v celoti velja Zakon o varstvu osebnih podatkov (ZVOP-1).

S Splošno uredbo so se okrepile pravice posameznika, poleg obstoječe pravice do dostopa do osebnih podatkov ter pravice do popravka še pravica do pozabe, izbrisa, omejitve obdelave, ugovora in prenosljivosti podatkov. Precej večji poudarek je zdaj na transparentnosti obdelave, tj. 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); 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. Njen 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 upravljavca ali obdelovalca. Ostali nadzorni organi bodo v postopkih nadzora sodelovali kot zadevni organi.

Splošna uredba zajema tudi ustanovitev Evropskega odbora za varstvo podatkov (EOVP, angl. European Data Protection Board (EDPB)). 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).

Časovni razvoj Zakona o varstvu osebnih podatkov.

3.2 INŠPEKCIJSKI NADZOR V LETU 2019

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 glede njihovega posredovanja tujim uporabnikom osebnih podatkov;
- izvajanje določb Splošne uredbe glede obdelave na podlagi pogodbe o obdelavi osebnih podatkov.

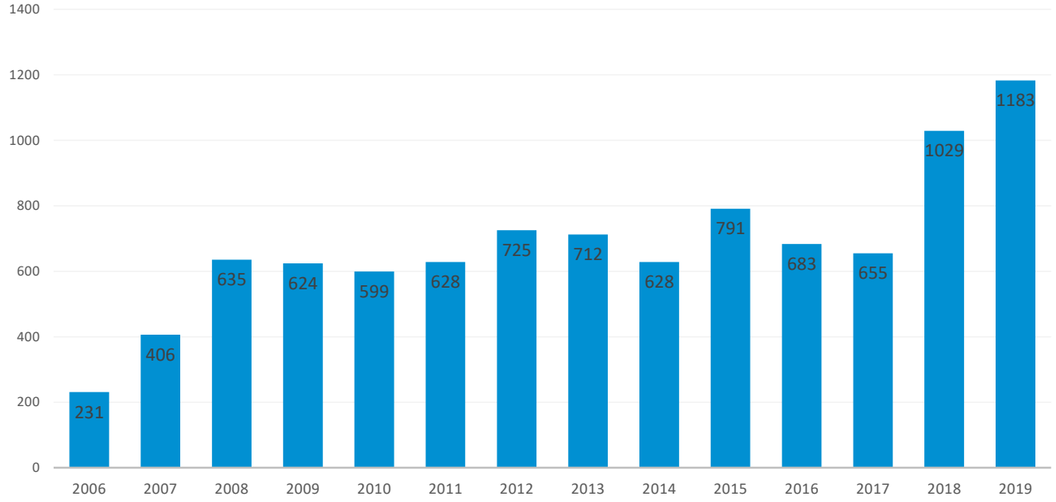
Splošna uredba daje Informacijskemu pooblaščencu v členu 58 naslednja inšpekcijska pooblastila:

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 preglede potrdil skladnosti obdelav (certifikatov);
- da upravljavca ali obdelovalca uradno obvesti o domnevni kršitvi Splošne 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 EU ali postopkovnim pravom države članice.

2. Popravljalna pooblastila:
- da izda upravljavcu ali obdelovalcu opozorilo, da bi predvidena dejanja obdelave verjetno kršila določbe Splošne uredbe;
- da upravljavcu ali obdelovalcu izreče opomin, kadar so bile z dejanji obdelave kršene določbe Splošne uredbe;
- da upravljavcu ali obdelovalcu odredi, naj ugodi zahtevam posameznika, na katerega se nanašajo osebni podatki, glede uresničevanja njegovih pravic na podlagi Splošne uredbe;
- da upravljavcu ali obdelovalcu odredi, naj dejanja obdelave, če je to ustrezno, na določen način in v določenem roku uskladi z določbami Splošne 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.

Informacijski pooblaščenec je leta 2019 zaradi suma kršitev določb Splošne uredbe in/ali ZVOP-1 vodil 1.183 inšpekcijskih zadev, od tega 337 v javnem in 846 v zasebnem sektorju, kar pomeni, da se število inšpekcijskih zadev še vedno povečuje. V primerjavi z letom 2018, ki je bilo glede porasta števila inšpekcijskih zadev rekordno (57 % porast inšpekcijskih postopkov glede na leto 2017), je število inšpekcijskih zadev znova naraslo, in sicer za 15 %.

Število inšpekcijskih zadev med letoma 2006 in 2019.



Posameznemu državnemu nadzorniku za varstvo osebnih podatkov je bilo leta 2017 dodeljenih v povprečju 61, leta 2018 92 in leta 2019 74 inšpekcijskih zadev. Število zadev na državnega nadzornika se je v letu 2019 glede na leto 2017 povečalo, glede na leto 2018 pa se je kljub povečanju skupnega števila zadev zmanjšalo zaradi zaposlitve novih državnih nadzornikov.

Število dodeljenih inšpekcijskih zadev na posameznega nadzornika v letih 2017, 2018 in 2019.

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

Sum kršitve	Število prijav
nezakonito razkrivanje osebnih podatkov: posredovanje osebnih podatkov nepooblaščenim uporabnikom in nezakonita objava osebnih podatkov	405
nezakonita obdelava osebnih podatkov pri izvajanju neposrednega trženja	150
nezakonito zbiranje oz. zahtevanje osebnih podatkov	114
nezakonito izvajanje videonadzora	112
neustrezno zavarovanje osebnih podatkov	96
nezakonit vpogled v osebne podatke	83
obdelava osebnih podatkov v nasprotju z namenom zbiranja	36
Hekerski napadi in vdori v informacijske sisteme	32
Zavrnitev izbrisa osebnih podatkov	31
Piškotki	13
Zavrnitev posredovanja osebnih podatkov	10
Razno (npr. obdelava osebnih podatkov po preteku roka hrambe; uporaba netočnih podatkov; kršitev pravice do seznanitve z lastnimi osebnimi podatki in pravice do ugovora; sumi kršitev, ki ne sodijo v pristojnost Informacijskega pooblaščenca, npr. kršitev pravil v postopkih pri drugih organih, kazniva dejanja zoper čast in dobro ime)	38

3.2.1 INŠPEKCIJSKI NADZOR V JAVNEM SEKTORJU

Zaradi suma kršitev določb Splošne uredbe in/ali ZVOP-1 je Informacijski pooblaščenec zoper zavezance v javnem sektorju v letu 2019 vodil 337 zadev, 319 jih je začel na podlagi prejetih prijav, 18 pa po uradni dolžnosti.

Informacijski pooblaščenec je 128 prijaviteljem pisno pojasnil, zakaj v prijavi opisano ravnanje ne pomeni kršitve zakonodaje s področja varstva osebnih podatkov, v 34 primerih pa je po preučitvi prijav zaključil, da uvedba inšpekcijskih postopkov ne bi bila smiselna, ker je šlo za enkratna dejanja oz. kršitve varstva osebnih podatkov v preteklosti, ki jih z inšpekcijskimi ukrepi za nazaj ni več mogoče preprečiti ali odpraviti. V teh primerih je zoper 24 kršiteljev uvedel postopke o prekršku oz. jim je izrekel ukrepe v skladu z Zakonom o prekrških (ZP-1), v devetih primerih je ocenil, da uvedba postopka o prekršku ne bi bila smiselna, ker v prijavi opisano ravnanje predstavlja prekršek neznatnega pomena, v enem primeru pa postopka ni uvedel zaradi zastaranja pregona. Šest prijaviteljev je Informacijski pooblaščenec napotil na pravico do seznanitve z lastnimi osebnimi podatki, dve prijavi je odstopil v reševanje pristojnim organom, v štirih primerih pa ni uvedel postopka, ker iz prijave ni bilo razvidno, za kakšno kršitev naj bi šlo, prijavitelj pa po pozivu prijave ni dopolnil oz. v prijavi ni posredoval svojih podatkov, zaradi česar ga Informacijski pooblaščenec niti ni mogel pozvati k posredovanju dodatnih podatkov, ki bi bili potrebni za uvedbo inšpekcijskega postopka.

Leta 2019 je bil v javnem sektorju zaključen 101 inšpekcijski postopek. Informacijski pooblaščenec je 41 postopkov ustavil, ker so zavezanci ugotovljene nepravilnosti odpravili, v 39 postopkih ni zaznal kršitev določb Splošne uredbe ali ZVOP-1, 21 postopkov pa je ustavil zato, ker je šlo za kršitve, ki so predstavljale enkratna dejanja v preteklosti, ki jih z inšpekcijskimi ukrepi za nazaj ni bilo več mogoče odpraviti.

3.2.2 INŠPEKCIJSKI NADZOR V ZASEBNEM SEKTORJU

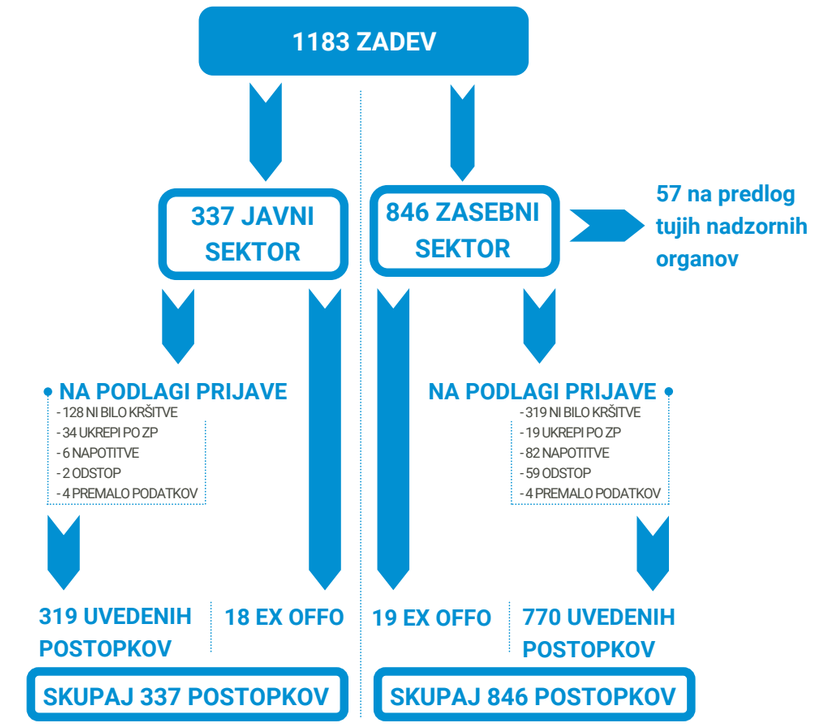
Informacijski pooblaščenec je zoper zavezance v zasebnem sektorju vodil 846 zadev, od tega 770 na podlagi prejetih prijav, 19 postopkov je uvedel po uradni dolžnosti, preostali (57) pa so bili uvedeni po iniciativi drugih nadzornih organov v EU v okviru čezmejnega sodelovanja, kjer je Informacijski pooblaščenec sodeloval kot zadevni organ (več v poglavju 3.2.4.).

Po preučitvi prijav je Informacijski pooblaščenec 319 prijaviteljev obvestil, da postopka inšpekcijskega nadzora ne bo uvedel, ker iz njihove prijave ne izhaja sum kršitev določb Splošne uredbe in ZVOP-1, 82 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. Informacijski pooblaščenec je 59 prijav odstopil v reševanje pristojnim organom (v večini primerov Agenciji RS za komunikacijska omrežja in storitve), na podlagi 26 prijav inšpekcijskega postopka ni uvedel, ker je šlo za enkratna dejanja oz. kršitve varstva osebnih podatkov v preteklosti, ki jih z inšpekcijskimi ukrepi za nazaj ni bilo več možno preprečiti ali odpraviti. Ugotovljene kršitve je obravnaval v okviru pristojnosti, ki jih ima kot prekrškovni organ, in sicer je 19 kršiteljem izrekel ukrepe po ZP-1, v šestih primerih je ocenil, da ukrepa po ZP-1 ne bo izrekel, ker gre za prekršek neznatnega pomena, v enem primeru pa uvedba prekrškovnega postopka ni bila dopustna zaradi zastaranja pregona. Sedem prijav je vsebovalo premalo podatkov za uvedbo inšpekcijskega postopka, poleg tega so bile anonimne in Informacijski pooblaščenec prijaviteljev ni mogel pozvati k dopolnitvi.

Leta 2019 je Informacijski pooblaščenec pri zavezancih v zasebnem sektorju ustavil 231 postopkov: 109 postopkov je ustavil, ker ni bilo kršitev določb ZVOP-1, 92 postopkov je ustavil po tem, ko so zavezanci odpravili ugotovljene nepravilnosti, 30 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 zavezanec vložil tožbo na Upravno sodišče RS.

Informacijski pooblaščenec je prejel dve sodbi Upravnega sodišča RS v zvezi s tožbama, vloženima leta 2017 in 2018 zoper ureditveno odločbo in sklep o ustavitvi inšpekcijskega postopka. Sodišče je obema tožbama ugodilo, odločbo in sklep odpravilo ter zadevi vrnilo Informacijskemu pooblaščencu v ponoven postopek.

Pregled inšpekcijskih zadev v javnem in zasebnem sektorju leta 2019.



3.2.3 PRIJAVA KRŠITEV VARNOSTI OSEBNIH PODATKOV

Skladno s členom 33 Splošne uredbe so zavezanci dolžni obvestiti nadzorni organ (Informacijskega pooblaščenca) o zaznanih kršitvah 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.

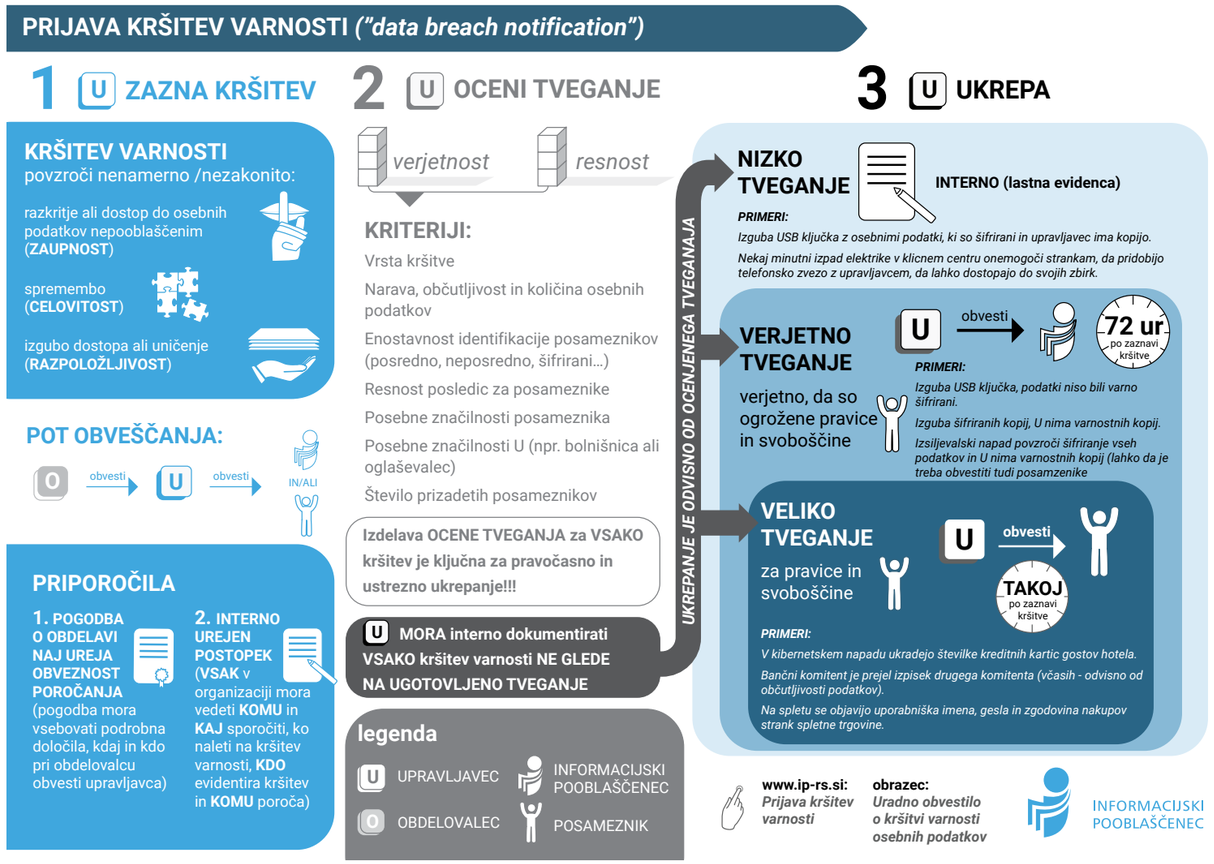
Informacijski pooblaščenec je leta 2019 prejel 137 uradnih obvestil o kršitvi varnosti osebnih podatkov, t. i. samoprijav, ki so jih poslali zavezanci. 80 obvestil so poslali zavezanci iz zasebnega sektorja (npr. banke, telekomunikacijski operaterji, zavarovalnice), 57 pa zavezanci iz javnega sektorja (predvsem zdravstvene in izobraževalne ustanove).

Kršitve varnosti osebnih podatkov so se najpogosteje nanašale na:

- posredovanje dokumentov z osebnimi podatki (npr. zdravniških izvidov, računov, dokumentov v upravnih postopkih, debetne kartice) napačnim osebam kot posledica nenamerne človeške napake ali netočnih podatkov v zbirkah osebnih podatkov (npr. e-naslovov strank) – 26,
- izguba dostopa do osebnih podatkov (onemogočanje dostopa do podatkov zaradi kriptiranja z zlonamerno programsko kodo, t. i. izsiljevalski virus, izguba ali kraja uporabniškega imena in gesla) – 21,
- izguba ali kraja prenosnega računalnika ali drugih nosilcev osebnih podatkov (USB-ključ, zdravstveni karton, zvezek z osebnimi podatki strank) – 11,
- nezakonito razkritje osebnih podatkov (e-naslovov) pri pošiljanju e-sporočila več prejemnikom – 8,
- hekerski vdor – 6,
- nepooblaščen dostop do osebnih podatkov s strani zaposlenih – 6,
- razkritje osebnih podatkov zaradi napake v aplikaciji oz. tehnične napake – 5,
- neustrezno zagotavljanje varnosti osebnih podatkov na spletni strani – 5,
- pošiljanje zlonamerne e-pošte in objava lažne spletne strani (ang. *phishing*) – 5.

Informacijski pooblaščenec je v pomoč upravljavcem na svoji spletni strani pojasnil, katere kršitve pomenijo kršitve varnosti v smislu Splošne uredbe ter o katerih kršitvah in v kolikšnem času so ga dolžni obvestiti. Za obveščanje je odprl namenski poštni predal (prijava-krsitev@ip-rs.si), na spletni strani je dostopen tudi obrazec Uradno obvestilo o kršitvi varnosti osebnih podatkov, ki ga lahko upravljavci uporabijo za obveščanje, objavljene pa so tudi smernice Evropskega odbora za varstvo podatkov v zvezi z uradnim obvestilom o kršitvi varstva osebnih podatkov in infografika Prijava kršitev varnosti (*Data breach notification*).

Prijave kršitev varstva osebnih podatkov leta 2019 – infografika.



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 Lihtenštajn) pri čezmejnih primerih, in sicer prek naslednjih mehanizmov:

- **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).

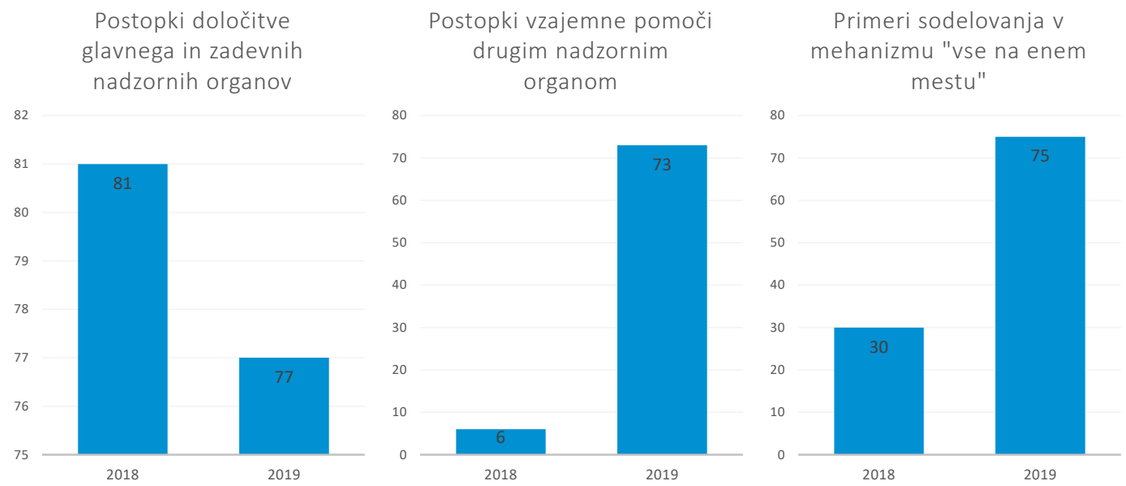
Sodelovanje po mehanizmu »vse na enem mestu« se lahko prične, ko je ugotovljeno, kateri nadzorni organ bo v postopku prevzel vlogo vodilnega in kateri organ(i) bodo v postopku sodelovali kot zadevni organi. Vodilni organ prihaja iz tiste države članice EGS, kjer ima upravljavec osebnih podatkov, ki posluje čezmejno, sedež oz. ustanovitev, ki prevzema odgovornost za obdelavo osebnih podatkov. Nadzorni organi iz drugih držav članic EGS pa se postopku nadzora priključijo kot zadevni organi, kadar ima upravljavec 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 zadržke. V primeru nestrinjanja med vodilnim in zadevnimi organi o sporu odloči EOVP.

Sodelovanje v okviru vseh treh mehanizmov poteka prek informacijskega sistema za notranji trg (Internal

Market Information System, sistem 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.

V letu 2019 je Informacijski pooblaščenec izvedel 148 postopkov sodelovanja po členih 60 in 61 Splošne uredbe v zvezi z upravljavci, ki izvajajo čezmejno obdelavo osebnih podatkov, v 77 postopkih se je opredelil za zadevni nadzorni organ (po členu 56 Splošne uredbe). V nadaljevanju so podrobneje predstavljeni različni postopki sodelovanja.

Sodelovanje Informacijskega pooblaščenca v čezmejnih postopkih nadzor v letu 2019.



