INFORMACIJSKI POOBLAŠČENEC

LETNO POROČILO

Informacijskega pooblaščenca za leto 2020

UVODNA BESEDA INFORMACIJSKE POOBLAŠČENKE

Spoštovani,

leta 2020 so delo Informacijskega pooblaščenca na obeh področjih zaznamovale posledice epidemije, ki je v Sloveniji in Evropski uniji močno zarezala tudi v temeljne pravice posameznikov. Ukrepi, povezani z epidemijo covid-19, so na področju obeh pravic prinesli številne izzive, ki si jih pred tem nismo niti predstavljali. Tako v Sloveniji kot širše družbena dogajanja v letu 2020 kažejo, kako krhko je ravnovesje med različnimi temeljnimi pravicami in kako zlahka nekatere pravice zdrsnejo povsem v ozadje. V takih trenutkih je od učinkovitosti varstva posameznih pravic odvisno, kam se družba obrne. Vsaka posamezna institucija mora dosledno uresničevati Ustavo RS tudi v praksi.

Skrbi in izzivi, glede katerih so se posamezniki in organizacije obračali na Informacijskega pooblaščenca v letu 2020, so bili raznoliki, a vsi odraz razmer, v katerih živimo. Poleg neposredne pomoči zdravstvene stroke in ukrepov na področju zdravja so države kot eno temeljnih orodij za učinkovito obvladovanje epidemije prepoznale različne oblike obdelave osebnih podatkov s pomočjo najrazličnejših aplikacij in tehnologij. Neredko se je zdelo, da pri tem cilj opravičuje sredstva in da bi lahko varstvo podatkov doživelo dramatičen korak nazaj. Zato smo Svetovna skupščina za zasebnost, Evropski odbor za varstvo podatkov ter državni nadzorni organi za varstvo podatkov opozarjali, da morajo biti aplikacije, ukrepi in drugi načini obdelave osebnih podatkov za učinkovito obvladovanje epidemije sorazmerni ter v skladu s temeljnimi načeli varstva zasebnosti.

V letu 2020 se je v praksi pokazalo, kako bistvena sta transparentna javna uprava in učinkovit dostop do informacij javnega značaja v časih, ko so temeljne pravice drastično omejene. To potrjuje vnovična rast števila pritožb v zvezi z zahtevami za dostop do informacij javnega značaja, Informacijski pooblaščenec pa je prejel tudi bistveno več zaprosil za mnenja oz. pojasnila s tega področja. Informacijski pooblaščenec je zaznal zlasti povečanje števila primerov, v katerih so prosilci zahtevali informacije, ki se nanašajo na področje javnega zdravja ter s tem povezano porabo javnega denarja.

Analiza dela Informacijskega pooblaščenca v letu 2020 kaže, da na področju dostopa do informacij javnega značaja med izzivi zlasti izstopa trend rasti pritožb zoper državne organe (delež teh pritožb znaša kar 43 %). Podobno kot v letu 2019 je Informacijski pooblaščenec tudi v letu 2020 zaznal številne postopkovne kršitve, ki kažejo na to, da zavezanci pri obravnavi zahtev ne namenijo dovolj pozornosti postopkovnim vprašanjem, posledica pa je nepopolno oz. napačno ugotovljeno dejansko stanje.

Na področju varstva osebnih podatkov in zasebnosti smo bili tudi v letu 2020 priča bistvenemu povečanju števila prijav in števila pritožb v zvezi z uveljavljanjem pravic posameznikov. Hkrati so tudi leto 2020 zaznamovali precejšnji izzivi, ker Slovenija kot edina država v Evropski uniji dve leti po začetku uporabe Splošne uredbe še ni sprejela nacionalnih predpisov za njeno uporabo. Na to je v svoji resoluciji ob drugi obletnici začetka uporabe Splošne uredbe opozoril tudi Evropski parlament, že več kot tri leta pa na to opozarja tudi Informacijski pooblaščenec. Novembra 2020 je bil vendarle sprejet Zakon o varstvu osebnih podatkov na področju obravnavanja kaznivih dejanj za prenos Direktive za organe kazenskega pregona.

Na področju dostopa do informacij javnega značaja je bilo sicer število pritožbenih zadev v letu 2020 za 4,6 % višje kot leta 2019 (leta 2020 je bilo vloženih 565 pritožbenih zadev). Med pritožbami zaradi molka organa znova izstopajo organi državne uprave (ministrstva in organi v sestavi), zoper katere je bilo vloženih največ pritožb zaradi molka (39 %). Gre za zavezance, ki bi morali biti sposobni vse zahteve obravnavati pravočasno (v roku 20 delovnih dni). Zmanjšalo pa se je število pritožb zaradi molka občinskih organov. Informacijski pooblaščenec je vodil 14 postopkov zoper poslovne subjekte pod prevladujočim vplivom, kar predstavlja le 2,6 % vseh pritožbenih zadev.

Visok delež pritožb zaradi molka v skupnem deležu vseh pritožb (43 %), ki se z leti ne zmanjšuje, na kar Informacijski pooblaščenec opozarja že nekaj let, kaže, da bo v prihodnje treba več napora vložiti v promocijo zakona in aktivnejše usposabljanje zavezancev za njegovo uporabo v praksi, kar je primarno naloga Ministrstva za javno upravo. Informacijski pooblaščenec kot pritožbeni organ lahko organom svetuje le neformalno, na podlagi primerov iz prakse. Leta 2020 je podal 413 pisnih odgovorov na zaprosila zavezancev, primere iz prakse pa je redno objavljal na svoji spletni strani.

Na področju varstva osebnih podatkov je Informacijski pooblaščenec leta 2020 obravnaval 1018 prijav oz. pobud za uvedbo inšpekcijskega postopka, kar je največ doslej. Poleg tega je prejel 226 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 200 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 104 postopkih opredelil za zadevni nadzorni organ (po členu 56 Splošne uredbe). 22 postopkov čezmejnega sodelovanja je Informacijski pooblaščenec sprožil na podlagi prejete prijave oz. pritožbe. Informacijski pooblaščenec je v letu 2020 prejel tudi pet obvestil o kršitvah podatkov o pacientih na podlagi 46. člena Zakona o pacientovih pravicah ter 120 uradnih obvestil o kršitvi varnosti osebnih podatkov na podlagi 33. člena Splošne uredbe. Prijave, ki jih je v obravnavanem obdobju prejel in obravnaval Informacijski pooblaščenec, so bile vložene iz podobnih razlogov kot v preteklih letih; med razlogi so bili posredovanje osebnih podatkov neupravičenim osebam, uporaba osebnih podatkov za namene neposrednega trženja, izvajanje videonadzora, nezakonito ali prekomerno zbiranje osebnih podatkov, uporaba osebnih podatkov za namene, ki so v nasprotju z namenom njihovega zbiranja, nezakoniti vpogledi v zbirke osebnih podatkov ter neustrezno zagotavljanje varnosti osebnih podatkov. 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.

Informacijski pooblaščenec v svojih postopkih vedno znova ugotavlja, da večina zavezancev želi delovati skladno z zakoni, a zavezanci potrebujejo pomoč in jasna navodila. To se je v času epidemije izkazalo zlasti na področju delovnih razmerij in izobraževanja. V času epidemije je postalo jasno, kako bistveni so jasni predpisi in razumljiva opredelitev obveznosti zavezancev in posameznikov. Do hudih težav in stisk je prihajalo prav zaradi nejasnih navodil, zaradi česar posameznih uradnih odločitev ni bilo mogoče izvajati v praksi. Posebne okoliščine, ki so zaznamovale leto 2020, so vplivale tudi na področje skladnosti in preventive. Ne glede na to je Informacijski pooblaščenec tudi na tem področju varstva podatkov v letu 2020 nadaljeval okrepljeno delovanje: svetoval je 3.183 posameznikom in pravnim osebam, in sicer je izdal 1.331 pisnih mnenj ter odgovoril na 1.852 telefonskih klicev. Informacijski pooblaščenec uspešno kandidira na razpisih Evropske komisije za projekte iz programa REC (Rights, Equality and Citizenship Programme); cilj je prav dodatna krepitev vseh omenjenih aktivnosti. V letu 2020 je Informacijski pooblaščenec na svoji spletni strani zasnoval posebno podstran, na kateri je objavljal mnenja, stališča in priporočila, ki se nanašajo na varstvo osebnih podatkov v času epidemije.

Glede drugih mehanizmov Splošne uredbe velja poudariti, da je Slovenija druga država, ki je uspešno pripravila standardne pogodbene klavzule za ureditev pogodbene obdelave osebnih podatkov skladno s členom 28 Splošne uredbe, ki jih je potrdil Evropski odbor za varstvo osebnih podatkov. Na voljo so na spletni strani Informacijskega pooblaščenca.

Številni nepričakovani izzivi in iz teh izhajajoče izkušnje v letu 2020 so tudi na ravni Evropske unije (EU) in pri sodelovanju v okviru Evropskega odbora za varstvo podatkov (EOVP) pokazali, kako pomembna sta sodelovanje nadzornih organov in hitro izvajanje čezmejnih postopkov, hkrati pa se je ob tem razkrilo veliko razlik v nacionalnih procesnih pravilih v državah članicah EU. Tudi to je eden od razlogov za izzive na področju nadzora, na kar je v svoji resoluciji opozoril tudi Evropski parlament. Sodišče EU pa je s sodbo v primeru Schrems II, s katero je razveljavilo odločitev Evropske komisije o ustreznosti varstva podatkov v okviru zasebnostnega ščita, ki je subjektom iz EU omogočal prenos podatkov iz EU v ZDA, jasno sporočilo, da visoki standardi varstva osebnih podatkov ostajajo v središču pozornosti EU kot tudi v mednarodnih odnosih EU z drugimi državami.

Svet se je v letu 2020 nepovratno spremenil in čakajo nas izjemni izzivi. Ti terjajo odločno ukrepanje vseh pristojnih organov za učinkovito zavarovanje vseh temeljnih pravic, ki so zapisane v naši Ustavi in že več kot 70 let v Evropski konvenciji človekovih pravic. Veliko je razlogov za skrbi, ni pa razloga za malodušje. Leto 2020 je pokazalo tudi to, da smo ljudje povezani in da znamo zahtevati svoje pravice.

Informacijski pooblaščenec si bo z dobro ekipo strokovnjakov, konstruktivnim sodelovanjem z vsemi deležniki in odprtostjo do posameznikov ter organizacij tudi v letu 2021 prizadeval zavarovati obe pravici, ki sta mu zaupani.

Mojca Prelesnik, informacijska pooblaščenka

STRNJEN PREGLED LETA 2020

DOSTOP DO INFORMACIJ JAVNEGA ZNAČAJA

Informacijski pooblaščenec ugotavlja, da je na področju dostopa do informacij javnega značaja skupno število pritožbenih zadev v letu 2020 naraslo na 565 pritožb (v letu 2019 je obravnaval 540 pritožb). To kaže, da so posamezniki aktivno uveljavljali svoje pravice kljub sprejetju interventnega Zakona o začasnih ukrepih v zvezi s sodnimi, upravnimi in drugimi javnopravnimi zadevami za obvladovanje širjenja nalezljive bolezni SARS-CoV-2 (covid-19), s katerim so se spomladi za dva meseca prekinili vsi roki v nenujnih upravnih postopkih.

Informacijski pooblaščenec je v letu 2020 glede na epidemiološko situacijo zaznal povečanje števila primerov, ki se nanašajo na zahteve po informacijah s področja javnega zdravja in s tem povezano porabo javnega denarja. Gre za informacije, ki so pogosto v širšem javnem interesu, zato Informacijski pooblaščenec zavezance poziva, da pri odločanju o teh zahtevah postopajo hitro in pri presoji upoštevajo drugi odstavek 6. člena Zakona o dostopu do informacij javnega značaja (ZDIJZ), ki ureja test javnega interesa.

Skupno število pritožb zaradi molka (231) je bilo v letu 2020 na primerljivi ravni kot v letu 2019 (235). Razveseljivo je, da se je po več letih rasti zmanjšalo število pritožb zoper molk občin (teh pritožb je bilo v letu 2020 56), skrb vzbujajoča pa je ugotovitev, da hkrati raste skupno število pritožb zoper državne organe (245 pritožb, od tega 91 pritožb zoper molk). Informacijski pooblaščenec je v letu 2020 zaznal tudi povečano število pritožb zoper pravosodne organe (sodišča in državna tožilstva), kar gre pripisati sodbi Vrhovnega sodišča RS, da se za dostop do informacij iz sodnih spisov uporabljajo (le) določbe procesnih zakonov. Zaznati je bilo različno prakso posameznih sodišč in tožilstev v zvezi s procesno obravnavo zahtev po ZDIJZ in ZMed, kar je vodilo v neenako obravnavo prosilcev. Omenjena problematika je bila delno urejena s sprejemom zadnje novele Zakona o kazenskem postopku.

Informacijski pooblaščenec je v letu 2020 prejel kar 30 % več zaprosil za mnenja oz. pojasnila s področja dostopa do informacij javnega značaja (413) v primerjavi v letom 2019. Informacijski pooblaščenec na področju dostopa do informacij javnega značaja kot pritožbeni organ zavezancem in javnosti lahko svetuje le neformalno, na podlagi lastne prakse. Primere iz svoje prakse zato redno objavlja na svoji spletni strani.

Informacijski pooblaščenec na podlagi analize konkretnih primerov ugotavlja, da so primeri, s katerimi se srečujejo zavezanci, vsebinsko in procesno vse bolj kompleksni ter terjajo poglobljeno poznavanje tako področja dela organa kot tudi dobro poznavanje pravil upravnega postopka. Hkrati pa Informacijski pooblaščenec opaža, da zavezanci premalo pozornosti posvečajo postopkovnim vprašanjem in ugotavljanju dejanskega stanja v zadevah. Skrb vzbujajoč je znova tudi visok delež pritožb zaradi molka v skupnem deležu vseh pritožb (43 %).

Vse to kaže, da bo resorno Ministrstvo za javno upravo moralo aktivneje pristopiti k usposabljanju zavezancev za uporabo ZDIJZ, k čemur je ministrstvo pozval tudi Informacijski pooblaščenec. Prav tako bi moralo ministrstvo v prihodnje več napora vložiti v promocijo zakona. Informacijski pooblaščenec zavezance v zvezi s tem poziva, da za izvajanje nalog, ki jih predvideva ZDIJZ, določijo uradno osebo z dobrim poznavanjem strokovnega področja dela organa in hkrati ustreznimi postopkovnimi znanji s področja dostopa do informacij javnega značaja in upravnega postopka. Pri obravnavi zadev morajo zavezanci ustrezno proučiti vse procesne vidike zadeve, kar omogoča popolno in pravilno ugotovitev dejanskega stanja, pri čemer so zavrnitve zaradi zlorabe pravic s strani prosilca dopustne zgolj kot izjema in morajo biti te določbe ZDIJZ uporabljene vedno restriktivno, medtem ko je dokazno breme v celoti na zavezancu.

V letu 2020 je Informacijski pooblaščenec vodil 14 pritožbenih postopkov zoper poslovne subjekte pod prevladujočim vplivom, kar predstavlja le 2,6 % vseh pritožbenih zadev. Informacijski pooblaščenec ugotavlja, da število teh pritožb že vsa leta ostaja nizko.

V letu 2020 Informacijski pooblaščenec zaradi kršitev ZDIJZ ni uvedel nobenega postopka s prekrški, je pa v zadevi pod opr. št. 090-112/2015 zoper Ekonomsko fakulteto v Ljubljani uvedel postopek izvršbe s prisilitvijo, ker zavezanec prosilki še vedno ni posredoval informacij javnega značaja, kot mu je bilo naloženo.

VARSTVO OSEBNIH PODATKOV

Informacijski pooblaščenec se je v letu 2020 na področju varstva osebnih podatkov znova soočal s številnimi težavami in izzivi zaradi pravne neurejenosti področja v Republiki Sloveniji. Še vedno namreč ni bil sprejet nov Zakon o varstvu osebnih podatkov (ZVOP-2) za uporabo Splošne uredbe o varstvu podatkov, Zakon o varstvu osebnih podatkov na področju obravnavanja kaznivih dejanj (ZVOPOKD), s katerim se v slovenski pravni red prenaša Direktiva (EU) 2016/680 (t. i. Direktiva za organe kazenskega pregona), pa je bil sprejet šele konec leta 2020 in je začel veljati z 31. 12. 2020. Vse to je povzročilo precej odprtih vprašanj tako upravljavcev in obdelovalcev osebnih podatkov kot tudi Informacijskega pooblaščenca.

Nesprejetje novega ZVOP-2 je izrazito negativno vplivalo na vodenje prekrškovnih postopkov in izrekanje glob za ugotovljene kršitve. Informacijski pooblaščenec namreč zaradi odsotnosti ZVOP-2 v letu 2020 v primeru ugotovljenih kršitev določb Splošne uredbe zavezancem ni mogel izrekati sankcij za kršitve. Usklajenost nacionalnih določb in izrečenih sankcij s Splošno uredbo je še posebej pomembna z vidika usklajevanja praks v državah članicah EU, v katerih se uporablja Splošna uredba, ter z vidika sodelovanja Informacijskega pooblaščenca v Evropskem odboru za varstvo osebnih podatkov. Izrečene globe glede podobnih prekrškov v podobnih okoliščinah v različnih državah ne bi smele odstopati, kar še zlasti velja v primerih čezmejnega sodelovanja pri inšpekcijskem nadzoru.

Trend povečanega števila prijav, kršitev varstva osebnih podatkov in pritožb v zvezi z uveljavljanjem pravic posameznikov se je nadaljeval tudi v letu 2020. Informacijski pooblaščenec je prejel 1018 prijav oz. pobud za uvedbo inšpekcijskega postopka, kar je največ doslej. Poleg omenjenih prijav je Informacijski pooblaščenec v letu 2020 prejel še pet primerov prijav nedovoljenega sporočanja ali druge nedovoljene obdelave osebnih podatkov o pacientih na podlagi 46. člena Zakona o pacientovih pravicah (ZPacP), 12 pritožb zoper odločitev upravljavca po 41. členu ZPacP, sedem pritožb zoper odločitev upravljavca po 42. členu ZPacP, 36 pritožb zaradi kršitev upravljavca po 30. členu ZVOP-1, 171 pritožb posameznikov zaradi kršitev pravice do vpogleda v lastne osebne podatke po členu 15 Splošne uredbe in odločitve upravljavca v zvezi s tem (od tega je bilo 82 pritožb vloženih zaradi molka upravljavca), pet pritožb zaradi kršitve pravice do popravka osebnih podatkov po členu 16 Splošne uredbe, 11 pritožb zaradi kršitve pravice do izbrisa osebnih podatkov po členu 17 Splošne uredbe ter eno pritožbo zaradi kršitve pravice do omejitve obdelave osebnih podatkov po členu 18 Splošne uredbe. Vse to kaže, da se posamezniki vse bolj zavedajo svojih pravic.

Informacijski pooblaščenec je v letu 2020 prejel tudi 120 uradnih obvestil o kršitvi varnosti osebnih podatkov na podlagi člena 33 Splošne uredbe. Obvestila o kršitvi varnosti osebnih podatkov Informacijskemu pooblaščencu so se najpogosteje nanašala na posredovanje osebnih podatkov nepooblaščenim ali napačnim osebam, nepooblaščeno dostopanje do osebnih podatkov zaradi programske napake ali zlorabe pooblastil s strani zaposlenih, napade na informacijski sistem z izsiljevalskim virusom in kriptiranjem podatkov, objave osebnih podatkov strank upravnega postopka ter izgube ali kraje nosilcev osebnih podatkov (npr. osebnih računalnikov in USB-ključkov). Občutno se je povečalo število napadov na informacijski sistem z izsiljevalskim virusom in kriptiranjem podatkov, kar je upravljavcem osebnih podatkov, ki niso izvajali ustreznih tehničnih in organizacijskih ukrepov za zagotavljanje varnosti obdelave osebnih podatkov, povzročilo velike stroške in težave.

Prijave, ki jih je prejel in obravnaval Informacijski pooblaščenec, so bile vložene iz podobnih razlogov kot v preteklih letih, številnim prijavam pa so tudi v letu 2020 botrovale pomanjkljive informacije, posameznikom podane s strani upravljavcev, ki osebne podatke zbirajo. Ti namreč posamezniku pogosto še vedno ne zagotovijo preglednih, razumljivih in lahko dostopnih informacij o obdelavi, kot jim nalagata člena 12 in 13 Splošne uredbe.

Leto 2020 je zaznamovalo tudi večje število prijav in zaprosil za mnenja, prejetih v zvezi z varstvom osebnih podatkov v času epidemije (covid-19). Informacijski pooblaščenec je zato na svoji spletni strani pripravil posebno podstran na to temo. Informacijski pooblaščenec je v letu 2020 svetoval 3.183 posameznikom in pravnim osebam, ki so se nanj obrnili z vprašanji s področja varstva osebnih podatkov: izdal je 1.331 pisnih mnenj in napotitev na mnenja, državni nadzorniki pa so pri telefonskem svetovanju sprejeli 1.852 klicev. Ne glede na posebne okoliščine je Informacijski pooblaščenec v letu 2020 izvedel 34 brezplačnih predavanj za zavezance, večino z uporabo spletnih orodij. Uspešno je izvajal tudi projekt iDECIDE, ki ga financira Evropska unija, namenjen pa je ozaveščanju treh ciljnih populacij: mladoletnikov, starejše populacije in delovne populacije. Posebno pozornost je Informacijski pooblaščenec posvečal pooblaščenim osebam za varstvo osebnih podatkov, saj so prav ti multiplikatorji v skrbi za varstvo podatkov znotraj svojih organizacij. Pooblaščeno osebo je že imenovalo več kot 2300 zavezancev, nekaj sto pa jih po oceni Informacijskega pooblaščenca te obveznosti še ni izpolnilo.

Zamujanje s sprejemom ZVOP-2 se kaže tudi na področju preventive in skladnosti, saj zavezanci posledično – dokler ne bodo jasno opredeljeni pogoji v ZVOP-2 – ne morejo uporabiti certifikacije po Splošni uredbi. Med pomembnejšimi dosežki v letu 2020 na tem področju pa velja poudariti, da je Slovenija kot druga država uspešno pripravila standardne pogodbene klavzule za ureditev pogodbene obdelave osebnih podatkov skladno s členom 28 Splošne uredbe. Gre za vzorčno pogodbo, ki jo lahko uporabijo upravljavci podatkov za najem storitev pogodbenih obdelovalcev in jo je potrdil Evropski odbor za varstvo podatkov.

Zavedanje pomena varstva osebnih podatkov in zasebnosti v družbi je po izkušnjah Informacijskega pooblaščenca kljub izzivom leta 2020 med splošnim prebivalstvom ostalo na visoki ravni, s precej večjo zaskrbljenostjo pa Informacijski pooblaščenec spremlja upoštevanje teh temeljnih človekovih pravic pri odločevalcih. Leta 2020 je Informacijski pooblaščenec izdal 85 mnenj na predloge sprememb predpisov. Pri tem je opazil tudi skrb vzbujajoč trend nesistemskega urejanja nekaterih resnih posegov v zasebnost ter poskusov zniževanja že dosežene ravni varstva osebnih podatkov. To se je kazalo tudi v primeru nejasnih ali odsotnih navodil zavezancem za izvajanje ukrepov v zvezi z epidemijo. Zlasti izrazito se je to pokazalo na področju šolanja in izobraževanja ter v delovnih okoljih, kar je vodilo v pretirane posege in stiske tako pri posameznikih kot tudi v šolah, podjetjih in drugih organizacijah. V zvezi z uvajanjem mobilne aplikacije za sledenje stikom so bila opozorila Informacijskega pooblaščenca večinoma preslišana in ocenjujemo, da je prav zaradi neustreznega komuniciranja, vztrajanja pri obvezni uporabi aplikacije in drugih nejasnostih prišlo do padca zaupanja v takšno rešitev. Na drugi strani se kažejo primeri dobrih praks, na primer uvajanje e-vinjet, pri katerem je predlagatelj pravočasno pridobil stališča Informacijskega pooblaščenca in jih vgradil v določbe zakonodaje.

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. Med drugim je omogočila in formalizirala postopek sodelovanja 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. Informacijski pooblaščenec je leta 2020 sodeloval v 123 postopkih medsebojne pomoči med nadzornimi organi po členu 61 Splošne uredbe, na temelju postopkov določitve vodilnega in zadevnih nadzornih organov pa je Informacijski pooblaščenec v tem letu aktivno sodeloval v 77 postopkih čezmejnega sodelovanja pri inšpekcijskem nadzoru nad podjetji, ki poslujejo čezmejno. 22 postopkov čezmejnega sodelovanja je sprožil Informacijski pooblaščenec, in sicer na podlagi prejete prijave oz. pritožbe. Informacijski pooblaščenec je ob sodelovanju španskega nadzornega organa obravnaval tudi primer pilotnega projekta vkrcavanja potnikov z uporabo biometrije na ljubljanskem letališču, ki ga je izvajala španska družba Amadeus; ugotovil je kršitve določb ZVOP-1 o biometriji.

Čezmejni primeri pa se niso nanašali le na storitve priljubljenih spletnih velikanov, ki so v veliki meri še v teku (vodilni organ je na Irskem), temveč tudi na neustrezna ravnanja z osebnimi podatki s strani raznolikih akterjev iz številnih držav članic EU. Primeri spornih praks so vključevali pretirane zahteve po podatkih za identifikacijo strank, za namen izbrisa podatkov, neustrezno izvrševanje pravice do dostopa, posredovanje podatkov tretjim osebam. Pogosto so se primeri nanašali na kršitve varnosti osebnih podatkov; med prizadetimi so bili tudi uporabniki iz Slovenije. Informacijski pooblaščenec je kot zadevni nadzorni organ sodeloval v postopkih nadzora v zvezi s kršitvijo varstva osebnih podatkov pri podjetjih, kot so Nintendo, TicketMaster, Marriot Hotels, Twitter, National Australia Bank, British Airways itd., ki so bili zaključeni v letu 2020.

Sodelovanje v čezmejnih primerih pomeni velik izziv v smislu dodatnih potrebnih resursov, tako finančnih kot kadrovskih. Izkušnje v letu 2020 so pokazale tudi na druge izzive sodelovanja po poglavju 7 Splošne uredbe, in sicer so bila v ospredju predvsem vprašanja glede izvedbe postopkov po Splošni uredbi. Leto 2020 je zaznamovala tudi izvedba prvega odločanja Evropskega odbora za varstvo podatkov v postopku spora po členu 65, ki je zadevala primer družbe Twitter. Odločitev odbora je za vodilni nadzorni organ zavezujoča in v zadevnem primeru je bilo vodilnemu organu naloženo, da mora v končni odločbi pri izreku sankcije upoštevati vsa merila iz člena 83 Splošne uredbe, da bo sankcija primerna in odvračalna.

Evropski odbor za varstvo podatkov aktivno pristopa h grajenju enotnih rešitev izzivov, ki nastajajo zaradi 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) ter pripravlja nadaljnje smernice glede postopkov po členih 60 in 65 Splošne uredbe. Prav tako je odbor v letu 2020 aktivno prispeval k razlagam številnih določb Splošne uredbe s smernicami in priporočili, med drugim glede konceptov upravljavca in obdelovalca, glede ciljanja uporabnikov na družbenih omrežjih, glede omejitev po členu 23 Splošne uredbe, glede glasovnih pomočnikov in povezanih avtomobilov, primerov kršitev varstva podatkov ter glede najbolj perečih vprašanj obdelav osebnih podatkov v zvezi z ukrepanjem glede obvladovanja epidemije covid-19.

Leta 2020 je bila na ravni EU sprejeta pomembna sodba v primeru Schrems II, s katero je Sodišče EU razveljavilo odločitev Evropske komisije o ustreznosti varstva podatkov v okviru zasebnostnega ščita, ki je subjektom iz EU omogočal prenose podatkov iz EU v ZDA. Evropski odbor za varstvo podatkov je v odzivu na razveljavljeni zasebnostni ščit sprejel več priporočil glede ustreznih dopolnilnih ukrepov za prenos podatkov v ZDA in kriterijev za ocenjevanje vpliva nacionalne zakonodaje v državi prejemnici na varstvo prenesenih podatkov.

KAZALO

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
ZVOP-2 — Predlog novega Zakona o varstvu osebnih podatkov
ZInfP — Zakon o Informacijskem pooblaščencu
ZVOPOKD — Zakon o varstvu osebnih podatkov na področju obravnavanja kaznivih dejanj
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
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
ZVDAGA — Zakon o varstvu dokumentarnega in arhivskega gradiva ter arhivih

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, pravice dostopa do informacij javnega značaja in pravice do varstva osebnih podatkov.

Državni zbor Republike Slovenije je 30. 11. 2005 sprejel Zakon o Informacijskem pooblaščencu (ZInfP), s katerim je bil 31. 12. 2005 ustanovljen nov samostojen in neodvisen državni organ. Zakon je združil dva organa, in sicer Pooblaščenca za dostop do informacij javnega značaja, ki je imel že prej status neodvisnega organa, in Inšpektorat za varstvo osebnih podatkov, ki je deloval kot organ v sestavi Ministrstva za pravosodje. Informacijski pooblaščenec je tako postal tudi državni nadzorni organ za varstvo osebnih podatkov. Delo je začel 1. 1. 2006.

ZInfP je v slovenski pravni red prinesel pomembne novosti. S tem zakonom je bil namreč ustanovljen nov državni organ, Informacijski pooblaščenec, ki ima 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 prekrškovne 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.

Neodvisnost Informacijskega pooblaščenca je tudi temeljna zahteva za nadzorne organe skladno z **Uredbo (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) ter **Direktivo (EU) 2016/680 Evropskega parlamenta in Sveta** z dne 27. aprila 2016 o varstvu posameznikov pri obdelavi osebnih podatkov, ki jih pristojni organi obdelujejo za namene preprečevanja, preiskovanja, odkrivanja ali pregona kaznivih dejanj ali izvrševanja kazenskih sankcij, in o prostem pretoku takih podatkov ter o razveljavitvi Okvirnega sklepa Sveta 2008/977/PNZ (Direktiva (EU) 2016/680). Informacijski pooblaščenec tako kot nadzorni organ spremlja uporabo Splošne uredbe in Direktive (EU) 2016/680, da se zaščitijo temeljne pravice in svoboščine posameznikov v zvezi z obdelavo osebnih podatkov ter olajša prost pretok osebnih podatkov v Evropski uniji. Splošna uredba in Direktiva (EU) 2016/680 določata naloge, ki jih mora vsak nadzorni organ opraviti na svojem ozemlju, ter pri tem opredeljujeta pooblastila nadzornih organov. Okrepljeno je tudi sodelovanje med nadzornimi organi v Evropski uniji, še posebej z ustanovitvijo Evropskega odbora za varstvo podatkov (EOVP).

Od 17. 7. 2014 Informacijskega pooblaščenca vodi pooblaščenka Mojca Prelesnik.

LETO 2020 V ŠTEVILKAH

48
zaposlenih

2.321,085,00
EUR proračuna

Varstvo osebnih podatkov

1208
inšpekcijskih postopkov

96
prekrškovnih postopkov

1331
pisnih mnenj

1852
ustnih mnenj

107
postopkov odločanja o vodilnem nadzornem organu

5
novih smernic

1
obrazec za zavezance

3
infografike

34
predavanj

120
prijav kršitev varnosti

6
mnenj na prejete ocene učinka

2320
imenovanih pooblaščenih oseb za varstvo podatkov

1
preventivna aktivnost za skladnost

77
mednarodnih sodelovanj po načelu “vse na enem mestu”

123
postopkov vzajemne pomoči drugim nadzornim organom EU

85
mnenj na predpise

Informacije javnega značaja

565
vloženih pritožb

328
izdanih odločb

144
pozivov zaradi molka

34
in camera ogledov

29 dni
povprečen čas reševanja pritožbenih zadev

411
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. 2020 so bili pri Informacijskem pooblaščencu zaposleni en funkcionar in 47 javnih uslužbencev, od tega 46 javnih uslužbencev 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. 2020.

	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				2			**2**
Asistent svetovalca				2			**2**
Raziskovalec pooblaščenca			1	1			**2**
Sistemski administrator			1				**1**
Strokovni sodelavec za finančne in kadrovske zadeve		1					**1**
Poslovni sekretar			2				**2**
Dokumentalist		1					**1**
Projektni sodelavec	2						**2**

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.

Ključen predpis s področja varstva osebnih podatkov v EU je **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 2020 ni bil sprejet.

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. Splošna uredba določa tudi pooblastila nadzornih organov, ki jih lahko uporabijo pri izvajanju svojih pristojnosti (preiskovalna pooblastila, popravljalna pooblastila ter pooblastila v zvezi z dovoljenji in svetovalnimi pristojnostmi).

Glede na to, da novi Zakon o varstvu osebnih podatkov (ZVOP-2) še ni bil sprejet, se poleg določb 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, ter relevantne določbe 2. člena ZInfP, npr.:

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. dajanje predhodnih mnenj 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 (48. člen ZVOP-1);
7. sodelovanje z državnimi organi, pristojnimi organi Evropske unije za varstvo posameznikov pri obdelavi osebnih podatkov, mednarodnimi organizacijami, tujimi nadzornimi organi za varstvo osebnih podatkov, zavodi, združenji, nevladnimi organizacijami s področja varstva osebnih podatkov ali zasebnosti ter drugimi organizacijami in organi glede vseh vprašanj, ki so pomembna za varstvo osebnih podatkov (47. člen ZVOP-1).

Republika Slovenija je zamujala tudi z implementacijo **Direktive (EU) 2016/680** in **Direktive (EU) 2016/681** Evropskega parlamenta in Sveta z dne 27. aprila 2016 o uporabi podatkov iz evidence podatkov o potnikih (PNR) za preprečevanje, odkrivanje, preiskovanje in pregon terorističnih in hudih kaznivih dejanj v delu, ki se nanaša na položaj in naloge pooblaščenih oseb za varstvo osebnih podatkov. Omenjeni direktivi sta bili v pravni red Republike Slovenije preneseni z Zakonom o varstvu osebnih podatkov na področju obravnavanja kaznivih dejanj (ZVOPOKD), ki je pričel veljati z 31. 12. 2020. Skladno z ZVOPOKD pa Informacijski pooblaščenec deluje kot pritožbeni, inšpekcijski in prekrškovni organ, in sicer skrbi za enotno uresničevanje ukrepov na področju varstva osebnih podatkov po določbah ZVOPOKD, tako da se zaščitijo človekove pravice in temeljne svoboščine posameznikov v zvezi z obdelavo osebnih podatkov ter se omogoči prost pretok osebnih podatkov

med državami članicami Evropske unije v skladu z določbami ZVOPOKD. Pristojnosti Informacijskega pooblaščenca so določene v prvem odstavku 76. člena ZVOPOKD, skladno s prvim odstavkom 77. člena ZVOPOKD pa Informacijski pooblaščenec ni pristojen za izvajanje nadzora in za prekrškovni nadzor glede obdelav osebnih podatkov, ki se obdelujejo v kazenskih zadevah sodišča, izvedenih v okviru neodvisnega sodniškega odločanja ali odločanja strokovnih sodelavcev ali sodniških pomočnikov po odredbi sodnika, kot to opredeljuje zakon, ki ureja sodišča, ali po določbah drugih zakonov, ki določajo njihovo samostojno delovanje. V letu 2020 so se za posameznike in upravljavce po Direktivi (EU) 2016/680 Evropskega parlamenta in Sveta do vključno 30. 12. 2020 še uporabljale relevantne določbe ZVOP-1.

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)** 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 Informacijski pooblaščenec:
- 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.

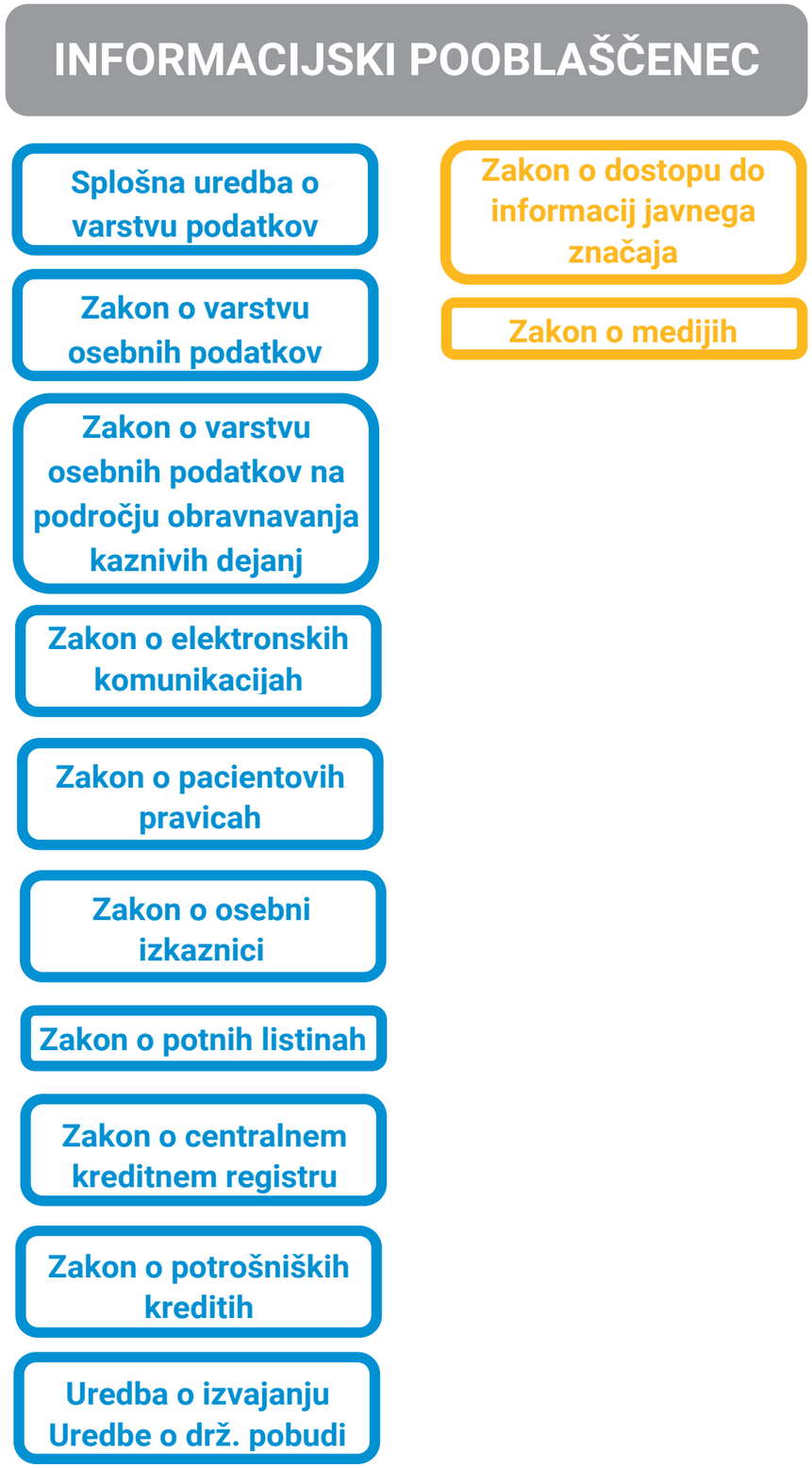
ZPotK-2 v 78. členu ohranja leta 2013 dodeljeno pristojnost Informacijskega pooblaščenca v zvezi z izvajanjem nadzora nad dajalci kreditov in kreditnimi posredniki glede izvajanja 10. in 42. člena v delu, ki se nanaša na informiranje, zbiranje in obdelavo osebnih podatkov pri izvedbi ocene kreditne sposobnosti 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.

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.

Pristojnosti Informacijskega pooblaščenca opredeljujejo tudi pravila **Schengenskega informacijskega sistema (in druga generacija sistema, t. i. SIS II)**, ki nacionalnim organom kazenskega pregona ter pravosodnim in upravnim organom omogočajo izmenjavo in dostop do podatkov o prestopu zunanjih meja in vizumski politiki, v sistem pa so poleg tega vključeni tudi podatki o evropskem zapornem nalogu, izročitvi, biometrični podatki in podatki o iskanju zaradi terorističnih aktivnosti. Pravni okvir SIS II vključuje: **Uredbo (ES) št. 1987/2006 Evropskega parlamenta in Sveta z dne 20. decembra 2006 o vzpostavitvi, delovanju in uporabi druge generacije schengenskega informacijskega sistema (SIS II); Sklep Sveta 2007/533/PNZ z dne 12. junija 2007 o vzpostavitvi, delovanju in uporabi druge generacije schengenskega informacijskega sistema (SIS II) in Uredbo (ES) št. 1986/2006 Evropskega parlamenta in Sveta z dne 20. decembra 2006 o dostopu služb držav članic, pristojnih za izdajo potrdil o registraciji vozil, do druge generacije schengenskega informacijskega sistema (SIS II)**. Informacijski pooblaščenec na podlagi 60. člena Sklepa Sveta 2007/533/PNZ ter 44. člena Uredbe (ES) št. 1987/2006 nadzira zakonitost obdelave osebnih podatkov v SIS II na svojem ozemlju in pri prenosu s svojega ozemlja, vključno z izmenjavo in nadaljnjo obdelavo dopolnilnih podatkov.

Pristojnosti Informacijskega pooblaščenca.



1.3 FINANČNO POSLOVANJE V LETU 2020

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 2020 veljavni proračun na integralnih postavkah 2.321.085,00 EUR, od tega na postavki plače 1.948.180,00 EUR, na postavki materialni stroški 311.005,00 EUR in na postavki investicije 61.900,00 EUR. Evidentiranih odredb na integralnih postavkah je bilo na dan 31. 12. 2020 2.303.264,28 EUR, od tega na postavki plače 1.930.874,18 EUR, na postavki materialni stroški 310.955,29 EUR in na postavki investicije 61.434,81 EUR.

Proračun Informacijskega pooblaščenca 2015—2020.

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
2020	2.321.085,00 EUR

Informacijski pooblaščenec je v letu 2020 razpolagal z namenskimi sredstvi v znesku 7.317,92 EUR. Porabe namenskih sredstev v letu 2020 ni bilo.

V proračun leta 2021 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).

Zaradi izredne situacije – razglasitve epidemije – in močnega poslabšanja kazalnikov gospodarskih gibanj je Vlada RS na podlagi zakonodaje, ki ureja izvrševanje proračuna, zadržala izvrševanje proračuna za leto 2020 ter izvedla ukrep proporcionalnega zmanjšanja pravic porabe v višini 30 % sprejetega proračuna. Na osnovi Sklepa Vlade RS št. 41003-2/2020/1 z dne 13. 3. 2020 je bilo na postavko Tekoča proračunska rezerva pri Ministrstvu za finance z integralne postavke prenesenih 114.300,00 EUR.

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

Proračun Informacijskega pooblaščenca 2020.

	Veljavni proračun v EUR	Prevzete obveznosti v EUR	Razpoložljiv proračun v EUR konec leta
Informacijski pooblaščenec	**2.415.237,05**	**2.390.066,91**	**25.170,14**
Podprogrami			
OPRAVLJANJE DEJAVNOSTI	**2.321.085,00**	**2.303.264,28**	**17.820,72**
PP 1271 Materialni stroški	311.005,00	310.955,29	49,71
PP 1273 Investicije	61.900,00	61.434,81	465,19
PP 1267 Plače	1.948.180,00	1.930.874,18	17.305,82
NAMENSKA SREDSTVA	**7.317,92**	**0,00**	**7.317,92**
7459 Namenska sr. kupnine	7.317,92	0,00	7.317,92
Donacije – EU projekti	**86.834,13**	**86.802,63**	31,50
PP 9958 Mednarodna spl. str.	0,14	0,00	0,14
PP130134 projekt Taiex	2,99	0,00	2,99
PP 190100 RAPiD.si	7.132,00	7.105,58	26,42
PP200001 iDecide	79.699,00	79.697,05	1,95

Za materialne stroške je bilo leta 2020 porabljenih 310.955,29 EUR, in sicer za pisarniški in splošni material in storitve 64.498,03 EUR (pisarniški material, čiščenje poslovnih prostorov, storitve varovanja zgradb in prostorov, spremljanje medijev in arhiviranje, stroški prevajalskih storitev, reprezentanca ter drugi splošni material in storitve), za posebni material in storitve 3.923,80 EUR (nakup drobnega inventarja, zdravniški pregledi zaposlenih), za energijo, vodo, komunalne storitve, pošto in komunikacijo 38.635,01 EUR (električna energija, ogrevanje, voda in komunalne storitve, odvoz smeti, stroški telefonov ter poštne storitve), za prevozne stroške in storitve 4.929,36 EUR (vzdrževanje, popravila, zavarovanje in registracija dveh službenih vozil, gorivo za službeni vozili, najem vozil oz. taksi storitve ter drugi prevozni in transportni stroški), za izdatke za službena potovanja 5.737,95 EUR (stroški, povezani s službenimi potovanji zaposlenih, dnevnice, nočnine, letalske karte, hotelske storitve in stroški prevozov), za tekoče vzdrževanje 6.548,80 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), za poslovne najemnine in zakupnine 160.214,12 EUR (najemnina in zakupnine za poslovne objekte in parkirne prostore, najem programske računalniške opreme – IUS-INFO in prekrškovni portal), za druge operativne odhodke pa je bilo porabljenih 26.468,22 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 1.427,33 EUR. Informacijski pooblaščenec konec leta 2020 s postavke materialni stroški ni prerazporedil prostih pravic porabe v Tekočo proračunsko rezervo pri Ministrstvu za finance, ker ni bilo prostih sredstev.

Za investicije je bilo do konca leta 2020 porabljenih 61.434,81 EUR. Sredstva so bila porabljena za nakup pisarniškega pohištva in pisarniške opreme v znesku 2.769,80 EUR (trije pisarniški stoli in sedem predalnikov), strojne računalniške opreme v znesku 8.350,85 EUR (dvanajst monitorjev, trije tiskalniki in osem računalnikov), strežnikov in diskovnih sistemov v znesku 35.872,31 EUR (vzpostavitev redundančnega strežniškega sistema IPRS), opreme za hlajenje in ogrevanje v znesku 227,81 EUR, telekomunikacijske opreme v znesku 419,60 EUR, druge opreme in napeljave v znesku 5.740,10 EUR (nadgradnja sistema za evidenco in kontrolo prisotnosti), nematerialnega premoženja v znesku 7.886,81 EUR (licence za sistem za evidenco in kontrolo prisotnosti, vzpostavitev klasifikacijskega načrta, licenca Amebis Besana in licenca EvenTrack), za nakup druge nelicenčne programske opreme pa je bilo porabljenih 167,53 EUR. Konec leta 2020 je bilo stanje razpoložljivega proračuna na postavki investicije 0,85 EUR.

S postavke investicije Informacijski pooblaščenec v letu 2020 prostih pravic porabe ni prerazporedil v Tekočo proračunsko rezervo pri Ministrstvu za finance, ker ni bilo prostih sredstev.

Za plače zaposlenih je bilo porabljenih 1.930.874,18 EUR oz. 99,11 % glede na veljavni proračun za leto 2020. Glede na predhodna leta se je poraba sredstev povečala zaradi sprostitve napredovanj, realizacije dogovora o plačah in 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 (EU) 2016/680 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. Porabljena sredstva v višini 1.930.874,18 EUR so bila namenjena za osnovne plače in dodatke v znesku 1.540.392,17 EUR, za regres za letni dopust je bilo namenjenih 45.218,06 EUR, za povračila in nadomestila 58.322,57 EUR, sredstva za delovno uspešnost z naslova povečanega obsega dela zaradi povečanega pripada zadev so znašala 17.768,45 EUR, za druge izdatke zaposlenim je bilo porabljenih 1.876,91 EUR, za prispevke delodajalcev za pokojninsko in invalidsko zavarovanje 136.916,63 EUR, za prispevke za zdravstveno zavarovanje 110.567,59 EUR, za prispevke za zaposlovanje 857,09 EUR, za prispevek za starševsko varstvo 1.559,59 EUR, premije kolektivnega dodatnega pokojninskega zavarovanja na podlagi Zakona o dodatnem pokojninskem zavarovanju javnih uslužbencev pa so znašale 17.395,12 EUR. Informacijski pooblaščenec je leta 2020 od Zavoda za zdravstveno zavarovanje Slovenije z naslova refundacij boleznin in invalidnin prejel sredstva na postavko za plače v višini 30.277,72 EUR. S postavke plače je Informacijski pooblaščenec v letu 2020 na podlagi Sklepa Vlade št. 41012-110/2020/2 prerazporedil 3.000,00 EUR na postavko materialni stroški zaradi plačila računa Zavarovalnice Triglav, d. d., za najem poslovnega prostora za december 2020.

Namenska sredstva kupnine – v leto 2020 je bilo prenesenih **7.317,92 EUR** finančnih sredstev kupnin. Leta 2020 na postavki ni bilo niti prilivov niti odlivov. Preostanek finančnih sredstev v višini 7.317,92 EUR se prenese v leto 2021.

Mednarodna spletna stran info-commissioners.org – iz leta 2019 je bilo prenesenih 0,14 EUR finančnih sredstev. Leta 2020 na tej postavki ni bilo porabe. Projekt se leta 2021 konča, preostanek sredstev bo nakazan na podračun izvrševanja proračuna.

Projekt Taiex – iz leta 2019 je bilo v leto 2020 prenesenih 2,99 EUR. Za projekt Taiex leta 2020 ni bilo niti prilivov niti odlivov. Projekt se leta 2021 zaključi, preostanek sredstev bo nakazan na podračun izvrševanja proračuna.

Projekt RAPiD.Si – Informacijski pooblaščenec je v letih 2019, 2020 in 2021 kot vodilni in edini partner izvajal 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 je trajal 36 mesecev, osredotočal se je na aktivnosti izobraževanja in ozaveščanja predvsem malih in srednje velikih slovenskih podjetij ter na dejavnosti ozaveščanja splošne slovenske javnosti o novih pravilih Evropske unije glede varstva osebnih podatkov, ki jih prinaša uveljavitev Splošne uredbe in novega ZVOP-2. Za sodelovanje v projektu je Informacijski pooblaščenec prejel evropska namenska sredstva v načrtovani višini 84.539,00 EUR, sam pa je v okviru svojih aktivnosti za izvajanje projekta z integralnih proračunskih sredstev zagotovil 21.130,00 EUR. Sredstva so bila 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 je 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 v proračun uvrščen nov projekt NRP 1215-19-0001, s katerim so bile povečane pravice porabe za leto 2019, in sicer za 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.

Poraba leta 2020 za potrebe projekta je bila na evropski postavki PP 190100 7.105,58 EUR, na postavki integralna sredstva PP1271 pa 408,00 EUR. Projekt se je končal v letu 2020, in sicer je bilo oktobra oddano poročilo. Dne 18. 12. 2020 je bil Informacijskemu pooblaščencu nakazan končni priliv v znesku 16.907,80 EUR. Sredstva bodo porabljena v letu 2021.

Projekt iDecide – posamezniki odločajo — Informacijski pooblaščenec je v letu 2020 kot vodilni in edini partner začel izvajati dvoletni projekt iDecide – REC-AG-2019/REC-RDAT-TRAI-AG-2019 – »Individuals decide – Raising awareness about data protection rights (iDecide)«**,** št. pogodbe: 874507. Projekt financira Evropska komisija, in sicer v okviru Programa za pravice, enakost in državljanstvo 2020–2023.

Projekt bo trajal 48 mesecev, osredotočal pa se bo na izobraževanje treh ciljnih skupin (starejših mladoletnikov (15–18 let), starejših (nad 65 let) in delovne populacije o reformi zakonodajnega okvira s področja varstva osebnih podatkov in o temeljnih pravicah, ki jih zagotavlja zakonodaja s področja varstva osebnih podatkov. Cilj projekta iDecide je povečanje zavedanja o reformi okvira za varstvo osebnih podatkov v splošni javnosti v Republiki Sloveniji, še posebej glede pravic posameznikov. Za sodelovanje v projektu bo Informacijski pooblaščenec prejel evropska sredstva v načrtovani višini 194.346,24 EUR, sam pa bo v okviru svojih aktivnosti za izvajanje projekta v 48 mesecih trajanja projekta iz integralnih proračunskih sredstev zagotovil 48.586,56 EUR, skupno torej 242.932,80 EUR. Sredstva bodo porabljena za pokrivanje stroškov v zvezi z delom zaposlenih, za pokrivanje povečanega obsega dela zaposlenih, za stroške poti do krajev izvedbe predavanj, za tisk izobraževalnih materialov in organizacijo seminarjev ter za druge stroške v zvezi s pripravo in izvedbo navedenih aktivnosti ter materialnih stroškov, ki jih bo s tem imel Informacijski pooblaščenec.

Projekt se je v letu 2020 izvajal po predvidenem načrtu; zasnovano in oblikovano je bilo izobraževalno gradivo za vse tri starostne skupine. Zaposleni so nudili strokovno pomoč javnosti prek telefonske linije za svetovanje, prek e-pošte in spletnih strani, kot predavatelji pa so sodelovali na različnih izobraževalnih dogodkih. Zaradi

epidemioloških razmer je bila izvedba seminarjev prestavljena v leto 2021. Večji del porabljenih sredstev je bil namenjen za pokrivanje stroškov dela zaposlenih, del pa tudi za tisk brošur. Za projekt je bilo leta 2020 na PP 200001 porabljenih 79.697,05 EUR, na postavki integralna sredstva PP 1271 materialni stroški pa 91,50 EUR.

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).