Opredelitve vodilnega in zadevnih nadzornih organov po členu 56 Splošne uredbe

Temelj za izvedbo čezmejnega sodelovanja po členu 60 Splošne uredbe je opredelitev vodilnega in zadevnih nadzornih organov po členu 56 Splošne uredbe. V 77 tovrstnih postopkih leta 2019 se je Informacijski pooblaščenec opredelil za zadevni organ. Sedem postopkov ugotavljanja je pričel Informacijski pooblaščenec, in sicer na podlagi prijave domnevne kršitve varstva osebnih podatkov v čezmejnem primeru. 70 postopkov ugotavljanja je bilo začetih na iniciativo drugih organov v EU, Informacijski pooblaščenec pa se je opredelil za zadevni nadzorni organ predvsem:

- ker ima upravljavec 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. spletne velikane (Facebook, Google, Amazon, Apple, PayPal, WhatsApp, Twitter, Instagram, Microsoft itd.). Številna od navedenih 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 sodelovanja, organi iz drugih držav članic pa v postopku sodelujejo v skladu s pooblastili, ki jih določa Splošna uredba.

Postopki sodelovanja po členu 60 Splošne uredbe (»vse na enem mestu«)

Na temelju postopkov določitve vodilnega in zadevnih nadzornih organov je Informacijski pooblaščenec v letu 2019 **aktivno sodeloval v 75 postopkih** čezmejnega sodelovanja pri inšpekcijskem nadzoru nad podjetji, ki poslujejo čezmejno. V teh postopkih je pričakovan sprejem odločitve nadzornih organov po členu 60 Splošne uredbe, po t. i. mehanizmu »vse na enem mestu«. Takšna odločitev je formalno zavezujoča tudi za Informacijskega pooblaščenca. Vodilni nadzorni organ v največjem številu primerov predstavlja irski nadzorni organ, pogosto v tej vlogi nastopajo tudi nadzorni organi Luksemburga, Francije, Nizozemske, Nemčije, Francije in Avstrije. 14 tovrstnih postopkov sodelovanja je sprožil Informacijski pooblaščenec, in sicer na

podlagi prejete prijave oz. pritožbe zoper ravnanje zavezanca, ki je ustanovljen v drugi članici EU ali pa ima ustanovitve v različnih članicah v EU oz. so dejanja obdelave osebnih podatkov zadevala posameznike iz različnih držav članic EU.
61 tovrstnih postopkov je bilo pričetih s strani drugih organov v EU in pogosto zadevajo priljubljene ponudnike komunikacijskih spletnih storitev oz. spletne velikane (Facebook, Google, Amazon, Apple, PayPal, WhatsApp, Twitter, Instagram, Microsoft itd.). Postopki zadevajo skladnost njihovih praks s Splošno uredbo, npr.:

- 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, kot npr. zaradi izkoriščanja varnostnih ranljivosti.

V 12 primerih je sodelovanje zadevalo kršitev varstva osebnih podatkov zaradi vdorov v informacijske sisteme in pomanjkljivega zavarovanja osebnih podatkov in je bil prek mehanizma čezmejnega sodelovanja Informacijski pooblaščenec obveščen o kršitvi, ki je zadevala slovenske uporabnike storitev upravljavca (najpogosteje je šlo za spletne in IT-storitve).

Postopki čezmejnega sodelovanja po členu 60 so v letu 2019 zadevali tako primere, ki jih Informacijski pooblaščenec obravnava v okviru inšpekcijskega nadzora (73 primerov), kot tudi postopke glede vpogleda v lastne osebne podatke s čezmejnim značajem (dva primera), kjer je prosilec Informacijskemu pooblaščencu podal prijavo zoper upravljavca iz druge države članice EU (Avstrije).

Leta 2019 je bilo v primerih, v katerih je sodeloval Informacijski pooblaščenec, izdanih osem osnutkov odločb in ena končna odločba po členu 60 Splošne uredbe. Primeri čezmejnega sodelovanja se ne zaključijo nujno z izdajo končne odločbe, saj zakonodaja nekaterih držav članic EU v primerih, ko zavezanci prostovoljno izpolnijo zahteve prijaviteljev, pozna tudi prijateljske poravnave. V teku pa ostaja večina postopkov zoper velika multinacionalna podjetja; ti postopki so v fazi konzultacije med organi. V večini teh primerov kot vodilni nastopa irski nadzorni organ.

Postopki »vse na enem mestu« v letu 2019.

75 **Postopkov čezmejnega sodelovanja pri inšpekcijskem nadzoru nad podjetji, ki poslujejo čezmejno “vse na enem mestu”**
- 14 na podlagi prijav, ki jih je glede čezmejnih zavezancev prejel IP
- 61 na iniciativo drugih nadzornih organov

Postopki zagotavljanja medsebojne pomoči med nadzornimi organi po členu 61 Splošne uredbe

Informacijski pooblaščenec je leta 2019 sodeloval v 73 postopkih zagotavljanja medsebojne pomoči med nadzornimi organi po členu 61 Splošne uredbe. V 40 primerih se je odzval na zahteve drugih organov, 33 zahtev za sodelovanje pa je poslal drugim organom v EU. Postopki po členu 61 se razlikujejo glede na njihovo prostovoljno naravo v smislu formalno določenih rokov. Podrobnejši prikaz postopkov je razviden iz spodnje razpredelnice.

67 **Postopkov prostovoljne medsebojne pomoči med nadzornimi organi po členu 61**

- 36 odzivov na zahteve drugih organov
- 31 zahtev s strani Informacijskega pooblaščenca

6 **Postopkov medsebojne pomoči med nadzornimi organi po členu 61**

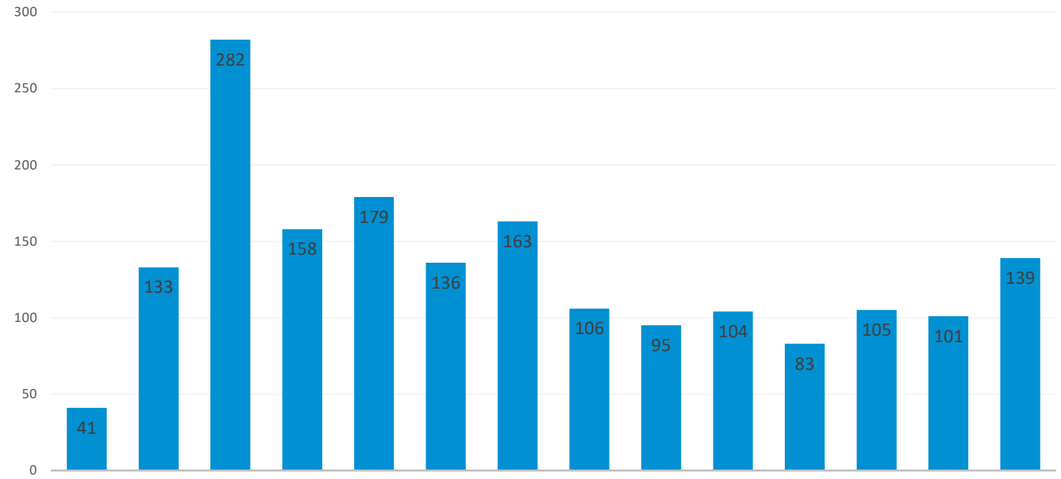
- 4 odzivi na zahteve drugih organov
- 2 zahteve s strani Informacijskega pooblaščenca

Postopki prostovoljne pomoči običajno zadevajo zahteve nadzornih organov v EU za podajo pojasnil glede konkretnih čezmejnih primerov, ki jih obravnavajo, ali glede usmeritev pri obravnavi določene tematike ter posredovanje prijav, kadar je za nadzor nad obdelavo podatkov določenega zavezanca krajevno pristojen obravnavati nadzorni organ v drugi državi članici. Postopki medsebojne pomoči pa običajno pomenijo zahtevo za izvedbo ukrepov zoper zavezance, ki izvajajo čezmejno obdelavo osebnih podatkov.

3.2.5 PREKRŠKOVNI POSTOPKI

Informacijski pooblaščenec je zaradi suma kršitev določb ZVOP-1 leta 2019 uvedel 139 postopkov o prekršku, od tega je 83 postopkov uvedel zoper pravne osebe javnega sektorja in njihove odgovorne osebe, 32 zoper pravne osebe zasebnega sektorja in njihove odgovorne osebe, 24 pa zoper posameznike (v to število so vključeni tudi postopki zoper odgovorne osebe državnih organov in samoupravnih lokalnih skupnosti, saj v skladu z ZP-1 Republika Slovenija in samoupravne lokalne skupnosti za prekrške ne odgovarjajo, odgovarjajo le njihove odgovorne osebe – teh je bilo 19).

Število uvedenih postopkov o prekršku med letoma 2006 in 2019.



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 dva predlagatelja obvestil, da na podlagi njunih predlogov ne bo uvedel postopka o prekršku, ker je pregon že zastaral, en postopek o prekršku pa je ustavil.

Informacijski pooblaščenec je v prekrškovnih postopkih leta 2019 izdal:
- **65 odločb o prekršku (44 glob in 21 opominov),**
- **10 opozoril.**

Poleg opozoril, ki so bila izrečena v prekrškovnih postopkih, je Informacijski pooblaščenec v skladu z načelom ekonomičnosti izrekel tudi 54 opozoril po 53. členu ZP-1 v okviru postopkov inšpekcijskega nadzora.

Poleg 65 odločb, ki so po ZP-1 najprej izdane brez obrazložitve, je bilo na podlagi napovedi zahtev za sodno varstvo izdanih 11 odločb z obrazložitvijo, pri čemer en kršitelj po prejemu odločbe z obrazložitvijo zahteve za sodno varstvo ni vložil. Kršitelji so zoper izdane odločbe o prekršku vložili deset zahtev za sodno varstvo (zoper 15,4 % odločb). Vse zahteve za sodno varstvo so bile vložene zoper odločbe, s katerimi je Informacijski pooblaščenec kršiteljem izrekel globe. Relativno majhen delež vloženih zahtev za sodno varstvo kaže na to, da storilci storjene prekrške priznavajo in se zavedajo svoje odgovornosti.

Kršitve varstva osebnih podatkov leta 2019.

Vrsta kršitve	Število kršitev (v okviru enega postopka je lahko več kršitev)
Nezakonita obdelava osebnih podatkov (8. člen ZVOP-1)	68
Neustrezno zavarovanje osebnih podatkov (24. in 25. člen ZVOP-1)	42
Nezakonit namen zbiranja in nadaljnje obdelave osebnih podatkov (16. člen ZVOP-1)	8
Kršitve določb v zvezi z izvajanjem videonadzora (74., 75., 76. in 77. člen ZVOP-1)	8
Neizpolnjevanje ukrepov, izrečenih v postopkih inšpekcijskega nadzora, kršitev drugega odstavka 29. člena ZIN	3
Kršitve določb o neposrednem trženju (72. in 73. člen ZVOP-1)	2
Upravljavec ni zagotavljal zunanje sledljivosti oz. evidence posredovanja osebnih podatkov (tretji odstavek 22. člena ZVOP-1)	1
Nezakonita obdelava občutljivih oz. posebnih vrst osebnih podatkov (13. člen ZVOP-1)	1
Neustrezno zavarovanje občutljivih osebnih podatkov (14. člen ZVOP-1)	1
Nezakonito kopiranje osebnih dokumentov (4. a člen ZPLD-1 in 4. člen ZOIzk-1)	1
Operater pred izvajanjem letalskih dejavnosti ni izvedel ocene učinkov in je ni posredoval Informacijskemu pooblaščencu (peti odstavek 19. člena Uredbe o sistemih brezpilotnih zrakoplovov)	1

Informacijski pooblaščenec poudarja, da je na vodenje prekrškovnih postopkov in izrekanje sankcij za ugotovljene kršitve zelo vplivalo dejstvo, da v Sloveniji še vedno ni sprejet sistemski predpis za uporabo Splošne uredbe in prenos Direktive za organe kazenskega pregona (t. i. ZVOP-2). Informacijski pooblaščenec tako 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 oz. za zavezance, za katere velja ZVOP-1 v celoti.

Leta 2019 je Informacijski pooblaščenec prejel devet sodb, s katerimi so okrajna sodišča odločila o zahtevah za sodno varstvo, ki so jih storilci vložili zoper odločbe o prekrških, izdane v letih 2017, 2018 in 2019:

- zahteva za sodno varstvo je bila zavrnjena kot neutemeljena, odločba Informacijskega pooblaščenca pa potrjena – 6,
- 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 – 1.

Sodba, s katero je okrajno sodišče postopek o prekršku ustavilo, še ni pravnomočna, ker je Informacijski pooblaščenec zoper njo vložil pritožbo.

3.2.6 IZBRANI PRIMERI OBDELAVE OSEBNIH PODATKOV

V nadaljevanju so predstavljeni primeri, v zvezi s katerimi je Informacijski pooblaščenec prejel večje število prijav, uradnih obvestil in vprašanj, ter primeri najpogostejših kršitev varstva osebnih podatkov, ki jih je Informacijski pooblaščenec zaznal v inšpekcijskih postopkih v letu 2019.

Izsiljevalski virusi

Med varnostnimi incidenti, katerih število se povečuje iz leta v leto, predstavljajo velik delež t.i. izsiljevalski virusi (angl. *ransomware*). Iz Poročila o kibernetski varnosti za leto 2018 nacionalnega odzivnega centra za kibernetsko varnost SI-CERT izhaja, da je SI-CERT v letu 2018 prejel 100 prijav izsiljevalskih virusov, pri čemer je bilo potrjenih okužb 61. Do nedavnega so bile žrtve vdorov izbrane naključno, kot del širše kampanje širjenja virusov, v zadnjem času pa so postali ti napadi ciljani, tj. storilci si izberejo točno določeno žrtev (npr. institucijo) z namenom povzročiti ji čim večjo škodo in od nje izsiliti odkupnino. Kadar je s takšnim vdorom ogrožena varnost osebnih podatkov in s tem pravic posameznikov, je treba v reševanje incidenta vključiti tudi Informacijskega pooblaščenca, ki ima na podlagi Splošne uredbe na tem področju določene pristojnosti (člena 33 in 34 Splošne uredbe).

Pri izsiljevalskih virusih, ki imajo obliko zlonamerne programske opreme, napadalec zaklene in šifrira podatke o računalniku ali napravi žrtve, nato pa zahteva odkupnino za obnovitev dostopa. Določena izsiljevalska programska oprema (npr. Cryptolocker) šifrira uporabniške datoteke s ključem, ki ga pozna samo napadalec, druga (npr. Winlocker) pa blokira dostop do sistema, a pusti datoteke nedotaknjene. V mnogih primerih mora žrtev spletnim prevarantom v določenem času plačati odkupnino, običajno v valuti bitcoin, ki je težko izsledljiva, ali pa tvega, da bo za vedno izgubila dostop do svojih podatkov. Plačilo odkupnine seveda ne zagotavlja, da bo dostop do zaklenjenih in šifriranih podatkov obnovljen, s plačilom odkupnine pa se spodbuja in podpira razvoj še naprednejših tehnik izsiljevanja spletnih kriminalcev.

Če napadalci žrtvi ne ponudijo ključa za dešifriranje (kljub plačilu odkupnine), morda ta ne bo uspela ponovno dobiti dostopa do svojih podatkov ali naprave. Usmeritve v zvezi z varnostnimi ukrepi na področju varstva osebnih podatkov upravljavcem in obdelovalcem nudi Splošna uredba. Ta sledi standardom na področju informacijske varnosti, kjer je glavno načelo, da je treba varnostne ukrepe prilagoditi glede na tveganja, ki pretijo varovani dobrini. Tveganja se običajno ocenjuje kot kombinacijo verjetnosti, da se bo neki nezaželen dogodek zgodil, in resnosti posledic, če se to dejansko zgodi. Splošna uredba zato v členu 32 določa, da se pri določanju ustrezne ravni varnosti upoštevajo zlasti tveganja, ki jih pomeni obdelava, zlasti zaradi nenamernega ali nezakonitega uničenja, izgube, spremembe, nepooblaščenega razkritja ali dostopa do osebnih podatkov, ki so poslani, shranjeni ali kako drugače obdelani. Odločitev o tem, kakšno stopnjo varnosti potrebuje določen zavezanec, je zato njegova, pri tem pa mora upoštevati stopnjo tehnološkega razvoja in stroške izvajanja ter naravo, obseg, okoliščine in namen obdelave, pa tudi tveganja za pravice in svoboščine posameznikov, ki se razlikujejo po verjetnosti in resnosti. Zaščita pred izsiljevalskimi virusi obsega tako tehnične ukrepe, med katere spadajo uporaba antivirusnih programov, požarnega zidu, filtrov na strežnikih, VPN-povezav, sistemov za nadzor in preprečevanje vdorov, redno posodabljanje vseh varnostnih programov itd., kot tudi redno izobraževanje in ozaveščanje uporabnikov oz. zaposlenih z namenom prepoznave morebitnih škodljivih priponk v elektronskih sporočilih. Kljub vsem varnostnim mehanizmom pa najboljšo zaščito pred izsiljevalskimi virusi še vedno predstavlja ustrezna varnostna kopija, replikacija te na eno ali več drugih lokacij ter redno preverjanje njihovega delovanja in zmožnosti obnovitve podatkov.

V primeru vdora izsiljevalskega virusa, pri katerem so ogroženi osebni podatki posameznikov, govorimo o kršitvi varstva osebnih podatkov, tj. kršitev varnosti, ki povzroči nenamerno ali nezakonito uničenje, izgubo, spremembo, nepooblaščeno razkritje ali dostop do osebnih podatkov, ki so poslani, shranjeni ali kako drugače obdelani. O takšni kršitvi je treba obvestiti Informacijskega pooblaščenca in v nekaterih primerih tudi posameznike, na katere se nanašajo osebni podatki, ki so bili predmet kršitve. Na podlagi člena 33 Splošne uredbe mora upravljavec brez nepotrebnega odlašanja, najpozneje pa v 72 urah po seznanitvi s kršitvijo o njej uradno obvestiti Informacijskega pooblaščenca, razen če ni verjetno, da bi bile s kršitvijo varstva osebnih podatkov ogrožene pravice in svoboščine posameznikov. Kadar uradno obvestilo Informacijskemu

pooblaščencu ni podano v 72 urah, mu je treba priložiti tudi navedbo razlogov za zamudo. Kadar pa je verjetno, da bi kršitev varstva osebnih podatkov povzročila veliko tveganje za pravice in svoboščine posameznikov, mora upravljavec brez nepotrebnega odlašanja o kršitvi obvestiti tudi posameznike, na katere se nanašajo osebni podatki, ki so bili predmet kršitve, z namenom, da se posameznike seznani z ukrepi, ki so bili sprejeti s strani upravljavca, ter z namenom ublažitve morebitnih škodljivih učinkov kršitve na pravice in svoboščine posameznikov (člen 34 Splošne uredbe).

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

Leta 2019 je kar nekaj bolnišnic skladno s 46. členom ZPacP Informacijskega pooblaščenca obvestilo o nezakonitih vpogledih v osebne podatke pacientov, ki so jih ugotovili v internih postopkih, nekaj prijav pa je Informacijski pooblaščenec prejel s strani posameznikov, ki so hoteli pridobiti tudi seznam oseb, ki so vpogledale v njihove osebne podatke. V zvezi s temi prijavami Informacijski pooblaščenec pojasnjuje, da postopek inšpekcijskega nadzora, v katerem preverja zakonitost obdelave osebnih podatkov določenega posameznika, ki se vodijo v določeni zbirki, uvede zgolj v primeru, če posameznik v prijavi izkaže konkretne 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 inšpekcijskega postopka ni dovolj.

V primeru potrjenega suma nezakonitega vpogleda v osebne podatke pacientov Informacijski pooblaščenec kršitelju praviloma izreče globo. Zaposleni v določeni zdravstveni ustanovi 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 ali drugim pooblaščenim uporabnikom). Nekateri zaposleni, čeprav so njihova osebna imena zabeležena v dnevnikih sledljivosti obdelave osebnih podatkov, se želijo izogniti odgovornosti za storjeni prekršek tako, 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, zaradi česar so neznane osebe z uporabo gesel kršiteljev 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 se po koncu 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 odjavljajo iz sistema in več oseb (kljub temu, da je upravljavec določil posamične dostopne pravice) uporablja isto geslo, tudi ni zagotovljena ustrezna 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.

Osebnih podatkov zaposlenih pri zavezancu, ki so (nedovoljeno) obdelovali pacientove osebne podatke, ta pacient ni upravičen pridobiti na podlagi pravice do seznanitve z lastno zdravstveno dokumentacijo iz 41. člena ZPacP, ker izpisi dnevnikov sledljivosti obdelave osebnih podatkov ne sodijo med zdravstveno dokumentacijo. Prav tako jih ni upravičen pridobiti na podlagi pravice do seznanitve z lastnimi osebnimi podatki, ki jo določa člen 15 Splošne uredbe in skladno s katerim ima posameznik, na katerega se osebni podatki nanašajo, pravico od upravljavca dobiti informacije o uporabniku ali kategorijah uporabnikov, ki so jim bili ali jim bodo razkriti osebni podatki, zlasti uporabnike v tretjih državah ali mednarodnih organizacijah (c točka). Splošna uredba tu ni prinesla nobenih sprememb, saj tudi ZVOP-1 v delu, ki se je nanašal na vsebino pravice do seznanitve z lastnimi osebnimi podatki (30. člen) in definicijo pojma uporabnik (8. točka 6. člena), ni zajemal zaposlenih znotraj upravljavca. Kljub navedenemu pacient, ki sumi na nezakonito obdelavo osebnih podatkov s strani zaposlenih v zdravstveni ustanovi, v kateri je bil obravnavan, ni prikrajšan za pravno varstvo, saj lahko pri Informacijskem pooblaščencu vloži prijavo zaradi domnevne kršitve varstva osebnih podatkov. Informacijski pooblaščenec v inšpekcijskem postopku ugotavlja, ali in kdo je znotraj upravljavca nezakonito obdeloval osebne podatke, pacient pa lahko v tem postopku skladno z določbami drugega odstavka 82. člena ZUP uveljavlja pravico do vpogleda v inšpekcijski spis, vendar mora za takšen vpogled izkazati pravno korist. Če Informacijski pooblaščenec ugotovi nezakonito obdelavo osebnih podatkov, zoper kršitelja uvede postopek po ZP-1. Posameznik, katerega osebne podatke je določen zaposleni pri določenem upravljavcu obdeloval nezakonito, ima v postopku o prekršku položaj oškodovanca, zato lahko na podlagi 102. člena ZP-1 v povezavi z drugim odstavkom 58. člena ZP-1 opravi vpogled v prekrškovni spis in tako pridobi tudi osebne podatke kršitelja.