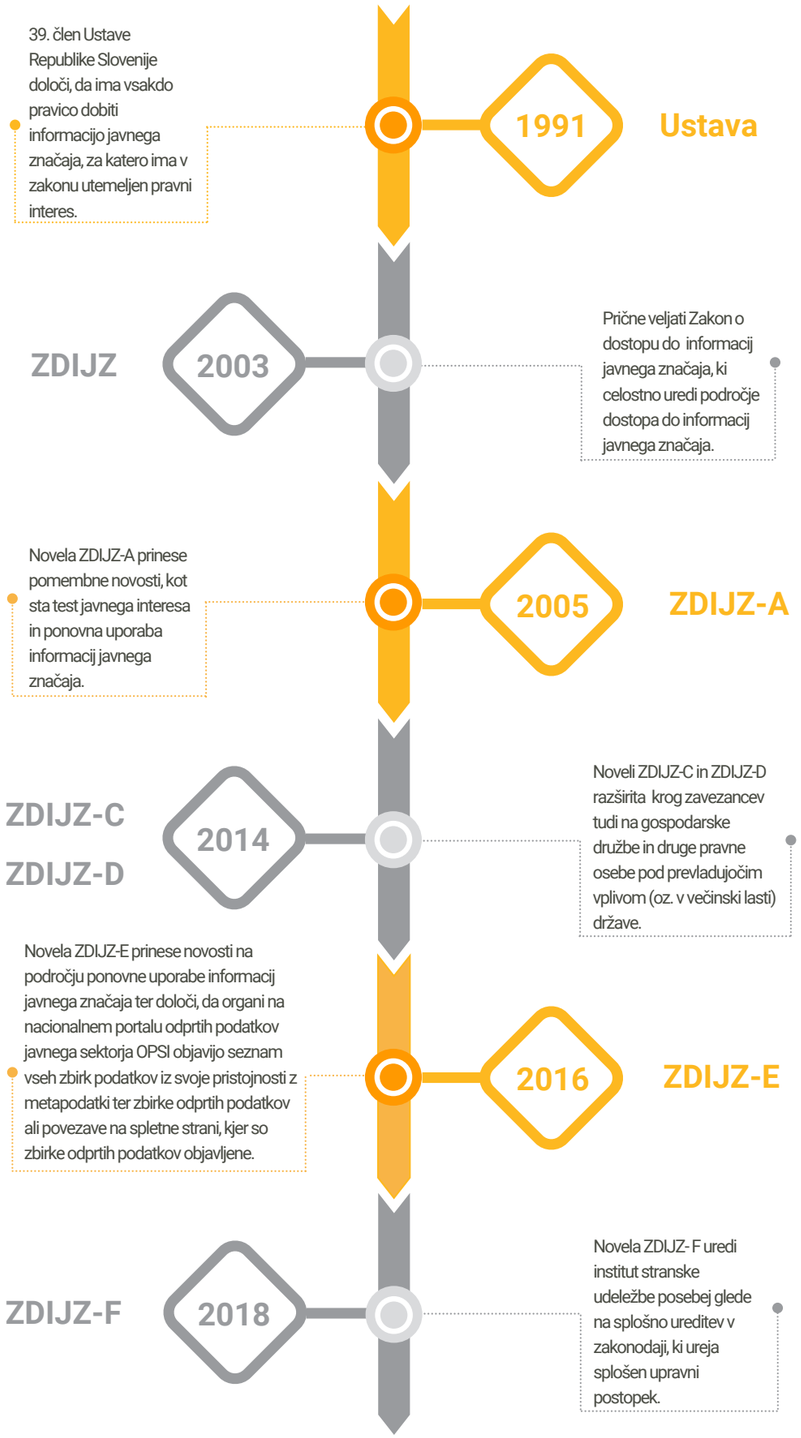
Leta 2005 je bil z novelo ZDIJZ-A narejen še korak naprej. Novela je namreč zožila možnost neupravičenega zapiranja dostopa do informacij in uvedla številne novosti, kot so ponovna uporaba informacij javnega značaja in pristojnosti upravne inšpekcije na področju izvajanja tega zakona. Najpomembnejša 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 a26.a določa, da je stranka v postopku z zahtevo za dostop do informacij 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. poenostavljeni 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 2020 je Informacijski pooblaščenec vodil 565 pritožbenih postopkov, od tega 331 postopkov zaradi zavrnitve dostopa do zahtevane informacije (med njimi je bilo 11 pritožbenih postopkov zoper poslovne subjekte pod prevladujočim vplivom oseb javnega prava) in 234 postopkov zaradi t. i. molka organa oz. neodzivnosti (med njimi so bili trije pritožbeni postopki zoper poslovne subjekte pod prevladujočim vplivom oseb javnega prava).

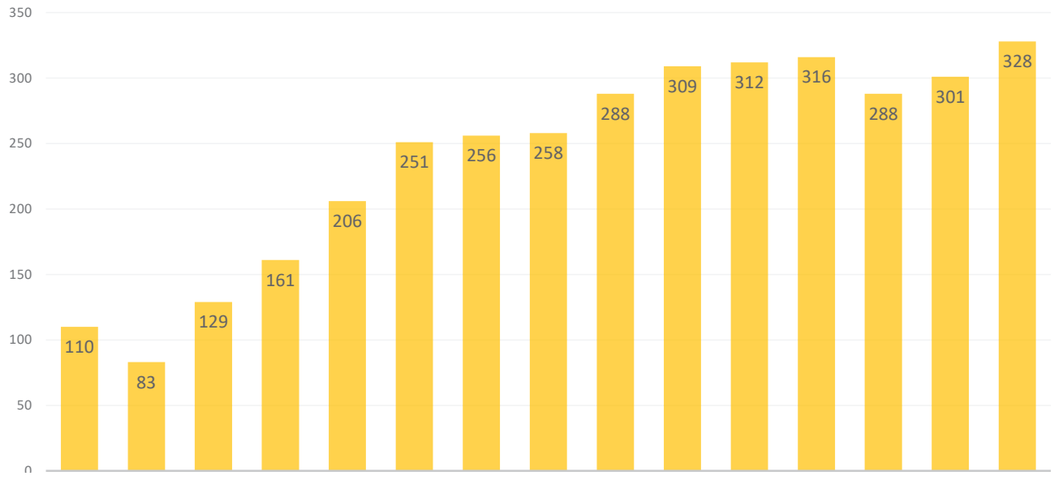
Leta 2020 je Informacijski pooblaščenec odgovoril na 411 pisnih prošenj za neformalno pomoč ali mnenje, ki jih je prejel od zavezancev prve stopnje in prosilcev, odgovoril pa je tudi na 632 zaprosil v okviru telefonskega dežurstva. Vsem je odgovoril v okviru svojih pristojnosti, največkrat jih je napotil 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 zavrnili zahteve po dostopu do informacij javnega značaja ali zahteve po njihovi ponovni uporabi, je Informacijski pooblaščenec v letu 2020 izdal 328 odločb, pet pritožb prosilcev je s sklepom zavrgel (pritožbe so bile nedovoljene), v dveh primerih pa je zaradi umika pritožbe prosilca izdal sklep o ustavitvi postopka. Informacijski pooblaščenec je tako izdal 281 odločb, ki so se nanašale na pritožbene postopke, začete v letu 2020, in 47 odločb, ki so se nanašale na postopke, začete pred letom 2020. Med reševanjem pritožb je na terenu opravil 34 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 (328):
- pritožbo zavrnil – 139,
- pritožbi delno ali v celoti ugodil oz. rešil zadevo v korist prosilca – 109,
- pritožbi ugodil in zadevo vrnil v ponovno odločanje prvostopenjskemu organu – 69,
- pritožbo zavrgel – 8,
- odločbo prvostopenjskega organa razglasil za nično – 3.

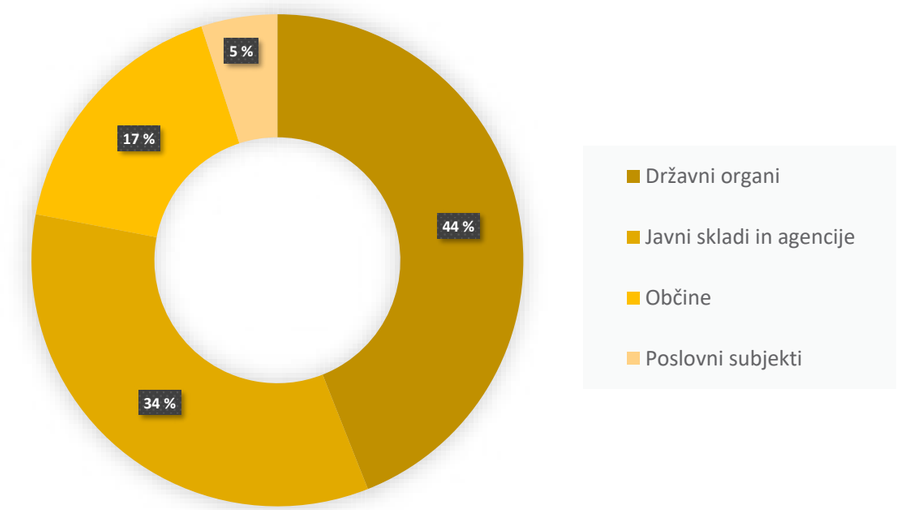
Število izdanih odločb na področju dostopa do informacij javnega značaja med letoma 2006 in 2020.



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

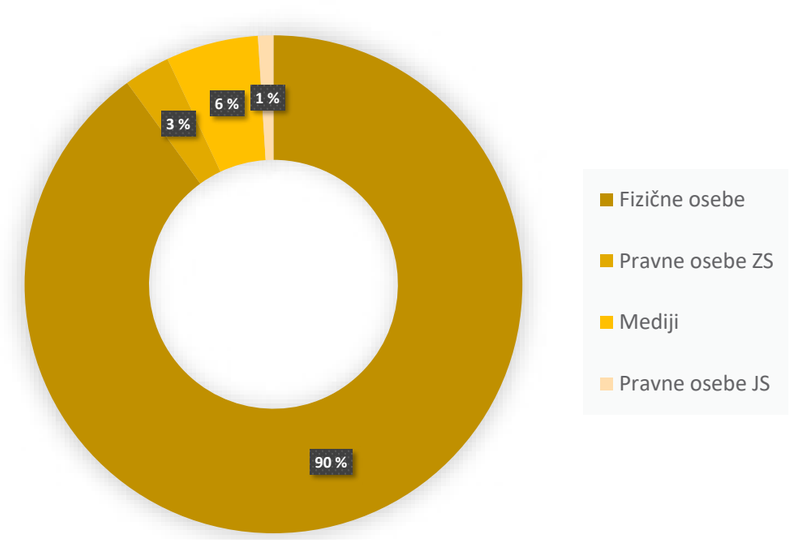
- državni organi – 146, od tega ministrstva in organi v sestavi ter upravne enote 104, sodišča, vrhovno državno tožilstvo in državno odvetništvo pa 42,
- javni skladi, zavodi, agencije, izvajalci javnih služb, nosilci javnih pooblastil in druge pravne osebe javnega prava – 111,
- občine – 56,
- poslovni subjekti pod prevladujočim vplivom države, občin ali drugih oseb javnega prava – 15.

Zoper katere zavezance so bile vložene pritožbe?



V 295 primerih so bili prosilci fizične osebe, v 10 primerih so se pritožile pravne osebe zasebnega sektorja, v 20 primerih novinarji in medijske hiše, trikrat pa so se pritožile pravne osebe javnega sektorja.

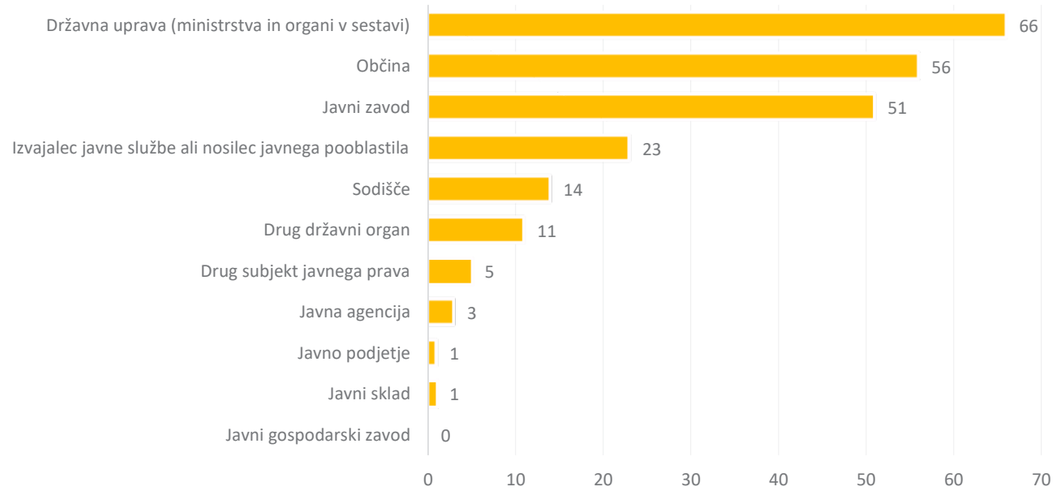
Pritožbe zoper zavrnitve dostopa do informacij.



2.2.2 PRITOŽBE ZOPER MOLK

Informacijski pooblaščenec je v letu 2020 prejel 231 pritožb zaradi molka organa in tri pritožbe zaradi neodziva poslovnih subjektov pod prevladujočim vplivom. Po podatkih je bilo največ molka med organi državne uprave (ministrstva, organi v sestavi itd.), in sicer 66, 56 med občinami ter 51 med javnimi zavodi. Informacijski pooblaščenec je zaznal tudi povečanje števila pritožb zoper sodišča (14).

Zoper katere zavezance so bile vložene pritožbe?



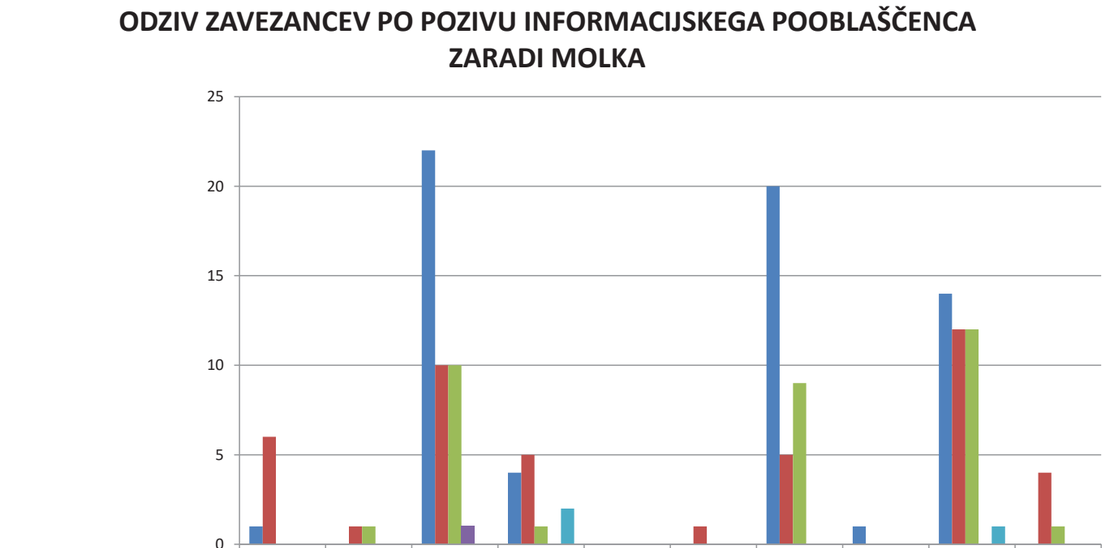
Po preizkusu formalnih predpostavk Informacijski pooblaščenec v 87 primerih postopka zaradi molka ni uvedel, in sicer je v 22 primerih pritožbo s sklepom zavrgel: v 17 primerih zaradi preuranjenosti, v enem primeru zaradi pomanjkljive vloge, ki je prosilec kljub pozivu k dopolnitvi ni dopolnil, v enem primeru zato, ker je vlogo vložila neupravičena oseba, in v treh primerih zato, ker pritožba ni bila dovoljena. V osmih primerih je prosilec tekom postopka pritožbo umaknil, saj je od zavezanca prejel zahtevano informacijo. Informacijski pooblaščenec v nobenem primeru ni prevzel pritožbe v odločanje in sam ni meritorno odločil. V eni zadevi je izdal sklep o ustavitvi, štiri zadeve pa ima Informacijski pooblaščenec še odprte in v postopku.

V 52 primerih je Informacijski pooblaščenec postopek z molkom zaključil tako, da je prosilcem pojasnil:

- da za reševanje njihove vloge ni pristojen, in jim svetoval, kako ravnati v zvezi z njihovo zahtevo,
- da vloga, ki so jo vložili pri zavezancu, ni formalno popolna,
- da zavezanci utemeljeno niso obravnavali njihove vloge po ZDIJZ, temveč na drugi pravni podlagi,
- da zaradi prekinitve teka rokov zaradi epidemije covid-19 roki po ZDIJZ ne tečejo.

V pritožbenih postopkih zaradi molka je Informacijski pooblaščenec v 144 primerih zavezance pozval, naj o zahtevi prosilca čim prej odločijo. Po pozivu Informacijskega pooblaščenca so v 62 primerih zavezanci prosilcu informacijo posredovali, v 44 primerih so prosilcu dostop zavrnili ter mu izdali zavrnilno odločbo, v 34 primerih pa so prosilcu le delno omogočili dostop (določene podatke so zakrili oz. omogočili dostop le do določenih informacij, dostop do preostalih pa so z odločbo zavrnili). V enem primeru so zavezanci zahtevo prosilca s sklepom zavrgli. V treh primerih so organi vlogo prosilca za dostop do dokumentov odstopili v reševanje drugemu organu.

Kako so ravnali zavezanci po pozivu Informacijskega pooblaščenca zaradi molka?



	Drug državni organ	Drug subjekt javnega prava	Državna uprava (ministrstva in organi v sestavi)	Izvajalec javne službe ali nosilec javnega pooblastila	Javna agencija	Javni sklad	Javni zavod	Javno podjetje	Občina	Sodišče
OMOGOČILI DOSTOP	1		22	4			20	1	14	
ZAVRNILNA ODLOČBA	6	1	10	5		1	5		12	4
DELNO OMOGOČILI		1	10	1			9		12	1
ORGAN S SKLEPOM ZAVRGEL			1							
ODSTOPIL DRUGEMU ORGANU				2					1	

2.3 ŠTEVILO VLOŽENIH TOŽB IN PREJETIH SODB

Pritožba zoper odločbo Informacijskega pooblaščenca ni dopustna, mogoče pa je sprožiti upravni spor. Leta 2020 je bilo na Upravnem sodišču RS vloženih 36 tožb zoper odločbe Informacijskega pooblaščenca (zoper 10,97 % izdanih odločb). Delež je relativno majhen, kar kaže na uveljavitev transparentnosti in odprtosti javnega sektorja, pa tudi na sprejemanje odločb Informacijskega pooblaščenca s strani zavezancev in prosilcev.

Upravno sodišče je leta 2020 odločilo o 17 tožbah, ki so bile vložene zoper odločbe Informacijskega pooblaščenca, in:

- tožbo zavrnilo – 11,
- tožbi ugodilo, izpodbijano odločbo oz. del odločbe odpravilo in zadevo vrnilo Informacijskemu pooblaščencu v ponovno odločanje – 3,
- tožbi ugodilo, izpodbijano odločbo odpravilo in zadevo vrnilo okrajnemu sodišču v ponovno odločanje – 1,
- tožbi delno ugodilo tako, da je v enem delu spremenilo izrek izpodbijane odločbe, v preostalem delu pa je tožbo zavrnilo – 1,
- tožbi v celoti ugodilo tako, da je v celoti spremenilo izrek izpodbijane odločbe – 1.

Leta 2020 je en zavezanec na Vrhovno sodišče RS vložil revizijo zoper sodbo Upravnega sodišča.

2.4 STORJENI PREKRŠKI PO ZDIJZ, ZInfP IN ZMed

Leta 2020 Informacijski pooblaščenec ni izdal nobene odločbe o prekršku zaradi kršitev določb ZDIJZ, ZInfP ali Zmed, je pa v zadevi pod opr. št. 090-112/2015 zoper Ekonomsko fakulteto v Ljubljani uvedel postopek izvršbe s prisilitvijo, ker zavezanec, kljub temu da je odločba Informacijskega pooblaščenca postala pravnomočna in izvršljiva že v letu 2016, prosilki še vedno ne želi posredovati informacij javnega značaja, kot mu je bilo naloženo.

2.5 IZBRANI PRIMERI NA PODROČJU DOSTOPA DO INFORMACIJ JAVNEGA ZNAČAJA

Zaposleni v javnih podjetjih niso javni uslužbenci, zato so njihovi osebni podatki varovani

Novinarka je od Javnega podjetja Marjetica Koper, d. o. o., želela prejeti odgovor na vprašanje, od kdaj je določen posameznik zaposlen pri organu in na katerem delovnem mestu je zaposlen. Organ ji na zastavljeno vprašanje ni želel odgovoriti zaradi varstva osebnih podatkov. Temu je prosilka v pritožbi nasprotovala in navedla, da gre za osebne podatke javnega uslužbenca, ki niso varovani, za razkritje teh podatkov naj bi bil podan tudi javni interes. V pritožbenem postopku je Informacijski pooblaščenec ugotovil, da je razkritje osebnih podatkov v postopku dostopa do informacij javnega značaja dopustno le, kadar gre za osebne podatke, ki hkrati pomenijo, npr. podatke, povezane z opravljanjem javne funkcije ali delovnega razmerja javnega uslužbenca (1. alineja tretjega odstavka 6. člena ZDIJZ). Po preučitvi zadeve je Informacijski pooblaščenec zaključil, da tovrstna pravna podlaga v obravnavanem primeru ne obstaja. Iz 1. člena Zakona o javnih uslužbencih namreč izhaja, da so javni uslužbenci posamezniki, ki so sklenili delovno razmerje v javnem sektorju, pri čemer javna podjetja in gospodarske družbe, v katerih ima večinski delež oz. prevladujoči vpliv država ali lokalna skupnost, niso del javnega sektorja po tem zakonu. To pomeni, da zaposleni v javnih podjetjih niso javni uslužbenci in posledično uporaba tretjega odstavka 6. člena ZDIJZ kot pravna podlaga za posredovanje njihovih osebnih podatkov javnosti ne pride v poštev. Po oceni Informacijskega pooblaščenca za razkritje varovanih osebnih podatkov tudi prevladujoč javni interes ni bil podan. Posameznik, na katerega se je nanašala zahteva, namreč ni bil niti absolutno javna oseba niti vodilni predstavnik javnega podjetja (npr. direktor). Prav tako prosilka ni izkazala, da bi bili zahtevani podatki povezani z delom javnega podjetja ali pomembni za širši krog uporabnikov javnih storitev, ki jih podjetje izvaja. Informacijski pooblaščenec je zato pritožbo zavrnil kot neutemeljeno.

KLJUČNE BESEDE: mediji, osebni podatek, test interesa javnosti, številka odločbe 090-277/2019

Prosilec ne more več kot enkrat zahtevati istih informacij javnega značaja, če so mu bile zahtevane informacije že posredovane

Novinarka je na Ministrstvo za kmetijstvo, gozdarstvo in prehrano naslovila vprašanje, ali je ministrica v povezavi z afero mleto meso že odredila napovedani notranji nadzor, kdo ga bo izvajal, kakšen je njegov namen in kdaj bodo znane ugotovitve. Organ je dostop do sklepa o imenovanju komisije za notranji nadzor nad delom Uprave RS za varno hrano, veterinarstvo in varstvo rastlin zavrnil s sklicevanjem na izjemi varstva tajnih podatkov (1. točka prvega odstavka 6. člena ZDIJZ) in notranje delovanje organa (11. točka prvega odstavka 6. člena ZDIJZ). Organ je navedel, da zahtevani sklep nosi oznako tajnosti INTERNO, poleg tega dokument vsebuje podatke o usmeritvi in nalogah imenovane komisije, ki še ni končala svojega dela, zato bi predčasno razkritje povzročilo motnje pri delovanju komisije in škodovalo izvedbi nadzora. Prosilka je v pritožbi oporekala oznaki tajnosti, saj zahtevani podatki niso s točno opredeljenih področij po Zakonu o tajnih podatkih. Oporekala je tudi prekrivanju podatkov o članih komisije za notranji nadzor, saj so to javni uslužbenci in mora biti delo take komisije transparentno, v prehranski aferi pa je izpolnjen tudi javni interes. V pritožbenem postopku je Informacijski pooblaščenec pri organu opravil ogled *in camera* ter ugotovil, da ima zahtevani dokument vidno oznako stopnje tajnosti INTERNO, ki jo je določila ministrica. Tekom pritožbenega postopka je Informacijski pooblaščenec ugotovil, da je organ spremenil svojo odločitev iz izpodbijane odločbe in prosilki zahtevano informacijo javnega značaja posredoval, ker so razlogi, zaradi katerih je dostop do zahtevane informacije z izpodbijano odločbo zavrnil, prenehali. Da je zahtevani sklep prejela, je potrdila tudi prosilka. Posledično prosilka v obravnavani zadevi ni imela več pravovarstvenega interesa, ker je organ njeni zahtevi za dostop do informacije javnega značaja že ugodil. Ker so bile zahtevane informacije prosilki posredovane in v pritožbenem postopku svojega pravnega položaja ni mogla več izboljšati, je Informacijski pooblaščenec njeno pritožbo zavrgel. Takšno stališče je zavzelo tudi sodišče v svojih odločitvah št. I U 1590/2010 in št. I U 1245/2010.

KLJUČNE BESEDE: mediji, kršitev postopka, številka odločbe 090-265/2019

Podatki o območju izkoriščanja cementnega laporja in apnenca so okoljski podatki, ki so absolutno javni

Prosilec je od Ministrstva za infrastrukturo zahteval dokument, ki prikazuje meje povečanega pridobivalnega prostora »Deskle-Lastivnica-Perunk«: situacijski načrt – mapna kopija z vrisanim kamnolomom in pridobivalnim prostorom. Organ je zahtevo zavrnil s sklicevanjem na poslovno skrivnost (2. točka prvega odstavka 6. člena ZDIJZ) in Zakon o rudarstvu, po katerem je zavezan s temi podatki ravnati kot s poslovno skrivnostjo. Prosilec se z zavrnitvijo dostopa ni strinjal, ker zahtevani dokument kot priloga k odločbi, ki jo je kot informacijo javnega značaja že prejel, predstavlja le dodatno pojasnilo, na katerem je v grafični obliki prikazano območje pridobivanja, ki je določeno v odločbi. Posredovanju zahtevanega dokumenta je nasprotovala tudi stranska udeleženka. Zatrjevala je, da podatek o območju kamnoloma ni okoljski podatek, ki bi ga kot javnega določal Zakon o varstvu okolja (ZVO-1). V pritožbenem postopku je Informacijski pooblaščenec ugotovil, da pri zahtevanih informacijah ne gre za podatke, ki bi bili poslovna skrivnost že po samem zakonu. Ker je stranska udeleženka sklep o poslovni skrivnosti sprejela po vložitvi zahteve za dostop do informacij javnega značaja, je Informacijski pooblaščenec zaključil, da ni izpolnjen subjektivni kriterij poslovne skrivnosti kot tudi ne pogoj občutne škode, ki ga zahteva objektivni kriterij poslovne skrivnosti. Poslovna skrivnost po ZDIJZ ni zavarovana absolutno, zato je Informacijski pooblaščenec v obravnavani zadevi presojal, ali je zahtevani dokument tudi okoljski podatek, ki je absolutno javen na podlagi 2. alineje tretjega odstavka 6. člena ZDIJZ. Zahtevani dokument predstavlja grafični prikaz mej povečanega pridobivalnega prostora »Deskle-Lastivnica-Perunk«, kjer se stranski udeleženki kot nosilki rudarske pravice dovoljuje izkoriščanje cementnega laporja in apnenca, ter se nanaša na območje izkoriščanja kamenin. Kamenine in mineralne snovi pa predstavljajo del okolja, kot ga definira 1.3. točka 3. člena ZVO-1. Glede na to, da zahtevani dokument vsebuje podatke o območju pridobivalnega prostora, na katerem je stranski udeleženki dovoljeno izkoriščanje teh kamenin, nedvomno vsebuje okoljske informacije. Informacijski pooblaščenec je zaključil, da so zahtevani podatki okoljski podatki in kot taki absolutno javni. Odločitev Informacijskega pooblaščenca je potrdilo tudi Upravno sodišče.