Obveščanje posameznikov o obdelavi osebnih podatkov

Upravljavci osebnih podatkov morajo poleg zakonitosti obdelave osebnih podatkov zagotoviti tudi poštenost in preglednost njihove obdelave. To storijo tako, da posameznikom posredujejo ustrezne informacije o obdelavi osebnih podatkov. Glede obveščanja posameznika o obdelavi osebnih podatkov Splošna uredba razlikuje med dvema vrstama pridobivanja osebnih podatkov: v členu 13 so določene informacije, ki jih upravljavci posredujejo takrat, kadar osebne podatke zbirajo neposredno od posameznika, na katerega se nanašajo, člen 14 pa določa informacije, ki jih morajo upravljavci zagotoviti, kadar osebnih podatkov ne pridobijo neposredno od posameznika, na katerega se nanašajo, ampak npr. iz drugih zbirk osebnih podatkov. Tudi ZVOP-1 je določal informacije, ki so jih morali upravljavci posredovati posameznikom (v 19. členu), a je Splošna uredba nabor informacij močno razširila. Informacijski pooblaščenec je glede (ne)ustreznosti obveščanja prejel številna vprašanja, v inšpekcijskih postopkih pa je pogosto tudi ugotovil kršitve.

V primeru zbiranja osebnih podatkov neposredno od posameznika, ki je praviloma primarno, mora upravljavec posameznika seznaniti z naslednjimi informacijami: identiteta in kontaktni podatki upravljavca; kontaktni podatki pooblaščene osebe za varstvo podatkov, kadar ta obstaja; namene, za katere se osebni podatki obdelujejo, in pravno podlago za njihovo obdelavo; morebitne zakonite interese, za uveljavljanje katerih si prizadeva upravljavec ali tretja oseba; morebitne uporabnike ali kategorije uporabnikov osebnih podatkov; ali upravljavec namerava prenesti osebne podatke v tretjo državo ali mednarodno organizacijo; obdobje hrambe osebnih podatkov; obstoj pravic posameznika (pravica do dostopa do osebnih podatkov, do popravka ali izbrisa osebnih podatkov, pravica do omejitve obdelave in ugovora, pravica do prenosljivosti podatkov, pravica do preklica privolitve in pravica do vložitve pritožbe pri nadzornem organu); ali je zagotovitev osebnih podatkov statutarna ali pogodbena obveznost ter ali mora posameznik, na katerega se nanašajo osebni podatki, zagotoviti osebne podatke in kakšne so morebitne posledice, če jih ne; obstoj avtomatiziranega sprejemanja odločitev, vključno z oblikovanjem profilov.

Informiranje posameznika po členu 13 Splošne uredbe je treba izvesti ne glede na to, na kateri pravni podlagi (privolitev, zakonska podlaga, zakoniti interesi, izvrševanje pogodbe ipd.) se osebni podatki zbirajo. Dolžnost obveščanja tudi ni vezana na zahtevo posameznika, ampak jo mora upravljavec izpolniti avtomatično. Splošna uredba upravljavcem namreč ne daje možnosti za posredovanje informacij zgolj v primeru, če bi jih posameznik zahteval, in tudi ne omogoča izbire o tem, katere informacije bo upravljavec posredoval, ampak je dolžan posredovati vse predpisane informacije. Način posredovanja informacij je odvisen od načina zbiranja osebnih podatkov in se šteje kot ustrezen le takrat, če upravljavec kasneje lahko dokaže, da je posameznikom ob zbiranju res posredoval ustrezne informacije. Izbor ustreznega načina obveščanja je odvisen od okoliščin konkretnega primera, pomembno je, da so informacije podane v jedrnati, pregledni, razumljivi in lahko dostopni obliki ter v jasnem in preprostem jeziku, kot to določa člen 12(1) Splošne uredbe. Upravljavec lahko informacije posreduje npr. na samem obrazcu, v katerega posameznik vpisuje osebne podatke, na ločenem dokumentu, ki ga posamezniku predloži pred oz. ob izpolnjevanju obrazca, ustno, če tako zahteva posameznik (takšen način posredovanja informacij je težje dokazljiv), ali na drug način, ki izpolnjuje zahtevo po lahko dostopni obliki ter zahtevo po informiranju v času, ko upravljavec pridobi podatke. Ustrezne informacije morajo biti posameznikom na voljo tudi v primeru posredovanja osebnih podatkov prek spleta, zato mora biti spletna stran oblikovana tako, da mora posameznik pred vnosom oz. posredovanjem svojih osebnih podatkov prebrati predpisane informacije.

Informacijski pooblaščenec svetuje, da upravljavec pri pripravi informacij izhaja iz namenov obdelave osebnih podatkov, ki jih določa zakonodaja ali ki jih je določil sam. Nameni obdelave osebnih podatkov morajo biti čim bolj natančno opredeljeni in ne smejo biti prepuščeni naknadni volji upravljavca osebnih podatkov. Neopredeljen oz. nejasno opredeljen namen obdelave osebnih podatkov pomeni, da se zbrani podatki lahko uporabljajo za različne in posameznikom, na katere se ti podatki nanašajo, neznane namene, kar je v nasprotju tako s Splošno uredbo kot z ZVOP-1, ki upravljavcem prepovedujeta nadaljnjo obdelavo osebnih podatkov za druge namene oz. naknadno spremembo namena obdelave. Da bo namen obdelave posameznikom razumljiv, je treba navesti tudi vrste osebnih podatkov, ki se zbirajo oz. obdelujejo za posamezen namen. Informacijski pooblaščenec je v pomoč upravljavcem pri zagotovitvi informacij pripravil obrazec Obvestilo posameznikom po 13. členu Splošne uredbe o varstvu podatkov (ang. GDPR) glede obdelave osebnih podatkov, ki je objavljen na https://www.ip-rs.si/obrazci/varstvo-osebnih-podatkov/.

Razkrivanje osebnih podatkov v odločbah centrov za socialno delo

Informacijski pooblaščenec že več let prejema večje število prijav zoper centre za socialno delo, v katerih prijavitelji navajajo, da so na center vložili vlogo za oprostitev doplačila stroškov institucionalnega varstva, nato pa so prejeli odločbo, v kateri so našteti vsi njihovi prejemki, vključno s prejemki njihovih partnerjev, center pa je odločbo vročil tudi nekaterim njihovim sorodnikom.

Informacijski pooblaščenec na podlagi prejetih prijav postopka inšpekcijskega nadzora ni uvedel, ker je šlo za obdelavo osebnih podatkov v postopkih odločanja o plačilu institucionalnega varstva in ker mora v primerih, ko gre za obdelavo osebnih podatkov v konkretnih upravnih postopkih, spoštovati sklep Ustavnega sodišča RS št. U-I-92/12-13 z dne 10. 10. 2013, s katerim je Ustavno sodišče odločilo, da Informacijski pooblaščenec nima podlage za neposredno poseganje v vodenje postopkov, opravljanje procesnih dejanj in odločanje javnopravnih organov v posamičnih in konkretnih zadevah ter da inšpekcijskega nadzora nad izvajanjem ZVOP-1 ne sme izvajati tako, da pri izvrševanju svojih zakonsko določenih pooblastil poseže v posamične pravne postopke, ki jih vodijo zanje pristojni državni organi. Prav tako ne sme preverjati, ali se v teh postopkih ustavnoskladno in zakonito spoštuje varstvo osebnih podatkov. Kot je v navedenem sklepu ugotovilo Ustavno sodišče, bi bila zakonska podlaga, ki bi to omogočala, v nasprotju z načelom samostojnosti pristojnega državnega organa pri odločanju (drugi odstavek 120. člena Ustave RS za upravne organe, 125. člen Ustave RS za sodišča), v nasprotju z rednim sistemom pravnih sredstev oz. vzpostavljeno hierarhično strukturiranostjo državne oblasti (načelo večstopenjskega odločanja) in s tem v nasprotju z načeli pravne države (2. člen Ustave RS). V posamičnem pravnem postopku, ki ga v skladu z zakonsko določenimi pristojnostmi vodi pristojni organ, je mogoče preverjati pravilnost (zakonitost) vodenja postopka in izpodbijati končne odločitve samo v postopkih s pravnimi sredstvi, ki jih določa zakon. O teh sredstvih pa lahko odločajo le z zakonom določeni državni organi na način, ki ga določa zakon.

Glede na zgoraj navedeni sklep Informacijski pooblaščenec ni pristojen preverjati, ali je pooblaščena uradna oseba na centru za socialno delo zakonito vodila določen postopek oz. ali je za odločanje v postopku potrebovala določene osebne podatke ter zakaj jih je navedla v obrazložitvi odločbe. Posamezniki, ki so prejeli odločbo centra za socialno delo, imajo možnost svoje pravice uveljavljati v okviru pravnih sredstev, ki so jim na voljo v konkretnem upravnem postopku in ki so navedena v pravnem pouku odločbe (pritožba na Ministrstvo za delo, družino, socialne zadeve in enake možnosti). Če menijo, da pooblaščena oseba na centru za socialno delo ni ravnala strokovno, se lahko obrnejo tudi na socialno inšpekcijo, ki izvaja nadzor nad centri za socialno delo.

Kljub neuvedbi inšpekcijskih postopkov zaradi nepristojnosti je Informacijski pooblaščenec prijaviteljem pojasnil, na kateri pravni podlagi centri za socialno delo obdelujejo osebne podatke v postopkih odločanja o oprostitvi plačila institucionalnega varstva. Splošna uredba med dopustnimi pravnimi podlagami za obdelavo osebnih podatkov v točki (c) člena 6(1) določa, da je obdelava osebnih podatkov zakonita, če je (med drugim) potrebna za izpolnitev zakonske obveznosti, ki velja za upravljavca, torej center za socialno delo. Na podlagi tretjega odstavka 37. člena Zakona o uveljavljanju pravic iz javnih sredstev (ZUPJS) se pravica, ki jo oseba kot zavezanec po predpisih o socialnem varstvu uveljavlja za oprostitev plačila socialnovarstvene storitve, uveljavlja s samostojno vlogo hkrati z vlogo upravičenca do uveljavljanja oprostitve plačila socialnovarstvenih storitev. Center za socialno delo v tem primeru z eno odločbo odloči o pravicah in obveznostih upravičenca in njegovega zavezanca. Obrazložitev odločb o pravicah iz javnih sredstev v skladu z drugim odstavkom 37. člena ZUPJS vsebuje vrsto in višino dohodkov iz 12. člena tega zakona ter vrsto in vrednost premoženja iz 17. člena tega zakona, ki so bili upoštevani pri izračunu dohodka na družinskega člana. Natančnejša obrazložitev je potrebna le, če posamezni pravici iz javnih sredstev ni ugodeno. V tem primeru se obrazloži tisti del izreka, s katerim pravica ni bila priznana. Center za socialno delo torej nima možnosti, da v odločbi o upravičenosti do oprostitve plačila institucionalnega varstva ne navede dohodkov ter premoženja vseh zavezancev za plačilo stroškov institucionalnega varstva. Odločbo mora vročiti vsem zavezancem, ki se tako seznanijo z osebnimi podatki ostalih zavezancev. Ob tem Informacijski pooblaščenec poudarja, da morajo vsi prejemniki odločbe varovati osebne podatke, ki jih vsebuje, kar pomeni, da jih ne smejo razkrivati nepooblaščenim osebam ali uporabljati v nasprotju z namenom, za katerega so jih pridobili, tj. uveljavljanje pravic pred pristojnimi organi. V primeru nezakonitega razkrivanja odločbe bi šlo za kršitev, katere sankcioniranje je v pristojnosti Informacijskega pooblaščenca, saj na odločbi navedeni podatki izvirajo iz zbirk osebnih podatkov, zaradi česar so predmet varstva po Splošni uredbi in ZVOP-1.

Videonadzor iz zasebne hiše

Informacijski pooblaščenec vsako leto prejme precej prijav zoper posameznike, ki namestijo kamere na svojo hišo, pri čemer pa naj ne bi snemali samo svoje lastnine, ampak tudi sosedovo parcelo in/ali javne površine.

Splošna uredba se skladno s točko (c) člena 2(2) ne uporablja za obdelavo osebnih podatkov s strani fizične osebe med potekom popolnoma osebne ali domače dejavnosti, prav tako se po prvem odstavku 7. člena ZVOP-1 ne uporablja za obdelavo osebnih podatkov, ki jo izvajajo posamezniki izključno za osebno uporabo, družinsko življenje ali za druge domače potrebe. Videonadzor, ki ga posameznik izvaja iz svoje hiše, se tako praviloma šteje kot obdelava osebnih podatkov za osebno uporabo in domače potrebe, razen v primeru, ko snema tudi javne površine ali prostor, ki ni v njegovi lasti. Takšno stališče izhaja iz sodbe Sodišča EU v zadevi Ryneš proti Úřad pro ochranu osobních údajů, št. C-212/13 z dne 11. 12. 2014, s katero je sodišče odločilo, da uporaba videonadzornega sistema, ki ga je sicer posameznik namestil na družinsko hišo zaradi varovanja premoženja, zdravja in življenja lastnikov hiše, vendar pa se z njim nadzira tudi javni prostor, ne pomeni obdelave podatkov, ki se opravi med potekom popolnoma osebne ali domače dejavnosti. Zato mora biti izvajanje takšnega videonadzora skladno z ZVOP-1 in Splošno uredbo.

Informacijski pooblaščenec inšpekcijski postopek uvede le takrat, ko za to obstaja utemeljen sum kršitve določb ZVOP-1 in Splošne uredbe in ko je to v javnem interesu. V primeru suma izvajanja videonadzora javnih površin s strani posameznikov to pomeni, da mora razpolagati z dokazi, da posameznik dejansko snema površine, ki niso v njegovi lasti, česar pa kamere na zunanji strani hiše same po sebi še ne izkazujejo. Upoštevati je namreč treba, da samo glede na položaj nameščene kamere še ni mogoče ugotoviti, kaj kamera dejansko snema, če sploh, saj se v praksi pogosto dogaja, da posamezniki namestijo slepe kamere, ki v resnici ne snemajo, a imajo preprečevalni učinek, ali pa so posnetki tako slabe kvalitete, da posnetih oseb sploh ni mogoče prepoznati. V obeh primerih zbirka osebnih podatkov ne nastaja, zato Informacijski pooblaščenec ni pristojen ukrepati.

Za uvedbo inšpekcijskega postopka zoper posameznika, ki izvaja videonadzor s kamerami, ki jih je namestil na svojih objektih, v katerih ni registrirane nobene dejavnosti, Informacijski pooblaščenec torej potrebuje dokaze o nezakonitosti izvajanja videonadzora, npr. konkreten videonadzorni posnetek, iz katerega je razvidno, da posameznik z videonadzornim sistemom dejansko snema površine, ki niso v njegovi lasti, in da so posnetki takšne kvalitete, da je posameznika na njih mogoče prepoznati. To je pomembno, ker vstop v stanovanje zaradi ustavne določbe nedotakljivosti stanovanja ni dopusten brez odredbe sodišča, poleg tega pa že zgolj sama uvedba inšpekcijskega postopka zoper posameznika pomeni poseg v njegovo zasebnost.

Če prijavitelj predloži ustrezna dokazila, Informacijski pooblaščenec uvede inšpekcijski postopek, v katerem presoja, ali ima posameznik za izvajanje videonadzora nad javnimi površinami za namen varovanja svojega premoženja pravno podlago v točki (f) člena 6(1) Splošne uredbe, ki določa, da je obdelava osebnih podatkov (videoposnetkov) dopustna, 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. Presoditi je torej treba, ali je interes imetnika videonadzornega sistema zakonit in dovolj močan, da prevlada nad interesi snemanih posameznikov. Zakonit interes imetnika videonadzora je utemeljen v 33. členu Ustave RS, ki določa pravico do zasebne lastnine, in v 34. členu, ki določa pravico do osebnega dostojanstva in varnosti, snemani posameznik pa uživa varstvo pravic zasebnosti in osebnostnih pravic na podlagi 35. člena Ustave RS, še posebej pravico do varstva osebnih podatkov iz 38. člena Ustave RS. Dopustnost izvajanja videonadzora in snemanja javnih površin s strani posameznika je odvisna predvsem od tega, ali svojega premoženja ne more učinkovito zavarovati na drug način.

Informacijski pooblaščenec pojasnjuje, da lahko posameznik s kamero oz. kamerami, s katerimi snema svoje premoženje, ki se nahaja ob javni cesti (npr. dvoriščna vrata, ograja), zajame tudi del te ceste, katerega nadzor je po naravi stvari nujen, da se doseže namen izvajanja videonadzora (če npr. nekdo poškoduje dvoriščna vrata, ga kamera, če ne bi pokrivala dela ceste, ne bi mogla posneti, zaradi česar posameznik ne bi mogel najti povzročitelja škode in zahtevati odškodnine). To pomeni, da mora posameznik pri določitvi dela javne ceste, ki ga bo zajela kamera, upoštevati načelo sorazmernosti. Če kamera zajame večji del ceste, kot je nujno potrebno, potem je treba del slike programsko zakriti, kar omogočajo vsi sodobnejši videonadzorni sistemi. Ker posameznik posname tudi mimoidoče, ki se gibajo po tem delu ceste, Informacijski pooblaščenec poudarja, da čeprav mimoidoči ne morejo pričakovati takšne stopnje zasebnosti kot na svojem zemljišču, to

ne pomeni, da lahko posameznik videoposnetke pregleduje kadar koli in jih uporablja za katere koli namene. Vpogled v arhiv videoposnetkov je namreč dopusten le v primeru incidenta (npr. poškodovanje premoženja), videoposnetki pa se lahko uporabljajo le za namen uveljavljanja pravic pred pristojnimi organi.

Če posameznik izkaže, da je snemanje dela javne površine zakonito, mora objaviti obvestilo o izvajanju videonadzora, ki vsebuje informacije iz tretjega odstavka 74. člena ZVOP-1 (da se izvaja videonadzor, naziv (ime) osebe, ki ga izvaja, in telefonsko številko za pridobitev informacije, kje in koliko časa se shranjujejo posnetki iz videonadzornega sistema). V nasprotnem primeru mora izvajanje takšnega videonadzora prekiniti.

V primerih, ko posameznik ne snema javnih površin, ampak posest drugega posameznika, Informacijski pooblaščenec inšpekcijskega postopka praviloma ne uvede. Ker posameznik s snemanjem tuje lastnine posega v osebnostne pravice snemanega posameznika, lahko slednji v skladu s 134. členom Obligacijskega zakonika (OZ) vloži tožbo in sodišču predlaga, da odredi prenehanje snemanja, na podlagi 179. člena OZ pa lahko zahteva odškodnino, če mu je zaradi snemanja nastala škoda. Če posameznik z izvajanjem videonadzora občutno poseže zasebnost drugega posameznika ali v njegovo družinsko življenje, ima slednji na razpolago tudi kazenskopravno sodno varstvo, saj bi lahko šlo za kaznivo dejanje neupravičenega slikovnega snemanja iz 138. člena Kazenskega zakonika. Pregon za to kaznivo dejanje se začne na predlog, ki ga na pristojni policijski postaji ali na pristojnem državnem tožilstvu vloži oškodovanec.

Pravica do izbrisa osebnih podatkov, ki so objavljeni v spletnih medijih

Pravico do izbrisa oz. »pravico do pozabe« Splošna uredba ureja v členu 17. Iz prvega odstavka izhaja, da mora upravljavec na zahtevo posameznika, na katerega se nanašajo osebni podatki, brez nepotrebnega odlašanja izbrisati osebne podatke v zvezi z njim kadar: osebni podatki niso več potrebni za namene, za katere so bili zbrani ali kako drugače obdelani; posameznik prekliče privolitev v obdelavo osebnih podatkov in kadar za obdelavo ne obstaja nobena druga pravna podlaga; posameznik obdelavi ugovarja v skladu s členom 21 (tj. obdelavi za namene neposrednega trženja in obdelavi iz zakonitih interesov ali v javnem interesu), za njihovo obdelavo pa ne obstajajo nobeni prevladujoči zakoniti razlogi; so bili osebni podatki obdelani nezakonito; je osebne podatke treba izbrisati za izpolnitev pravne obveznosti v skladu s pravom EU ali pravom države članice, ki velja za upravljavca; so bili osebni podatki zbrani v zvezi s ponudbo storitev informacijske družbe od mladoletne osebe. Če so izpolnjeni pogoji za izbris objavljenih osebnih podatkov, skladno z drugim odstavkom upravljavec ob upoštevanju razpoložljive tehnologije in stroškov izvajanja sprejme razumne ukrepe, da upravljavce, ki obdelujejo osebne podatke, obvesti, da posameznik zahteva, naj izbrišejo morebitne povezave do teh osebnih podatkov ali njihove kopije.

Pravica do izbrisa ni neomejena. Splošna uredba v tretjem odstavku člena 17 določa, da se prvi in drugi odstavek ne uporabljata, če je obdelava potrebna za uresničevanje pravice do svobode izražanja in obveščanja; za izpolnjevanje pravne obveznosti obdelave na podlagi prava Unije ali prava države članice, ki velja za upravljavca, ali za izvajanje naloge v javnem interesu ali pri izvajanju javne oblasti, ki je bila dodeljena upravljavcu; iz razlogov javnega interesa na področju javnega zdravja; za namene arhiviranja v javnem interesu, za znanstvene ali zgodovinsko-raziskovalne namene ali statistične namene in če je potrebna za uveljavljanje, izvajanje ali obrambo pravnih zahtevkov.

Po začetku uporabe Splošne uredbe je Informacijski pooblaščenec prejel nekaj pritožb posameznikov, ker so upravljavci osebnih podatkov (medijske hiše) zavrnili njihove zahteve za izbris osebnih podatkov oz. člankov, ki vsebujejo njihove osebne podatke, s spletnih strani.

Pri odločanju o pritožbi posameznika Informacijski pooblaščenec najprej preveri, ali so objavljeni podatki predmet varstva po ZVOP-1 ali Splošni uredbi. V nasprotnem primeru ni pristojen odločati, saj so predmet varstva po Splošni uredbi in ZVOP-1 samo tisti osebni podatki, ki so del zbirk osebnih podatkov ali obdelani z avtomatiziranimi sredstvi. Če gre za podatke iz zbirk ali za podatke, ki so avtomatizirano obdelani, Informacijski pooblaščenec nadalje oceni, ali so v članku navedeni osebni podatki ustrezni, relevantni in omejeni na obseg, potreben za namene medijskega poročanja, ter pretehta, ali je izpolnjen kateri od pogojev za izbris oz. ali je podana izjema, na podlagi katere se izbris osebnih podatkov zavrne.