KLJUČNE BESEDE: okoljski podatki, poslovna skrivnost, številka odločbe 090-230/2019

Če obravnavani dokument ne ustreza vsebini zahtevanega dokumenta, ga ni moč šteti za predmet zahteve

Prosilec je od Komisije za preprečevanje korupcije želel prejeti zbirko podatkov, in sicer evidenco zadev s področja nesorazmerno povečanega premoženja iz 45. člena Zakona o integriteti in preprečevanju korupcije (ZIntPK). Organ je dostop do zahtevane evidence zavrnil, ker z njo ne razpolaga. ZIntPK sicer zahteva, da organ vodi evidenco zadev s področja nesorazmerno povečanega premoženja iz 45. člena ZIntPK, ki obsega: osebno ime, funkcijo oz. položaj zavezancev iz prvega odstavka 41. člena tega zakona, seznam obvestil po drugem odstavku 45. člena tega zakona, seznam obvestil iz četrtega odstavka 45. člena tega zakona, seznam sprejetih odločitev po petem odstavku 45. člena tega zakona in seznam ukrepov po šestem odstavku 45. člena tega zakona, vendar evidence s tovrstnimi podatki organ nima. Organ je podrobno pojasnil vse zakonske prepreke, ki onemogočajo vzpostavitev take evidence. Prosilec se z odločitvijo organa ni strinjal in je v pritožbi navedel, da Excelova tabela, ki jo je vzpostavila uslužbenka, ki ni več zaposlena pri organu, kljub morebitnim manjkajočim podatkom vsebinsko ustreza zahtevanemu dokumentu. V pritožbenem postopku je Informacijski pooblaščenec v celoti sledil argumentom organa, zato je pritožbo zavrnil kot neutemeljeno. Ključno je bilo dejstvo, da je v Excel tabelo organ vpisoval druge vrste podatkov, kot jih predvideva zakon, ostalih delov Excel tabele pa organ niti ni izpolnjeval. Prosilec je izrecno zahteval »Evidenco zadev s področja nesorazmerno povečanega premoženja iz 45. člena ZIntPK«, za katero je zakon določil vsebino oz. nabor podatkov, ki jih mora zajemati (enajsta alineja drugega odstavka 76. člena ZIntPK), zato je samo ta dokument, z zakonsko opredeljeno vsebino, predmet zahteve, na katero sta bila organ in Informacijski pooblaščenec tudi vezana. V Excel tabeli, s katero organ razpolaga, so bili vsebovani drugi podatki oz. podatki, ki jih enajsta alineja drugega odstavka 76. člena ZIntPK ne določa, zato je ni bilo mogoče obravnavati kot predmet zahteve niti z vidika »osnutka, delnega izdelka«. Pri Excel tabeli ni bilo ugotovljeno zgolj, da gre za »manjkajoče podatke«, temveč je bilo ugotovljeno, da vsebuje povsem druge podatke, kot jih predvideva zakon. Če organ, kot je pojasnil na ogledu *in camera*, ne izvaja postopkov po drugem, četrtem, petem in šestem odstavku 45. člena ZIntPK, je logično, da takšne evidence, kot jo predvideva zakon, ne more voditi. Informacijski pooblaščenec zato ni videl razloga, da ne bi sledil ugotovitvi organa, da z dokumentom ne razpolaga. Pritožbo je zavrnil kot neutemeljeno.

KLJUČNE BESEDE: ali dokument obstaja?, številka odločbe 090-23/2020

Transparentnost postopkov javnega naročanja se nadaljuje tudi po podpisu pogodbe z izbranim izvajalcem

Prosilec je od Družbe za avtoceste v Republiki Sloveniji, d. d., zahteval dokumente v zvezi z javnim naročilom elektronskega cestninskega sistema. Organ je zahtevo delno zavrnil s sklicevanjem na poslovno skrivnost (2. točka prvega odstavka 6. člena ZDIJZ) in izjemo varstva osebnih podatkov (3. točka prvega odstavka 6. člena ZDIJZ). Organ se je opredelil do vsakega posameznega zahtevanega dokumenta tako z vidika obstoja izjeme poslovne skrivnosti kot varstva osebnih podatkov. Prosilka je v pritožbi zatrjevala, da bi moral organ izjemo poslovne skrivnosti presojati po Zakonu o poslovni skrivnosti (ZPosS) in ne po materialnem pravu, veljavnem v času, ko je zahtevani dokument nastal. Prav tako se ni strinjala s prekritjem določenih osebnih podatkov. Informacijski pooblaščenec je v pritožbenem postopku ugotovil, da je organ glede določenih dokumentov dostop neutemeljeno zavrnil, saj izjema poslovne skrivnosti ni bila izkazana ali pa je šlo za podatke, ki so izkazovali porabo javnih sredstev oz. izpolnjevanje pogojev v postopku javnega naročanja. Ker je Informacijski pooblaščenec še posebej poudaril, da se s podpisom pogodbe z izbranim izvajalcem v postopku javnega naročanja transparentnost postopka ne konča, temveč bi lahko rekli, da se glavni nadzor z izborom šele začenja, ima javnost pravico pridobiti tudi podatke o tem, ali izbrani izvajalec dejansko izpolnjuje pogodbene obveznosti, za katere se porabljajo javna sredstva, v nasprotnem primeru mu namreč javna sredstva ne pripadajo oz. nastopijo okoliščine v skladu s pogodbo (npr. pogodbene kazni, škoda ipd.). Tako je npr. odobril dostop do dokumentov, ki so v neposredni zvezi z izvrševanjem sklenjene pogodbe (npr. aneks k pogodbi, cenik rezervnih delov), dostop do dokumentov, ki so vselej javni po ZJN-2 in tudi po ZJN-3 (npr. specifikacija storitev in blaga), dostop do dokumentov, ki poleg meril razpisne dokumentacije vsebujejo tudi pogoje (npr. ponudbe za aneks, obrazložitev in opis sprememb, ki jih je na podlagi zahtev naročnika pripravil ponudnik in se nanašajo na opise sprememb pogodbenih del), dostop do dokumentov, ki poleg skupne vrednosti investicijskih in operativnih stroškov vsebujejo tudi podatke o ločenih stroških, dostop do dokumentov, ki izkazujejo izpolnjevanje pogodbenih obveznosti (npr. podatki o testiranju in funkcionalnem preizkusu delovanja sistema), dostop do dokumentov, ki jih je organ ustvaril na podlagi 95. člena ZJN-3 in se nanašajo na izvajanje pogodbe, sklenjene v okviru javnega naročila

(npr. zapisnik o izvedenih pogajanjih), dostop do dokumentov, ki izkazujejo ugotovitve organa kot naročnika, ali je izvajalec opravil in uspešno izpolnil svoje pogodbene obveznosti za vzpostavitev sistema (npr. potrdilo o uspešno izvedenih testiranjih). Informacijski pooblaščenec je pritrdil odločitvi organa v tistih delih zahtevane dokumentacije, kjer je naročnik predvidel »prosti tekst« in podatki niso izkazovali izpolnjevanja pogojev razpisa. Tako je za varovane osebne podatke npr. štel življenjepise ključnega osebja, ki bo izvajalo pogodbena dela, ker niso bili zahtevani posebni pogoji (npr. izkušnje, reference, izobrazba ipd.). Za varovane osebne podatke je štel tudi osebna imena predstavnikov naročnika in izvajalca ter osebe, ki je pisala zapisnik, osebna imena posameznikov, ki so zaposleni pri organu ali izvajalcu oz. pogodbenih partnerjih. Za poslovno skrivnost je štel vse tiste dokumente, ki niso predstavljali izpolnjevanja razpisnih pogojev ali meril. Informacijski pooblaščenec je pri tem poudaril, da izjeme poslovne skrivnosti, če je ta izkazana, ni mogoče v celoti spregledati, še posebej v delu, kadar je javno naročilo, tako kot v obravnavanem primeru, »usmerjeno« na »prosti tekst« s ciljem, da ponudnik izkaže inovativnost pri predlaganju določenih rešitev, tehnično, organizacijsko in razvojno znanje. Kjer je šlo za podatke, ki so bili rezultat vseh prednosti, izkušenj, opreme, kadrovske usposobljenosti ter organizacije pri izvajalcu, je Informacijski pooblaščenec menil, da je poleg subjektivnega kriterija izkazan tudi objektivni kriterij poslovne skrivnosti. Enako je odločil za dokumente, ki vsebujejo podrobne tehnične informacije in rešitve, ki so plod tehničnega znanja v zvezi z relevantno tehnologijo. V obravnavani zadevi je Informacijski pooblaščenec tako pritožbi delno ugodil.

KLJUČNE BESEDE: javna naročila, poslovna skrivnost, številka odločbe 090-11/2020

Letne ocene javnih uslužbencev so prosto dostopne informacije javnega značaja

Prosilec je od Urada Vlade RS za oskrbo in integracijo migrantov zahteval posredovanje informacije o letnih ocenah javnih uslužbencev znotraj organa za leti 2017 in 2018 (samo ime in ocena, brez obrazložitve). Organ je zahtevo zavrnil z argumentom, da z dokumentom »Informacija o letnih ocenah javnih uslužbencev organa za leti 2017 in 2018«, iz katere bi izhajali zaprošeni podatki (ime javnega uslužbenca in njegova ocena), ne razpolaga. Prosilec je v pritožbi poudaril, da je bila z zahtevo organu prepuščena izbira vira in načina podajanja zahtevane informacije, zato je bila zavrnitev neutemeljena. Pristop organa je bil po mnenju prosilca v nasprotju z načeli dostopnosti informacij javnega značaja, saj je organ v izpodbijani odločbi ugotovil, da so dokumenti, iz katerih je bilo te informacije mogoče razbrati, pri organu obstajali. V pritožbenem postopku je Informacijski pooblaščenec organ pozval, da mu dostavi zahtevane dokumente. Organ je posredoval seznam vseh zaposlenih in njihove ocene. Informacijski pooblaščenec je ugotovil, da je organ razpolagal s 27 letnimi ocenami javnih uslužbencev za leto 2017 in s 27 letnimi ocenami javnih uslužbencev za leto 2018. Organ se v konkretnem primeru pri tolmačenju zahteve ne bi smel omejiti le na dokument, poimenovan kot »Informacija o letnih ocenah javnih uslužbencev organa za leto 2017 in 2018«, ampak bi moral zahtevo prosilca tolmačiti širše. Širše razumevanje zahteve prosilca je Informacijskega pooblaščenca privedlo do ugotovitve drugačnega dejanskega stanja, kot je izhajalo iz izpodbijane odločbe. Z dokumenti o zahtevanih informacijah je organ razpolagal, pri čemer informacije niso sodile med varovane osebne podatke. ZDIJZ dostop do osebnih podatkov dovoli, če gre za podatke o porabi javnih sredstev ali za podatke, povezane z opravljanjem javne funkcije ali delovnega razmerja javnega uslužbenca (1. alineja tretjega odstavka 6. člena ZDIJZ). V kontekstu te določbe se podatki o imenih, priimkih in ocenah javnih uslužbencev ne štejejo med varovane osebne podatke, saj gre za podatke, ki so v neposredni povezavi z opravljanjem delovnega razmerja javnega uslužbenca. Prav tako imajo za posledico potencialno porabo javnih sredstev, saj se o pravici javnega uslužbenca do napredovanja odloča prav na podlagi treh letnih ocen. Informacijski pooblaščenec je tako pritožbi prosilca ugodil in odločil, da mu mora organ posredovati elektronske kopije letnih ocen javnih uslužbencev organa za leto 2017 (27 ocen) in 2018 (27 ocen) na način, da bodo iz njih razvidni ime, priimek in skupna letna ocena posameznega javnega uslužbenca.

KLJUČNE BESEDE: javni uslužbenci, osebni podatki, številka odločbe 090-55/2020

Oskrba zapuščenih živali sodi v okvir izvajanja javne službe, zato so ti podatki informacije javnega značaja

Prosilka je od Zavetišča Zonzani, d. o. o., zahtevala podatke o psu po evidenčni številki, in sicer status psa (oddan ali evtanaziran), kopijo kartoteke (brez čipa in potnega lista) in račun, ki je bil izstavljen. Organ je prosilki posredoval anonimizirano odločbo Uprave RS za varno hrano, veterinarstvo in varstvo rastlin, dostop do preostalih podatkov pa zavrnil, ker ne gre za informacije javnega značaja, ki bi jih bil dolžan posredovati kot

subjekt pod prevladujočim vplivom oseb javnega prava (4.a člen ZDIJZ). Prosilka je vložila pritožbo in navedla, da ni zahtevala nobenih osebnih podatkov ali podatkov, ki bi bremenili kakšno osebo, zato je pričakovala, da bo njeni pritožbi ugodeno. Informacijski pooblaščenec je štel obvestilo organa kot zavrnilno odločbo. V obravnavanem primeru je bilo sporno, ali je zahtevane informacije mogoče šteti v delovno področje organa v okviru njegove zavezanosti po ZDIJZ. Informacijski pooblaščenec je ugotovil, da organ kot izvajalec javne službe zagotavljanja zavetišča za zapuščene živali sodi med organe, ki so zavezanci po prvem odstavku 1. člena ZDIJZ in ne 1.a člena, kot je zatrjeval organ. Zakon o zaščiti živali (ZZZiv) določa, da je zagotovitev zavetišča lokalna zadeva javnega pomena, ki se izvršuje kot javna služba. Tako ni bilo dvoma, da zavetišče, na katerega občina s pogodbo prenese izvajanje določenega dela ali vseh nalog javne službe zagotavljanja zavetišča za zapuščene živali, postane izvajalec javne službe, torej izvajalec javnopravnih nalog. V obravnavanem primeru nedvomno ni šlo za subjekt pod prevladujočim vplivom oseb javnega prava, ki po definiciji predstavlja tisto gospodarsko družbo in druge pravne osebe zasebnega prava, ki so pod neposrednim ali posrednim prevladujočim vplivom, posamično ali skupaj, Republike Slovenije, samoupravnih lokalnih skupnosti in drugih oseb javnega prava. Pri konkretnem zavetišču gre za povsem zasebno družbo. Tudi iz Registra zavezancev za informacije javnega značaja je bilo razvidno, da je bil organ vanj vpisan kot izvajalec javne službe na podlagi pogodbe o izvajanju dejavnosti oskrbe in namestitve zapuščenih živali. Ker je v obravnavanem primeru prosilka zahtevala informacije (brez osebnih podatkov), ki so nastale v okviru izvajanja javne službe organa, je Informacijski pooblaščenec odločil, da gre za prosto dostopne informacije javnega značaja. Pritožbi prosilke je tako ugodil in organu odredil, da ji posreduje zahtevane dokumente na način, da prekrije podatke, ki jih ni zahtevala.

KLJUČNE BESEDE: ali spada v delovno področje?, ali je organ zavezanec?, številka odločbe 090-70/2020

Ravnanje policije v primeru migrantske politike je v javnem interesu

Prosilec je od Ministrstva za notranje zadeve zahteval dostop do vseh poročil o nadzoru nad policijo, ki jih je organ izdal v letu 2019. Organ je kot predmet zahteve prepoznal dve poročili, in sicer (1) Redni nadzor nad spoštovanjem človekovih pravic v postopkih z ilegalnimi migranti in (2) Redni nadzor nad izvajanjem policijskih pooblastil pri varovanju državne meje. Organ je dostop do zahtevanih dokumentov zavrnil s sklicevanjem na izjemo varstva tajnih podatkov (1. točka prvega odstavka 6. člena ZDIJZ), saj sta bili obe poročili označeni s stopnjo tajnosti INTERNO. Prosilec je vložil pritožbo in zahteval, da Informacijski pooblaščenec presodi, ali je označba stopnje tajnosti na dokumentih ustrezna. Informacijski pooblaščenec je zaprosil tudi za izvedbo testa javnega interesa. V pritožbenem postopku je Informacijski pooblaščenec ugotovil, da so bili glede zahtevanih poročil izpolnjeni tako materialni kot formalni pogoji za tajne podatke in je bila posledično tudi podana izjema varstva tajnih podatkov. Ob izvedbi testa prevladujočega interesa javnosti je Informacijski pooblaščenec ugotovil, da je njegovo izvajanje v konkretnem primeru dovoljeno, saj sta bila dokumenta označena z najnižjo stopnjo tajnosti (INTERNO). V obravnavanem primeru so razlogi za varovanje zahtevanih podatkov izhajali iz ocene možnih škodljivih posledic, vendar je pri tehtanju, ali javni interes za njihovo razkritje prevlada, Informacijski pooblaščenec upošteval vsebino obeh poročil (tj. nadzor nad delom policije in ugotovljene pomanjkljivosti v zvezi z izvajanjem policijskih pooblastil pri nadzoru državne meje in v postopkih z ilegalnimi migranti). Javnost ima pravico, da se seznani z informacijami o tem, ali policija izvaja naloge zakonito, enotno, predvidljivo, in če jih ne, kje so bile ugotovljene pomanjkljivosti ter kakšni so predlagani ukrepi. Informacije, iz katerih izhaja, kako policija izvaja policijska pooblastila in kakšne pomanjkljivosti so bile v zvezi s tem ugotovljene, so torej v javnem interesu. Ustrezna javna razprava o tem vprašanju je mogoča le ob dostopnosti vseh relevantnih informacij, zato je pomembno, da se javnost z njimi seznani. Informacijski pooblaščenec je opravil presojo sorazmernosti in omogočil dostop le do tistih delov obeh poročil, ki navajajo zakonske in podzakonske podlage za delovanje policije in kažejo na skupne ugotovitve in predlagane ukrepe v zvezi z ugotovljenimi pomanjkljivostmi, pri čemer z razkritjem teh delov zahtevanih poročil ne more priti do razkritja posebnih metod in tehnik dela policije. Tako je Informacijski pooblaščenec pritožbi prosilca delno ugodil in organu naložil, da iz zahtevanih poročil delno umakne stopnjo tajnosti INTERNO ter ju v tem delu posreduje prosilcu.

KLJUČNE BESEDE: tajni podatki, test interesa javnosti, številka odločbe 090-38/2020

Prosilci so upravičeni do dokumentov in ne zgolj do izpisov podatkov

Prosilec je od Elektra Maribor Energija plus, d. o. o., zahteval pogodbo o sodelovanju med zavezancem ter subjektom, ki se ukvarja z izterjavo, anekse k pogodbi ter informacijo o skupnem znesku, ki je bil izplačan subjektu. Ker je zavezanec poslovni subjekt pod prevladujočim vplivom oseb javnega prava, je prosilcu posredoval višino izplačil družbi Izterjava, d. o. o., in pogodbo o upravljanju terjatev v tistih delih, za katere je menil, da so absolutno javni podatki. Glede ostalih delov pogodbe je dostop zavrnil s sklicevanjem na poslovno skrivnost (2. točka prvega odstavka 6. člena ZDIJZ). Prosilec je v pritožbi oporekal temu, da prekriti deli predstavljajo poslovno skrivnost; s predmetno pogodbo se je želel seznaniti v celoti. Informacijski pooblaščenec je v pritožbenem postopku ugotovil, da je vsebina zahtevane pogodbe s pogodbenim določilom in internim aktom zavezanca določena kot poslovna skrivnost po subjektivnem kriteriju (prvi odstavek 39. člena ZGD-1). Glede na to, da je bila zahtevana pogodba podpisana avgusta 2018, torej pred uveljavitvijo Zakona o poslovni skrivnosti, ki je stopil v veljavo aprila 2019, je Informacijski pooblaščenec pri presoji poslovne skrivnosti upošteval določbi 39. in 40. člena ZGD-1, ki sta veljali v času nastanka zahtevanih podatkov. Kot veleva ZDIJZ, so pri subjektu pod prevladujočim vplivom absolutno javni podatki o vrsti posla, pogodbenem partnerju, pogodbeni vrednosti in višini posameznih izplačil, datumu in trajanju posla ter enaki podatki iz morebitnega aneksa k pogodbi. Informacijski pooblaščenec je ugotovil, da je zavezanec prosilcu posredoval dele zahtevane pogodbe, ki izkazujejo podatke o vrsti posla, pogodbenem partnerju ter datumu in trajanju posla, ni pa mu posredoval podatka o pogodbeni vrednosti in višini posameznih izplačil. Glede na to, da je bila vsebina zahtevane pogodbe tudi določilo glede pogodbene vrednosti (podatkov o višini posameznih izplačil pogodba ni vsebovala), je Informacijski pooblaščenec zavezancu odredil, da prosilcu posreduje tudi ta podatek. Pri tem je Informacijski pooblaščenec vztrajal pri ustaljeni praksi, da je prosilec upravičen do dokumenta samega (in ne zgolj do izpisa podatkov, ki jih na podlagi zahtevanega dokumenta pripravijo zavezanci).

KLJUČNE BESEDE: poslovni subjekt pod prevladujočim vplivom, poslovna skrivnost, številka odločbe 09021-2/2020

Mnenje etične komisije bolnišnice je bilo delno razkrito zaradi pomembnosti tematike, ki je tudi v javnem interesu

Prosilec je od Splošne bolnišnice dr. Franca Derganca Nova Gorica želel prejeti mnenje etične komisije glede vnaprejšnjega ocenjevanja oz. »triažiranja« vseh prebivalcev v domovih za starejše. Organ je zahtevo zavrnil s sklicevanjem na izjemo varstva osebnih podatkov (3. točka prvega odstavka 6. člena ZDIJZ) in izjemo notranjega delovanja organa (11. točka prvega odstavka 6. člena ZDIJZ). Pojasnil je, da zaprošeni dokument vsebuje podrobne vsebinske razprave, iz katerih izhajajo osebna mnenja, pogledi in stališča ter odnos posameznih članov bolnišnične etične komisije do obravnavane teme, kar predstavlja varovane osebne podatke. Iz zahtevanega dokumenta je tako razvidno, kakšno je bilo mnenje posameznega člana, kdo od članov je kaj povedal in kakšna so bila individualna stališča do obravnavane teme. Prosilec se je zoper odločitev pritožil in navedel, da so informacije o aktivnosti triaže, ki so efektivno pomenile vnaprejšnjo klasifikacijo stanovalcev na tiste, ki naj bi v primeru obolelosti dobili »pravico« do zdravljenja v bolnišnici, ter tiste, ki je ne bi, v javnem interesu. Prosilec se ni strinjal, da iz zahtevanega dokumenta ni možno izločiti varovanih podatkov in da delni dostop ni mogoč. Informacijski pooblaščenec je v pritožbenem postopku ugotovil, da so osebni podatki članov etične komisije v zahtevanem dokumentu navedeni v zvezi z opravljanjem njihove javne funkcije, zato niso varovani (1. alineja tretjega odstavka 6. člena ZDIJZ). Etična komisija je tematiko v zahtevanem dokumentu obravnavala v okviru izvajanja nalog, ki jih določata sklep o imenovanju in poslovnik etične komisije, zato se ti podatki v zahtevanem dokumentu pojavljajo v zvezi z izvajanjem teh (javnopravnih) nalog in ne v zasebnem svojstvu tam navedenih posameznikov. Prav tako zahtevani dokument ni vseboval nobenih osebnostnih značilnosti posameznikov – članov etične komisije niti njihovega vedenja, čustev in odnosa do določene tematike. Ker je zahtevani dokument vseboval stališča posameznih članov etične komisije, ki so o zadevni temi razpravljali na za javnost zaprti seji, je Informacijski pooblaščenec ugotovil, da so izpolnjeni pogoji za obstoj izjeme notranjega delovanja organa. Vendar ob tem ni bilo mogoče slediti stališču organa, da je treba iz tega razloga dostop v celoti zavrniti in da delni dostop (7. člen ZDIJZ) do zahtevanega dokumenta ni mogoč. Kot relevantno okoliščino za razkritje je Informacijski pooblaščenec upošteval pomembnost tematike, ki je bila obravnavana, in sicer z vidika posledic, ki jih ima za uporabnike zdravstvenih storitev in za javnost na splošno. Informacijski pooblaščenec je ocenil, da se s prekritjem podatkov o identiteti razpravljavcev lahko zavarujejo podatki, ki predstavljajo notranje delovanje (podatki o tem, kdo je izrazil določeno mnenje), medtem ko odločitev komisije in vsebina razmišljanja nista

varovana (ker iz tega izhajajo vsebinski razlogi za sprejete sklepe). Test prevladujočega interesa javnosti je Informacijski pooblaščenec tako izvedel v okviru presoje izjeme notranjega delovanja in instituta delnega dostopa. Pritožbi prosilca je delno ugodil.

KLJUČNE BESEDE: osebni podatek, javni uslužbenci, test interesa javnosti, številka odločbe 090-140/2020

Mnenje etične komisije bolnišnice sodi v sfero, povezano z delovnim razmerjem javnega uslužbenca, zato je prosto dostopno

Prosilka je od Splošne bolnišnice Slovenj Gradec želela prejeti mnenje etične komisije o izjavah njenega direktorja na družbenem omrežju Twitter. Organ je zahtevo zavrnil s sklicevanjem na varstvo osebnih podatkov. Navedel je, da zahtevani dokument kot celota predstavlja etično presojo izjav direktorja na družbenem omrežju, sama vsebina pa so varovani osebni podatki, ker je šlo za izrazito osebne izpovedi članov etične komisije, za njihova osebna mnenja oz. stališča glede izjav direktorja, ki se kot takšna nanašajo na točno določeno osebo. Prosilka se je na odločitev pritožila, ker so bile predmet presoje etične komisije izjave direktorja bolnišnice, ki so vodile do njegovega odstopa s funkcije, podatki pa so bili v zvezi z delovnim razmerjem oz. z opravljanjem javne funkcije in zato niso bili varovani. Informacijski pooblaščenec je v pritožbenem postopku ugotovil, da iz zahtevanega mnenja etične komisije niso bili razvidni osebni podatki članov etične komisije niti njihova osebna stališča in odnos do obravnavane tematike. Zahtevano mnenje je vsebovalo le osebne podatke o javnem uslužbencu, na katerega se je mnenje nanašalo, ter osebni imeni predsednika etične komisije in strokovne direktorice, ki ji je bilo mnenje posredovano. Informacijski pooblaščenec tako ni sledil stališču organa, da bi z javnim razkritjem zahtevanega mnenja posegli v integriteto članov komisije in v integriteto bolnišnice, ker je šlo za izrazito osebne izpovedi članov etične komisije, za njihova osebna mnenja oz. stališča glede izjav direktorja na družbenem omrežju. Ker iz zahtevanega mnenja sama razprava, osebni pogledi ali izjave prisotnih niso bili razvidni, pri tem pa je končno stališče etične komisije glede opisanega ravnanja predstavljalo podatek, ki je spadal v sfero, povezano z delovnim razmerjem javnega uslužbenca, je Informacijski pooblaščenec zaključil, da je zahtevano mnenje prosto dostopno.

KLJUČNE BESEDE: osebni podatek, javni uslužbenci, številka odločbe 090-143/2020

Odpravnina, ki pripada direktorju javnega podjetja, je absolutno javen podatek

Novinar je na podlagi Zakona o medijih na javno podjetje Mariborski vodovod, d. d., naslovil vprašanje, kolikšna odpravnina pripada direktorju po sporazumu o prekinitvi pogodbe in kolikšna po pogodbi o poslovodenju. Organ je prosilca glede podatkov o pogodbeni vrednosti odpravnine napotil na svojo spletno stran. Dostop do podatkov o višini odpravnine po sporazumu je zavrnil s sklicevanjem na izjemo poslovne skrivnosti (2. točka prvega odstavka 6. člena ZDIJZ). Prosilec se je na odgovor organa pritožil, saj pogodba o zaposlitvi oz. poslovodenju in podatek o višini odpravnine direktorju javnega podjetja v 100-odstotni občinski lasti ne moreta nositi oznake zaupno. V pritožbenem postopku je Informacijski pooblaščenec ugotovil, da je bila pritožba zoper zavrnilni odgovor dovoljena, saj je zavrnilni oz. delno zavrnilni odgovor na vprašanje izhajal iz dokumenta, zadeve, dosjeja, registra, evidence ali drugega dokumentarnega gradiva. Glede obstoja poslovne skrivnosti je Informacijski pooblaščenec ugotovil, da je zahtevani podatek označen kot poslovna skrivnost, vendar organ ni izkazal, da ima ta podatek zanj tržno vrednost oz. da gre za informacijo, ki ni splošno znana ali lahko dosegljiva osebam v krogih, ki se običajno ukvarjajo s to vrsto informacij. Po prvem odstavku 2. člena Zakona o poslovni skrivnosti (ZPosS) pojem poslovne skrivnosti namreč zajema nerazkrito strokovno znanje, izkušnje in poslovne informacije, ki izpolnjujejo naslednje zahteve: (a) je skrivnost, ki ni splošno znana ali lahko dosegljiva osebam v krogih, ki se običajno ukvarjajo s to vrsto informacij, (b) ima tržno vrednost, (c) imetnik poslovne skrivnosti je v danih okoliščinah razumno ukrepal, da jo ohrani kot skrivnost. Tako v konkretnih okoliščinah niso bili izpolnjeni pogoji za poslovno skrivnost. Ne glede na to pa se po ZPosS za poslovno skrivnost ne morejo določiti informacije, ki so po zakonu javne, ali informacije o kršitvi zakona ali dobrih poslovnih običajev. Tako je Informacijski pooblaščenec ocenil, da je podatek o bruto višini odpravnine podatek o porabi javnih sredstev in kot tak absolutno javen po 1. alineji tretjega odstavka 6. člena ZDIJZ.

KLJUČNE BESEDE: poslovna skrivnost, številka odločbe 090-187/2020

Seznanitev javnosti z oceno možnih škodljivih posledic, s katero je določena tajnost odredb o spremljanju mednarodnih sistemov zvez, ne more povzročiti motenj pri delovanju organa

Prosilec je od Slovenske obveščevalno-varnostne agencije želel pridobiti ocene možnih škodljivih posledic, s katerimi je določena tajnost odredb o spremljanju mednarodnih sistemov zvez med letoma 2012 in 2020. Organ je zahtevo zavrnil s sklicevanjem na varstvo notranjega delovanja oz. dejavnosti organa (11. točka prvega odstavka 6. člena ZDIJZ). Navedel je, da ocena možnih škodljivih posledic ni označena s stopnjo tajnosti. Vendar kot obvezna priloga dokumentarnemu gradivu organa, ki je označeno z ustrezno stopnjo tajnosti, predstavlja sestavni del dokumentacije, ki je označena s stopnjo tajnosti in je bila sestavljena v zvezi z notranjim delovanjem oz. dejavnostjo organa, njeno razkritje pa bi povzročilo motnje pri delovanju oz. dejavnosti organa. Da lahko organ izvaja svoje pristojnosti oz. naloge, ima v skladu z Zakonom o Slovenski obveščevalno-varnostni agenciji (ZSOVA) urejena določena področja delovanja, med katera sodijo tudi posebne oblike pridobivanja podatkov in konkretno spremljanje mednarodnih sistemov zvez. Dokumenti organa, v katerih so neposredno ali posredno navedene kakršne koli informacije o izvajanju nalog organa, bi nepoklicanim osebam, med katerimi so lahko tudi pripadniki tujih obveščevalnih služb, razkrili podatke, iz katerih izhaja postopek oz. način dela organa na področju spremljanja mednarodnih sistemov zvez. Ocena je obvezna priloga dokumentom, ki vsebujejo tajne podatke, in je tako neločljivo povezana z dokumenti, katerih tajnost se z njo določa in varuje. V konkretnem primeru zahteve sploh ni mogoče obravnavati v skladu z ZDIJZ, saj je ZDIJZ v tem segmentu v koliziji z 19. členom Zakona o tajnih podatkih (ZTP), pri čemer je treba upoštevati 19. člen kot specialno določbo, ki ureja specifično področje. Prosilec se je zoper odločitev organa pritožil, saj zaprošene ocene možnih škodljivih posledic po dosedanji praksi uporabe ZTP ne morejo oz. ne smejo vsebovati tajnih podatkov, kot jih opredeljuje ZTP. Zato tudi dejstvo, da so pisne ocene osnova za določitev tajnih podatkov oz. priloga dokumenta, ki vsebuje tajni podatek, v povezavi z 19. členom ZTP ni in ne more biti pravno pomembno. Ključen pomen in namen pisne ocene možnih škodljivih posledic (t. i. škodnega testa) je torej možnost nadzora, da tajnost ni uporabljena zato, da bi se skrivalo in prikrivalo nezakonita ravnanja, zlorabo oblasti oz. bi se onemogočalo pridobivanje informacij javnega značaja ter učinkovit nadzor tudi javnosti nad zakonitostjo in ustavno skladnostjo delovanja oblastnih organov ter nosilcev javnih funkcij in upravljavcev javnih zadev. Informacijski pooblaščenec je pri organu opravil ogled *in camera*. V pritožbenem postopku je ugotovil, da obstaja ena takšna ocena možnih škodljivih posledic, ki pa ni označena z nobeno stopnjo tajnosti, kar pomeni, da sama ocena možnih škodljivih posledic ni tajni podatek. Ker predmet zahteve za dostop do informacij javnega značaja ni tajni podatek, tudi 19. člena ZTP v obravnavani zadevi ni bilo mogoče upoštevati kot posebno ureditev. Ta določba je namreč relevantna samo v primeru tajnih podatkov. Informacijski pooblaščenec se ni strinjal z organom, da zahtevani dokument izpolnjuje pogoje za obstoj izjeme notranjega delovanja organa. Pisna ocena možnih škodljivih posledic praviloma ni dokument, ki bi bil sestavljen samo v zvezi z notranjim delovanjem oz. dejavnostjo organa, saj ni namenjen izključno uslužbencem organa (ne gre za dokument, ki bi bil izdelan le zaradi nekih notranjih potreb organa oz. zaradi oblikovanja stališč v zvezi z delom organa), temveč je namenjen tudi zunanjemu krogu oseb, in sicer za izvajanje nadzora bodisi s strani pristojnih organov bodisi s strani javnosti na podlagi pravice dostopa do informacij javnega značaja. Poleg tega je Informacijski pooblaščenec ugotovil, da zahtevani dokument vsebuje le splošne podatke o nalogah organa in postopkih oz. načinu njegovega dela na področju spremljanja mednarodnih sistemov zvez, in sicer v obsegu, ki izhaja iz ZSOVA. Informacijski pooblaščenec je zaključil, da v obravnavanem primeru izjema notranjega delovanja organa ni bila podana. Pritožbi prosilca je ugodil in organu naložil, da mu posreduje zahtevani dokument.

KLJUČNE BESEDE: notranje delovanje, tajni podatki, številka odločbe 090-169/2020

Nadzorni odbor občine sodi med druge nadzorne organe, pristojne za finančni nadzor, ki jih zajema določba drugega odstavka 5.a člena ZDIJZ

Prosilec je Občino Lendava zaprosil za posredovanje osnutka poročila nadzornega odbora občine in odzivno poročilo na osnutek poročila o opravljenem nadzoru pri izvedbi nakupa poslovnega objekta Krona. Organ je zahtevo prosilca zavrnil s sklicevanjem na izjemo varstva nadzornega postopka (drugi odstavek 5.a člena ZDIJZ). Pri tem je zatrdil, da ima Nadzorni odbor Občine Lendava status nadzornega organa, organ pa se zavezuje, da bo sledil ugotovitvam in predlogom nadzornega odbora in bo ravnal skladno z zaključki iz končnega poročila, ki predlaga, da se zadeva preda v reševanje pristojnim organom za ugotavljanje suma oškodovanja občinskega premoženja. Dodal je še, da poslovnik Nadzornega odbora Občine Lendava določa, da osnutek poročila o nadzoru ni informacija javnega značaja. Prosilec je ugovarjal odločitvi organa, da je nadzorni odbor občine nadzorni organ, ki ga določa drugi odstavek 5.a člena ZDIJZ. Navedel je, da je

bila določba dodana v zakon z namenom varstva nadzornih postopkov, ki jih vodijo slovenski regulatorji s finančnega področja, kar pa nadzorni organ občine ni. Opozoril je še, da ne drži navedba organa, da je nadzorni postopek še v teku. Za uporabo navedene izjeme morajo biti izpolnjeni trije kumulativni pogoji, in sicer, 1. podatek mora biti pridobljen ali sestavljen zaradi nadzornega postopka, 2. nadzorni postopek mora izvajati Banka Slovenije, organ, pristojen za nadzor trga vrednostnih papirjev ali zavarovalniški nadzor, ali drug nadzorni organ, specializiran za finančni nadzor, ter 3. nadzorni postopek mora biti v teku oz. če je že končan, mora veljati, da bi razkritje informacij povzročilo škodo drugi osebi. V pritožbenem postopku je Informacijski pooblaščenec ugotovil, da nadzorni organ občine glede na opredelitev njegovega statusa v Zakonu o lokalni samoupravi sodi med druge nadzorne organe, pristojne za finančni nadzor, ki jih omenja ZDIJZ v drugem odstavku 5.a člena. Prav tako ni bilo dvoma, da sta bila zahtevana dokumenta sestavljena zaradi nadzornega postopka, ki ga je nadzorni odbor občine uvedel s sklepom. V obravnavani zadevi je bilo evidentno, da je nadzorni postopek že zaključen, organ pa ni uspel izkazati škode, ki bi z razkritjem zahtevanih informacij nastala drugi osebi. Pavšalne navedbe o negativnem vplivu razkritja zahtevanih informacij na poslovanje in dobro ime prodajalca, tj. pravne osebe, ki je z organom (tj. v obravnavani zadevi z občino) sklenila pravni posel, po mnenju Informacijskega pooblaščenca niso zadostile dokaznim standardom o nastanku škode. Poleg tega je organ porabnik javnih sredstev, zato na trgu ne nastopa brez omejitev, česar se morajo zavedati tudi poslovni subjekti, ki vstopajo v takšna obligacijska razmerja. Informacijski pooblaščenec je tako ugotovil, da v obravnavani zadevi pogoji za sklicevanje na izjemo po drugem odstavku 5.a člena ZDIJZ niso bili izpolnjeni, zato je pritožbi ugodil. Na drugačno odločitev ni moglo vplivati niti določilo v poslovniku nadzornega odbora občine, da osnutek poročila ni informacija javnega značaja, saj je dostop do informacij javnega značaja ustavna pravica, ki jo je dovoljeno omejiti samo z zakonom, poslovnik pa to ni.

KLJUČNE BESEDE: varstvo nadzornega postopka, številka odločbe 090-284/2020

Kadar se prosilec v zahtevi sklicuje na prevladujoč javni interes za razkritje, mora o tem odločiti Vlada RS, če je zavezan organ državne uprave

Organ je od Inšpektorata za javni sektor zahteval kopijo poročila Slovenske obveščevalno-varnostne agencije o izvedenih ukrepih, ki jih je odredila upravna inšpekcija. Zaprosil je, da se dostop do podatkov dovoli, če je javni interes glede razkritja močnejši od javnega interesa drugih oseb za omejitev dostopa. Organ je zahtevo zavrnil s sklicevanjem na izjemo tajnih podatkov (1. točka prvega odstavka 6. člena ZDIJZ), saj je bil zahtevani dokument označen s stopnjo tajnosti ZAUPNO. Prosilec se je pritožil, ker iz izpodbijane odločbe ni bilo razvidno, da je organ ugotavljal, ali so izpolnjeni vsi formalni in materialni pogoji za določitev tajnega podatka. Izpostavil je tudi določbo drugega odstavka 6. člena ZDIJZ, ki opredeljuje absolutne in relativne izjeme dostopa do informacij javnega značaja, v povezavi z drugim odstavkom 21. člena ZDIJZ, iz katerih izhajata pravica in dolžnost predstojnika, da tudi brez (izrecne) zahteve prosilca (samoiniciativno) oceni, ali je morda javni interes glede razkritja močnejši od javnega interesa ali interesa drugih oseb za omejitev dostopa do zahtevane informacije. Informacijski pooblaščenec je pri organu opravil ogled *in camera*, se seznanil z zahtevanim dokumentom in pridobil oceno možnih škodljivih posledic za zapisnik organa, ki mu je sledilo predmetno poročilo SOVE. Informacijski pooblaščenec je v pritožbenem postopku ugotovil, da se je prosilec v zahtevi skliceval na javni interes, zato bi o dostopu do zahtevanega dokumenta morala odločiti vlada. Tako določa drugi odstavek 21. člena ZDIJZ. Ker se je torej prosilec v zahtevi skliceval na javni interes, bi moral organ zahtevo, skupaj s predlogom odločitve, poslati v odločitev vladi. Ker organ tega ni storil, je Informacijski pooblaščenec štel, da je v postopku na prvi stopnji prišlo do bistvenih kršitev pravil upravnega postopka, saj je odločbo izdal stvarno nepristojen organ. Informacijski pooblaščenec je izpodbijano odločbo odpravil in zadevo vrnil prvostopenjskemu organu v ponovni postopek.

KLJUČNE BESEDE: kršitev pravil postopka, številka odločbe 090-297/2020

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 hkrati 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 skupaj z Ministrstvom za javno upravo, Tehnološkim parkom Ljubljana in Gospodarsko zbornico Slovenije organiziral virtualni dogodek z naslovom *Etika pri ponovni uporabi podatkov v digitalni družbi*, na katerem je beseda tekla o etiki pri urejanju razmerij na področju odprtih podatkov, namen dogodka pa je bil sprožiti procese, ki bodo odločevalcem dali odziv skupnosti glede prehoda v digitalno družbo.

V okviru dogodka, ki je potekal prek *on-line* video povezave, je pozdravni nagovor podala tudi informacijska pooblaščenka Mojca Prelesnik, ki je poudarila, da je etika pri urejanju razmerij na področju odprtih podatkov vedno bolj pomembna, pri čemer je enoznačno definicijo etike sicer težko podati, a je pomembno, da družba na tem področju določi vsaj minimalna pravila skupnega ravnanja. Tudi na področju etike pri ponovni uporabi podatkov iščemo ravnovesje med dvema človekovima pravicama: pravico do svobode izražanja in s tem povezano pravico do pridobivanja in uporabe podatkov ter pravico do varstva zasebnosti in s tem povezanega varstva osebnih podatkov. Poudarila je, da lahko samo s povezovanjem različnih mnenj in pristopov dobimo celovite rešitve, te pa vodijo v boljšo, bolj odprto družbo in v večjo družbeno blaginjo.

2.6.2 Mednarodno sodelovanje

Na pobudo Informacijskega pooblaščenca Republike Slovenije je 20. oktobra 2020 potekala ustanovna konferenca združenja Iniciative 2020, v katero smo se povezali pritožbeni organi s področja dostopa do informacij javnega značaja iz Slovenije, Hrvaške, Bosne in Hercegovine, Črne gore, Srbije, Kosova in Severne Makedonije. Namen združenja je krepitev sodelovanja in izmenjava dobrih praks pri promociji in varstvu pravice dostopa do informacij javnega značaja.

V okviru srečanja, ki je zaradi epidemioloških razmer potekalo prek videokonference, so udeleženci predstavili organizacijo, pravno ureditev in način delovanja posameznih pritožbenih organov s področja dostopa do informacij javnega značaja. Izpostavljeni so bili težave in izzivi, s katerimi se srečujemo v praksi (npr. molk organa, uporaba testa interesa javnosti, tehtanje med pravico dostopa do informacij javnega značaja in varstvom osebnih podatkov, izjeme od prosto dostopnih informacij) ter možne rešitve.

Pritožbene organe druži podoben zgodovinski in pravni okvir, v praksi se srečujemo s podobnimi izzivi. Za dobro medsebojno sodelovanje in izmenjavo izkušenj med organi v prihodnje je bila sprejeta skupna deklaracija o sodelovanju. Pritožbeni organi so z deklaracijo potrdili namero, da letno sodelujejo na konferencah, katerih namen je strokovno sodelovanje na področju dostopa do informacij javnega značaja, obravnava aktualnih vprašanj na področju dostopa do informacij javnega značaja ter izmenjava dobrih praks in izkušenj.

2.7 SPLOŠNA OCENA IN PRIPOROČILA

Tudi na področju dostopa do informacij javnega značaja so leto 2020 zaznamovale izredne razmere, povezane z epidemijo covid-19. Po sprejetju interventnega Zakona o začasnih ukrepih v zvezi s sodnimi, upravnimi in drugimi javnopravnimi zadevami za obvladovanje širjenja nalezljive bolezni SARS-CoV-2 (covid-19) so se prekinili vsi roki v nenujnih upravnih postopkih, tudi v postopkih odločanja o zahtevah za dostop do informacij po ZDIJZ in ZMed. Posledično v času od 29. 3. 2020 do 1. 6. 2020 roki za odločanje niso tekli in so začeli teči šele s 1. 6. 2020, iztekli pa so se 20. delovni dan od tega dneva, torej 29. 6. 2020.

Ker roki za odločanje v postopkih po ZDIJZ in ZMed niso tekli, je Informacijski pooblaščenec v prvi polovici leta 2020 zaznal upad prejetih pritožb, že v poletnih mesecih pa se je število pritožb precej povečalo. Skupno število pritožbenih zadev na področju dostopa do informacij javnega značaja je v letu 2020 tako naraslo (v letu 2020 je Informacijski pooblaščenec obravnaval 565 pritožb, kar je več kot v letu 2019, ko je obravnaval 540 pritožb). Skupno število pritožb zaradi molka je bilo v letu 2020 (231) na primerljivi ravni kot v letu 2019 (235), pri čemer je razveseljivo dejstvo, da se je po več letih rasti zmanjšalo število pritožb zoper molk občin. V letu 2020 je bilo teh pritožb 56, kar je opazno manj kot v letu 2019, ko jih je bilo 67.

Če trend števila pritožb zoper občine pada, pa je skrb vzbujajoča ugotovitev, da raste število pritožb zoper državne organe. V letu 2020 se je zoper to skupino zavezancev povečalo tako skupno število pritožb (245, v letu 2019 jih je bilo 222) kot število pritožb zaradi molka (v letu 2020 je bilo takih pritožb 91, leto pred tem pa 77).

Ob tem je Informacijski pooblaščenec v letu 2020 zaznal tudi povečano število pritožb zoper pravosodne organe (sodišča in državna tožilstva), ki je bilo posledica sodbe Vrhovnega sodišča RS št. X IPS 4/2020 z dne 27. 5. 2020, s katero je to zavzelo stališče, da se za dostop do informacij iz sodnih spisov uporabljajo (le) določbe procesnih zakonov, po ZDIJZ pa prosilci (novinarji in splošna javnost) do teh informacij niso več upravičeni. Posledično je Informacijski pooblaščenec kot drugostopenjski organ od junija 2020 naprej prejel več pritožb prosilcev, ki predstavljajo splošno javnost, medije ipd., da določena sodišča in tožilstva o njihovih zahtevah za dostop do informacij javnega značaja, ki se nanašajo na informacije iz sodnih in kazenskih spisov, procesno ne odločajo po ZDIJZ in ZMed, kljub jasni navedbi prosilcev, da uveljavljajo pravico na navedeni pravni podlagi. Zaznati je bilo različno prakso posameznih sodišč in tožilstev v zvezi s procesno obravnavo zahtev po ZDIJZ in ZMed, kar je vodilo v neenako obravnavo prosilcev v smislu izvrševanja njihove pravice dostopa do informacij javnega značaja na eni strani in pravice dostopa do dokumentov iz sodnih (in tožilskih) spisov v kontekstu procesne zakonodaje. Omenjena problematika je bila delno urejena s sprejemom zadnje novele Zakona o kazenskem postopku (ZKP-O), s katero je bilo v 128. členu določeno, da lahko v skladu z zakonom, ki ureja dostop do informacij javnega značaja, vsakdo zahteva od organa, da mu omogoči dostop do informacij javnega značaja v posameznih kazenskih zadevah. To seveda ne pomeni, da so prosilcem zdaj prosto dostopne vse informacije iz kazenskih zadev, ampak le, da lahko te informacije zahtevajo, organi pa morajo njihove zahteve procesno obravnavati in odločiti po ZDIJZ (pri čemer zahtevo zavrnejo, če gre npr. za varovane osebne podatke ali če bi razkritje lahko škodljivo vplivalo na izvedbo (pred) - kazenskega postopka).

Informacijski pooblaščenec je v letu 2020 prejel tudi bistveno več zaprosil za mnenja oz. pojasnila s področja dostopa do informacij javnega značaja. Če je bilo teh zaprosil v letu 2019 300, je število v letu 2020 naraslo na 411, kar je skoraj 30-odstotno povečanje. Ker je Informacijski pooblaščenec na področju dostopa do informacij javnega značaja pritožbeni organ, lahko zavezancem in javnosti svetuje le neformalno, v okviru dosedanje prakse. 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 zavezancem in seznanjati javnost s pomenom te temeljne človekove pravice.

Številna vprašanja glede uporabe ZDIJZ, ki jih zavezanci naslavljajo na Informacijskega pooblaščenca, kažejo, da imajo zavezanci pri izvajanju tega zakona v praksi še vedno težave. Na podlagi analize konkretnih primerov iz prakse Informacijski pooblaščenec ugotavlja, da so primeri, s katerimi se zavezanci srečujejo, vsebinsko in procesno vedno bolj kompleksni ter terjajo poglobljeno poznavanje področja dela organa in dobro poznavanje pravil upravnega postopka. Ker je na podlagi 32. člena ZDIJZ resorno ministrstvo, zadolženo za usposabljanje zavezancev za uporabo zakona v praksi, Ministrstvo za javno upravo, ga Informacijski pooblaščenec poziva, naj bolj aktivno pristopi k tej nalogi in temu področju nameni več pozornosti. Delež pritožb zaradi molka v skupnem deležu vseh pritožb (43 %) je namreč visok in se ne zmanjšuje, na kar Informacijski pooblaščenec opozarja že nekaj let. Zato bo v prihodnje treba več napora vložiti v promocijo zakona in aktivnejše

usposabljanje zavezancev za uporabo le-tega v praksi, to pa je primarno naloga Ministrstva za javno upravo.

V letu 2020 je Informacijski pooblaščenec vodil 14 pritožbenih postopkov zoper poslovne subjekte pod prevladujočim vplivom, kar predstavlja le 2,6 % vseh pritožbenih zadev. Informacijski pooblaščenec ugotavlja, da število teh pritožb že vsa leta ostaja majhno.

V letu 2020 Informacijski pooblaščenec zaradi kršitev ZDIJZ ni uvedel nobenega postopka s prekrški, je pa v zadevi pod opr. št. 090-112/2015 zoper Ekonomsko fakulteto v Ljubljani uvedel postopek izvršbe s prisilitvijo, ker zavezanec, kljub temu da je odločba Informacijskega pooblaščenca postala pravnomočna in izvršljiva že v letu 2016, prosilki še vedno ne želi posredovati informacij javnega značaja, kot mu je bilo naloženo.

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

- Glede na posebne epidemiološke razmere v zvezi s preprečevanjem širjenja bolezni SARS-CoV-2 (covid-19) je Informacijski pooblaščenec v letu 2020 zaznal povečanje števila primerov, v katerih so prosilci zahtevali informacije, ki se nanašajo na področje javnega zdravja in s tem povezano porabo javnega denarja (npr. različne statistike o obolelosti in smrtnosti, nabavo zaščitne opreme, cepljenje …). Ker gre za informacije, ki so pogosto v širšem javnem interesu, Informacijski pooblaščenec zavezance poziva, da pri odločanju o teh zahtevah postopajo hitro in pri presoji upoštevajo drugi odstavek 6. člena ZDIJZ, ki določa, da se ne glede na morebitne izjeme 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.
- Kot že navedeno, je Informacijski pooblaščenec na podlagi analize konkretnih primerov ugotovil, da so primeri, s katerimi se srečujejo zavezanci, vsebinsko in procesno vedno bolj kompleksni ter terjajo poglobljeno poznavanje področja dela organa in dobro poznavanje pravil upravnega postopka. V zvezi s tem Informacijski pooblaščenec zavezance poziva, da za izvajanje nalog, ki jih predvideva ZDIJZ, določijo uradno osebo, ki dobro pozna strokovno področje dela organa, obenem pa ima tudi ustrezno znanje s področja dostopa do informacij javnega značaja in upravnega postopka za izdajo upravne odločbe.
- Informacijski pooblaščenec je, podobno kot v letu 2019, tudi v letu 2020 zaznal številne postopkovne kršitve, ki kažejo na to, da zavezanci pri obravnavi zahtev ne namenijo dovolj pozornosti postopkovnim vprašanjem, posledica pa je nepopolno oz. napačno ugotovljeno dejansko stanje, zaradi česar se izpodbijane odločbe ne da preizkusiti. Ker se število tovrstnih primerov glede na skupno število pritožbenih postopkov povečuje (v letu 2019 je znašalo 17 %, v letu 2020 pa že 24 %), Informacijski pooblaščenec zavezancem predlaga, da pri obravnavi zahtev posebej natančno preučijo procesne vidike (vključitev stranskih udeležencev, določno oblikovanje izreka odločbe, natančna obrazložitev, oprta na ugotovljeno dejansko stanje) in da uradne osebe, če je to potrebno, napotijo na dodatno izobraževanje s področja upravnega postopka.
- Ker je Informacijski pooblaščenec v letu 2020 zaznal povečanje števila primerov, v katerih so se zavezanci sklicevali, da gre za zlorabo pravice s strani prosilca, velja opozoriti, da mora uporaba določbe petega odstavka 5. člena ZDIJZ v praksi ostati restriktivna, dokazno breme, da gre za zlorabo, pa je na strani zavezanca. Tudi sodna praksa je zavzela stališče, da lahko organ zaradi zlorabe pravice zahtevo prosilca zavrne le v izjemnih primerih. Za zavrnitev zahteve s sklicevanjem na zlorabo tako ne zadošča zgolj pavšalno sklicevanje na predmetno zakonsko določbo, ampak mora organ z dejstvi to konkretno izkazati in v zavrnilni odločbi ustrezno obrazložiti.