Pri presoji utemeljenosti posameznikove zahteve za izbris objave s strani medijev je treba upoštevati predvsem določbo točke (a) člena 17(3) Splošne uredbe, ki izključuje pravico do izbrisa oz. iz katere izhaja, da posameznik ni upravičen do izbrisa njegovih osebnih podatkov, če je obdelava potrebna za uresničevanje

pravice do svobode izražanja in obveščanja. Svobodo izražanja ureja 39. člen Ustave RS in 10. člen Evropske konvencije o človekovih pravicah. Prvi odstavek 39. člena Ustave RS določa, da je zagotovljena svoboda izražanja misli, govora in javnega nastopanja, tiska in drugih oblik javnega obveščanja in izražanja ter da lahko vsakdo svobodno zbira, sprejema in širi vesti in mnenja. Temeljna pravica do svobode izražanja je zagotovljena vsakomur, tako fizičnim kot pravnim osebam. Ustavno sodišče RS v svojih odločitvah poudarja, da ima svoboda govora še poseben pomen, ko gre za izražanje v okviru novinarskega poklica, saj so široke meje svobode tiska eden od temeljev sodobne demokratične družbe. Novinarsko delo predstavlja pomemben dejavnik pri raziskovanju in obravnavi pozitivne in negativne družbene realnosti, pomembno poslanstvo novinarskega poročanja je njegova informativna funkcija.

V skladu s tretjim odstavkom 15. člena Ustave RS se človekove pravice in temeljne svoboščine lahko omejijo predvsem zaradi človekovih pravic oz. temeljnih svoboščin drugih ljudi. Enako kot za pravico do svobode izražanja tudi za pravico do informacijske zasebnosti oz. pravico do varstva osebnih podatkov, ki jo ureja 38. člena Ustave RS, velja, da ni neomejena. V primeru, ko pride do kolizije dveh sobivajočih pravic, se nasprotje med pravicami uskladi z metodo praktične konkordance, ki pomeni oblikovanje pravila, veljavnega za konkreten primer. Odločiti je treba, kateri pravici je treba glede na konkretne okoliščine dati prednost in katera se mora zaradi aktiviranja nujne, ustavno varovane vsebine druge pravice umakniti oz. se mora umakniti del upravičenj, ki sestavljajo to pravico. Iz sodne prakse izhaja, da je za uravnoteženje med pravico do zasebnosti in pravico do svobode izražanja Evropsko sodišče za človekove pravice razvilo niz meril, ki jih je treba upoštevati, med drugim: prispevek k razpravi v splošnem interesu, poznanost prizadete osebe, predmet objave, predhodno ravnanje zadevne osebe, vsebino, obliko in posledice objave, način in okoliščine, v katerih so bile informacije pridobljene, in verodostojnost informacij.

Informacijski pooblaščenec dodaja, da navedbe posameznika, da mu zaradi objave določenih podatkov oz. zaradi proste dostopnosti določenih člankov nastaja škoda, ne vplivajo na presojo pravice do izbrisa. Ta pravica se namreč presoja le po merilih, ki so določena v členu 17 Splošne uredbe. Če posameznik meni, da članek vsebuje očitke oz. neresnične informacije, ki lahko škodujejo njegovi časti in dobremu imenu ter mu povzročajo škodo, ima pravico do pravnega varstva, ki je v stvarni pristojnosti sodišč. Informacijski pooblaščenec je namreč pristojen le za tisti del pravice do zasebnosti, ki se nanaša na varstvo osebnih podatkov, ki ga ureja 38. člen Ustave RS, nima pa stvarne pristojnosti v zvezi z zahtevki posameznikov, ki temeljijo na 35. členu Ustave RS. To pomeni, da ima posameznik, tudi če ni upravičen do izbrisa njegovih osebnih podatkov na podlagi člena 17 Splošne uredbe, pravico do morebitnega drugega pravnega varstva z zahtevki, s katerimi lahko varuje svojo osebnostno pravico do lastne podobe.

Uveljavljanje pravic pri upravljavcih iz drugih držav članic EU

Informacijski pooblaščenec prejema pritožbe in prijave posameznikov iz Slovenije glede izvajanja svojih pravic po Splošni uredbi, ki se lahko nanašajo na upravljavce iz drugih držav EU, npr. na delodajalce v primeru sosednjih držav ali na ponudnike spletnih storitev, ki so na voljo čezmejno. Pritožbe se lahko nanašajo na to, da upravljavec posamezniku ne omogoči seznanitve z lastnimi osebnimi podatki, najdejo pa se tudi primeri, ko posameznik npr. zahteva izbris svojih podatkov. Informacijski pooblaščenec v primeru, da gre za čezmejno obdelavo osebnih podatkov (upravljavec je bil ustanovljen v drugi državi članici EU), najprej locira organ, ki bo pristojen zadevo obravnavati glede na svojo ozemeljsko pristojnost ali kot glavni organ v postopku čezmejnega sodelovanja. V primeru, da je upravljavec ustanovljen v drugi državi članici EU (npr. v Avstriji) in ne gre za čezmejno sodelovanje, pač pa za individualen primer kršitve, Informacijski pooblaščenec uporabi mehanizme sodelovanja iz člena 61 Splošne uredbe in pristojnemu nadzornemu organu posreduje pritožbo v obravnavo. Obveščanje pritožnika v takem primeru še vedno izvaja Informacijski pooblaščenec. Kadar prijava ali pritožba zaradi neupoštevanja pravic posameznika ni le individualne narave, temveč kaže na sistemsko pomanjkljivost pri upravljavcu, ki izvaja obdelavo podatkov čezmejne narave, prvi korak obravnave primera vključuje postopek ugotavljanja vodilnega organa in zadevnih organov po členu 56 Splošne uredbe. Vodilnemu organu Informacijski pooblaščenec posreduje v angleški jezik prevedeno prijavo oz. pritožbo ter z njim aktivno sodeluje prek neformalnih konzultacij do izdaje končne odločitve. Postopki čezmejnega sodelovanja po Splošni uredbi so pri uveljavljanju pravic zelo dobrodošlo novo orodje, ki izkazuje dobre rezultate. Primeri, v katerih Informacijski pooblaščenec pred Splošno uredbo zaradi omejitev pri ozemeljski pristojnosti ni mogel uradno posredovati, se lahko zdaj prek postopkov po členih 61 in 60 Splošne uredbe učinkovito razrešijo v korist pravic posameznikov.

Nadzor nad tehnološkimi velikani zaradi personaliziranega oglaševanja

Ponudniki zelo priljubljenih spletnih storitev, družbenih omrežij in komunikacijskih platform (Facebook, Google, Twitter, Amazon idr.) svoje brezplačne storitve zelo pogosto monetizirajo s pomočjo personaliziranega in ciljanega oglaševanja, ki temelji na zbiranju ogromnih količin podatkov posameznikov, njihovi analizi, tudi s pomočjo umetne inteligence, ter na predvidevanjih o interesih, željah in potrebah posameznikov, ki so jim prikazani zanje relevantni oglasi. 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 razkritjih glede uporabe podatkov posameznikov za namen politične promocije pred volitvami in referendumi prek družabnih omrežij. Informacijski pooblaščenec kot zadevni nadzorni organ sodeluje v vrsti postopkov zoper omenjena podjetja in njihovo obdelavo osebnih podatkov za namen personaliziranega oglaševanja, tudi na podlagi prijav in pritožb nevladnih in potrošniških organizacij ter njihovih ugotovitev v nedavnih poročilih. V večini primerov je vodilni nadzorni organ irski nadzorni organ za varstvo osebnih podatkov. Postopki so v teku in na ravni konzultacij med nadzornimi organi, prve odločitve naj bi bile sprejete v letu 2020. Kot zadevni nadzorni organ v teh postopkih Informacijski pooblaščenec lahko poda formalni ugovor na osnutek odločbe, ki ga pripravi vodilni nadzorni organ. Ta mora ugovore zadevnih nadzornih organov upoštevati pri pripravi končne odločbe po členu 60 Splošne uredbe. V primeru, da se vodilni nadzorni organ in zadevni nadzorni organi glede končne odločitve ne strinjajo oz. ugovori zadevnih nadzornih organov niso upoštevani, se zadeva na podlagi člena 65 Splošne uredbe predloži v odločanje EOVP.

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. do 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. avtentikacijo ali za ugotavljanje identitete oz. identifikacijo).

Informacijski pooblaščenec je leta 2019 prejel šest vlog za izdajo dovoljenja za uvedbo biometrijskih ukrepov. Dva vlagatelja sta po pozivu za dopolnitev vloge svoji vlogi umaknila, zaradi česar je Informacijski pooblaščenec oba postopka ustavil. Izdal je tri odločbe:

- Enemu vlagatelju je za namen varovanja poslovnih skrivnosti in zagotavljanja varnosti njegovega premoženja in tretjih oseb dovolil izvajanje biometrijskih ukrepov za vstopanje v poslovne prostore vlagatelja na njegovem sedežu, in sicer z enim čitalcem prstnih odtisov na glavnem vhodu in z dvema čitalcema na dveh notranjih vhodih ter za vstopanje v dve varni sobi, v katerih se odvijajo najbolj občutljivi procesi s področja vlagateljeve dejavnosti (upravljanje digitaliziranih sredstev).
- Eno vlogo za izvajanje biometrijskih ukrepov je zavrnil, ker je vlagatelj želel biometrijske ukrepe z uporabo naprave za prepoznavo obraza in prstnega odtisa uvesti zaradi poenostavitve postopka registracije delovnega časa zaposlenih. Biometrijskih ukrepov, ki se uvajajo le zato, ker so bolj priročni ali bolj ekonomični od drugih sistemov registracije delovnega časa, ki temeljijo na npr. brezkontaktnih karticah, namreč ni mogoče opredeliti kot nujno potrebne za dosego namenov, opredeljenih v prvem odstavku 80. člena ZVOP-1.
- Eni vlogi je delno ugodil tako, da je vlagatelju dovolil izvajanje biometrijskih ukrepov z uporabo čitalnika prstnega odtisa kot edinega načina za vstopanje v strežniško sobo, v kateri se nahajajo strežniki in druga oprema oz. sredstva informacijske tehnologije, katerih pravilno delovanje je nujno in ključno za opravljanje dejavnosti vlagatelja, poleg tega pa ta oprema oz. sredstva vsako zase, zlasti pa skupaj predstavljajo premoženje večje vrednosti. Vlagatelju pa ni dovolil izvajanja biometrijskih ukrepov na glavnem vhodu v poslovno stavbo, ker v stavbo vstopa večje število posameznikov (vsi zaposleni in obiskovalci), ki uporabljajo tudi RFID-kartice. Izvajanje biometrijskih ukrepov je namreč lahko učinkovito, če gre za prostore, v katere lahko vstopajo le pooblaščene osebe, in če ti ukrepi predstavljajo edini način vstopanja v zavarovane prostore.

3.3.2 POVEZOVANJE ZBIRK OSEBNIH PODATKOV

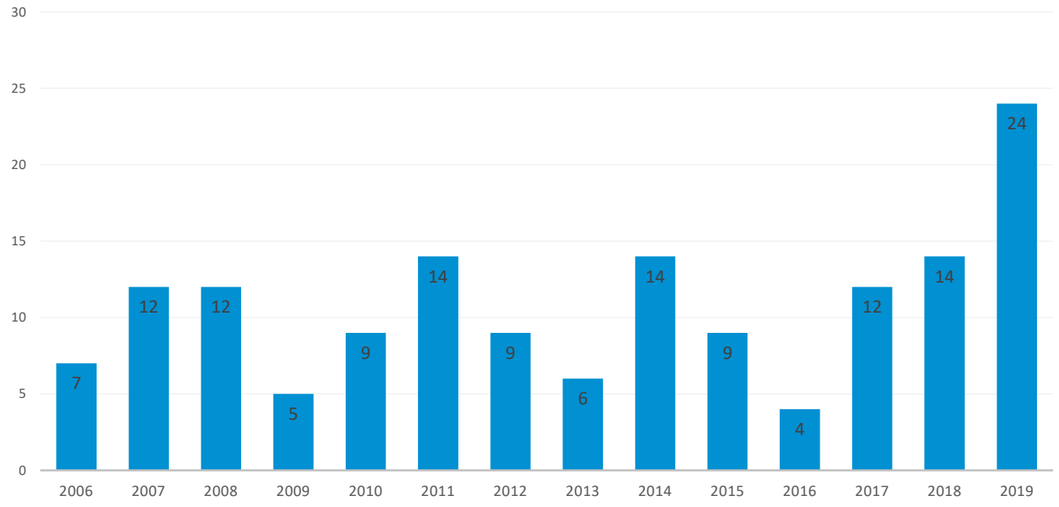
Povezovanje zbirk osebnih podatkov urejajo 84., 85. in 86. člen ZVOP-1. 84. člen ZVOP-1 določa, da če najmanj ena izmed zbirk osebnih podatkov, ki naj bi se jih povezovalo, vsebuje občutljive osebne podatke ali če bi bila posledica povezovanja razkritje občutljivih podatkov ali je za povezovanje potrebna uporaba istega povezovalnega znaka, povezovanje brez predhodnega dovoljenja Informacijskega pooblaščenca ni dovoljeno. Ta povezavo dovoli na podlagi pisne vloge upravljavca osebnih podatkov, če ugotovi, da ta zagotavlja ustrezno zavarovanje osebnih podatkov. Postopki in ukrepi za zavarovanje morajo biti ustrezni glede na tveganje, ki ga predstavljata obdelava in narava osebnih podatkov, ki se obdelujejo. Poleg ugotavljanja ustreznosti zavarovanja osebnih podatkov mora Informacijski pooblaščenec pri odločanju o izdaji dovoljenja za povezovanje zbirk osebnih podatkov opraviti tudi vsebinski preizkus, ali za povezovanje zbirk osebnih podatkov obstaja ustrezna zakonska podlaga. V okviru povezave zbirk osebnih podatkov se lahko posredujejo oz. obdelujejo le tisti osebni podatki, ki jih določa veljavna zakonodaja. Povezovanje zbirk predstavlja avtomatsko in elektronsko povezovanje zbirk osebnih podatkov, ki jih vodijo upravljavci za različne namene, in sicer tako, da se določeni podatki samodejno ali na zahtevo prenesejo ali vključijo v drugo povezano zbirko ali v več povezanih zbirk. Zbirki osebnih podatkov sta povezani, če se določeni podatki iz ene zbirke neposredno vključijo v drugo zbirko, s čimer se druga zbirka spremeni (poveča, ažurira ipd.); pri tem gre lahko zgolj za enosmeren tok prenosa podatkov.

Informacijski pooblaščenec je leta 2019 prejel 24 vlog za pridobitev dovoljenja za povezovanje zbirk osebnih podatkov. En vlagatelj je vlogo umaknil, zato je Informacijski pooblaščenec postopek ustavil. Informacijski pooblaščenec je izdal 23 odločb (šest v postopkih iz leta 2018), s katerimi je upravljavcem dovolil povezovanje zbirk osebnih podatkov.

Izdane odločbe glede povezovanja javnih evidenc

	Upravljavec 1	Zbirka osebnih podatkov 1	Upravljavec 2	Zbirka osebnih podatkov 2	Povezovalni znak
1.	Zavod RS za zaposlovanje	Evidenca brezposelnih oseb	Finančna uprava RS	Davčni register	davčna številka
2.	KDD – Centralna klirinško depotna družba	Centralni register nematerializiranih papirjev (CRVP)	Ministrstvo RS za notranje zadeve	Centralni register prebivalstva (CRP)	EMŠO
3.	Splošna bolnišnica »dr. Franca Derganca« Nova Gorica	Osnovna medicinska dokumentacija (OMD)	Ministrstvo RS za notranje zadeve	Centralni register prebivalstva (CRP)	EMŠO
			Ministrstvo RS za notranje zadeve	Matični register (MR)	EMŠO
4.	Ministrstvo za javno upravo	Elektronska evidenca dokumentarnega gradiva organov	Ministrstvo RS za notranje zadeve	Centralni register prebivalstva (CRP)	EMŠO ali davčna številka
5.	Zavod RS za zaposlovanje	Evidenca brezposelnih oseb in Evidenca iskalcev zaposlitve	Študentska organizacija Slovenije	Evidenca študentskega dela	EMŠO
6.	Študentska organizacija Slovenije	Evidenca študentskega dela (EŠD)	Ministrstvo RS za izobraževanje, znanost in šport	Centralna evidenca udeležencev vzgoje in izobraževanja (Ceuviz)	EMŠO
			Ministrstvo RS za izobraževanje, znanost in šport	Evidenčni in analitski informacijski sistem visokega šolstva v RS (eVŠ)	EMŠO
7.	Finančna uprava RS	Evidenca o odmeri dohodnine od dohodka iz oddajanja premoženja v najem	Ministrstvo za okolje in prostor, Geodetska uprava RS	Register nepremičnin	EMŠO
8.	Finančna uprava RS	- Evidenca o davkih, - Evidenca o vodenju finančnega nadzora, - Evidenca o hrambi blaga, - Evidenca trošarin, - Evidenca o davčni izvršbi in - Evidenca motornih vozil	Ministrstvo za infrastrukturo	Evidenca registriranih vozil	(EMŠO) ali MŠ ali registrska številka vozila
9.	Študentska organizacija Slovenije	Evidenca študentskega dela (EŠD)	Zavod ŠOUM	Zbirka osebnih podatkov dijakov in študentov, ki so opravljali študentsko delo	EMŠO
10.	Študentska organizacija Slovenije	Evidenca študentskega dela (EŠD)	Zamorc, podjetje za opravljanje in posredovanje storitev, Škofja Loka, d. o. o.	Zbirka osebnih podatkov dijakov in študentov, ki so opravljali študentsko delo	EMŠO
11.	Študentska organizacija Slovenije	Evidenca študentskega dela (EŠD)	Študentski, posredovanje dela in ostale poslovne storitve, d. o. o.	Zbirka osebnih podatkov dijakov in študentov, ki so opravljali študentsko delo	EMŠO
12.	Študentska organizacija Slovenije	Evidenca študentskega dela (EŠD)	Študentski servis, posredovanje delovne sile, trgovina, gostinstvo, gradbeništvo, nepremičnine in storitve, d. o. o.	Zbirka osebnih podatkov dijakov in študentov, ki so opravljali študentsko delo	EMŠO
13.	Študentska organizacija Slovenije	Evidenca študentskega dela (EŠD)	ŠS storitveno podjetje, d. o. o.	Zbirka osebnih podatkov dijakov in študentov, ki so opravljali študentsko delo	EMŠO
14.	Študentska organizacija Slovenije	Evidenca študentskega dela (EŠD)	MS Servis posredovanje, d. o. o.	Zbirka osebnih podatkov dijakov in študentov, ki so opravljali študentsko delo	EMŠO
15.	Študentska organizacija Slovenije	Evidenca študentskega dela (EŠD)	Kadring – kadrovsko in poslovno svetovanje, d. o. o.	Zbirka osebnih podatkov dijakov in študentov, ki so opravljali študentsko delo	EMŠO
16.	Študentska organizacija Slovenije	Evidenca študentskega dela (EŠD)	Mladinski servis, Pomurski študentski servis, d. o. o.	Zbirka osebnih podatkov dijakov in študentov, ki so opravljali študentsko delo	EMŠO
17.	Študentska organizacija Slovenije	Evidenca študentskega dela (EŠD)	Cifra, finančne in računovodske svetovalne storitve, d. o. o.	Zbirka osebnih podatkov dijakov in študentov, ki so opravljali študentsko delo	EMŠO
18.	Študentska organizacija Slovenije	Evidenca študentskega dela (EŠD)	Alt Lakoše, d. o. o.	Zbirka osebnih podatkov dijakov in študentov, ki so opravljali študentsko delo	EMŠO
19.	Študentska organizacija Slovenije	Evidenca študentskega dela (EŠD)	Agencija M servis, Kadrovske storitve, d. o. o.	Zbirka osebnih podatkov dijakov in študentov, ki so opravljali študentsko delo	EMŠO
20.	Študentska organizacija Slovenije	Evidenca študentskega dela (EŠD)	Agado, d. o. o.	Zbirka osebnih podatkov dijakov in študentov, ki so opravljali študentsko delo	EMŠO
21.	Študentska organizacija Slovenije	Evidenca študentskega dela (EŠD)	Adecco H.R., d. o. o.	Zbirka osebnih podatkov dijakov in študentov, ki so opravljali študentsko delo	EMŠO
22.	Ministrstvo za izobraževanje, znanost in šport	Centralna evidenca udeležencev vzgoje in izobraževanja (CEUVIZ)	Ministrstvo za izobraževanje, znanost in šport	- Evidenca upravičencev do sofinanciranja plačil staršev za vrtec iz državnega proračuna (SPS), - Evidenca prijavljenih kandidatov za vpis v 1. letnik srednje šole (VPIS V SS), - Evidenca vpisanih v dijaške domove (VPIS V DD) in - Evidenca študentov in diplomantov v zbirki podatkov evidenčnega in analitskega informacijskega sistema visokega šolstva v Republiki Sloveniji (eVŠ)	EMŠO
23.	Ministrstvo za pravosodje	zbirka Evropskega informacijskega sistema kazenskih evidenc (ECRIS)	Ministrstvo RS za notranje zadeve	Centralni register prebivalstva (CRP)	kombinacija osebnih podatkov ime, priimek in datum rojstva

Število vlog za izdajo odločbe glede povezljivosti zbirk osebnih podatkov med letoma 2006 in 2019.



3.3.3 PRENOS OSEBNIH PODATKOV V TRETJE DRŽAVE

Splošna uredba ureja prenos podatkov v tretje države in 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 ustrezno 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.

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

Pridobitev dovoljenja oz. odločbe nadzornega organa glede ustreznosti zaščitnih ukrepov iz člena 46, ki predstavljajo podlago za prenos podatkov, je potrebna le še takrat:

- 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 zavezujočih poslovnih pravil, mora le-te predhodno odobriti pristojni nadzorni organ (člen 47(1)).