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. 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).

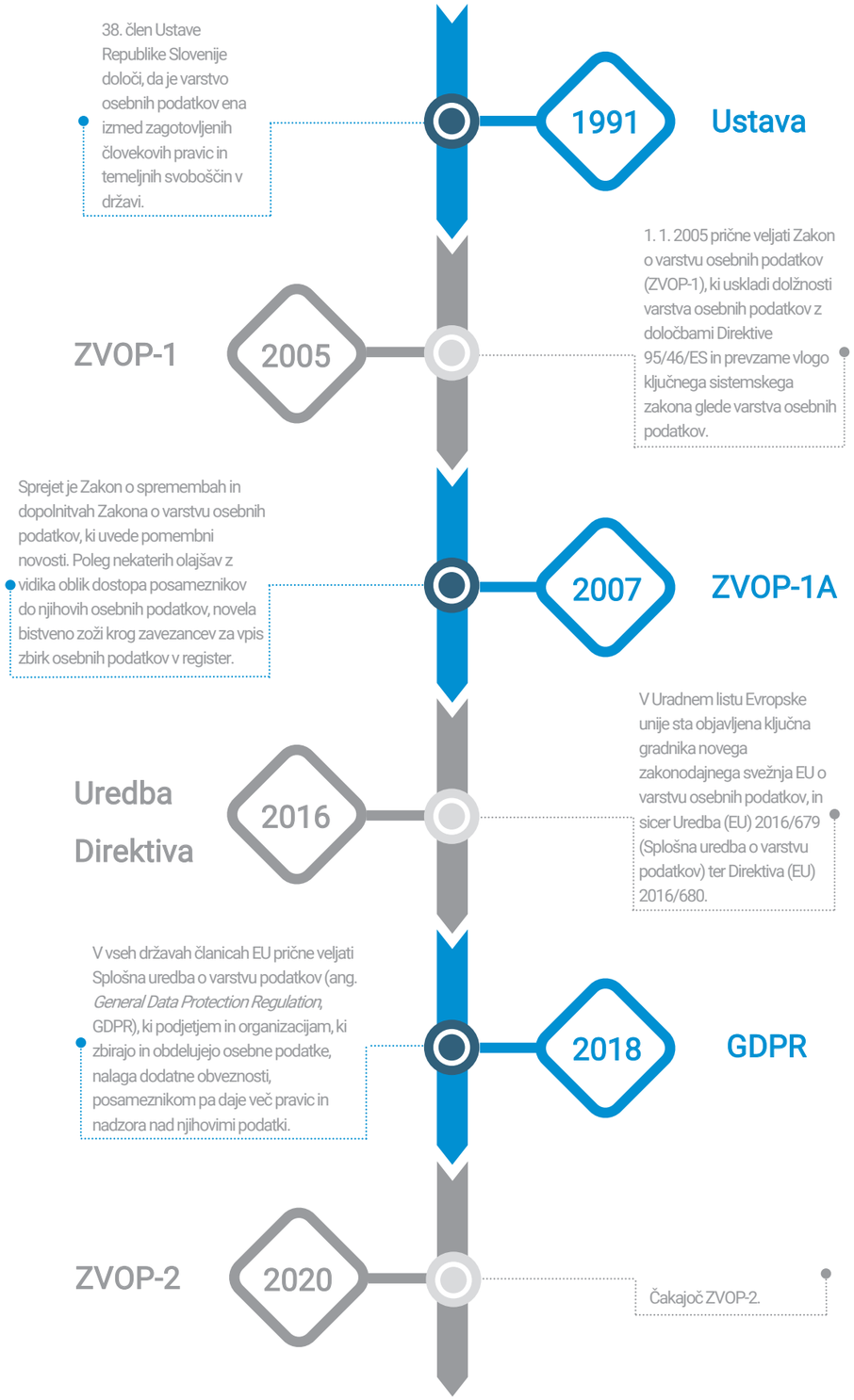
Splošna uredba o varstvu podatkov (Splošna uredba; angl. General Data Protection Regulation (GDPR)) je začela veljati 25. 5. 2016, uporablja pa se neposredno od 25. 5. 2018. Direktiva (EU) 2016/680 je bila v nacionalno zakonodajo prenesena z Zakonom o varstvu osebnih podatkov na področju obravnavanja kaznivih dejanj (ZVOPOKD), ki je začel veljati 31. 12. 2020.

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 2020

Postopek inšpekcijskega nadzora, ki ga izvaja Informacijski pooblaščenec oz. državni nadzorniki za varstvo osebnih podatkov, poleg ZVOP-1, Zakona o Informacijskem pooblaščencu (ZInfP), Splošne uredbe in Zakona o varstvu osebnih podatkov na področju obravnavanja kaznivih dejanj (ZVOPOKD) 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.

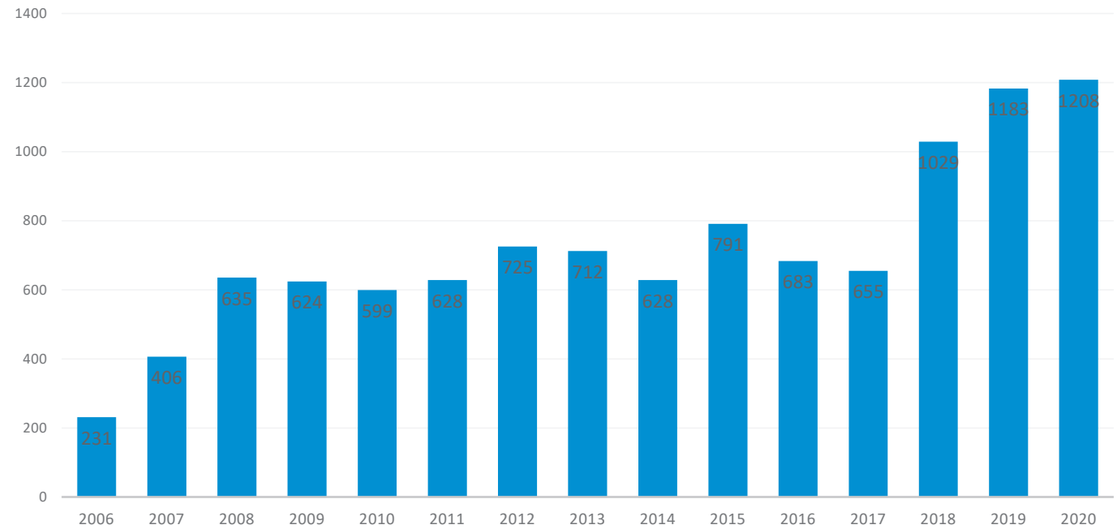
Splošna uredba daje Informacijskemu pooblaščencu v členu 58 naslednja inšpekcijska pooblastila:

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, katerih osebni podatki so bili 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 2020 zaradi suma kršitev določb Splošne uredbe in/ali ZVOP-1 vodil 1.208 inšpekcijskih zadev, od tega 405 v javnem in 803 v zasebnem sektorju, kar pomeni, da se število inšpekcijskih zadev še vedno povečuje. V primerjavi z letom 2019, ko se je število inšpekcijskih zadev povečalo za 15 % glede na leto 2018, se je povečanje števila inšpekcijskih zadev v letu 2020 nekoliko ustalila – v primerjavi z letom 2019 je število naraslo za 2 %.

Število inšpekcijskih zadev med letoma 2006 in 2020.



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	276
Nezakonito izvajanje videonadzora	169
Nezakonito zbiranje oz. zahtevanje osebnih podatkov	149
Nezakonita obdelava osebnih podatkov pri izvajanju neposrednega trženja	100
Neustrezno zavarovanje osebnih podatkov	90
Nezakonit vpogled v osebne podatke	59
Hekerski napadi in vdori v informacijske sisteme	32
Obdelava osebnih podatkov v nasprotju z namenom zbiranja	28
Piškotki	9
Zavrnitev posredovanja osebnih podatkov	4
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)	102

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 2020 vodil 405 zadev, 326 jih je začel na podlagi prejetih prijav, 79 pa po uradni dolžnosti.

Informacijski pooblaščenec je 69 prijaviteljem pisno pojasnil, zakaj v prijavi opisano ravnanje ne pomeni kršitve zakonodaje s področja varstva osebnih podatkov, v 22 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 13 kršiteljev uvedel postopke o prekršku oz. jim je izrekel ukrepe v skladu z Zakonom o prekrških (ZP-1), v šestih primerih je ocenil, da uvedba postopka o prekršku ne bi bila smotrna, ker v prijavi opisano ravnanje predstavlja prekršek neznatnega pomena, v dveh primerih postopka ni uvedel zaradi zastaranja pregona, v enem primeru pa prekrškovnega postopka ni začel zaradi vložene kazenske ovadbe. V 13 zadevah Informacijski pooblaščenec ni uvedel postopka, saj so bile zatrjevane nepravilnosti že odpravljene. Osem prijaviteljev je Informacijski pooblaščenec napotil na pravico do seznanitve z lastnimi osebnimi podatki, v petih 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 niti ni mogel pozvati k posredovanju dodatnih podatkov, ki bi bili potrebni za uvedbo inšpekcijskega postopka. V štirih zadevah prijavitelji pri utemeljevanju kršitve niso navedli ustreznih dokazov, v 18 zadevah pa je Informacijski pooblaščenec ugotovil, da za zatrjevane kršitve ni pristojen.

Informacijski pooblaščenec je v letu 2020 zavezancem v javnem sektorju izdal 32 tako imenovanih predodločb ter sedem ureditvenih odločb, vse ostale kršitve so zavezanci sami prostovoljno odpravili takoj po pozivu državnega nadzornika za varstvo osebnih podatkov.

Leta 2020 je bilo v javnem sektorju 195 inšpekcijskih postopkov zaključenih z izdajo sklepa o ustavitvi postopka. Informacijski pooblaščenec je 57 postopkov ustavil, ker so zavezanci ugotovljene nepravilnosti odpravili, v 91 postopkih ni zaznal kršitev določb Splošne uredbe ali ZVOP-1, 47 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 803 zadeve, od tega jih je 658 vodil na podlagi prejetih prijav, 72 postopkov je uvedel po uradni dolžnosti, preostali (73) pa so bili uvedeni po iniciativi drugih nadzornih organov v EU v okviru čezmejnega sodelovanja; Pri slednjih je Informacijski pooblaščenec sodeloval kot zadevni organ (več v poglavju 3.2.4.).

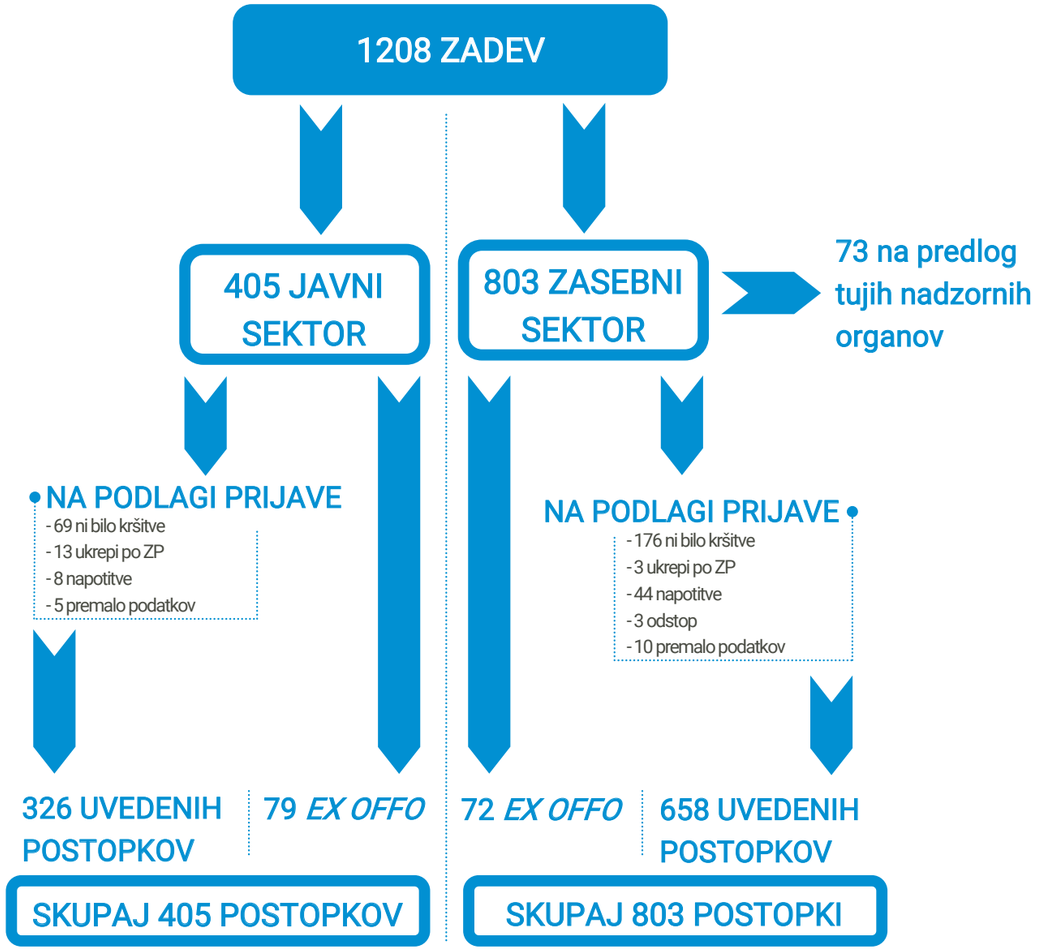
Po preučitvi prijav je Informacijski pooblaščenec 176 prijaviteljev obvestil, da postopka inšpekcijskega nadzora ne bo uvedel, ker iz njihove prijave ne izhaja sum kršitev določb Splošne uredbe in ZVOP-1, 44 prijaviteljev pa je napotil na pravice, ki jih morajo pri upravljavcih osebnih podatkov uveljavljati sami, največkrat na pravico do seznanitve z lastnimi osebnimi podatki in pravico do ugovora. Informacijski pooblaščenec je tri prijave odstopil v reševanje pristojnim organom, na podlagi 14 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 trem kršiteljem izrekel ukrepe po ZP-1, v osmih primerih je ocenil, da ukrepa po ZP-1 ne bo izrekel, ker gre za prekršek neznatnega pomena, v enem primeru uvedba prekrškovnega postopka ni bila dopustna zaradi zastaranja pregona, v dveh primerih pa prekrškovnega postopka ni začel zaradi vložene kazenske ovadbe. V 51 primerih Informacijski pooblaščenec ni uvedel postopka, ker niso bili predloženi ustrezni dokazi, ki bi utemeljevali zatrjevano kršitev, v 77 primerih pa za ukrepanje ni bil pristojen. Deset prijav je vsebovalo premalo podatkov za uvedbo inšpekcijskega postopka, poleg tega so bile anonimne in Informacijski pooblaščenec prijaviteljev ni mogel pozvati k dopolnitvi. V treh primerih inšpekcijski postopek ni bil uveden, ker je kršitelj nepravilnosti že odpravil.

Informacijski pooblaščenec je v letu 2020 zavezancem v zasebnem sektorju izdal 91 tako imenovanih predodločb ter 9 ureditvenih odločb, vse ostale kršitve so zavezanci sami prostovoljno odpravili takoj po pozivu državnega nadzornika za varstvo osebnih podatkov.

Leta 2020 je Informacijski pooblaščenec pri zavezancih v zasebnem sektorju s sklepom ustavil 347 postopkov: 161 postopkov je ustavil, ker ni bilo kršitev določb ZVOP-1, 133 postopkov je ustavil po tem, ko so zavezanci odpravili ugotovljene nepravilnosti, 53 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 eno sodbo Upravnega sodišča RS v zvezi s tožbo, vloženo leta 2017 zoper ureditveno odločbo. Sodišče je tožbo zavrnilo in potrdilo pravilnost odločitve Informacijskega pooblaščenca.

Pregled inšpekcijskih zadev v javnem in zasebnem sektorju leta 2020.



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, najpozneje pa v 72 urah. Kadar je verjetno, da bo kršitev varnosti osebnih podatkov povzročila veliko tveganje za pravice in svoboščine posameznikov, mora upravljavec o kršitvi obvestiti 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 2020 prejel 120 uradnih obvestil o kršitvi varnosti osebnih podatkov, t. i. samoprijav, ki so jih poslali zavezanci. 57 obvestil so poslali zavezanci iz zasebnega sektorja (npr. banke, telekomunikacijski operaterji, zavarovalnice), 63 pa zavezanci iz javnega sektorja (predvsem zdravstvene in izobraževalne ustanove).

Kršitve varnosti osebnih podatkov so se 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) – 22,
- nezakonito razkritje osebnih podatkov nepooblaščenim osebam – 21,
- hekerski vdor – 17,
- nepooblaščen dostop do osebnih podatkov s strani zaposlenih – 15,
- nezakonito objavo osebnih podatkov na spletu – 11,
- izgubo 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) – 8,
- neustrezno zagotavljanje varnosti osebnih podatkov na spletni strani – 7,
- izgubo ali krajo prenosnega računalnika ali drugih nosilcev osebnih podatkov (USB-ključek, zdravstveni karton, zvezek z osebnimi podatki strank) – 6,
- nezakonito razkritje osebnih podatkov (e-naslovov) pri pošiljanju e-sporočila več prejemnikom hkrati – 4,
- razkritje osebnih podatkov zaradi napake v aplikaciji oz. tehnične napake – 3,
- pošiljanje zlonamerne e-pošte in objava lažne spletne strani (ang. *phishing*) – 3,
- nezakonit izvoz osebnih podatkov pri pogodbeni obdelavi podatkov – 3.

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 e-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*).

Poleg prijav kršitev varnosti osebnih podatkov, ki jih je Informacijski pooblaščenec prejel s strani družb, ki imajo sedež samo v Republiki Sloveniji in obdelujejo osebne podatke posameznikov iz Slovenije, je sodeloval tudi v številnih čezmejnih postopkih nadzora, tj. v postopkih nadzora nad družbami, ki poslujejo čezmejno, in sicer preko mehanizma »vse na enem mestu« (angl. *one stop shop*), v katerih postopek nadzora vodi t. i. vodilni nadzorni organ, pri tem pa sodeluje z drugimi organi za varstvo osebnih podatkov, kot je določeno v členu 60 Splošne uredbe. Kot zadevni nadzorni organ je Informacijski pooblaščenec sodeloval v postopkih nadzora v zvezi s kršitvijo varnosti osebnih podatkov pri podjetjih, kot so Nintendo, TicketMaster, Marriot Hotels, Twitter, National Australia Bank, British Airways itd.; ti postopki so bili zaključeni leta 2020.

V omenjenih primerih je sodelovanje najpogosteje zadevalo kršitev varnosti osebnih podatkov zaradi vdora v informacijske sisteme in zaradi pomanjkljivega zavarovanja osebnih podatkov. Informacijski pooblaščenec je bil prek mehanizma čezmejnega sodelovanja obveščen o kršitvah, s katerimi so bili prizadeti tudi slovenski uporabniki storitev upravljavca (najpogosteje je šlo za spletne in IT-storitve).

V enem izmed zgoraj omenjenih primerov je junija 2018 neidentificirani napadalec prek orodja, ki uporabnikom omogoča oddaljen dostop do omrežja, pridobil dostop do informacijskega sistema, vdor pa je upravljavcu ostal neopažen vse do septembra 2018. Potem ko je napadalcu uspelo dostopiti do samega sistema, se

je po njem širil; informacijski sistem mu je uspelo spremeniti do te mere, da je bilo omogočeno odtekanje podatkov o imetnikih kartic s spletnega mesta upravljavca na zunanjo domeno tretje osebe, ki jo je nadziral napadalec.

Upravljavec je ocenil, da je bilo prizadetih 429.612 oseb, na katere so se nanašali osebni podatki, kot so uporabniško ime in gesla pogodbenih izvajalcev, zaposlenih in članov izvršnega kluba, imena in naslovi strank, nešifrirani podatki o plačilnih karticah, vključno s številkami kartic in številkami CVV ter datumi veljavnosti plačilne kartice.

Upravljavec je takoj izvedel ukrepe za ublažitev in zmanjšanje škode, ki bi jo lahko utrpeli prizadeti posamezniki, na katere so se nanašali osebni podatki, in sicer z izvajanjem popravljalnih ukrepov, vključno z obveščanjem bank in plačilnih shem, posameznikov, na katere so se nanašali osebni podatki, in drugih regulatorjev oz. nadzornih organov, ki se ukvarjajo z zaščito podatkov; sodeloval je z drugimi regulativnimi in vladnimi organi ter ponudil povračilo stroškov posameznikom (strankam), ki so utrpeli finančno izgubo zaradi kraje njihovih podatkov o plačilnih karticah. Upravljavec je izvedel tudi številne tehnične ukrepe za zmanjšanje tveganja podobnega napada v prihodnosti.

Nadzorni organ, ki je vodil postopek, je ugotovil, da upravljavec osebnih podatkov svojih strank ni obdeloval na način, ki bi zagotavljal ustrezno varnost, vključno z zaščito pred nedovoljeno ali nezakonito obdelavo ter pred nenamerno izgubo, uničenjem ali poškodbami z uporabo ustreznih tehničnih in organizacijskih ukrepov, kot to od upravljavca zahtevata člena 5 (1) (f) in 32 Splošne uredbe. Nadzorni organ je zaključil, da obstaja več ustreznih ukrepov, ki bi jih upravljavec lahko upošteval, da bi zmanjšal tveganje, da bi napadalec dostopal do njegovega omrežja. Upravljavec bi lahko obravnaval vsak korak napada ter preprečil ali zmanjšal njegov vpliv, če bi izvedel enega ali več primernih ukrepov, ki so mu bili na voljo. Nadzorni organ je bil tudi mnenja, da bi, če bi upravljavec izvedel strožje preizkuse ali teste notranjega nadzora, odkril in ustrezno odpravil številne ugotovljene nepravilnosti v zvezi z varnostjo podatkov.

Nadzorni organ je zaključil, da ugotovljene kršitve pomenijo resno neskladnost z obveznostmi iz Splošne uredbe in upravljavcu naložil globo v višini 20 milijonov funtov, potem ko je upošteval vrsto olajševalnih dejavnikov in tudi vpliv pandemije covid-19.

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:

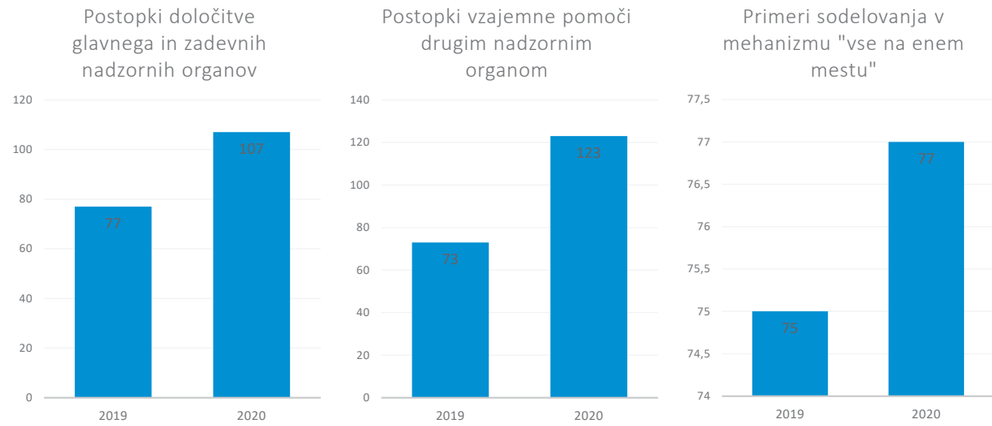
- **po načelu »vse na enem mestu« (angl. *one stop shop*)**, ki predvideva, da postopek nadzora v čezmejnem primeru obdelave osebnih podatkov vodi t. i. vodilni organ in pri tem sodeluje z drugimi organi za varstvo osebnih podatkov (člen 60 Splošne uredbe);
- **vzajemna pomoč** med organi za varstvo 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 načelu »vse na enem mestu« se lahko začne, ko je ugotovljeno, kateri nadzorni organ bo v postopku prevzel vlogo vodilnega in kateri organ(i) bodo v postopku sodeloval(i) kot zadevni organ(i). Vodilni organ prihaja iz tiste države članice EGS, kjer ima upravljavec osebnih podatkov, ki posluje čezmejno, glavno ustanovitev – sedež, ki prevzema odgovornost za obdelavo osebnih podatkov. Nadzorni organi iz drugih držav članic EGS se postopku nadzora pridružijo kot zadevni organi, kadar ima upravljavec na njihovem ozemlju npr. podružnice ali poslovne enote oz. kadar obdelava osebnih podatkov pomembno vpliva na posameznike v njihovih državah. 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 Evropski odbor za varstvo osebnih podatkov.

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

V letu 2020 je Informacijski pooblaščenec izvedel 200 postopkov sodelovanja po členih 60 in 61 Splošne uredbe v zvezi z upravljavci, ki izvajajo čezmejno obdelavo osebnih podatkov. Ob tem se je v 104 postopkih opredelil za zadevni nadzorni organ (po členu 56 Splošne uredbe) ter bil trikrat pozvan, da se opredeli za vodilni nadzorni organ. V nadaljevanju so podrobneje predstavljeni različni postopki sodelovanja.

Sodelovanje Informacijskega pooblaščenca v čezmejnih postopkih nadzora v letu 2020.