Informacijski pooblaščenec je leta 2019 prejel eno vlogo, s katero je vlagatelj zaprosil za odobritev določenega upravnega dogovora, ki se nanaša na prenose osebnih podatkov, pridobljenih pri opravljanju nalog oz. izvajanju pooblastil in odgovornosti med določenimi finančnimi nadzornimi organi Evropskega gospodarskega prostora (EGP) in določenimi finančnimi nadzornimi organi zunaj EGP, kot so javni organi, regulatorji in/ali nadzorniki trgov vrednostnih papirjev in/ali izvedenih finančnih instrumentov. Informacijski pooblaščenec je v postopku ugotovil, da upravni dogovor, ki ga je želel izvoznik podatkov uporabiti kot pravno podlago za prenos osebnih podatkov organom finančnega nadzora zunaj EGP, zagotavlja ustrezne zaščitne ukrepe in daje posameznikom, na katere se nanašajo osebni podatki, na voljo izvršljive pravice in učinkovita pravna sredstva. Zato je vlagatelju dovolil, da po prejemu odločbe na podlagi upravnega dogovora iz točke (b) člena 46(3) Splošne uredbe, in sicer »Administrative Arrangement for the transfer of personal data between European Economic Area (EEA) Financial Supervisory Authorities and non-EEA Financial Supervisory Authorities«, o katerem je EOVP dne 12. 2. 2019 že izdal pozitivno mnenje, osebne podatke, pridobljene pri

opravljanju nalog oz. izvajanju pooblastil in odgovornosti, prenaša finančnim nadzornim organom v tretjih državah, s katerimi bo podpisal predmetni upravni dogovor.

Informacijski pooblaščenec ima na svoji spletni strani objavljene smernice, v katerih je podrobno predstavljena ureditev prenosov osebnih podatkov v tretje države in mednarodne organizacije po Splošni uredbi. Smernice so dostopne na tej povezavi.

3.3.4 PRAVICE POSAMEZNIKOV

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. Po členu 15 Splošne uredbe je posameznik upravičen, da mu upravljavec na njegovo zahtevo: (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; (3) če se osebni podatki posameznika pri upravljavcu res obdelujejo, je posameznik upravičen tudi do naslednjih dodatnih informacij:

- namen obdelave podatkov,
- vrsta podatkov,
- uporabniki podatkov,
- obdobje hrambe podatkov,
- obstoj pravic posameznika v zvezi z njegovimi podatki,
- vir podatkov in
- obstoj 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.

Splošna 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 zoper upravljavčevo odločitev o posamezniku (npr. o njegovih pravicah in dolžnostih), če je bila odločitev sprejeta izključno z avtomatizirano obdelavo osebnih podatkov.
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 neobstoj pravne podlage za obdelavo podatkov, neobstoj 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.

Za zahteve posameznikov, ki se nanašajo na področje preprečevanja, odkrivanja, preiskovanja in pregona kaznivih dejanj ter izvrševanja kazenskih sankcij, se tudi po 25. 5. 2018 še vedno uporabljata 30. in 31. člen ZVOP-1. Po 30. členu ZVOP-1 je ureditev sicer nekoliko drugačna, vendar bistvenih razlik glede vsebine pravic 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 predpisanem roku ali če njegovo zahtevo zavrne, lahko posameznik vloži pritožbo pri Informacijskem pooblaščencu.

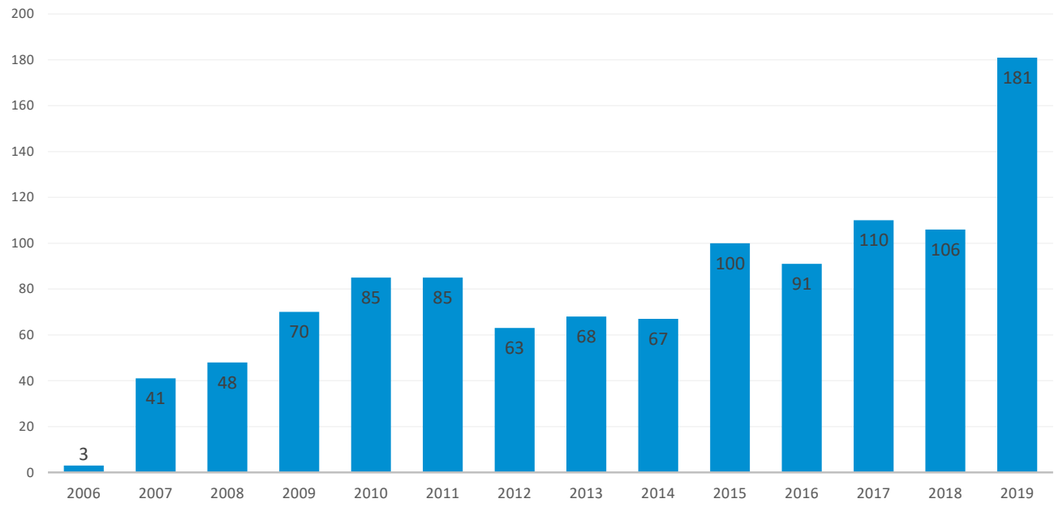
Informacijski pooblaščenec na pritožbeni stopnji odloča tudi o posebnih pravicah glede seznanitve z zdravstveno dokumentacijo po ZPacP, in sicer o:

1. pravici 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. pravici svojcev in drugih upravičenih oseb do seznanitve z zdravstveno dokumentacijo umrlega pacienta;

3. pravici določenih drugih oseb do seznanitve z zdravstveno dokumentacijo pacienta.

Informacijski pooblaščenec je leta 2019 prejel 181 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. Skrb vzbujajoče je, da je v primerjavi z letom 2018 prejel 75 pritožb (71 %) več, saj je mogoče zaključiti, da številni upravljavci osebnih podatkov ne izpolnjujejo svojih obveznosti in posameznikom ne omogočajo izvrševanja pravic, ki jim jih zagotavljajo različni predpisi.

Število pritožb v zvezi s pravico do seznanitve z lastnimi osebnimi podatki med letoma 2006 in 2019.



Vložene pritožbe so v 70 primerih zadevale upravljavce iz javnega sektorja (zlasti ministrstva in organe v njihovi sestavi, sodišča, javne zdravstvene zavode in centre za socialno delo), 111 pritožb pa se je nanašalo na upravljavce iz zasebnega sektorja (npr. banke, zavarovalnice, operaterje elektronskih komunikacij, društva, odvetnike in zasebne izvajalce zdravstvene dejavnosti). Le 17 pritožb se je nanašalo na pravico do seznanitve z zdravstveno dokumentacijo po ZPacP, vse preostale so se nanašale na pravico do seznanitve z lastnimi osebnimi podatki po Splošni uredbi oz. ZVOP-1. V več kot polovici primerov (v 98 primerih, torej v 54 %) so se posamezniki pritožili, ker jim upravljavci na njihove zahteve sploh niso odgovorili oz. so bili v molku, drugi pa so se pritožili zato, ker so upravljavci njihove vloge zavrnili ali ker jim niso posredovali vseh zahtevanih podatkov. Razlog za molk je bil (glede na odziv po prejemu poziva Informacijskega pooblaščenca) pri večini upravljavcev nepoznavanje pravice posameznikov do seznanitve z lastnimi osebnimi podatki in dolžnosti upravljavcev v zvezi z njenim izvrševanjem.

V 62 primerih, ki so se vodili zaradi molka upravljavca, so upravljavci po prejemu poziva Informacijskega pooblaščenca o zahtevah posameznikov odločili na način, da so jim posredovali zahtevane podatke in dokumente ali zahteve obrazloženo zavrnili s formalnim obvestilom (zoper katerega je možna vsebinska pritožba), zaradi česar je Informacijski pooblaščenec postopke ustavil. 16 posameznikov je Informacijskega pooblaščenca po vložitvi pritožbe obvestilo, da umikajo pritožbe, ker so s strani upravljavca prejeli ustrezna pojasnila in podatke, Informacijski pooblaščenec pa je nato postopke s sklepom ustavil.

Leta 2019 je Informacijski pooblaščenec, vključno s postopki, začetimi v letu 2018, izdal 38 upravnih odločb, kar je enkrat več kot leta 2018. V 19 odločbah je pritožbam posameznikov v celoti ugodil in upravljavcem naložil posredovanje določenih osebnih podatkov, v 11 odločbah je pritožbam ugodil delno, z osmimi odločbami je pritožbe posameznikov kot neutemeljene zavrnil. Večina upravljavcev je odločbe izvršila in posameznikom posredovala zahtevane dokumente oz. podatke, dva upravljavca pa sta zoper odločbi sprožila upravni spor pred Upravnim sodiščem RS. Tožbi sta vložila tudi dva posameznika, eden zoper zavrnilno odločbo, izdano decembra 2018, eden pa zoper sklep o zavrženju vloge zaradi nepristojnosti.

Informacijski pooblaščenec je s sklepom zavrgel 33 pritožb, in sicer 22 pritožb, ker je v postopku ugotovil, da je upravljavec zahtevi prosilca že v celoti ugodil, zaradi česar prosilec ni imel (več) pravnega interesa, 11 pritožb pa zaradi postopkovnih pomanjkljivosti (nepopolna, prepozna ali preuranjena vloga, vloga se ni nanašala na pravico do seznanitve z lastnimi osebnimi podatki). Osmim posameznikom je Informacijski pooblaščenec posredoval predlog za ravnanje, tri pritožbe pa je odstopil v reševanje pristojnim organom.

En pritožbeni postopek je Informacijski pooblaščenec prekinil do odločitve Ustavnega sodišča RS, ker je vložil zahtevo za presojo ustavnosti četrtega odstavka 149.b člena Zakona o kazenskem postopku (ZKP).

3.3.5 ZAHTEVA ZA OCENO USTAVNOSTI

Informacijski pooblaščenec lahko z zahtevo začne postopek za oceno ustavnosti oz. zakonitosti predpisov na podlagi 23.a člena Zakona o Ustavnem sodišču (ZUstS), če se pojavi vprašanje ustavnosti ali zakonitosti v zvezi s postopkom, ki ga vodi.

Zahteva za oceno ustavnosti četrtega odstavka 149.b člena ZKP

Informacijski pooblaščenec je na podlagi tretje alineje prvega odstavka 2. člena ZInfP v zvezi s 30. členom ZVOP-1 začel pritožbeni (drugostopenjski) postopek zoper operaterja elektronskih komunikacij kot upravljavca osebnih podatkov, in sicer na podlagi vložene pritožbe posameznika zoper zavrnilni odgovor upravljavca. Upravljavec je zavrnil posameznikovo zahtevo v delu, kjer je zahteval tudi seznam uporabnikov, katerim so bili posredovani njegovi podatki, kdaj, na kakšni podlagi in za kakšen namen, kot to omogoča 4. točka prvega odstavka 30. člena ZVOP-1. Pri tem se je skliceval na četrti odstavek 149.b člena ZKP, ki določa, da operater svoji stranki ali tretji osebi ne sme razkriti, da je ali da bo določene podatke posredoval pristojnemu organu (prvi odstavek tega člena) ali policiji (tretji odstavek tega člena) za namen odkritja storilca ali kaznivega dejanja, ki se preganja po uradni dolžnosti. Posameznik se je v pritožbenem postopku omejil le na podatke o uporabnikih njegovih osebnih podatkov, ki oz. če so bili posredovani v zvezi s 149.b členom ZKP, kar pomeni, da je od upravljavca želel prejeti podatke o posredovanju njegovih prometnih podatkov (telefonska številka, datum komunikacije, čas komunikacije, trajanje klica, vrsta komunikacije, količina podatkov in kraj) upravičenim organom po prvem odstavku 149.b člena ZKP, ne glede na to, ali je nastopal kot osumljenec ali kot tretja, naključno udeležena oseba.

Za meritorno odločitev o posameznikovi pravici do seznanitve z lastnimi osebnimi podatki je v pritožbenem postopku, poleg ostalih pogojev, neizogibno treba ugotoviti, ali je v področnih zakonih ali višjih predpisih določena omejitev pravice do seznanitve z lastnimi osebnimi podatki in ali omejitev v konkretnem primeru pride v poštev. V obravnavanem primeru se je izkazalo, da je taka omejitev res določena v četrtem odstavku 149.b člena ZKP, tako kot je zatrjeval upravljavec. Vendar pa je Informacijski pooblaščenec, izhajajoč iz dosedanje prakse, primerljivih predpisov in splošnih standardov na področju varstva osebnih podatkov, ugotovil, da obstajajo resni in objektivni razlogi, da omenjena zakonska omejitev ni v skladu z Ustavo RS.

Po mnenju Informacijskega pooblaščenca ni problematičen sam obstoj omejitve pravice do seznanitve z lastnimi osebnimi podatki, ki jo določa četrti odstavek 149.b člena ZKP. Sama omejitev pravice ter cilji oz. razlogi zanjo so legitimni in skladni s tedaj veljavno Direktivo 95/46/ES (13. člen) in sedaj veljavno Splošno uredbo (člen 23), saj iz obeh izhaja, da države članice lahko sprejmejo predpise za omejitev obsega pravic posameznikov, kadar taka omejitev predstavlja potreben in sorazmeren ukrep v demokratični družbi, med drugim za zagotavljanje preprečevanja, preiskovanja, odkrivanja ali pregona kaznivih dejanj ali izvrševanja kazenskih sankcij. Prav tako ni problematičen tisti del četrtega odstavka 149.b člena ZKP, ki se nanaša na bodoče posredovanje podatkov, torej da bo operater določene podatke posredoval pristojnemu organu ali policiji, ampak le del, ki govori o preteklem posredovanju podatkov pristojnim organom.

Obravnavana omejitev oz. izjema od splošne pravice do seznanitve z lastnimi osebnimi podatki po mnenju Informacijskega pooblaščenca ni v skladu z Ustavo RS oz. je nesorazmerna, ker brez očitno utemeljenega razloga trajno (ni pogojena z določeno časovno točko oz. dogodkom) in brezpogojno (ne določa izjem od omejitve ali pogojev, kdaj so dopustne izjeme glede načina izvrševanja pravice), torej absolutno omejuje posameznike pri uveljavljanju pravice do seznanitve z lastnimi osebnimi podatki, ki jo posamezniki sicer imajo po 38. členu Ustave RS, po 30. členu ZVOP-1 in po členu 15 Splošne uredbe.

Nevarnost razkritja prometnih komunikacijskih podatkov osumljencu, udeležencu ali s kaznivim dejanjem kako drugače povezanim osebam (npr. pričam, žrtvam ali svojcem osumljenca) je v tem, da lahko takšno razkritje ogrozi uspešno in učinkovito odkritje, preiskavo in pregon konkretnega kaznivega dejanja s strani pristojnih organov, kar pomeni, da je lahko prizadet javni interes, ki ga zasleduje kazensko pravo. Toda te kazenskopravne interese je utemeljeno, tj. smiselno, legitimno, primerno in neizogibno, treba varovati le do neke časovne točke, ko interesi preprečevanja, preiskovanja, odkrivanja in pregona kaznivih dejanj dejansko (v konkretnem primeru glede na okoliščine konkretnega primera) ali abstraktno (teoretično, na splošno) ne morejo biti več ogroženi. Primerne časovne točke bi lahko bile na primer: zastaranje kazenskega pregona za kaznivo dejanje, v zvezi s katerim so se obdelovali osebni podatki posameznika pri operaterjih, organih odkrivanja in pregona kaznivih dejanj ter sodiščih; pravnomočna obsodilna, zavrnilna ali oprostilna sodba sodišča; pravnomočna odločitev državnega tožilca, da ne bo začel pregona; pravnomočna odločitev o uvedbi kazenskega postopka. Zato ni utemeljenih razlogov, da bi moralo varstvo interesov preprečevanja, odkrivanja, preiskovanja in pregona kaznivih dejanj trajati neomejeno (izjema bi lahko veljala le za nezastarljiva kazniva dejanja), ampak bi morali biti tudi podatki o posredovanju prometnih podatkov glede telefonske komunikacije, ki jih ima operater, podvrženi sprostitvi v trenutku, ko navedeno varstvo ni več nujno potrebno in vsebinsko utemeljeno za dosego zasledovanih ciljev.

Zaradi masovnih izmenjav osebnih podatkov je v praksi pogosto, da z istimi ali istovrstnimi osebnimi podatki razpolaga več upravljavcev, posameznik pa ima možnost, da pod enakimi pogoji uresničuje pravico do seznanitve pri katerem koli od njih ali pri vseh. Zato bi tudi v konkretnem primeru bilo prav, da posameznik pod določenimi pogoji pridobi želene podatke pri vseh štirih možnih upravljavcih: policiji, državnem tožilstvu, sodišču in tudi pri operaterju. Primerjava s področnimi procesno-organizacijskimi zakoni je pokazala, da je obravnavana omejitev pretirana, ker zakonodajalec v področnih zakonih (Zakon o državnem tožilstvu, Zakon o nalogah in pooblastilih policije) ni določil absolutnih, temveč le relativne omejitve pri uresničevanju pravice do seznanitve z lastnimi osebnimi podatki, kamor sodijo tudi prometni podatki glede telefonske komunikacije, poleg tega omejitve pravice do seznanitve ne določa niti ZEKom-1, ki ureja delovanje operaterjev. Pravica do seznanitve zato ne učinkuje enako v razmerju do sodišča (kot izdajatelja odredbe) in v razmerju do operaterja (kot vira podatkov), čeprav gre za primerljive podatke in čeprav bi pravica do seznanitve z enakimi ali istovrstnimi podatki morala imeti enake ali vsaj podobne učinke in pogoje, ne glede na to, kdo je upravljavec osebnih podatkov.

Informacijski pooblaščenec je izpostavil tudi, da sta z omejitvijo prizadeti dve kategoriji oseb, in sicer osebe, zoper katere so potekale aktivnosti pri preiskovanju, odkrivanju ter pregonu kaznivih dejanj, in tretje osebe, ki s kaznivim dejanjem nimajo nobene zveze, saj so le naključno ali neodvisno od kaznivega dejanja vstopile v komunikacijo z osebo, v katero so sicer usmerjene aktivnosti iz prvega odstavka 149.b člena ZKP.

Zakonodajalec je po vložitvi zahteve za oceno ustavnosti predpis v tem delu delno dopolnil in določil rok, v katerem operater oz. ponudnik storitev informacijske družbe svojemu uporabniku, naročniku ali tretjim osebam ne sme razkriti, da je ali da bo v skladu s tem členom posredoval določene podatke. Tega ne sme razkriti 24 mesecev po preteku meseca, v katerem se je zaključilo izvrševanje odredbe. Preiskovalni sodnik lahko z odredbo določi drugačen rok, rok lahko podaljša za največ 12 mesecev, vendar ne več kot dvakrat, rok lahko skrajša ali prepoved seznanitve odpravi.

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 upravljavcev in obdelovalcev ter širše javnosti.

Leta 2019 je Informacijski pooblaščenec svetoval 3.284 posameznikom in pravnim osebam, ki so se nanj obrnili z vprašanji s področja varstva osebnih podatkov.

Informacijski pooblaščenec je izdal **1.261 pisnih mnenj in napotitev na mnenja**. 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. Na spletni strani https://www.ip-rs.si/vop/ je objavljenih več kot 5.000 mnenj, ki so razvrščena v 48 vsebinskih področij. Uporabniki lahko brskajo po mnenjih, ki so bila izdana, preden je v veljavo stopila Splošna uredba, z ločenim iskalnikom pa lahko dostopajo do mnenj, ki so bila izdana po 25. maju 2018.

Informacijski pooblaščenec spodbuja svetovanje oz. posredovanje ustnih odgovorov na vprašanja, zato je v uradu vsak dan na voljo dežurni državni nadzornik za varstvo osebnih podatkov, ki na vprašanja odgovarja po telefonu. **Leta 2019 so državni nadzorniki sprejeli 2.023 klicev**.

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 osebnih podatkov, in skladno z 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.

Leta 2019 je **Informacijski pooblaščenec izdal 73 mnenj na predloge sprememb zakonov ter na predloge novih zakonov in drugih predpisov**, kar je nekoliko več kot leta 2018, ko jih je izdal le 60. Kljub rahlemu povečanju števila mnenj je to število še vedno precej manjše kot pred letom 2018, ko je Informacijski pooblaščenec v posameznih letih izdal tudi več kot 100 mnenj. Informacijski pooblaščenec poudarja, da pri predlagateljih predpisov, s katerimi se uvajajo nove kompleksne oblike obdelav osebnih podatkov ali obsežne obdelave osebnih podatkov z uporabo modernih tehnologij, pogreša zavedanje o nujnosti temeljite predhodne analize in naslovitve tveganj, ki jih takšne obdelave prinašajo. Zato priporoča, da v teh primerih predlagatelji vedno predhodno pripravijo oceno učinkov v zvezi z varstvom podatkov, s katero lahko pravočasno prepoznajo in naslovijo morebitna tveganja ter se tako izognejo nepotrebnim napakam in težavam ob pripravi predpisa, ter poskrbijo, da bo zakon dejansko skladen z načelom sorazmernosti z vidika posegov v zasebnost. Upoštevajoč velike stroške uvajanja novih tehnologij pri obdelavi osebnih podatkov pa nikakor ni zanemarljivo, da se le tako lahko pravočasno in realno oceni finančne posledice uvedbe nove oblike obdelave ter prepreči morebitne dodatne stroške ob njenem izvajanju.

Informacijski pooblaščenec je leta 2019 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 divjadi in lovstvu,
- Predlog Zakona o spremembah in dopolnitvah Zakona o referendumu in ljudski iniciativi,
- Predlog Zakona o mladoletnih storilcih kaznivih dejanj (dve mnenji),
- Predlog novele Zakona o pacientovih pravicah,
- Predlog Zakona o spremembah in dopolnitvah Zakona o preprečevanju pranja denarja in financiranja terorizma,
- Predlog sprememb Zakona o osebni izkaznici – medresorsko usklajevanje (drugi krog),
- Predlog Uredbe o izvajanju Uredbe (EU) o evropski državljanski pobudi,
- Predlog novega Stanovanjskega zakona,

- Predlog Zakona o spremembah in dopolnitvah Zakona o športu (ZŠpo-1-A),
- Nezagotavljanje ustavne pravice do varstva osebnih podatkov v Sloveniji – nevarnost izključitve organov pregona iz nadzora,
- Predlog Letnega programa statističnih raziskovanj za leto 2020,
- Predlog dopolnjenega besedila novega Zakona o računskem sodišču,
- Predlog novega člena 146 j Zakona o varstvu okolja,
- Predlog dopolnjenega Zakona o spremembah in dopolnitvah Zakona o centralnem kreditnem registru,
- Predlog sprememb Zakona o osebni izkaznici,
- Uredba o spremembah in dopolnitvah Uredbe o izvajanju podukrepa pomoč za zagon dejavnosti, namenjene razvoju majhnih kmetij iz Programa razvoja podeželja Republike Slovenije za obdobje 2014–2020,
- Priloge predlogov pravilnikov k predlogu Zakona o spremembah in dopolnitvah Zakona o tujcih,
- Dodatna pojasnila k Predlogu Zakona o spremembah in dopolnitvah Zakona o prevozih v cestnem prometu,
- Predlog Zakona o spremembah in dopolnitvah Zakona o celostni zgodnji obravnavi predšolskih otrok s posebnimi potrebami,
- Predlog Zakona o spremembah in dopolnitvah Zakona o kmetijstvu,
- Predlog Zakona o spremembah in dopolnitvah Zakona o urejanju trga dela (ZUTD-E),
- Predlog Zakona o obravnavi otrok in mladostnikov s čustvenimi in vedenjskimi težavami in motnjami,
- Predlog Zakona o spremembah in dopolnitvah Zakona o zaščiti živali,
- Osnutek novele Zakona o pacientovih pravicah in Pravilnika o naročanju,
- Osnutek Zakona o spremembah in dopolnitvah Zakona o tujcih,
- Predlog novega Zakona o varstvu osebnih podatkov – ZVOP-2 (štiri mnenja),
- Predlog Pravilnika o pogojih in postopkih za izvajanje Zakona o izvajanju rejniške dejavnosti,
- Predlog Zakona o spremembah in dopolnitvi Zakona o pravilih cestnega prometa,
- Osnutek Odredbe o določitvi programa strokovnega usposabljanja za varnostnika telesnega stražarja,
- Predlog Zakona o spremembah in dopolnitvah Zakona o prevozih v cestnem prometu,
- Predlog novega Zakona o računskem sodišču,
- Predlog Zakona o spremembah in dopolnitvah Zakona o preprečevanju pranja denarja in financiranja terorizma (ZPPDFT-1A),
- Predlog Zakona o zagotavljanju zemljišč za namene izvajanja raziskovalnih in izobraževalnih procesov s področja kmetijstva in gozdarstva,
- Osnutek Odredbe o določitvi standardov, ki so obvezni na področju zasebnega varovanja,
- Predlog sprememb Zakona o letalstvu (ZLet),
- Predlog Uredbe o izvajanju Uredbe (EU) o kliničnem preskušanju zdravil,
- Predlog Zakona o spremembah in dopolnitvah Stvarnopravnega zakonika,
- Predlog Zakona o spremembah in dopolnitvah Zakona o preprečevanju pranja denarja in financiranja terorizma (ZPPDFT-1B),
- Predlog besedila 3. podpoglavja novega Stanovanjskega zakona – javna stanovanja (pridobivanje podatkov in zbirke podatkov pri lastnikih),
- Predlog Zakona o izvajanju Uredbe (EU) Evropskega parlamenta in Sveta o sodelovanju med nacionalnimi organi, odgovornimi za izvrševanje zakonodaje o varstvu potrošnikov,
- Predlog besedila Zakona o spremembah in dopolnitvah Zakona o vrtcih – medresorsko usklajevanje,
- Predlog besedila sprememb členov 75.a in 75.b Zakona o integriteti in preprečevanju korupcije,
- Mnenje na predlog Zakona o spremembah in dopolnitvah Zakona o trgu finančnih instrumentov,
- Predlog Pravilnika o spremembah in dopolnitvah Pravilnika o pogojih in postopkih za izvajanje Zakona o izvajanju rejniške dejavnosti (dve mnenji),
- Predlog Pravilnika o izvajanju mediacije po Družinskem zakoniku,
- Predlog Zakona o spremembah in dopolnitvah Zakona o poklicnem in strokovnem izobraževanju,
- Predlog Zakona o spremembah in dopolnitvah Zakona o gimnazijah,
- Dopolnjen Predlog Zakona o postopku sodnega varstva nekdanjih imetnikov kvalificiranih obveznosti bank (ZPSVNIKOB),
- Predlog sprememb člena 43.e Zakona o tajnih podatkih,
- Predlog Pravilnika o tehničnih pregledih motornih in priklopnih vozil,
- Predlog Zakona o spremembah in dopolnitvah Zakona o matičnem registru (dve mnenji),
- Predlog Zakona o spremembah in dopolnitvah Energetskega zakona (dve mnenji),
- Predlog Pravilnika o ravnanju ob nesrečah in incidentih v železniškem prometu,
- Odredba o določitvi programa strokovnega usposabljanja za operaterja varnostnonadzornega centra,
- Predlog Zakona o kazenskem postopku (ZKP-N),
- Predlog Pravilnika o izvrševanju kazni zapora,
- Predlog Zakona o postopku sodnega varstva nekdanjih imetnikov kvalificiranih obveznosti bank,
- Predlog Uredbe o določitvi pogojev za dostop do drugih informacijskih sistemov EU za namene ETIAS,
- Predlog Uredbe o izvajanju uredbe (EU) o skladih denarnega trga,
- Predlog Pravilnika o registraciji motornih in priklopnih vozil,
- Predlog Zakona o spremembah Zakona o nematerializiranih vrednostnih papirjih (ZNVP-1B),
- Predlog Uredbe o izvedbi ukrepov kmetijske politike za leto 2019,
- Predlog Zakona o spremembah in dopolnitvah Zakona o nalogah in pooblastilih policije,
- Predlog Zakona o spremembah in dopolnitvah Zakona o varstvu pred ionizirajočimi sevanji in jedrski varnosti,
- Predlog Pravilnika o gradbiščih,
- Predlog Zakona o spremembah in dopolnitvah Zakona o tujcih.

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. Nadzorni organi za varstvo osebnih podatkov zato vedno več resursov namenjajo preventivnemu delovanju, katerega cilj je zavezancem, ki želijo spoštovati zakonodajo, dati na razpolago ustrezne informacije, orodja in mehanizme, s katerimi lahko bolje razumejo in upoštevajo zahteve zakonodaje. Splošna uredba je namreč zlasti za mala in srednje velika podjetja, ki nimajo lastnih pravnih oddelkov, precejšen zalogaj, zato jim je treba dati na voljo enostavna, razumljiva in uporabna orodja ter jim tako približati zakonodajo.

Med tovrstna orodja vsekakor sodijo smernice, mnenja, infografike, predavanja, srečanja pooblaščenih oseb in komunikacija z relevantnimi združenji zavezancev, kot so različne zbornice, prisotnost v medijih ter preventivne akcije za skladnost (angl. *privacy sweep*). Informacijski pooblaščenec redno posodablja svojo spletno stran, na kateri je objavljen bogat nabor uporabnih gradiv, prisoten je tudi na družabnih omrežjih Facebook in LinkedIn, kjer predvsem objavlja povezave na pomembne novosti na področju varovanja zasebnosti. Sektor za skladnost prav tako podaja mnenja na prejete ocene učinkov glede varstva osebnih podatkov in pokriva področji kodeksov ravnanja ter (bodoče) certifikacije.

Informacijski pooblaščenec je v letu 2019 izvajal projekt ozaveščanja RAPiD.Si, za katerega je pridobil evropska sredstva (več o tem v poglavjih 1.3 in 3.5.7), v letu 2020 pa bo začel izvajati nov projekt iDECIDE.

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

3.5.1 OBVEZNOSTI UPRAVLJAVCEV

V sklop mehanizmov za skladnost in upoštevanje načela odgovornosti sodijo naslednji mehanizmi, ki jih 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

Leta 2019 je Informacijski pooblaščenec zaznal splošni trend znatnega povečanja sklepanja pogodb o pogodbeni obdelavi osebnih podatkov med zavezanci. Tudi vprašanj s tega področja je bilo neprimerljivo več. Število mnenj v zvezi s pogodbeno obdelavo, ki jih je Informacijski pooblaščenec objavil na svoji spletni strani, se je tako od leta 2018 skoraj potrojilo (število mnenj iz rubrike »pogodbena obdelava« po letih: 2016: 8, 2017: 11, 2018: 17, **2019: 47**). Navedeno torej očitno kaže na večje zavedanje zavezancev o pomenu obveznosti s področja varstva osebnih podatkov, ki ga je prinesla Splošna uredba (obveznost ureditve razmerja pogodbene obdelave je namreč obstajala že po ZVOP-1).

Pri uporabi nove zakonodaje nastajajo tudi nova pravna vprašanja glede ustreznosti ureditve konkretnih razmerij – zlasti ali gre za razmerje pogodbene obdelave v smislu člena 28 Splošne uredbe oz. za razmerje skupnih upravljavcev v smislu člena 26 Splošne uredbe, ki je nov institut, ki ga je uvedla Splošna uredba. Na tem področju se je pokazala potreba po bolj koherentnem pristopu k izpolnjevanju obveznosti po Splošni uredbi za državne organe in druge javne institucije, ki so podprti z državno informacijsko infrastrukturo.

Največ vprašanj na tem področju je Informacijski pooblaščenec prejel s strani zasebnega sektorja; na to področje je usmeril mnoge preventivne aktivnosti – poleg rednega izdajanja mnenj in posodabljanja svojih smernic je v okviru projekta RAPiD.Si za srednja in mala podjetja dnevno izvajal brezplačno telefonsko svetovanje, izvedel več brezplačnih predavanj po vsej Sloveniji ter redno vsebinsko posodabljal pojasnila na spletnih straneh upravljavec.si in ip-rs.si.

Informacijski pooblaščenec je leta 2019 pristopil tudi k pripravi standardnih pogodbenih določil, ki bodo v veliko pomoč zavezancem za ureditev njihovih pogodbenih razmerij. Standardna pogodbena določila bodo v skladu s predpisanim postopkom predvidoma potrjena s strani Evropskega odbora za varstvo osebnih podatkov v letu 2020. Pričakujemo, da bo Informacijski pooblaščenec med prvimi nadzornimi organi v EU, ki bodo svoja standardna pogodbena določila predložili v potrditev pristojni evropski instituciji.

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 njeno 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.

V preventivni aktivnosti za skladnost (ang. privacy sweep) je Informacijski pooblaščenec 130 največjih delodajalcev v državi pozval k evidentiranju dejavnosti obdelav osebnih podatkov, ki se zbirajo ob uporabi službenih sredstev zaposlenih, kot je uporaba interneta, e-pošte, tiskalnikov in drugih delovnih sredstev. Med naslovniki je bilo 40 delodajalcev iz javnega in 90 iz zasebnega sektorja, ki so skupaj zaposlovali približno 146.000 oseb. Na poziv je odgovorilo 67 zavezancev (odziv ni bil obvezen), ki so skupaj zaposlovali približno 84.000 oseb. Dobra polovica prejemnikov se je odzvala in velik delež teh je tudi podal pojasnila o izvedenih ukrepih, zato ocenjujemo, da je bila preventivna aktivnost na tem področju uspešna. Velja izpostaviti, da sta dva zavezanca izrecno pohvalila tovrsten pristop k zagotavljanju skladnosti, saj naj bi bilo s preventivnimi pozivi in usmeritvami mogoče doseči izboljšave organsko namesto prisilno, z grožnjo sankcij.

Informacijski pooblaščenec je preventivno pozval k skladnosti tudi 40 spletnih trgovcev. Poziv se je v delu nanašal tudi na izpolnjevanje obveznosti po členu 30 Splošne uredbe, zlasti glede evidentiranj osebnih podatkov, ki nastajajo v zvezi z uporabniki njihovih spletnih mest. Odzvalo se je 21 zavezancev, od katerih so nekateri posredovali obsežna in konkretna pojasnila. Informacijski pooblaščenec ocenjuje, da je bila aktivnost uspešna, konkretne ugotovitve pa bodo narekovale načrtovanje inšpekcijskih aktivnosti v prihodnosti.

Ob izvedenih preventivnih aktivnostih so v pomoč zavezancem na spletni strani objavljena pojasnila, vključno

z dvema vzorcema evidenc dejavnosti obdelave (obrazec za upravljavce in obrazec za obdelovalce), s katerim lahko zavezanci enostavno in učinkovito popišejo svoje zbirke.

3.5.4 OCENE UČINKOV NA VARSTVO OSEBNIH PODATKOV

Ocene učinkov na varstvo osebnih podatkov predstavljajo eno ključnih orodij načela odgovornosti, katerih namen je pravočasna identifikacija in obvladovanje tveganj v povezavi z varstvom osebnih podatkov. Ocene učinkov so še zlasti pomembne takrat, kadar gre za nove projekte obdelave osebnih podatkov, ki predvidevajo množično obdelavo osebnih podatkov, še posebej kadar gre za uporabo modernih tehnologij, bolj ranljive skupine posameznikov in za obdelavo posebnih vrst osebnih podatkov. Klasičen primer projekta oz. sistema, kjer je tovrstna ocena učinkov ključna, je sistem elektronskih bolniških listov (eBOL), v katerem se obdelujejo podatki o zdravstvenem stanju, zdravniki pa vsako leto izdajo več kot milijon in pol bolniških listov.

V kolikor zavezanec ocenjuje, da obstajajo tveganja, ki niso obvladovana, se lahko po členu 36 Splošne uredbe obrne na Informacijskega pooblaščenca po mnenje na izdelano oceno učinka. Informacijski pooblaščenec oceno učinka najprej pregleda s formalnega vidika, tj. ali ustreza smernicam glede predvidene vsebine, nato pa oceno učinka še vsebinsko pregleda in izpostavi morebitne pomanjkljivosti ter poda priporočila. Leta 2019 je Informacijski pooblaščenec dopolnil smernice o ocenah učinka , in sicer je dodal prilogo 3 – seznam vrst dejanj obdelave, za katera velja zahteva po oceni učinka, ter prilogo 4 – seznam vrst dejanj obdelave, za katera velja zahteva po oceni učinka pri čezmejnih zadevah in ocena tveganja po izvedenih ukrepih. Glede na odzive zavezancev je tudi dopolnil smernice v delu, ki se nanaša na obravnavo tveganj, in sicer z dodatnim elementom, ki se nanaša na raven tveganja po izvedenih ukrepih.

Leta 2019 je Informacijski pooblaščenec v postopku predhodnega posvetovanja izdal mnenja o naslednjih ocenah učinkov:

- Mnenje glede ocene učinkov na varstvo osebnih podatkov v zvezi z uporabo sistema »Potrdila o upravičeni zadržanosti od dela v elektronski obliki« (eBOL),
- Mnenje glede ocene učinkov na varstvo osebnih podatkov v zvezi s predlagano spremembo Zakona o centralnem kreditnem registru (ZCKR),
- Mnenje glede ocene učinkov na varstvo osebnih podatkov pri uvajanju sistema izposoje električnih vozil,
- Mnenje glede ocene učinka na varstvo podatkov v zvezi z vzpostavitvijo aplikativno podprtega nadzora nad izvajanjem lastnih transakcij zaposlenih v virnih aplikacijah,
- Mnenje glede ocene učinka na varstvo podatkov glede pridobivanja podatkov po Stanovanjskem zakoniku,
- Mnenje glede ocene učinka v zvezi z varstvom osebnih podatkov pri uporabi podatkovnega vira ISPAP za izvajanje projekta »Skrinja 2.0 – vzpostavitev sistema poslovne analitike v državni upravi«,
- Mnenje glede ocene učinka v povezavi s predlagano spremembo Zakona o integriteti in preprečevanju korupcije (ZIntPK).

Informacijski pooblaščenec ugotavlja, da se znanje in kakovost izdelanih ocen učinkov izboljšujeta, še vedno pa zavezanci premalo pozornosti posvečajo tveganjem v povezavi z uveljavljanjem pravic posameznika. Informacijski pooblaščenec pričakuje, da se bo znanje za kakovostno izdelavo ocen učinka s časom povečevalo, s tem pa se bo bistveno zmanjšalo tveganje že pred uvedbo projektov obdelave osebnih podatkov.

3.5.5 POOBLAŠČENE OSEBE ZA VARSTVO PODATKOV

Določitev pooblaščenih oseb za varstvo osebnih podatkov (angl. Data Protection Officer; DPO) je eden ključnih mehanizmov v sklopu odgovornosti, ki jih je prinesla Splošna uredba. Pooblaščena oseba naj bi izvajala svetovalne in nadzorne naloge na področju varstva osebnih podatkov in naj bi delovala kot notranji revizor za varstvo osebnih podatkov, ki poleg nadzora tudi svetuje upravljavcem in obdelovalcem o njihovih obveznostih, izobražuje in ozavešča zaposlene. Informacijski pooblaščenec ugotavlja, da marsikje prihaja do nerazumevanja vloge pooblaščenih oseb, ki niso odgovorne za zagotovitev skladnosti z zakonodajo, temveč so odgovorne za nadzor, svetovanje in izobraževanje.

Do konca leta 2019 je pooblaščeno osebo prijavilo 2169 zavezancev. Pooblaščena oseba Informacijskega pooblaščenca je dostopna prek namenskega elektronskega predala dpo@ip-rs.si.

Informacijski pooblaščenec je konec leta 2019 z namenom pridobitve boljših informacij o položaju in praksi pooblaščenih oseb za varstvo podatkov izvedel anketo med (notranjimi) pooblaščenimi osebami za varstvo podatkov v javnem sektorju. Izmed okvirno 500 imenovanih oseb se jih je na anketo odzvalo točno 100. Anketa je bila uspešno izvedena, njene ključne ugotovitve pa so naslednje:

- Povprečni delež časa, ki ga pooblaščene osebe namenijo oz. ga imajo na voljo za opravljanje svojih nalog, znaša 13 % delovnega časa.
- Med nalogami, ki ne sodijo med naloge pooblaščenih oseb, so predvsem priprava obrazcev, priprava evidenc dejavnosti obdelave ter pisanje pravilnikov in internih aktov.
- Anketiranci so (na lestvici od 1 do 5) dobro ocenili predvsem neposreden dostop do vodstva (ocena 4,59), zaupanje in podporo vodstva (4,2) ter vedenje zaposlenih o tem, kdo je pooblaščena oseba (4,19).
- Nekoliko previsoko oceno ima trditev, da so pooblaščene osebe »odgovorne« za uskladitev z varstvom osebnih podatkov (ocena 3,5), pooblaščene osebe pa so tudi izpostavile pomanjkanje časa za opravljanje svojih nalog (ocena 2,79).
- Glede ključnih dejavnikov uspeha pooblaščenih oseb so anketiranci kot najpomembnejše izpostavili podporo vodstva (4,64), zaupanje vodstva (4,61) ter pravočasno vključenost v procese obdelav osebnih podatkov (4,54).

Anketiranci so med drugim izpostavili naslednje:

- Številne dojemajo kot odgovorne za uskladitev s Splošno uredbo. Koristno bi bilo več povezovanja s kolegi.
- Zelo pomembno bo dvigniti zavest o varstvu osebnih podatkov med državljani, saj je ta po njihovem mnenju trenutno prenizka.
- Področje delovanja je preveč prepuščeno delovanju posameznega organa, poleg tega je to področje preširoko in prezahtevno za kakovostno delo, če ima pooblaščena oseba poleg tega že nalog za 8-urni delovnik.
- Glede pooblaščenih oseb v javnem sektorju je treba poudariti, da se pojavlja problem neupoštevanja položaja pooblaščenih oseb in tudi konflikt interesov.
- Naloge pooblaščene osebe se naloži nekomu, ki dobro/vestno opravlja svoje delo, zato se mu doda še te naloge. Pričakuje se, da bo pooblaščena oseba naredila vse potrebno in da bo odgovarjala za nepravilnosti; nerazumevanje pojma pooblaščena/odgovorna oseba.

Pooblaščene osebe na neki način predstavljajo podaljšano roko Informacijskega pooblaščenca, zato jim bo ta v letu 2020 namenil več pozornosti, predvsem bo spodbujal in omogočal njihovo medsebojno povezovanje, izmenjave izkušenj in prakse z upoštevanjem sektorske specifike.

3.5.6 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 upravljavcev ali obdelovalcev, lahko pripravijo kodekse ravnanja oz. takšne kodekse spremenijo ali razširijo z namenom podrobneje obrazložiti uporabo Splošne uredbe (npr. glede zbiranja osebnih podatkov, ustreznih načinov informiranja in pridobivanja privolitve). Združenja, ki nameravajo pripraviti kodeks ravnanja oz. spremeniti ali razširiti veljavni kodeks, Informacijskemu pooblaščencu predložijo osnutek kodeksa, spremembo ali razširitev, Informacijski pooblaščenec pa poda mnenje, ali je oddani osnutek skladen s Splošno uredbo. Informacijski pooblaščenec osnutek potrdi, če oceni, da zagotavlja zadostne in ustrezne zaščitne ukrepe.

Leta 2019 je Informacijski pooblaščenec prejel samo en osnutek kodeksa, ki pa ga v mnenje ni predložil ustrezen subjekt, zato ga ni obravnaval. 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 teles, ki predstavljajo vrste upravljavcev ali obdelovalcev, kot takrat, kadar je odvisno od angažiranosti posameznih članov oz. članic, zato Informacijski pooblaščenec upa, da bodo zavezanci v bodoče prepoznali koristi kodeksov.

Splošna uredba prinaša tudi možnost certificiranja, ki pa bo predhodno terjala razvoj ustreznih sistemov za akreditacijo in certificiranje; aktivnosti z zvezi s slednjimi trenutno potekajo na evropskem nivoju. 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 največ treh let z možnostjo podaljšanja.

3.5.7 AKTIVNOSTI IZOBRAŽEVANJA IN OZAVEŠČANJA

Tudi leta 2019 je bil Informacijski pooblaščenec zelo aktiven na področju izobraževanja in ozaveščanja, in sicer prek svojega spletnega mesta (www.ip-rs.si) in prek različnih gradiv, organiziral je različne dogodke in brezplačna predavanja, prisoten je bil na družbenih omrežjih, sodeloval pa je tudi z drugimi organizacijami in v različnih projektih.

Informacijski pooblaščenec je leta 2019 izdal več različnih gradiv. Poleg mnenj med najpomembnejše sodijo **smernice**. Izdane so bile naslednje:

- Smernice o varstvu osebnih podatkov v delovnih razmerjih,
- Smernice o orodjih za zaščito zasebnosti na internetu,
- Smernice o uporabi GPS sledilnih naprav in varstvu osebnih podatkov.

Poleg smernic je Informacijski pooblaščenec v pomoč upravljavcem skladno s Splošno uredbo izdal priporočila glede urejanja skupnega upravljanja osebnih podatkov (člen 26 Splošne uredbe).