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 104 tovrstnih postopkih v letu 2020 se je Informacijski pooblaščenec opredelil za zadevni organ. Tri postopke ugotavljanja je začel Informacijski pooblaščenec, in sicer na podlagi prijave domnevne kršitve varstva osebnih podatkov v čezmejnem primeru. V 101 primeru je bil postopek ugotavljanja začet na iniciativo drugih organov v EU, Informacijski pooblaščenec pa se je opredelil za zadevni nadzorni organ, in sicer zato, ker:

- je imel upravljavec osebnih podatkov, zoper katerega je tekel postopek v drugi državi članici, v Sloveniji poslovno enoto ali je bil tu ustanovljen,
- so storitve upravljavca, zoper katerega je tekel postopek v drugi državi članici, uporabljali tudi posamezniki v Sloveniji in jih vprašanje domnevne kršitve varstva osebnih podatkov pomembno zadeva. To velja tudi v primerih priljubljenih ponudnikov komunikacijskih spletnih storitev, kot so Facebook, Google, Amazon, Apple, PayPal, WhatsApp, Twitter, Instagram, Microsoft itd.

Trikrat je bil Informacijski pooblaščenec pozvan, da se opredeli kot vodilni nadzorni organ, in sicer v zvezi s prijavami zoper zavezance v Sloveniji, ki naj bi izvajali čezmejno obdelavo osebnih podatkov.

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 2020 **obravnaval 77 zadev** 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. načelu »vse na enem mestu«. Vodilni nadzorni organ je v letu 2020 v največkrat predstavljal irski nadzorni organ, pogosto so v tej vlogi nastopali tudi nadzorni organi Luksemburga, Francije, Nizozemske, Nemčije, Francije in Avstrije.

22 postopkov čezmejnega 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. Med drugim so ti postopki zadevali pritožbe o spornih praksah spletnih družbenih omrežij, ki podatke svojih uporabnikov delijo z nepreglednim številom oglaševalskih partnerjev, in to ob nezadostnem obveščanju in ukrepih za zavarovanje podatkov. Informacijski pooblaščenec je ob sodelovanju španskega nadzornega organa obravnaval tudi primer pilotnega projekta vkrcavanja potnikov z uporabo biometrije na

ljubljanskem letališču, ki ga je izvajala španska družba Amadeus, pri čemer je ugotovil kršitve določb ZVOP-1 o biometriji.

55 tovrstnih postopkov je bilo začetih s strani drugih organov v EU in Informacijski pooblaščenec je v teh postopkih sodeloval kot zadevni organ. Primeri niso zadevali le storitev priljubljenih spletnih velikanov, ki so v veliki meri še v teku (vodilni organ je na Irskem), pač pa tudi neustrezna ravnanja z osebnimi podatki s strani različnih akterjev (letalskih družb, ponudnikov bančnih storitev, spletnih ponudnikov različnih storitev itd.) iz številnih držav članic EU. Primeri spornih praks so vključevali pretirane zahteve po podatkih za identifikacijo strank, za namen izbrisa podatkov, neustrezno izvrševanje pravice do dostopa, posredovanje podatkov tretjim osebam (npr. v oglaševalski sistem omrežja Facebook brez privolitve posameznika). Pogosto so se primeri nanašali na kršitve varnosti osebnih podatkov, med prizadetimi pa so bili tudi uporabniki iz Slovenije. V tem okviru je Informacijski pooblaščenec kot zadevni nadzorni organ sodeloval v postopkih nadzora v zvezi s kršitvijo varstva osebnih podatkov pri podjetjih, kot so Nintendo, TicketMaster, Marriot Hotels, Twitter, National Australia Bank, British Airways itd.; ti postopki so bili zaključeni v letu 2020.

Postopki čezmejnega sodelovanja po členu 60 so v letu 2020 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 (4 primeri), pri katerih je prosilec Informacijskemu pooblaščencu podal prijavo zoper upravljavca iz druge države članice EU.

V letu 2020 je bilo v postopkih sodelovanja »vse na enem mestu« izdanih 38 osnutkov odločb po členu 60. 29 postopkov se je končalo s končno odločbo po členu 60. V okviru spletne strani Evropskega odbora za varstvo podatkov je nastal tudi javni register končnih odločb v postopkih čezmejnega sodelovanja po členu 60; dostopne so na spletni strani https://edpb.europa.eu/our-work-tools/consistency-findings/register-for-article-60-final-decisions_en.

Primeri čezmejnega sodelovanja se ne končajo 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 ostaja še večina postopkov zoper velika multinacionalna podjetja, v večini teh primerov kot vodilni nastopa Irski nadzorni organ.

Postopki »vse na enem mestu« v letu 2020.

77 **postopkov čezmejnega sodelovanja pri inšpekcijskem nadzoru nad podjetji, ki poslujejo čezmejno (po načelu“vse na enem mestu”):**
- 22 na podlagi prijav, ki jih je glede čezmejnih zavezancev prejel Informacijski pooblaščenec,
- 55 na iniciativo drugih nadzornih organov.

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

Informacijski pooblaščenec je v letu 2020 sodeloval tudi v 123 postopkih zagotavljanja medsebojne pomoči med nadzornimi organi po členu 61 Splošne uredbe. Prejel je 96 zahtev drugih organov in se nanje, kadar je bilo potrebno, odzval, 27 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 naslednje grafike.

Postopki zagotavljanja medsebojne pomoči.

116 **postopkov prostovoljne medsebojne pomoči med nadzornimi organi po členu 61:**
- 50 zahtev drugih organov za informacije in pojasnila,
- 43 obvestil drugih organov glede konkretnih postopkov v teku,
- 23 zahtev s strani Informacijskega pooblaščenca.

7 **postopkov medsebojne pomoči med nadzornimi organi po členu 61:**
- 3 odzivi na zahteve drugih organov,
- 4 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 nadzorni organ v drugi državi članici. Postopki medsebojne pomoči pa običajno pomenijo zahtevo za izvedbo ukrepov zoper zavezance, ki izvajajo čezmejno obdelavo osebnih podatkov.

Postopek spora po členu 65 Splošne uredbe

Evropski odbor je v letu 2020 sprejel svojo prvo zavezujočo odločitev po členu 65 Splošne uredbe. Šlo je za primer družbe Twitter, ki je utrpela varnostni incident in s tem kršitev varstva osebnih podatkov, vendar tega ni pravočasno naznanila nadzornemu organu.

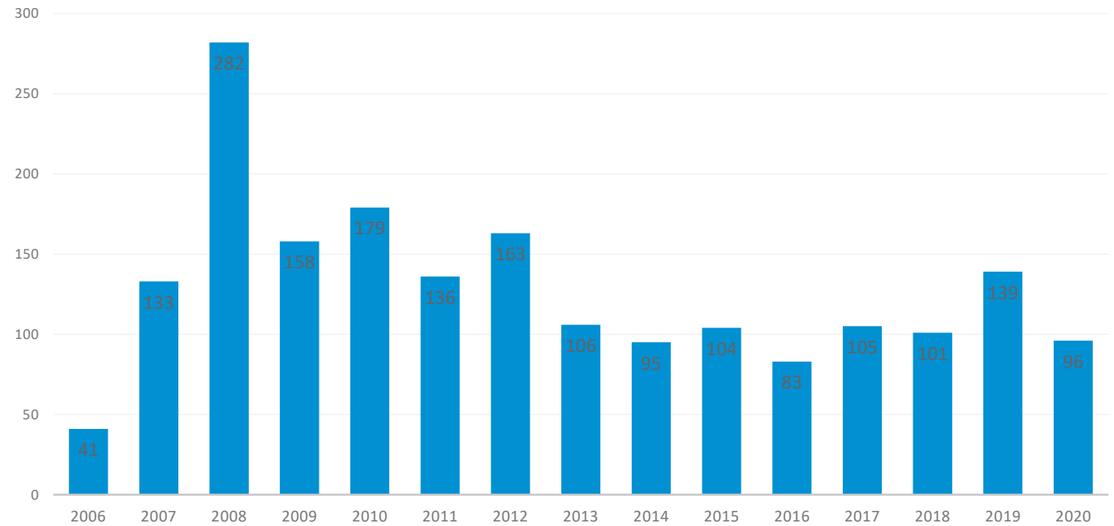
Kršitev varstva osebnih podatkov je pomenila napako (t. i. hrošča) v delovanju sistema Twitter. Uporabniki omrežja sami odločajo, ali bodo njihove objave (»čivki«) vidni javno ali želijo njihovo vidnost omejiti na zasebno in bodo lahko objavo videli le tisti sledilci, ki jih izberejo oni sami. Zaradi napake v sistemu so objave določenih uporabnikov postale javno vidne brez njihove vednosti in kljub temu, da so jih označili kot zasebne. Napaka je zadevala uporabnike androidnih naprav, ki so v svojem Twitter računu spremenili e-naslov, in sicer je to veljalo za njihove objave med 5. 9. 2017 in 11. 1. 2019. Prizadetih naj bi bilo več kot 80.000 uporabnikov iz Evrope. Twitter je o kršitvi varstva osebnih podatkov sicer obvestil Irski nadzorni organ, vendar ne v roku 72 ur po incidentu, kot to predpisuje člen 33 Splošne uredbe.

Irski vodilni nadzorni organ je osnutek odločitve predložil zadevnim organom iz vseh članic EU, tudi slovenskemu. Na osnutek odločitve je prejel več ugovorov, ki pa jih je zavrnil in zato zadevo predal v postopek odločanja po členu 65. Odločitev Evropskega odbora za varstvo podatkov po členu 65 je za vodilni nadzorni organ zavezujoča in jo mora upoštevati pri oblikovanju končne odločbe po členu 60. V zadevnem primeru je bilo vodilnemu organu naloženo, da mora v končni odločbi pri izreku sankcije upoštevati vsa merila iz člena 83 Splošne uredbe, da bo sankcija primerna in odvračalna. Vodilni nadzorni organ je v končni odločbi po členu 60 zavezancu Twitter zaradi kršitve člena 33 Splošne uredbe naložil globo v znesku 450.000 EUR.

3.2.5 PREKRŠKOVNI POSTOPKI

Informacijski pooblaščenec je zaradi suma kršitev določb ZVOP-1 v letu 2020 uvedel 96 postopkov o prekršku, od tega je 17 postopkov uvedel zoper pravne osebe javnega sektorja in njihove odgovorne osebe, 53 zoper pravne osebe zasebnega sektorja in njihove odgovorne osebe, 26 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 7).

Število uvedenih postopkov o prekršku med letoma 2006 in 2020.



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 enega predlagatelja obvestil, da na podlagi njegovega predloga ne bo uvedel postopka o prekršku, ker je pregon že zastaral, 14 postopkov o prekršku pa je ustavil.

Informacijski pooblaščenec je v prekrškovnih postopkih v letu 2020 izdal:
- **89 odločb o prekršku (58 glob in 31 opominov),**
- **15 opozoril.**

Poleg opozoril, ki so bila izrečena v prekrškovnih postopkih, je Informacijski pooblaščenec v skladu z načelom ekonomičnosti izrekel tudi 81 opozoril po 53. členu ZP-1 v okviru postopkov inšpekcijskega nadzora.

Poleg 89 odločb, ki so po ZP-1 najprej izdane brez obrazložitve, je bilo na podlagi napovedi zahtev za sodno varstvo izdanih 10 odločb z obrazložitvijo, pri čemer štirje kršitelji po prejemu odločbe z obrazložitvijo zahteve za sodno varstvo niso vložili. Kršitelji so zoper izdane odločbe o prekršku vložili šest zahtev za sodno varstvo (zoper 6,7 % odločb). Vse zahteve za sodno varstvo so bile vložene zoper odločbe, s katerimi je Informacijski pooblaščenec kršiteljem izrekel globe. Relativno majhen delež vloženih zahtev za sodno varstvo kaže na to, da storilci storjene prekrške priznavajo in se zavedajo svoje odgovornosti.

Kršitve varstva osebnih podatkov v letu 2020.

Vrsta kršitve	Število kršitev (v okviru enega postopka je lahko več kršitev)
Nezakonita obdelava osebnih podatkov (8. člen ZVOP-1)	39
Neustrezno zavarovanje osebnih podatkov (24. in 25. člen ZVOP-1)	18
Neizpolnjevanje ukrepov, izrečenih v postopkih inšpekcijskega nadzora, kršitev drugega odstavka 29. člena ZIN	14
Nezakonit namen zbiranja in nadaljnje obdelave osebnih podatkov (16. člen ZVOP-1)	10
Kršitve določb v zvezi z izvajanjem videonadzora (74., 75., 76. in 77. člen ZVOP-1)	8
Upravljavec ni zagotavljal zunanje sledljivosti oz. evidence posredovanja osebnih podatkov (tretji odstavek 22. člena ZVOP-1)	1
Kršitve določb o izvajanju biometrijskih ukrepov v zasebnem sektorju (80. člen ZVOP-1)	1
Kršitve določb glede roka hrambe osebnih podatkov (21. člen ZVOP-1)	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 (t. i. ZVOP-2), ZVOPOKD, ki je v slovenski pravni red prenesel Direktivo (EU) 2016/680, pa je začel veljati šele z 31. 12. 2020. 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.

V letu 2020 je Informacijski pooblaščenec prejel sedem 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, 2019 in 2020:
- zahteva za sodno varstvo je bila zavrnjena kot neutemeljena, odločba Informacijskega pooblaščenca pa potrjena – 2,
- 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,
- zahteva za sodno varstvo je bila zavrnjena, sodišče pa je odločbo Informacijskega pooblaščenca po uradni dolžnosti spremenilo tako, da je določilo milejšo sankcijo – 1,
- zahtevi za sodno varstvo je bilo delno ugodeno tako, da se je odločba Informacijskega pooblaščenca spremenila in se je ustavil postopek zoper odgovorno osebo in pravno osebo – 1,
- sodišče je odločbo o prekršku po uradni dolžnosti spremenilo tako, da je postopek zoper storilca in odgovorno osebo ustavilo – 1.

Informacijski pooblaščenec je prejel tudi eno sodbo, s katero je višje sodišče zavrnilo pritožbo Informacijskega pooblaščenca zoper sodbo okrajnega sodišča, ki je predhodno zahtevi za sodno varstvo ugodilo in postopek o prekršku zoper odgovorno osebo pravne osebe in pravno osebo ustavilo.

3.2.6 IZBRANI PRIMERI OBDELAVE OSEBNIH PODATKOV

V nadaljevanju so predstavljeni nekateri primeri, v zvezi s katerimi je Informacijski pooblaščenec prejel večje število prijav, uradnih obvestil in vprašanj. Predstavljene so tudi pomembnejše zadeve, ki jih je Informacijski pooblaščenec obravnaval v inšpekcijskih postopkih v letu 2020 v povezavi z epidemijo covid-19.

Vnašanje osebnih podatkov preko spletne strani https://covid-19-stats.si/

Informacijski pooblaščenec je kot nujno zadevo obravnaval prijavo suma kršitve varstva osebnih podatkov v zvezi z zbiranjem podatkov o počutju, ki so jih posamezniki lahko vnašali preko spletne strani https://covid-19-stats.si/ (t. i. COVID-19 SAMOPOROČANJE). Zbiranje podatkov prek te spletne strani je bilo namenjeno predstavitvi osveženih in podrobnih statistik o zdravih, okuženih, samoizoliranih in ozdravljenih prebivalcih na nivoju Slovenije, regije in posamezne občine, in sicer na način, da je posameznik na spletni strani označil, ali kaže katerega od simptomov obolelosti s covid-19, nato pa, glede na prisotnost ali odsotnost simptomov, označil zahtevane podatke (število družinskih članov gospodinjstva, simptome in datum zaznave prvih simptomov okužbe) ter vnesel svojo številko EMŠO ter regijo in občino bivališča. Opisano zbiranje in obdelavo osebnih podatkov je Informacijski pooblaščenec prepoznal kot sum nezakonite obdelave osebnih podatkov, tj. obdelave v nasprotju s členom 6 in 9 Splošne uredbe ter 8. in 13. členom ZVOP-1. Informacijski pooblaščenec je v postopku ugotovil, da je bilo na omenjeni spletni strani navedeno, da se osebni podatki ne zbirajo in ne obdelujejo, saj se vpisana številka EMŠO ne pošlje prek spleta na strežnik zavezanca in se posledično tudi ne shranjuje, saj se pred pošiljanjem številke EMŠO na napravi uporabnika le-ta anonimizira, s čimer naj bi bilo doseženo, da do na tak način šifriranih številk EMŠO, ki jih zavezanec hrani, ni mogoče več priti oz. dostopati. Zavezanec je na podlagi navedenega menil, da mu ni treba zagotavljati obveznosti iz Splošne uredbe in ZVOP-1.

Informacijski pooblaščenec je ugotovil, da na opisani način vrednosti številk EMŠO niso anonimizirane, temveč zgolj psevdonimizirane, kar pomeni, da imajo psevdonimizirane vrednosti še vedno naravo osebnega podatka, upravljavci takšnih podatkov pa morajo zagotavljati obveznosti iz Splošne uredbe in ZVOP-1. Zaradi navedenega je Informacijski pooblaščenec zavezanca pozval, naj izbriše vse podatke (surove in agregatne), ki jih je zbiral prek te spletne strani, kar je zavezanec tudi nemudoma storil.

Merjenje temperature zaposlenih in obiskovalcev

Upravljavci so kot priporočen ukrep s strani Vlade RS pogosto izvajali merjenje telesne temperature zaposlenim in obiskovalcem. Informacijski pooblaščenec je poudaril, da glede na veljavne predpise merjenje temperature ni nujen in smiseln ukrep v vseh okoliščinah, saj lahko ob neustreznem izvajanju vodi v množično in nezakonito zbiranje osebnih podatkov. Vsakršna obdelava osebnih podatkov, tudi npr. s termokamero, mora imeti ustrezno pravno podlago po členu 9 Splošne uredbe. Delodajalci in ostale organizacije, ki niso izvajalci zdravstvene dejavnosti (npr. vzgojno-izobraževalne ustanove), glede na določbe veljavne delovno-pravne in druge zakonodaje v običajnih razmerah niso upravičeni do obdelave zdravstvenih podatkov posameznikov, med katere sodi tudi podatek o telesni temperaturi. Dodatno je treba opozoriti, da nekatere tehnologije poleg merjenja telesne temperature omogočajo tudi izvajanje biometrijskih ukrepov (npr. prepoznavo obraza). Kot je Informacijski pooblaščenec večkrat poudaril, mora o potrebnosti in sorazmernosti tega ukrepa vedno presojati medicinska stroka (mnenje lahko poda npr. izbrani izvajalec medicine dela), ki mora pri presoji upoštevati veljavne predpise in zasledovati načelo sorazmernosti. Ukrepa obveznega merjenja telesne temperature tako ne bi smeli odrejati, če je mogoče primerljiv učinek doseči z milejšimi, manj invazivnimi ukrepi. Upravljavec naj skrbno presodi, katere osebne podatke je treba obdelovati v zvezi s takim ukrepom ter ali je nujno in primerno te podatke hraniti. Pri tem mora ustanova oz. podjetje upoštevati tudi vse relevantne določbe Splošne uredbe, npr. načela varstva osebnih podatkov, predhodno obveščanje posameznikov o ukrepu skladno s členom 13 Splošne uredbe, zagotovitev varnosti osebnih podatkov, določitev primernih rokov hrambe in zagotovitev točnosti in ažurnosti osebnih podatkov. V inšpekcijskih postopkih se je večinoma izkazalo, da so upravljavci uporabljali naprave za merjenje telesne temperature, ki so bile namenjene prostovoljni uporabi zaposlenih in obiskovalcev. Tako naprava pri enem izmed upravljavcev ni beležila podatkov o izmerjeni temperaturi, temveč se je rezultat zgolj prikazal posamezniku, ko je ta stal ob napravi, nato se je nemudoma izbrisal. Zaradi postavitve ekrana je bil vpogled mimoidočim onemogočen, naprava tudi ni oddajala nobenih zvokov ob morebitni zaznani povišani telesni temperaturi, z rezultatom se je torej lahko seznanila zgolj oseba, ki je napravo uporabila. Pri upravljavcu tako ni šlo za kršitve varstva osebnih podatkov, saj naprava ni omogočala shranjevanja podatkov, zajemanja in

obdelave slik oz. videoprenosa ter ni vsebovala programske opreme, ki bi omogočila izvajanje biometrične obdelave. Vsi zaposleni so bili predhodno obveščeni o namestitvi naprav za merjenje telesne temperature in o njihovem namenu.

Obdelava osebnih podatkov učencev pri izvajanju pouka na daljavo

Zaradi izrednih razmer so šole v letu 2020 izvajale pouk na daljavo in pri tem uporabljale orodja informacijske tehnologije. V enem od obravnavanih primerov v inšpekcijskem postopku naj bi učitelj športne vzgoje podal navodilo, da morajo učenci na svoje pametne telefone namestiti aplikacijo, ki beleži športne rezultate o vadbi učenca. Učencem je bilo tudi naročeno, naj posnetke športne vadbe posredujejo prek aplikacije, ki jo sicer uporabljajo pri pouku na daljavo. Aplikacije za spremljanje telesne aktivnosti oz. druge pametne naprave za spremljanje vadbe z namenom pošiljanja podatkov o opravljeni vadbi učitelju po mnenju Informacijskega pooblaščenca pretirano posegajo v pravico do varstva osebnih podatkov in zasebnost učencev, saj aplikacije obdelujejo vrsto zelo občutljivih osebnih podatkov. Pravna podlaga je v tem primeru sicer privolitev, ki pa pri izobraževanju na daljavo kot javnopravni nalogi skladno s Splošno uredbo ni ustrezna pravna podlaga. Pravna podlaga za obdelavo osebnih podatkov otrok v okviru izobraževanja na daljavo z uporabo orodij za izvajanje pouka prek spleta (kot je npr. Zoom) je bila po mnenju Informacijskega pooblaščenca točka (c) prvega odstavka člena 6 Splošne uredbe (obdelava je potrebna za izpolnitev zakonske obveznosti, ki velja za upravljavca) v zvezi s predpisi, ki opredeljujejo osnovnošolsko in srednješolsko izobraževanje, kot so Zakon o osnovni šoli, Zakon o gimnazijah ter Zakon o poklicnem in strokovnem izobraževanju. Navedeni predpisi določajo obveznost šol, da zagotavljajo predvidene oblike izobraževanja, ter dolžnost učencev in dijakov, da izpolnjujejo svoje šolske obveznosti. Pri tem je Informacijski pooblaščenec večkrat poudaril, da bi morale biti šole oz. učitelji opozorjeni na načelo najmanjšega obsega podatkov, po katerem se ne sme obdelovati več osebnih podatkov, kot je nujno potrebno za izvedbo izobraževalnega procesa (načelo minimizacije osebnih podatkov). Šole kot upravljavci osebnih podatkov pa so bile dolžne zagotoviti ustrezno zavarovanje osebnih podatkov v vseh fazah izvajanja učnega procesa na daljavo. Informacijski pooblaščenec je pozval Ministrstvo za izobraževanje, znanost in šport, da pravno podlago ustrezno konkretizirata z enotnimi navodili šolam. Tako bi bilo treba natančno opredeliti, v katerih primerih je npr. dovoljeno snemanje učnega procesa.

Aplikacija za sledenje stikom #Ostanizdrav in vabljenje posameznikov k namestitvi aplikacije s strani operaterjev

Informacijski pooblaščenec je v procesu sprejemanja Zakona o interventnih ukrepih za pripravo na drugi val covid-19, ki je uzakonil delovanje mobilne aplikacije, večkrat javno poudaril, da aplikacije za sledenje stikov nedvomno pomenijo obdelavo osebnih podatkov državljanov. Podatki o stikih posameznika ne predstavljajo anonimnih podatkov, temveč gre za obdelavo osebnih podatkov, pogosto tudi občutljivih osebnih podatkov, ki so varovani s Splošno uredbo, ZVOP-1 in Ustavo RS. Opozarjal je tudi na prostovoljno namestitev aplikacije. Namreč, pravne podlage za obvezno rabo aplikacije bi morale spoštovati temeljne standarde varstva pravic posameznikov: morale bi biti zakonite in ustavne, časovno omejene ter nujne in sorazmerne glede na zasledovani cilj (omejevanje epidemije covid-19). Ravno nujnost in sorazmernost pa je v primeru obvezne aplikacije zelo težko zagotoviti, saj si veliko število okuženih posameznikov ne more zagotoviti novejšega tipa pametnega telefona, ki omogoča zanesljivo delovanje aplikacije.

V inšpekcijskih postopkih je Informacijski pooblaščenec obravnaval veliko število prijav posameznikov, ki so bili prek prejetih SMS-sporočil povabljeni k namestitvi aplikacije #OstaniZdrav. V inšpekcijskem postopku je Informacijski pooblaščenec ugotovil, da je Nacionalni inštitut za javno zdravje skupaj z Uradom vlade za komuniciranje sooblikoval pobudo za operaterje in jih pozval, da pošljejo kratko sporočilo svojim naročnikom, v kolikor za to obstaja primerna pravna podlaga. Nacionalni inštitut za javno zdravje tako ni nastopal ne kot upravljavec ne kot obdelovalec osebnih podatkov. Zakonitost pošiljanja SMS-sporočil z namenom promocije aplikacije je urejeno z Zakonom o elektronskih komunikacijah (ZEKom-1), ki operaterjem elektronskih komunikacij postavlja omejitve glede dopustne obdelave osebnih podatkov pri zagotavljanju storitev (npr. za katere namene se lahko obdelujejo osebni podatki). Nadzor nad ZEKom-1 izvaja Agencija za komunikacijska omrežja in storitve Republike Slovenije, zato o tej zadevi Informacijski pooblaščenec ni bil pristojen dokončno odločati.

Zavarovanje osebnih podatkov

Nezakonito razkritje osebnih podatkov je ena pogostih kršitev, o katerih zavezanci sporočajo v okviru uradnih obvestil o kršitvi varnosti osebnih podatkov. Upravljavci morajo osebne podatke zavarovati tako, da izvajajo primerne tehnične in organizacijske ukrepe, ki zagotovijo njihovo varnost glede na konkretna opredeljena tveganja. Splošna uredba v členu 32 primeroma določa ukrepe, kot so: psevdonimizacija in šifriranje osebnih podatkov; zmožnost zagotoviti stalno zaupnost, celovitost, dostopnost in odpornost sistemov in storitev za obdelavo; zmožnost pravočasno povrniti razpoložljivost in dostop do osebnih podatkov v primeru fizičnega ali tehničnega incidenta ter postopek rednega testiranja, ocenjevanja in vrednotenja učinkovitosti tehničnih in organizacijskih ukrepov za zagotavljanje varnosti obdelave. Ob tem mora upravljavec upoštevati tudi še veljavno določbo 24. člena ZVOP-1, ki določa, da zavarovanje osebnih podatkov obsega organizacijske, tehnične in logično-tehnične postopke in ukrepe, s katerimi se varujejo osebni podatki, preprečuje slučajno ali namerno nepooblaščeno uničevanje podatkov, njihova sprememba ali izguba ter nepooblaščena obdelava teh podatkov, med drugim tako, da se preprečuje nepooblaščen dostop do osebnih podatkov pri njihovem prenosu, vključno s prenosom po telekomunikacijskih sredstvih in omrežjih ter zagotavlja učinkovit način blokiranja, uničenja, izbrisa ali anonimiziranja osebnih podatkov.