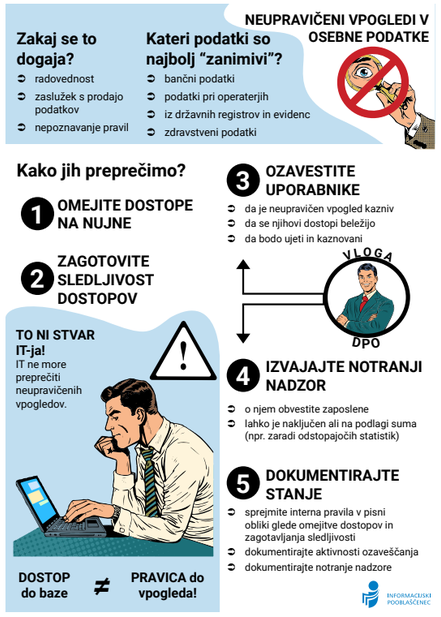
V pomoč zavezancem je Informacijski pooblaščenec pripravil tudi nova obrazca, in sicer:

- Vzorec zahteve za izvršitev pravice do prenosljivosti osebnih podatkov (člen 20 Splošne uredbe);
- Obrazec – Vloga za prenos osebnih podatkov v tretje države ali mednarodne organizacije.

Med izobraževalne aktivnosti Informacijskega pooblaščenca sodi tudi izdelava infografik, saj se je izkazalo, da je mogoče z njimi učinkovito in razumljivo vplivati na boljše splošno razumevanje ključnih elementov zakonodaje o varstvu podatkov. V letu 2019 je tako Informacijski pooblaščenec pripravil naslednje infografike:

- Prijava kršitve varnosti;
- Neupravičeni vpogledi v osebne podatke;
- Infografika o pogodbeni obdelavi;
- Prenos osebnih podatkov po Splošni uredbi v tretje države in mednarodne organizacije v dveh korakih;
- Roki hrambe dokumentov neizbranih kandidatov v zaposlitvenih postopkih;
- Statistika prejetih kršitev varnosti v letu 2018.

Infografika "Neupravičeni vpogledi v osebne podatke".



Informacijski pooblaščenec je ob **evropskem dnevu varstva osebnih podatkov** (28. januar) organiziral poseben dogodek na temo novosti Splošne uredbe, ki je potekal kot okrogla miza. Skupaj z zanimivimi gosti je predstavil izkušnje posameznikov in podjetij z novo uredbo ter osvetlil dobre in slabe prakse pri zagotavljanju ustrezne obveščenosti posameznika. Preveril je, ali Splošna uredba tudi v praksi pomeni ustrezno varstvo posameznika in s kakšnimi izzivi se soočajo podjetja v Sloveniji pol leta po začetku njene uporabe.

Okrogla miza ob Dnevu varstva osebnih podatkov 2019.

Informacijski pooblaščenec je že tradicionalno podelil priznanje **ambasador zasebnosti**, ki ga je za leto 2019 prejela Zveza potrošnikov Slovenije (ZPS), ker vztrajno in zavzeto brani interese potrošnikov na vseh področjih, pomembno delo pa opravlja tudi na področju varstva osebnih podatkov potrošnikov. Prav tako je tradicionalno podelil **priznanja prejemnikom mednarodnega certifikata za informacijsko varnost** po standardu ISO/EIC 27001:2013.

Ob obletnici začetka uporabe Splošne uredbe je Informacijski pooblaščenec 24. 5. 2019 organiziral **tiskovno konferenco**, na kateri je medijem in splošni javnosti predstavil prerez svojega dela in stanje na področju varstva osebnih podatkov, pojasnil, kako so podjetja in inštitucije implementirale Splošno uredbo, kaj je Splošna uredba prinesla posameznikom ter katere aktivnosti je na področju nadzora, skladnosti in preventive ter mednarodnega sodelovanja v letu dni uporabe Splošne uredbe izvajal sam.

Informacijski pooblaščenec je aktivno sodeloval tudi z drugimi deležniki. V okviru priprav na volitve v Evropski parlament je sodeloval pri izdelavi strokovnih gradiv, in sicer Vodnika za organizatorje volilnih kampanj, ki ga je izdalo Ministrstvo za javno upravo. Prispeval je uvodni nagovor ter **posebno poglavje o pravilih in pasteh pri obdelavi osebnih podatkov v volilnih kampanjah**. Gre za pomemben vidik volilnih dejavnosti in političnih kampanj, saj je spoštovanje pravil o varstvu podatkov ključno za zaščito demokracije. Obenem je to tudi sredstvo za ohranjanje zaupanja državljanov in integritete volitev.

Informacijski pooblaščenec je leta 2019 izvedel **102 brezplačni predavanji** za različne zbornice, združenja in druge javnosti po različnih dejavnostih v javnem in zasebnem sektorju.

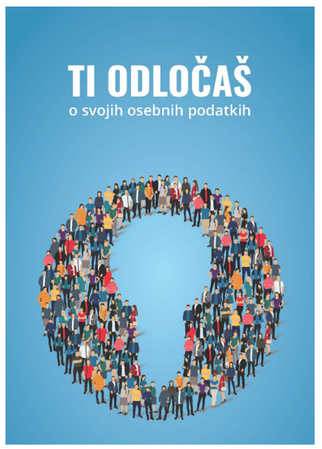
Informacijski pooblaščenec je uspešno nadaljeval aktivnosti v okviru projekta **RAPiD.Si**, ki je namenjen ozaveščanju in opolnomočenju posameznikov ter malih in srednje velikih podjetij o varstvu osebnih podatkov. V letu 2019 je:

- v osmih slovenskih mestih izvedel 15 brezplačnih predavanj, ki jih je skupaj obiskalo 614 udeležencev,
- odgovoril je na 601 klic na telefonsko številko 080 2900 (brezplačna svetovalna linija je bila odprta do konca oktobra 2019) in pri tem odgovoril na 1010 vprašanj,
- v sodelovanju z ZPS pripravil pet strokovnih člankov v reviji Obrtnik, namenjenih podjetjem, in šest člankov, namenjenih posameznikom,
- vsak mesec razposlal elektronski novičnik z aktualnimi vsebinami,
- redno tedensko objavljal zanimivosti s področja varstva osebnih podatkov na družabnih omrežjih Facebook in LinkedIn,
- dodajal vsebine na dve spletni strani, pripravljeni v okviru projekta: tiodlocas.si (namenjeni predvsem posameznikom) in upravljavec.si (namenjeni predvsem podjetjem),
- pripravil dve animaciji za spletno stran za posameznike tiodlocas.si.

Primer objave na LinkedIn poslovni strani Informacijskega pooblaščenca.

V okviru projekta RAPiD.Si je Informacijski pooblaščenec nadgradil aktivnosti s sodelovanjem z ZPS: v reviji ZPStest je bil prisoten z občasno rubriko, skupaj z ZPS pa je izdal **priročnik o varstvu osebnih podatkov potrošnikov z naslovom Ti odločaš**. V priročniku, ki je izšel v nakladi 5000 izvodov, prosto pa je dostopen tudi na spletu, je razumljivo pojasnjeno, na kakšen način mora upravljavec posameznika obvestiti o obdelavi podatkov, o tem, ali bo podatke posredoval tretjim osebam, koliko časa bo podatke hranil, predvsem pa o tem, kakšne so pravice posameznika in kako jih lahko uveljavlja ter kam se lahko obrne v primeru kršitev.

Brošura "Ti odločaš o svojih osebnih podatkih".



3.5.8 PREVENTIVNE AKTIVNOSTI ZA SKLADNOST

Informacijski pooblaščenec je leta 2019 okrepljeno izvajal preventivne aktivnosti za skladnost (ang. *privacy sweep*). S preventivnimi aktivnostmi želi doseči, da zavezanci brez uvajanja stroškovno in časovno zahtevnih inšpekcijskih postopkov tako za zavezance kot za nadzorni organ samostojno ocenijo lastno stanje na področju varstva osebnih podatkov in zadostijo zahtevam zakonodaje, v pomoč pa imajo s strani nadzornega organa na voljo ustrezne informacije in orodja. Povratne informacije zavezancev se upoštevajo pri strateškem načrtovanju inšpekcijskih in drugih aktivnosti Informacijskega pooblaščenca v prihodnjem letu.

Leta 2019 je Informacijski pooblaščenec izvedel naslednje preventivne aktivnosti za skladnost:

Zavezanci	Vsebina	Št. Prejemnikov
Operaterji brezpilotnikov	Operaterje brezpilotnikov (dronov) je pozval k izpolnitvi dolžnosti glede izdelave ocene učinkov, zavezanci so v pomoč prejeli povezave do vzorca ocene in ustreznih navodil. Več kot 90 % zavezancev je nato izpolnilo svoje obveznosti in uvedba prisilnih inšpekcijskih postopkov ni bila potrebna.	77
Spletne trgovine	Spletne trgovine je pozval k ureditvi obveščanja posameznika po členu 13 in 14 Splošne uredbe pri izvajanju spletnih nakupov. Zavezanci so prejeli povezave do obrazcev, navodil in pojasnil.	40
Veliki delodajalci	Največje delodajalce v državi je pozval k ureditvi evidence dejavnosti (člen 30 Splošne uredbe) glede osebnih podatkov zaposlenih, ki se zbirajo ob uporabi službenih delovnih sredstev. Ti podatki so namreč pogosto spregledani, posledično pa prihaja do njihove nenamenske uporabe in zlorab. Zavezanci so prejeli povezave do obrazcev, navodil in pojasnil.	130 (40 delodajalcev iz javnega in 90 iz zasebnega sektorja, ki imajo skupaj 146.000 zaposlenih
Posredovanje osebnih podatkov po telefonu	Na podlagi ugotovitev, da nekateri zavezanci posameznikom po telefonu razkrivajo preveč informacij, pri čemer jih ustrezno ne identificirajo, je relevantna združenja (npr. telekomunikacijska podjetja, dobavitelje energentov in upravnike, zdravstvene ustanove) pozval, da za identifikacijo posameznika prek telefona zahtevajo vsaj dva različna identifikatorja, s katerima po vsej verjetnosti razpolaga samo zadevni posameznik. Združenja so opozorilo in napotke posredovala svojim članom, nekatera so jih tudi objavila v svojih glasilih.	38 združenj

Na podlagi preliminarnih ugotovitev Informacijski pooblaščenec ocenjuje, da tovrstne preventivne aktivnosti **postopkovno in stroškovno učinkovito prispevajo k zagotavljanju višje skladnosti, saj imajo velik doseg in pomembno ozaveščevalno komponento**. Nekateri zavezanci so tovrsten pristop Informacijskega pooblaščenca k zagotavljanju skladnosti izrecno pohvalili, saj naj bi bilo s proaktivnimi pozivi in usmeritvami mogoče doseči izboljšave organsko namesto prisilno, z grožnjo sankcij. Preventivne aktivnosti zagotavljajo tudi pomembne povratne informacije sistemskega značaja, ki so koristne pri načrtovanju nadaljnjih aktivnosti Informacijskega pooblaščenca. Zlasti učinkovito se kaže tovrstno sodelovanje z zbornicami, združenji in podobnimi branžnimi povezavami.

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 aktivno deloval kot član Evropskega odbora za varstvo podatkov (EOVP), ki je neodvisni evropski organ za zagotavljanje dosledne uporabe pravil o varstvu podatkov v EU in za spodbujanje sodelovanja med organi EU za varstvo podatkov; deluje od maja 2018. 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 deluje v skladu s svojim pravilnikom in vodilnimi načeli.

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 se zagotovi dosledno uporabo Splošne uredbe;
- sprejemanje splošnih smernic za podrobnejšo opredelitev pogojev evropske zakonodaje o varstvu podatkov, s čimer svojim deležnikom zagotavlja dosledno razlago 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 s kodeksom ravnanja s čezmejnim vplivom ter v določenih primerih glede odobritve meril za pooblastitev organa za spremljanje skladnosti s kodeksom ravnanja; v zvezi z določitvijo standardnih določil o varstvu podatkov glede prenosa podatkov v tretje države; v zvezi z odobritvijo pogodbenih določil ali zavezujočih poslovnih pravil;
- reševanja sporov med nadzornimi organi (po členu 65 Splošne uredbe), npr. glede nasprotujočih si stališč o vsebini odločitve v čezmejnih primerih; o tem, kateri nadzorni organ je vodilni v določenem čezmejnem postopku; 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 področje svojega 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 2019 so se nadzorni organi v okviru odbora med drugim ukvarjali z vprašanji enotnega tolmačenja Splošne uredbe glede zakonite obdelave osebnih podatkov v okviru postopkov volitev, izvajanja pravice do pozabe v primerih spletnih brskalnikov, obdelave osebnih podatkov v postopkih kliničnega testiranja in postopkov čezmejnega sodelovanja, izvedena je bila tretja revizija delovanja mehanizma Ščit zasebnosti v zvezi z zagotavljanjem varstva podatkov po prenosu v Združene države Amerike, obravnavana so bila vprašanja in izzivi glede nadgrajevanja informacijskih sistemov v EU in digitalne infrastrukture sistemov eZdravja, obravnavana pa so bila tudi vprašanja razmerja med Splošno uredbo in direktivo o e-zasebnosti ter vplivi postopka izstopa Združenega kraljestva iz EU (Brexit) na varstvo podatkov v EU tako z vidika nadzornih postopkov kot tudi posledic za posameznike in podjetja.

Leta 2019 je odbor sprejel naslednje smernice:

- Smernice št. 5/2019 glede tolmačenja izvajanja pravice do pozabe v primerih spletnih brskalnikov;
- Smernice št. 4/2019 o členu 25 Splošne uredbe glede vgrajenega in privzetega varstva podatkov;
- Smernice št. 3/2019 o obdelavi osebnih podatkov v okviru sistemov videonadzora;
- Smernice št. 2/2019 glede tolmačenja pravne podlage po točki (b) člena 6(1) Splošne uredbe v zvezi s pogodbami o zagotavljanju spletnih storitev potrošnikom;
- Smernice št. 1/2019 o kodeksih ravnanja in organih za spremljanje na podlagi Uredbe (EU) 2016/679.

Poleg tega je odbor leta 2019 sprejel 17 mnenj, in sicer: osem mnenj v zvezi s seznami 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, dve mnenji glede osnutkov zahtev posameznih nacionalnih nadzornih organov držav članic za akreditacijo organa za spremljanje kodeksa ravnanja v skladu s členom 41 Splošne uredbe ter sedem mnenj na nekatere druge zgoraj omenjene teme.

Letno poročilo odbora je dostopno na https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_annual_report_2019_en.pdf

3.6.2 SODELOVANJE V DRUGIH NADZORNIH TELESIH EVROPSKE UNIJE

Informacijski pooblaščenec je leta 2019 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 Eurodacom.

V okviru nadzora nad obdelavo osebnih podatkov v okviru Europola in VIS sta bili sprejeti poročili o aktivnostih za obdobje 2017–2018. Europolov odbor za sodelovanje je posodobil seznam pristojnih organov držav članic za zagotavljanje pravice posameznikov do dostopa do osebnih podatkov ter pripravil prenovljen vodič za posameznike glede izvrševanja pravic dostopa, popravka, izbrisa in omejitve obdelave osebnih podatkov, ki se vodijo v okviru Europola. V okviru nadzora nad obdelavo osebnih podatkov v SIS II je bil sprejet in izveden vprašalnik v zvezi z razpisi ukrepov za osebe in stvari zaradi prikrite kontrole ali namenske kontrole na podlagi 36. člena Sklepa o vzpostavitvi, delovanju in uporabi druge generacije schengenskega informacijskega sistema (SIS II). V okviru nadzora nad obdelavo osebnih podatkov v okviru Eurodaca je bilo sprejeto poročilo o izvrševanju pravic posameznikov, na katere se nanašajo podatki v sistemu Eurodac, ter vodič, katerega namen je pomagati uradnim osebam in organom pri obveščanju prosilcev za azil in migrantov o obdelavi njihovih prstnih odtisov v sistemu Eurodac v razumljivi in dostopni obliki. V okviru nadzora nad VIS je bilo sprejeto poročilo o izvajanju usposabljanj s področja varstva podatkov.

Leta 2019 so bile sprejete tudi spremembe postopkovnih pravil EOVP, na podlagi katerih je bilo ustanovljeno novo nadzorno telo – CSC (Skupina za koordiniran nadzor nad obdelavo osebnih podatkov v okviru velikih informacijskih sistemov EU). Sčasoma se bo nadzor posameznih velikih informacijskih sistemov EU preselil pod okvir CSC.

Maja 2019 je bila v Republiki Sloveniji uspešno izvedena evalvacija izvajanja schengenskega pravnega reda z vidika varstva osebnih podatkov, pri kateri je aktivno sodeloval tudi Informacijski pooblaščenec.

3.6.3 SODELOVANJE V DRUGIH MEDNARODNIH TELESIH

POSVETOVALNI ODBOR T-PD

V okviru Sveta Evrope je predstavnik Informacijskega pooblaščenca tudi leta 2019 sodeloval v Posvetovalnem odboru, ustanovljenem s Konvencijo Sveta Evrope o varstvu posameznikov glede na avtomatsko obdelavo osebnih podatkov (Konvencija št. 108), v Odboru T-PD. Odbor 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, poročila nadzornih organov za varstvo osebnih podatkov iz držav članic Sveta Evrope o novostih in dosežkih na tem področju ter še posebej informacije, podane s strani nadzornih organov ob dnevu varstva osebnih podatkov. Odbor je leta 2019 aktivno obravnaval aktualne teme, kot so prepoznava obrazov, profiliranje in varstvo osebnih podatkov otrok v izobraževalnih sistemih. Izdal je Poročilo o umetni inteligenci, Smernice o umetni inteligenci in varstvu osebnih podatkov ter Mnenje na osnutek priporočila o vplivu algoritemskih sistemov na človekove pravice. Odbor je izdal tudi Mnenje o osnutku drugega dodatnega protokola k Budimpeštanski konvenciji o kibernetski kriminaliteti glede neposrednega razkritja podatkov o naročnikih in izvajanja zahtev druge pogodbenice za pospešeno pridobivanje podatkov. Sodeloval je na delu konference »Octopus«, ki je namenjena obravnavi vprašanj s področja kibernetskega kriminala. Prvič je Odbor podelil nagrado »Stefano Rodotà«, in sicer za projekt, ki preučuje zasebnost in varstvo podatkov z vidika otrokovih pravic.

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

Informacijski pooblaščenec je tudi leta 2019 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.

Aprila 2019 je Informacijski pooblaščenec prvič **gostil zasedanje IWGDPT**, ki se ga je udeležilo 30 predstavnikov nadzornih organov iz EU in tretjih držav.

Delovna skupina je na zasedanjih na Bledu in v Bruslju sprejela nove delovne dokumente, ki so pomemben znak konsenza glede določenih vprašanj varstva osebnih podatkov na mednarodni ravni, predvsem glede izzivov, ki jih prinašajo nove tehnologije.

Na zasedanju na Bledu je bil sprejet dokument o varstvu osebnih podatkov pri uporabi pametnih igrač; glavni poročevalec je bil Informacijski pooblaščenec. Dokument obravnava tveganja, ki nastajajo pri uporabi t. i. pametnih naprav, kot so govoreče igrače, pametne ure in druge naprave, ki so običajno povezane z internetom in ki ob nespametni uporabi in pogosto nejasnih informacijah o zajemu in obdelavi podatkov lahko predstavljajo tveganje za zasebnost tako otrok kot staršev in učiteljev (https://www.datenschutz-berlin.de /fileadmin/user_upload/pdf/publikationen/working-paper/2019/2019-IWGDPT-Working_Paper_Smart_Devices.pdf).

Varstvo osebnih podatkov otrok naslavlja tudi drugi dokument, ki je bil sprejet na Bledu, in sicer orisuje tveganja in podaja priporočila za varno uporabo spletnih storitev, ki ciljajo na otroke. Dokument zlasti poudarja pomen natančnih informacij, pridobitve ustreznih soglasij staršev ter vprašanja verifikacije starosti otrok na spletu (https://www.datenschutz-berlin.de/fileadmin/user_upload/pdf/publikationen/working-paper/2019/2019-IWGDPT-Working_Paper_Online_Services_for_Children.pdf).

Na zasedanju v Bruslju je bilo obravnavano glasovno upravljane naprav, veriženje podatkovnih blokov (angl. *blockchain*) ter vloga pravice do prenosljivosti osebnih podatkov. Sprejeti dokumenti bodo po pregledu javno objavljeni na spletni strani delovne skupine (https://www.datenschutz-berlin.de/working-paper.html).

Na zasedanju v Bruslju je bilo izglasovano tudi novo ime skupine. Namesto izraza »telekomunikacije«, ki je vsebinsko zastarel in preozek glede na dejansko delovno področje delovne skupine, bo v uporabi izraz »tehnologije«. Novo uradno ime skupine je tako International Working Group on Data Protection in Technology, kratica pa ostaja ista (IWGDPT).

SVETOVNA SKUPŠČINA ZA ZASEBNOST

Svetovna skupščina za zasebnost (prej imenovana 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 ter povezuje prizadevanja več kot 130 nadzornih organov za varstvo zasebnosti in podatkov z vsega sveta. Leta 2019 je bilo soglasno izbrano novo ime tega mednarodnega združenja glede na dejansko svetovno zastopanost in glede na zastavljeni cilj: doseči večjo prepoznavnost. V skladu s tem so bile sprejete strateške usmeritve za naslednje triletno obdobje, ki temeljijo na poudarjenih prizadevanjih za vzpostavitev mednarodnega okvira standardov varstva zasebnosti v svetu množične uporabe in razširjenosti modernih tehnologij, krepitvi različnih oblik sodelovanja pri izvajanju nadzorov, nadaljuje pa se tudi tematsko delo na področjih krepitve varstva podatkov v javnem sektorju, na področju digitalnega gospodarstva, v demokratičnih in političnih procesih ter v povezavi s širšim kontekstom zagotavljanja vseh temeljnih človekovih pravic. Med pomembnejšimi resolucijami, sprejetimi na zadnji konferenci v Tirani leta 2019, so resolucija o zagotavljanju pravice do varstva podatkov kot temeljnega predpogoja tudi za uveljavljanje drugih človekovih pravic ter resolucija o krepitvi sodelovanja med nadzornimi organi za varstvo podatkov in organi za varstvo potrošnikov za boljšo zaščito državljanov in potrošnikov v digitalnem gospodarstvu ter o promociji učinkovitih praktičnih čezmejnih mehanizmov sodelovanja nadzornih organov. Pomemben cilj konference je okrepiti sodelovanje nadzornih organov ter s tem dvigniti raven varstva osebnih podatkov v svetu. Osrednje razprave na konferenci leta 2019 so bile posvečene izzivom učinkovitega uveljavljanja varstva zasebnosti in sodelovanja

med nadzornimi organi za varstvo zasebnosti po svetu pri uveljavljanju varstva osebnih podatkov v svetu digitalnega gospodarstva.

INITIATIVE 20i7

Na tretjem srečanju Initiative 20i7, ki je maja 2019 potekalo v Budvi, so predstojniki nadzornih organov za varstvo osebnih podatkov iz Hrvaške, Srbije, Bosne in Hercegovine, Črne gore, Kosova, Makedonije in Slovenije izmenjali izkušnje in prakso pri izvajanju oz. približevanju standardom, ki jih je prinesla Splošna uredba.

Na zasedanju so nadzorni organi izdali tudi skupno izjavo za javnost, s katero so želeli opozoriti na počasno usklajevanje zakonodaje, saj večina držav še ni sprejela predpisov za implementacijo evropskega pravnega okvira (Splošne uredbe in Policijske direktive). Za vse države iz te regije je harmonizirana zakonodaja posebnega pomena za gopodarski razvoj, pravno varnost upravljavcev podatkov ter varovanje pravic in svoboščin posameznika, sprejeti zakoni pa ne smejo zniževati doseženega nivoja varstva posameznikov; posebej so pomembni natančno definirani postopki varovanja in uveljavljanja njihovih pravic (http://www.azlp.me/docs/naslovna/2019/Budva%2C%20maj%202019/Saop%C5%A1tenje%20ENG.docx).

Initiative 20i7 je nastala leta 2017 na pobudo Informacijskega pooblaščenca z namenom izmenjave prakse in znanj nadzornih organov za varstvo osebnih podatkov z območja nekdanje Jugoslavije, saj se ti soočajo s podobnimi strokovnimi vprašanji in izzivi. Informacijski pooblaščenec z zadovoljstvom ugotavlja, da je pobuda zaživela – leta 2020 bo potekalo že četrto srečanje pobude. Initiative 20i7 tako predstavlja primer dobre prakse čezmejnega sodelovanja, ki ga zlasti cenijo države na poti v EU, saj se soočajo s podobnimi težavami, kot sta se na tej poti srečali Slovenija in Hrvaška.

Srečanje pobude Intiative 20i7 v Budvi, 28.5.2019.

3.7 SPLOŠNA OCENA STANJA VARSTVA OSEBNIH PODATKOV

Delo Informacijskega pooblaščenca na področju varstva osebnih podatkov je leta 2019 v največji meri zaznamovala Splošna uredba, ki se je v vseh državah članicah EU začela neposredno uporabljati 25. maja 2018 in ki je naloge in pristojnosti Informacijskega pooblaščenca glede na ZVOP-1 še razširila. Zaradi potrebe po prilagoditvi področja obdelave osebnih podatkov se je precej povečal obseg aktivnosti tako pri upravljavcih osebnih podatkov kot pri Informacijskem pooblaščencu. Splošna uredba in Direktiva za organe kazenskega pregona terjata tudi sprejetje novega sistemskega Zakona o varstvu osebnih podatkov (ZVOP-2), s katerim bi se v Republiki Sloveniji v celoti zagotovilo njuno izvajanje. Republika Slovenija takšnega zakona leta 2019 še vedno ni sprejela. Rezultat tega je precej odprtih vprašanj, nejasnosti ter povsem praktičnih težav tako pri upravljavcih in obdelovalcih osebnih podatkov kot pri Informacijskem pooblaščencu.
Nesprejetje novega ZVOP-2 na samo izvajanje inšpekcijskega nadzora sicer ni bistveno vplivalo, je pa vplivalo na vodenje upravnih postopkov reševanja pritožb posameznikov v zvezi z uveljavljanjem njihovih pravic iz členov 13 do 22 Splošne uredbe, v katerih Informacijski pooblaščenec nastopa kot pritožbeni organ. Obseg pravic posameznika, na katerega se osebni podatki nanašajo, ter s tem povezane pristojnosti Informacijskega pooblaščenca kot pritožbenega organa so se glede na obstoječi ZVOP-1 občutno povečali, zaradi česar se je leta 2019 glede na leta pred tem občutno povečalo tudi število takšnih pritožb. Reševanje le-teh pa terja določitev posebnih pravil, s katerimi bi se rešila posamezna vprašanja upravnega postopka oz. bi se z njimi določil postopek njihovega reševanja. Nesprejetje novega zakona o varstvu osebnih podatkov (ZVOP-2) je zato povzročilo precej dilem, ki so se pojavile pri vodenju takšnih pritožbenih postopkov.

Še posebej negativno je nesprejetje ZVOP-2 vplivalo na vodenje prekrškovnih postopkov in izrekanje glob za ugotovljene kršitve, saj je lahko Informacijski pooblaščenec zaradi odsotnosti ZVOP-2 v obravnavanem obdobju v primeru ugotovljenih kršitev določb Splošne uredbe ali določb ZVOP-1 zavezancem v postopku inšpekcijskega nadzora odredil le odpravo ugotovljenih nepravilnosti, vzpostavitev zakonitega stanja ter prepovedal nezakonito obdelavo osebnih podatkov, postopek za prekrške pa je lahko uvedel le v primeru, če je šlo za kršitev tistih členov ZVOP-1, ki še veljajo, ali v primeru kršitev s strani zavezancev po Direktivi za organe kazenskega pregona. Informacijski pooblaščenec torej zaradi odsotnosti ZVOP-2 ni mogel izrekati sankcij za tiste kršitve, ki so določene zgolj v členu 83 Splošne uredbe, lahko pa je v okviru prekrškovnih postopkov sankcioniral kršitev tistih določb še vedno veljavnega ZVOP-1, ki niso v nasprotju s Splošno uredbo. Informacijski pooblaščenec je zato pristojno ministrstvo že večkrat opozoril na nujnost sprejetja novega zakona in ureditve in uskladitve prekrškovnih določb v ZVOP-2 z določbami Splošne uredbe. Usklajenost nacionalnih določb s Splošno uredbo je še posebej pomembna z vidika usklajevanja praks v državah članicah EU, v katerih se uporablja Splošna uredba. EOVP, katerega del je Informacijski pooblaščenec, namreč dela na oblikovanju mehanizma usklajevanja izrečenih glob, ki naj bi ga uporabljali vsi nadzorni organi in ki temelji na merilih za izrekanje glob na način in v višini, kot to določa člen 83 Splošne uredbe. Namen mehanizma je usklajevanje: izrečene globe glede podobnih prekrškov v podobnih okoliščinah naj se v različnih državah ne bi razlikovale, kar še zlasti velja v primerih čezmejnega sodelovanja pri inšpekcijskem nadzoru.

Število prijav, ki jih je leta 2019 prejel Informacijski pooblaščenec, se je glede na pretekla leta še nekoliko povečalo: Informacijski pooblaščenec je prejel 974 prijav oz. pobud za uvedbo inšpekcijskega postopka, kar je največ doslej.

Poleg zgoraj navedenih prijav je Informacijski pooblaščenec leta 2019 prejel in obravnaval še devet primerov nedovoljenega sporočanja ali druge nedovoljene obdelave osebnih podatkov o pacientih, ki so jih na podlagi 46. člena ZPacP poslali izvajalci zdravstvene dejavnosti, ter 137 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. 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 Informacijskemu pooblaščencu najpogosteje pošiljali zaradi izgube ali kraje nosilcev osebnih podatkov (npr. osebnih računalnikov in USB-ključkov), nepooblaščenega dostopanja do osebnih podatkov zaradi programske napake ali zlorabe pooblastil s strani zaposlenih, hekerskega napada na informacijski sistem, onemogočanja dostopa do podatkov zaradi kriptiranja z zlonamerno programsko kodo ter posredovanja osebnih podatkov nepooblaščenim ali napačnim osebam.

Informacijski pooblaščenec pri obravnavi prijav, ki jih je prejel s strani posameznikov, ugotavlja, da so bile prijave 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 pa je privolitev posameznika zgolj ena od šestih enakovrednih pravnih podlag, ki jih v zvezi z zakonitostjo obdelave osebnih podatkov določa člen 6 Splošne uredbe. Zaradi tega se je pri obravnavi prijav pogosto izkazalo, da so upravljavci pridobivali privolitve posameznikov tudi v primerih, ko je bila obdelava osebnih podatkov določena v zakonu ali potrebna za izvajanje pogodbe s posameznikom, ali pa je bil izpolnjen kakšen drug pogoj iz člena 6 Splošne uredbe in zaradi tega pridobivanje privolitve posameznika sploh ni bilo potrebno.

Do prijav in kršitev Splošne uredbe je pogosto prihajalo tudi zato, ker upravljavci posamezniku ob zbiranju

osebnih podatkov niso zagotovili ustreznih oz. popolnih informacij. Upravljavci so namreč dolžni sprejeti ustrezne ukrepe, s katerimi posamezniku, na katerega se nanašajo osebni podatki, ob zbiranju osebnih podatkov zahtevane informacije v zvezi z obdelavo osebnih podatkov zagotovijo v jedrnati, pregledni, razumljivi in lahko dostopni obliki ter v jasnem in preprostem jeziku. Vrste informacij, ki jih je treba zagotoviti posamezniku ob zbiranju njegovih osebnih podatkov, 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 tudi leta 2019 kljub ozaveščanju upravljavcev in kljub vzorcem takšnih obvestil, ki jih je Informacijski pooblaščenec pripravil in objavil na svoji spletni strani, še vedno spadajo med najpogosteje ugotovljene kršitve. Informacijski pooblaščenec v primeru ugotovljene kršitve določb členov 13 in 14 Splošne uredbe odredi odpravo ugotovljenih nepravilnosti, po uveljavitvi ZVOP-2 pa bo lahko za takšne kršitve izrekal tudi globe, določene v členu 83(4) Splošne uredbe.

Pri obravnavi prijav ter izvajanju preventivnih inšpekcijskih nadzorov, ki jih je Informacijski pooblaščenec leta 2019 izvajal 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, na katere se osebni podatki nanašajo, se ugotavlja, da so ugotovljene nepravilnosti ali pomanjkljivosti v veliki meri še vedno posledica nepoznavanja oz. nerazumevanja zakonodaje, kar pa gre pripisati tudi dejstvu, da ZVOP-2, ki bi jasneje določil posamezna pravila izvajanja Splošne uredbe, še vedno ni sprejet. Poleg nepoznavanja predpisov so ugotovljene kršitve pogosto posledica malomarnega ali neustreznega zagotavljanja varnosti osebnih podatkov ter namerne nezakonite obdelave osebnih podatkov s strani zaposlenih pri upravljavcih osebnih podatkov, ki se kaže zlasti z nezakonitimi vpogledi v zbirke osebnih podatkov, sporno obdelavo osebnih podatkov za namene neposrednega trženja ter izvajanjem videonadzora delovnih prostorov z namenom nadzora nad zaposlenimi.

Podobno kot v minulih letih je Informacijski pooblaščenec tudi leta 2019 vodil več inšpekcijskih in prekrškovnih postopkov zaradi nezakonitih vpogledov v zbirke osebnih podatkov s strani zaposlenih, ki so takšne vpoglede opravili bodisi zaradi radovednosti bodisi zaradi pridobivanja osebnih podatkov za lastne namene. Zaposleni so najpogosteje nezakonito vpogledovali v zbirke osebnih podatkov s področja notranjih zadev oz. policije ter v zbirke osebnih podatkov, ki jih vodijo zdravstvene institucije. Omenjene zbirke osebnih podatkov imajo zagotovljeno sledljivost obdelave osebnih podatkov, ki zagotavlja 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. Informacijski pooblaščenec je v primeru ugotovljenih kršitev vsem kršiteljem z odločbo o prekršku izrekel ustrezno sankcijo.

Informacijski pooblaščenec je v letu 2019 nadaljeval okrepljeno delovanje na področju skladnosti in preventive. Informacijski pooblaščenec ocenjuje, da se je poznavanje določb Splošne uredbe v letu 2019 izboljšalo in da se je med zavezanci izboljšalo razumevanje njenih ključnih konceptov, ostajajo pa številne pravne nejasnosti za upravljavce, ki so posledica tega, da Slovenija ni sprejela nacionalnega predpisa glede izvajanja Splošne uredbe in da določb Direktive za organe kazenskega pregona ni prenesla v slovenski pravni red. K izboljšavam je po oceni Informacijskega pooblaščenca pripomoglo tudi imenovanje pooblaščenih oseb za varstvo osebnih podatkov, ki jih je več kot 2000, saj med njihove naloge sodijo tudi naloge ozaveščanja, svetovanja in izobraževanja. Pooblaščene osebe za varstvo podatkov predstavljajo nekakšno podaljšano roko Informacijskega pooblaščenca, zato bo v prihodnosti treba več aktivnosti nameniti prav njim, saj se lahko z njihovo usposobljenostjo ozaveščevalni učinki multiplicirajo, s tem pa tudi skladnost zavezancev. Glede preostalih mehanizmov Splošne uredbe iz načela odgovornosti se izboljšuje znanje glede izvedb ocen učinkov na varstvo osebnih podatkov, ki so bistveni element preventivnega varstva osebnih podatkov, premalo pa je zavedanja o pomenu ocen učinkov kot ključnega elementa postopka priprav novih predpisov, ki predvidevajo resne posege v zasebnost posameznikov in/ali uvedbo modernih tehnologij. Prav tako pričakovanja niso bila izpolnjena glede kodeksov ravnanja, ki bi lahko združenjem upravljavcev omogočila doseganje skladnosti. Večja združenja, kot kaže, že imajo ustrezne vire in znanje ter predvidoma ne vidijo dodane vrednosti v kodeksih ravnanja, združenja manjših upravljavcev pa po naši oceni nimajo dovolj ustreznih sredstev in znanja za njihovo pripravo. Obenem so zahteve Splošne uredbe glede organov za spremljanje kodeksov, ki so v zasebnem sektorju obvezni, zelo visoke, saj terjajo finančno, strokovno in kadrovsko neodvisnost, s čimer pa se pod vprašaj postavi njihova izvedljivost. Zaradi odsotnosti nacionalnih izvedbenih predpisov je na ravni Slovenije povsem prezrto tudi področje vzpostavitev mehanizmov certificiranja za varstvo podatkov

ter pečatov in označb za varstvo podatkov za izkazovanje, da so dejanja obdelave s strani upravljavcev in obdelovalcev v skladu s Splošno uredbo.

Preventivne aktivnosti za skladnost, ki so se začele izvajati leta 2019, po oceni Informacijskega pooblaščenca predstavljajo zelo učinkovit način za doseganje skladnosti. Večina zavezancev ne želi kršiti zakonodaje in si želi biti skladna, zato jim je treba pri tem pomagati in jim ponuditi ustrezna orodja, kot so mnenja, smernice, obrazci, infografike idr. Kot zelo zgovoren primer lahko navedemo izpolnitev dolžnosti glede ocen učinkov pri operaterjih brezpilotnikov. Na podlagi podatkov Javne agencije za civilno letalstvo je Informacijski pooblaščenec ugotovil, da 77 zavezancev ni izpolnilo dolžnosti glede izvedbe ocene učinkov; po pozivu Informacijskega pooblaščenca z ustreznimi pojasnili in napotki je takih ostalo le še pet. Zagotavljanje skladnosti z uvedbami inšpekcijskih postopkov zoper toliko zavezancev bi prav gotovo trajalo neprimerno več časa in bi zahtevalo veliko več kadrovskih in finančnih sredstev. Posebej učinkovite se kažejo tovrstne aktivnosti v povezavi z združenji zavezancev, ki lahko ozaveščevalna gradiva učinkovito distribuirajo do svojih članov in tudi pozdravljajo takšen način sodelovanje z nadzornim organom.

Informacijski pooblaščenec uspešno kandidira na razpisih Evropske komisije za projekte iz programa REC (Rights, Equality and Citizenship Programme). Leta 2019 je uspešno nadaljeval izvajanje projekta RAPiD. Si, katerega glavni namen je izobraževanje in ozaveščanje predvsem manjših in srednje velikih podjetij ter posameznikov o reformi zakonodajnega okvira s področja varstva osebnih podatkov, v letu 2020 pa bo začel izvajati nov projekt iDECIDE, namenjen dvigovanju zavedanja o reformi okvira za varstvo osebnih podatkov predvsem med mladoletniki, starejšo in delovno populacijo.

Splošna uredba je prinesla pomembne novosti glede sodelovanja nadzornih organov za varstvo osebnih podatkov v državah članicah EU in EGS (Islandija, Norveška in Lihtenštajn) pri čezmejnih primerih po 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, in ki je uvedla mehanizme vzajemne pomoči in skupnega ukrepanja organov za varstvo osebnih podatkov v državah članicah EU. Informacijski pooblaščenec je leta 2019 sodeloval v 73 postopkih medsebojne pomoči med nadzornimi organi po členu 61 Splošne uredbe in v 77 postopkih ugotavljanja vodilnega organa po členu 56 Splošne uredbe. Od tega je sedem postopkov ugotavljanja začel Informacijski pooblaščenec. Na temelju postopkov določitve vodilnega in zadevnih nadzornih organov je Informacijski pooblaščenec leta 2019 aktivno sodeloval v 75 postopkih čezmejnega sodelovanja pri inšpekcijskem nadzoru nad podjetji, ki poslujejo čezmejno. V teh postopkih je pričakovan sprejem odločitve nadzornih organov po členu 60 Splošne uredbe, po t. i. mehanizmu »vse na enem mestu«. 61 tovrstnih postopkov je bilo začetih s strani drugih organov v EU in običajno zadevajo priljubljene ponudnike komunikacijskih spletnih storitev oz. spletne 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. 14 tovrstnih postopkov sodelovanja je sprožil Informacijski pooblaščenec, in sicer na podlagi prejete prijave oz. pritožbe zoper ravnanje zavezanca, ki je ustanovljen v drugi članici EU ali pa ima ustanovitve v različnih članicah v EU oz. so dejanja obdelave osebnih podatkov zadevala posameznike iz različnih držav članic EU.

Sodelovanje v čezmejnih primerih inšpekcijskega 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, ki jih uporabljajo posamezniki v vseh državah članicah EU in EGS, nadzorni organi za varstvo osebnih podatkov pa imajo zdaj na voljo mehanizme in orodja tesnega sodelovanja, s katerim imajo možnost nastopiti proti spornim praksam, ki škodijo pravicam posameznikov, z enim glasom.

Seveda pa tako sodelovanje za Informacijskega pooblaščenca, kot tudi za ostale nadzorne organe, pomeni velik izziv: potrebni so dodatni viri, tako finančni kot kadrovski – znanje, potrebno za obravnavo takih primerov, je namreč specifično, predvsem pa vključuje zelo različne discipline. Ključno je odlično poznavanje angleškega jezika, saj je angleščina v čezmejnih postopkih operativni jezik. Vodenje primerov čezmejne narave je kompleksno in zahteva veliko dodatnih resursov, tudi zaradi zahteve po zagotavljanju prevodov dokumentacije

(ki lahko obsega tudi celotna zelo obširna poročila). Dodatne vire zahteva že administriranje sodelovanja prek platforme IMI, ki jo je Informacijski pooblaščenec moral organizacijsko integrirati v svoje procese obravnave inšpekcijskih primerov in primerov odločanja o pravici do seznanitve z lastnimi osebnimi podatki. Vzpostaviti je moral interni sistem za sledenje postopkom v sistemu IMI ter za povezovanje informacij z evidencami, ki jih vodi na nacionalni ravni. Informacijski pooblaščenec je tako moral za izvajanje poglavja 7 Splošne uredbe nameniti dodatne vire (enakovredne 4–5 redno zaposlenim) za interno koordiniranje procesov sodelovanja in nacionalne prakse v nadzoru in pri pritožbah, za izobraževanje o tehničnem delovanju sistema IMI, o vodenju čezmejnih postopkov, poenotenju praks in stalnem sledenju praks, ki se razvijajo glede uporabe sistema IMI.

Izkušnje leta 2019 so pokazale tudi na druge izzive sodelovanja po poglavju 7 Splošne uredbe, predvsem z vidika razlik v nacionalnih procesnih pravilih v državah članicah EU (npr. glede pravic strank v postopkih, glede rokov za posamezna dejanja v postopkih, glede obveščanja prijaviteljev). Raznolika nacionalna pravila so zagotovo eden od razlogov, da so postopki sodelovanja po načelu »vse na enem mestu« v kompleksnejših primerih nadzora nad velikimi multinacionalnimi podjetji, daljši. Prve odločitve v tem okviru so pričakovane v letu 2020. Tudi različne interpretacije konceptov in norm sodelovanja, ki ga kot novost uvaja Splošna uredba, so se v konkretnih primerih leta 2019 izkazale kot velik izziv učinkovitemu vodenju tovrstnih postopkov. Odgovor na izziv deloma išče EOVP, ki aktivno pristopa k iskanju skupnih opredelitev in interpretacij konceptov v Splošni uredbi, deloma pa k reševanju lahko pristopi tudi evropski zakonodajalec, predvsem v okviru razmislekov o potencialni bodoči reviziji Splošne uredbe. Informacijski pooblaščenec je svoja videnja glede izzivov pri uporabi poglavja 7 Splošne uredbe za namen izvedbe postopkov revizije podal pristojnemu ministrstvu, prispeval pa je tudi k pripravi stališč EOVP na to temo.

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
mag. Kristina Kotnik Šumah, namestnica informacijske pooblaščenke
Karolina Kušević, svetovalka Pooblaščenca II
Matej Sironič, svetovalec Pooblaščenca za varstvo osebnih podatkov
Tina Ivanc, svetovalka Pooblaščenca za varstvo osebnih podatkov
Neja Domnik, raziskovalka Pooblaščenca
mag. Urban Brulc, samostojni svetovalec Pooblaščenca
dr. Jelena Burnik, vodja mednarodnega sodelovanja in nadzora
Manja Resman, svetovalka pooblaščenca II
mag. Eva Kalan Logar, vodja državnih nadzornikov

OBLIKOVANJE:
Darko Mohar
Tomaž Brodgesell

LEKTORIRALA:
Katja Klopčič Lavrenčič

Informacijski pooblaščenec Republike Slovenije
Dunajska cesta 22
1000 Ljubljana
www.ip-rs.si
gp.ip@ip-rs.si

ISSN 2670-5788

Ljubljana, maj 2020