Skladno s 25. členom ZVOP-1 pa morajo upravljavci v svojih aktih predpisati postopke in ukrepe za zavarovanje osebnih podatkov ter določiti osebe, ki so odgovorne za določene zbirke osebnih podatkov, in osebe, ki lahko zaradi narave njihovega dela obdelujejo določene osebne podatke.

Upravljavci morajo zagotoviti varnost podatkov tudi v primeru pošiljanja le-teh posameznikom po pošti. Na primer, Informacijski pooblaščenec je v inšpekcijskem nadzoru ugotovil, da izpis identifikacijske številke in črtne kode na ovojnici skupaj z imenom, priimkom, ulico, pošto, štirimestno oznako številke na ovojnici, v kateri je bila poslana personalna kartica, ter navedba teh podatkov na ovojnici, v kateri je bilo ločeno poslano geslo, skupaj s pripisom, da pošiljka vsebuje geslo za personalno kartico, ni v skladu z določbami Splošne uredbe in ZVOP-1 glede zavarovanja osebnih podatkov. Namreč, identifikacijska številka naslovnika personalne kartice predstavlja posameznikov osebni podatek, za katerega zavezanec v konkretnem primeru ni izkazal, da bi bil nujen za samo pošiljanje kartice in gesla. Črtna koda, natisnjena na ovojnici, predstavlja psevdonimiziran osebni podatek, ki ga sicer na prvi pogled ni mogoče povezati s posameznikom, vendar ima še vedno naravo osebnega podatka in je dostopen vsakomur, ki ima ustrezen čitalec črtnih kod. Upravljavec tako z razkritjem identifikacijske številke naslovnika in vsebino pošiljke ni zagotovil varstva osebnih podatkov, saj ni zagotovil, da se z osebnimi podatki, ki niso nujni za samo pošiljanje, ne bi seznanile nepooblaščene osebe.

Posredovanje posnetkov videonadzornega sistema

Pravila o zavarovanju osebnih podatkov, ki jih določata Splošna uredba in ZVOP-1 je treba upoštevati tudi, kadar upravljavec sicer na zakoniti pravni podlagi posreduje posnetke videonadzornega sistema tretji osebi. Upravljavec je na podlagi 10. člena Zakona o odvetništvu odvetniški družbi posredoval videoposnetke nadzornih kamer v skupnem trajanju 24 ur, pri čemer ni zagotovil zakritja osebnih podatkov oseb, ki so na posnetkih. Prav tako v notranjih aktih upravljavca ni bilo navedeno, kateri so kriteriji za presojo upravičenosti za posredovanje podatkov, vključno s presojo sorazmernosti same zahteve. Upravljavec je sicer v svojem Pravilniku o izvajanju videonadzora predvidel posredovanje videoposnetkov drugim uporabnikom oz. tretjim osebam, v kolikor so ti ustrezno obdelani na način, ki onemogoča posredno oziroma neposredno identifikacijo posameznika, vendar ni določil postopka oz. načina obdelave posnetkov, s katerim se lahko onemogoči (posredna oz. neposredna) identifikacija posameznikov. Upravljavci morajo vzpostaviti ustrezna pravila in postopke posredovanja videoposnetkov nadzornih kamer, vključno z navodili zaposlenim, ki posredovanje videoposnetkov izvajajo. Iz navodil mora biti nedvoumno in jasno razvidno, v katerih primerih je posredovanje posnetkov zakonito in sorazmerno, kakšni ukrepi so potrebni pred posredovanjem posnetkov ter način izvedbe teh ukrepov, da se zagotovi zavarovanje osebnih podatkov.

Izbris osebnih podatkov, ki se hranijo za namene arhiviranja v javnem interesu

Med pravice posameznika po Splošni uredbi uvrščamo tudi pravico do izbrisa oz. do pozabe, ki je določena v členu 17 Splošne uredbe. Skladno s členom 17(1) Splošne uredbe ima posameznik, na katerega se nanašajo osebni podatki, pravico doseči, da upravljavec brez nepotrebnega odlašanja izbriše osebne podatke v zvezi z njim, upravljavec pa ima obveznost osebne podatke brez nepotrebnega odlašanja izbrisati, kadar: osebni podatki niso več potrebni za namene, za katere so bili zbrani ali kako drugače obdelani; posameznik, na katerega se nanašajo osebni podatki, prekliče privolitev, na podlagi katere poteka obdelava in kadar za obdelavo ne obstaja nobena druga pravna podlaga; posameznik, na katerega se nanašajo osebni podatki, ugovarja obdelavi skladno s členom 21 (obdelavi, ki poteka zaradi opravljanja nalog v javnem interesu oz. na podlagi zakonitih interesov upravljavca), pa za njihovo obdelavo ne obstajajo nobeni prevladujoči zakoniti razlogi, ali pa posameznik, na katerega se nanašajo osebni podatki, obdelavi ugovarja v primeru neposrednega trženja; osebni podatki so bili obdelani nezakonito; osebne podatke je treba izbrisati za izpolnitev pravne obveznosti v skladu s pravom Unije ali pravom države članice, ki velja za upravljavca; osebni podatki so bili zbrani v zvezi s ponudbo storitev informacijske družbe od mladoletne osebe.

Pravica do izbrisa pa ni neomejena, saj Splošna uredba določa, da izbrisa osebnih podatkov ni mogoče uveljavljati, če je obdelava potrebna npr. za uresničevanje pravice do svobode izražanja in obveščanja; za namene arhiviranja v javnem interesu, za znanstveno- ali zgodovinskoraziskovalne namene ali statistične namene ali npr. za uveljavljanje, izvajanje ali obrambo pravnih zahtevkov.

V eni izmed obravnavanih inšpekcijskih zadev je posameznik pri svoji župniji vložil zahtevo za izbris svojih osebnih podatkov iz krstne matične knjige. Zatrjeval je, da že vrsto let ni več član Katoliške cerkve in posledično ne izpolnjuje cerkvene zakonodaje, zato podatki niso več potrebni za namene, za katere so bili zbrani in nadalje obdelani. Poudaril je tudi, da bi naj bila obdelava njegovih občutljivih osebnih podatkov nezakonita, saj naj bi Cerkev nikoli ne pridobila njegove svobodne privolitve za izvedbo krsta in obdelavo njegovih osebnih podatkov. Menil je, da javni in zakoniti interes, namen arhiviranja in statistični nameni niso izkazani oz. da nad njimi prevlada interes in temeljne pravice in svoboščine posameznika.

Opozorimo naj, da je skladno s svojimi pristojnostmi Informacijski pooblaščenec presojal zgolj posameznikovo zahtevo za izbris podatkov glede krsta ter se v postopku ni opredeljeval do morebitnega članstva posameznika v skupnosti upravljavca oziroma drugih vprašanjih, za katere Informacijski pooblaščenec ni pristojen. Informacijski pooblaščenec je v tej zadevi presojal določbo člena 17(3) Splošne uredbe, skladno s katero posameznik ne more zahtevati izbrisa podatkov v primeru, da je obdelava potrebna za namene arhiviranja v javnem interesu za znanstveno- ali zgodovinskoraziskovalne namene ali za statistične namene. Ugotovljeno je bilo, da upravljavec osebnih podatkov v t. i. krstni knjigi obdeluje osebne podatke posameznika, in sicer njegovo ime, priimek, datum rojstva, datum krsta, podatke o njegovih starših in botrih ter naslov stalnega prebivališča ob krstu. Upravljavec osebnih podatkov ni pridobil na podlagi privolitve posameznika, temveč so privolitev podali njegovi starši kot zakoniti zastopniki. Navedene osebne podatke upravljavec obdeluje, saj že sama hramba teh podatkov predstavlja obdelavo osebnih podatkov. Pri presoji, ali gre v danem primeru za namene arhiviranja v javnem interesu oz. za znanstveno- ali zgodovinskoraziskovalne namene, je Informacijski pooblaščenec upošteval vrsto in naravo zbirke oz. gradiva in ugotovil, da je gre pri tem za posebne matične, krstne knjige, ki jih upravljavec vodi dolgo časovno obdobje in katerih pomen in vrednost bi za navedene namene težko zavrnili, na kar kaže tudi določba 52. člena Zakona o varstvu dokumentarnega in arhivskega gradiva ter arhivih (ZVDAGA). ZVDAGA v 52. členu določa, da se arhivsko gradivo Rimskokatoliške cerkve odbere iz cerkvenega dokumentarnega gradiva v skladu z njenimi predpisi in ima lastnosti arhivskega gradiva po tem zakonu. Ministrstvo, pristojno za arhive, v dogovoru s Slovensko škofovsko konferenco določi posamezne pogoje za opravljanje arhivske dejavnosti in dogovorjena sredstva za opravljanje arhivske dejavnosti Rimskokatoliške cerkve.

Brisanje podatkov iz krstne knjige bi tako vsaj resno oviralo uresničevanje teh namenov, pri tem pa že sam ZVDAGA kakor tudi Splošna uredba določata obveznost sprejetja zaščitnih ukrepov za zavarovanje osebnih podatkov. Tako Informacijski pooblaščenec pritožbi posameznika glede izbrisa osebnih podatkov iz matične knjige ni ugodil. Posameznik se z odločitvijo Informacijskega pooblaščenca ni strinjal in je zoper odločitev vložil tožbo, tako da bo moralo o zadevi dokončno odločiti Upravno sodišče Republike Slovenije.

Zahteva za omejitev obdelave objavljenega prispevka

Med pravice posameznika po Splošni uredbi spada tudi pravica do omejitve obdelave (člen 18 Splošne uredbe). Posameznik, na katerega se nanašajo osebni podatki, ima pravico doseči, da upravljavec omeji obdelavo, kadar velja en od naslednjih primerov: posameznik, na katerega se nanašajo osebni podatki, oporeka točnosti podatkov, in sicer za obdobje, ki upravljavcu omogoča preveriti točnost osebnih podatkov; obdelava je nezakonita in posameznik, na katerega se nanašajo osebni podatki, nasprotuje izbrisu osebnih podatkov ter namesto tega zahteva omejitev njihove uporabe; upravljavec osebnih podatkov ne potrebuje več za namene obdelave, temveč jih posameznik, na katerega se nanašajo osebni podatki, potrebuje za uveljavljanje, izvajanje ali obrambo pravnih zahtevkov; posameznik, na katerega se nanašajo osebni podatki, je vložil ugovor v zvezi z obdelavo v skladu s členom 21(1), dokler se ne preveri, ali zakoniti razlogi upravljavca prevladajo nad razlogi posameznika, na katerega se nanašajo osebni podatki.

Kadar je bila obdelava osebnih podatkov omejena, se taki osebni podatki z izjemo njihovega shranjevanja obdelujejo le s privolitvijo posameznika, na katerega se nanašajo, ali za uveljavljanje, izvajanje ali obrambo pravnih zahtevkov ali zaradi varstva pravic druge fizične ali pravne osebe ali zaradi pomembnega javnega interesa EU ali države članice.

Ustava RS v 38. členu zagotavlja varstvo osebnih podatkov, vendar sama objava posameznikovih osebnih podatkov v medijih še ne pomeni nujno kršitve predpisov s področja varstva osebnih podatkov. V primeru objave osebnih podatkov gre namreč lahko tudi za poseg v širšo pravico do zasebnosti iz 35. člena Ustave RS in sodi v pristojnost sodišč. Ugoditev zahtevi posameznika za omejitev obdelave bi po drugi strani pomenila omejitev upravljavčeve pravice do svobode izražanja v korist pravici do varstva osebnih podatkov. Kot je poudarilo Ustavno sodišče v svoji odločbi, svoboda izražanja ni le neposreden izraz posameznikove osebnosti v družbi, temveč tudi konstitutivni element svobodne demokratične družbe. Prvi odstavek 39. člena Ustave RS zato kot poseben vidik varuje svobodo novinarskega izražanja, ki ne zagotavlja le posameznikove (novinarjeve) pravice, temveč se s tiskom in drugimi javnimi mediji uresničuje tudi demokratična pravica javnosti do obveščenosti o zadevah javnega pomena. Skladno s tretjim odstavkom 15. člena Ustave RS so človekove pravice in temeljne svoboščine omejene samo s pravicami drugih ljudi oz. v primerih, ki jih določa ustava. Pravica do informacijske zasebnosti kakor tudi pravica do svobode izražanja nista neomejeni, zato je treba v primeru kolizije dveh pravic v konkretnem primeru odločiti, kateri je treba dati prednost in katera se mora zaradi aktiviranja nujne, ustavno varovane vsebine druge pravice tej umakniti oziroma se mora umakniti del upravičenj, ki sestavljajo to pravico. Tako je Informacijski pooblaščenec presojal kolizijo teh dveh pravic v primeru, ko je posameznik želel uveljaviti pravico do omejitve obdelave članka, ki je bil objavljen na spletu. V postopku je bilo ugotovljeno, da je članek temeljil na podatkih, katerih vir je bilo predhodno poročanje drugih medijev in pripoved znanca posameznika, podatki pa niso bili pridobljeni iz zbirke podatkov. Upravljavec je na spletni strani tudi posamezniku omogočil prikaz nasprotnih dejstev. Glede na okoliščine kolizije obeh pravic je Informacijski pooblaščenec odločil, da bi ugoditev posameznikovi zahtevi za omejitev obdelave članka pomenila prekomeren poseg v pravico do svobode izražanja, zato posameznikovi zahtevi za omejitev obdelave osebnih podatkov ni ugodil. Posameznik se tudi v tem primeru z odločitvijo Informacijskega pooblaščenca ni strinjal in je zoper odločitev vložil tožbo, tako da bo moralo o zadevi dokončno odločiti Upravno sodišče Republike Slovenije.

Pravica do popravka osebnih podatkov v sistemu SISBON

Posameznik, na katerega se nanašajo osebni podatki, ima pravico doseči, da upravljavec brez nepotrebnega odlašanja popravi netočne osebne podatke, ki se nanj nanašajo. Posameznik, na katerega se nanašajo osebni podatki, ima ob upoštevanju namenov obdelave pravico do dopolnitve nepopolnih osebnih podatkov, vključno s predložitvijo dopolnilne izjave.

Informacijski pooblaščenec je odločal o pravici do popravka v zbirki osebnih podatkov centralnega kreditnega registra SISBON, ki ga upravlja Banka Slovenije. Poročanje v SISBON poteka skladno s priročnikom Banke Slovenije za poročanje poslovnih dogodkov. Podatki in informacije, ki se obdelujejo v sistemu SISBON, so namenjeni upravičencem (npr. bankam, kreditodajalcem, ponudnikom plačilnih storitev itd.) pri ocenjevanju kreditne sposobnosti kreditojemalcev in kreditnega tveganja, ki bi s sklenitvijo posameznega kreditnega posla nastalo za določenega upravičenca ali je nastalo v zvezi z izvajanjem kreditnega posla. Upravljavec (banka) je v obravnavani inšpekcijski zadevi prodal terjatev posameznika podjetju in v SISBON sporočil stanje dogodka »Zaključek posla, kjer dolg ni bil poravnan«. V trenutku vpisa je bilo navedeno stanje dogodka

vpisano skladno z veljavnimi pravili poročanja v SISBON. Od uveljavitve Zakona o centralnem kreditnem registru (ZCKR), od decembra 2016 dalje, pa se prodaja terjatev posameznikov v sistemu SISBON označuje z dogodkom »Zaključek posla zaradi odprodaje dolga«.

Posameznik je terjatve družbi poravnal konec marca 2017, vendar mu je navedeni vpis povzročal težave pri sklepanju kreditnih in drugih poslov z bankami. Banka je namreč posamezniku dvakrat zavrnila prošnjo za limit izključno zaradi vpisa, zabeleženega v SISBON. Posameznik je želel doseči, da bi se prodana terjatev v sistemu SISBON beležila kot »Zaključek posla zaradi odprodaje dolga«. Posameznik je na podlagi določb ZCKR od banke, ki je njegovo terjatev odprodala, zahteval popravo napačnih podatkov tako, da jih dopolni, izbriše ali spremeni ter zagotovi vpis pravilnega podatka. Banka je njegovo zahtevo zavrnila in pojasnila, da terjatve niso poplačane, da jih je upravljavec odstopil družbi, ki pa ni zavezana poročanju v SISBON, in da so terjatve zapisane skladno s pravili poročanja v SISBON. V SISBON prostega besedila ni bilo mogoče vpisovati in tudi popravki na posameznem dogodku oz. poslu niso mogoči in se spremenijo zgolj, če pride do spremembe poročanja vrste posla oz. dogodka. Vsak upravljavec lahko poroča v SISBON zgolj o svojih poslih, in če je terjatev člana prodana subjektu, ki ni član sistema SISBON, se s tem zaključi poročanje v SISBON in tega zapisa ne more popraviti niti noben član sistema niti sam upravljavec sistema. Podatki o posameznem kreditnem poslu se hranijo v SISBON za obdobje štirih let po prenehanju obveznosti, ki izhaja iz kreditnega posla. V trenutku predmetne zadeve pa status »Zaključek posla zaradi odprodaje dolga« še ni obstajal in sistem popravo tega podatka za nazaj ni dovoljeval.

Informacijski pooblaščenec je ugotovil, da upravljavec posamezniku z zavrnitvijo popravka oz. dopolnitvijo vpisa v SISBON ni omogočil uresničevanja pravice do popravka netočnih podatkov, poleg tega je kršil načelo točnosti podatkov iz Splošne uredbe. Dejstvo, da banka, ki je terjatev prodala, ni več v vlogi upnika, banke ne obvezuje odgovornosti za točnost in ažurnost podatkov, ki jih je v preteklosti vpisala v SISBON. Veljavna pravila vpisovanja dogodkov v SISBON posameznikom niso omogočala pravice do popravka netočnih podatkov, kar je imelo za posameznike resne posledice, saj so dajalci kreditov podatkom v SISBON očitno pripisovali odločilen pomen, podatki v SISBON pa glede na ugotovljeno niso mogli biti v vsakem trenutku in v vsakem primeru točni in ažurni.

Izvajanje biometričnega preverjanja potnikov na letališču

Informacijski pooblaščenec je v okviru čezmejnih inšpekcijskih postopkov vodil tudi postopek inšpekcijskega nadzora zoper špansko podjetje, ki deluje na področju sistema rezervacij letalskih kart, sedež ima v Madridu. Zaradi strožjega varstva osebnih podatkov na področju biometrije po ZVOP-1 v primerjavi s Splošno uredbo je Informacijski pooblaščenec postopek, ki sicer izpolnjuje vse pogoje čezmejne obdelave osebnih podatkov in ki bi ga moral, glede na sedež podjetja, voditi španski nadzorni organ, vodil kot »lokalni primer«. Takšno možnost predvideva Splošna uredba v postopkih čezmejnega sodelovanja: nadzornim organom, ki bi sicer v postopkih sodelovali zgolj kot zadevni nadzorni organi, omogoča, da imajo dejansko enake pristojnosti kot vodilni nadzorni organ. Informacijski pooblaščenec je v postopku preverjal zakonitost obdelave biometričnih osebnih podatkov v okviru pilotnega projekta vkrcavanja potnikov z uporabo biometrije na Letališču Jožeta Pučnika, ki ga je v celoti izvajalo špansko podjetje. Španskemu nadzornemu organu je glede na strožje določbe ZVOP-1 glede biometrijskih ukrepov predlagal, da vodi postopek na lokalni ravni, s čimer se je španski nadzorni organ strinjal. Splošna uredba tudi za takšne primere vodenja inšpekcijskih postopkov nadzornim organom omogoča uporabo mehanizma medsebojne pomoči (člen 61 Splošne uredbe), s pomočjo katerega je celotna komunikacija s podjetjem potekala prek španskega nadzornega organa.

Informacijski pooblaščenec je v postopku ugotovil, da je špansko podjetje z izvajanjem biometrijskih ukrepov v okviru pilotnega projekta vkrcavanja potnikov na Letališču Jožeta Pučnika kršilo določbe ZVOP-1, saj za takšno obdelavo osebnih podatkov Informacijskemu pooblaščencu ni posredovalo opisa nameravanih ukrepov in razlogov za njihovo uvedbo, da bi ta lahko odločil in zavezanca obvestil, da nameravana uvedba biometrijskih ukrepov ni v skladu z ZVOP-1. Poleg tega je podjetje biometrijske ukrepe izvajalo z namenom hitrejšega in učinkovitejšega prehoda potnikov prek letališkega sistema, nad potniki, ki niso bili njegovi zaposleni, in ne da bi za to prejel odločbo nadzornega organa, s katero bi bilo izvajanje biometrijskih ukrepov dovoljeno.

Vdor v informacijski sistem hotelske verige in kršitev varstva osebnih podatkov

Upravljavec – hotelska veriga – je pripojil družbo, v katere informacijski sistem je že pred pripojitvijo vdrl neznani napadalec. Upravljavec za vdor ni vedel ne v postopku pripojitve ne pozneje. Z vdorom je bil seznanjen šele, ko je napadalec sprožil varnostni alarm, med drugim v povezavi s tabelami, ki so vsebovale podatke o imetnikih kartic. Napadalec naj bi pridobil osebne podatke tako v šifrirani kot v nešifrirani obliki. Nešifrirani osebni podatki so vsebovali podatke iz profilov strank, vključno s podatki o rezervacijah. Šifrirani podatki pa so vsebovali 18,5 milijona številk potnih listin in 9,1 milijona številk plačilnih kartic. Upravljavec je o zaznanem vdoru obvestil posameznike in sprejel ukrepe za zmanjšanje posledic vdora. O vdoru oziroma kršitvi varnosti osebnih podatkov je obvestil vodilni nadzorni organ iz Združenega Kraljestva. V postopku smo kot zadevni organi sodelovali vsi organi iz držav članic EU. Prizadeti so bili tudi posamezniki iz Slovenije, kjer se prav tako nahaja hotel iz verige upravljavca.

Vodilni nadzorni organ je ugotovil, da upravljavec ni zagotovil ustreznih tehničnih in organizacijskih ukrepov za zagotovitev ustrezne ravni varnosti osebnih podatkov, kot je to določeno v členih 5(1)(f) in 32 Splošne uredbe. Vodilni nadzorni organ je med drugim ugotovil, da upravljavec ni dovolj učinkovito nadzoroval privilegiranih računov in zbirk ter da ni zagotovil, da bi bile aktivnosti v sistemu ustrezno nadzorovane. Ugotovljeno je bilo tudi, da upravljavec v nekaterih primerih ni zagotovil šifriranja vseh številk potnih listin ter drugih kategorij osebnih podatkov. Ob upoštevanju določenih olajševalnih okoliščin je vodilni nadzorni organ upravljavcu naložil globo v višini 18,4 milijona GBP.

Mobilna aplikacija za izvajanje potegavščin in snemanje brez vednosti osebe

Informacijski pooblaščenec je prejel prijavo posameznika iz RS zoper upravljavca iz Španije. Po postopku sodelovanja iz poglavja VII Splošne uredbe je španski nadzorni organ kot vodilni nadzorni organ na podlagi posredovane prijave uvedel in vodil postopek, v katerem je preverjal skladnost obdelav, ki jih izvaja upravljavec, z določbami Splošne uredbe. Upravljavec je razvil mobilno aplikacijo, katere namen je omogočiti posameznikom izvajanje telefonskih potegavščin, in sicer tako, da posameznik izbere osebo, ki jo bo upravljavec poklical in izvedel potegavščino, pri tem pa aplikacija pogovor tudi posname. Oseba, ki prejme klic s potegavščino, nima informacij o obdelavi osebnih podatkov in od upravljavca ne more zahtevati izbrisa posnetka. Španski nadzorni organ je v postopku predvsem preverjal skladnost obdelave osebnih podatkov tako posameznikov, ki želijo prek aplikacije izvesti potegavščino, kot tretjih oseb, ki prejmejo klic, in sicer je preverjal ustreznost pravnih podlag iz člena 6 ter informiranost glede obdelave osebnih podatkov iz členov 12, 13 in 14 Splošne uredbe. Vodilni nadzorni organ je med drugim ugotovil, da v obravnavanem primeru ne gre za zasebno rabo v smislu člena 2(2)(c) Splošne uredbe ter da je upravljavec odgovoren za obdelavo osebnih podatkov posameznikov, saj brez njegove aktivne vloge do obdelave sploh ne bi prišlo, poleg tega pa je prav navedena obdelava glavna dejavnost (in vir prihodkov) upravljavca. Upravljavec ni izkazal pravne podlage za obdelavo, saj privolitev od tretjih oseb ne pridobiva oziroma prelaga pridobitev privolitve na posameznika, ki želi izvesti potegavščino, zakoniti interes pa ne prevlada nad interesi in pravicami tretjih oseb, saj z njimi sploh niso seznanjene in mu zato ne morejo učinkovito ugovarjati. Upravljavec tudi ne zagotavlja ustreznega informiranja oseb, katerih osebne podatke obdeluje. Na podlagi ugotovljenega je španski nadzorni organ upravljavcu odredil, da v roku treh mesecev uskladi obdelavo osebnih podatkov z določbami Splošne uredbe, predvsem vzpostavi postopek, da se lahko poda ustrezna privolitev ter da zagotovi informacije o obdelavi osebnih podatkov. Navedeno mora upravljavec zagotoviti v vseh državah Evropskega gospodarskega prostora (EEA), v katerih je aplikacija dostopna. Ob upoštevanju nekaterih oteževalnih okoliščin je vodilni nadzorni organ upravljavcu naložil globo v višini 40.000 EUR (po 20.000 EUR za vsako od ugotovljenih kršitev).

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 2020 prejel pet vlog za izdajo dovoljenja za uvedbo biometrijskih ukrepov in tudi izdal pet odločb:

- Enemu vlagatelju je za namen opravljanja dejavnosti, varovanja poslovnih skrivnosti in zagotavljanja varnosti njegovega premoženja ter premoženja tretjih oseb dovolil izvajanje biometrijskih ukrepov za vstopanje v laboratorij znotraj poslovnih prostorov vlagatelja na njegovem sedežu, in sicer z uporabo enega čitalca prstnih odtisov ob vhodu v laboratorij, v katerem se odvijajo najbolj občutljivi procesi s področja vlagateljeve dejavnosti (izvajanje akreditiranih meritev sistemov).
- Tri vloge za izvajanje biometrijskih ukrepov je zavrnil, ker je vlagatelj želel biometrijske ukrepe z uporabo naprave za prepoznavo 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.
- Eno vlogo za izvajanje biometrijskih ukrepov za vstopanje v poslovne prostore vlagatelja je zavrnil zato, ker vlagatelj ni izkazal nujnosti uvedbe biometrijskih ukrepov za namen zagotavljanja varnosti njegovega premoženja. Vlagatelj namreč ni konkretiziral, kdo in na kakšen način ogroža njegovo premoženje, kakšna je njegova približna vrednost ter kakšne ukrepe za preprečevanje njegovega ogrožanja je že sprejel.

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.

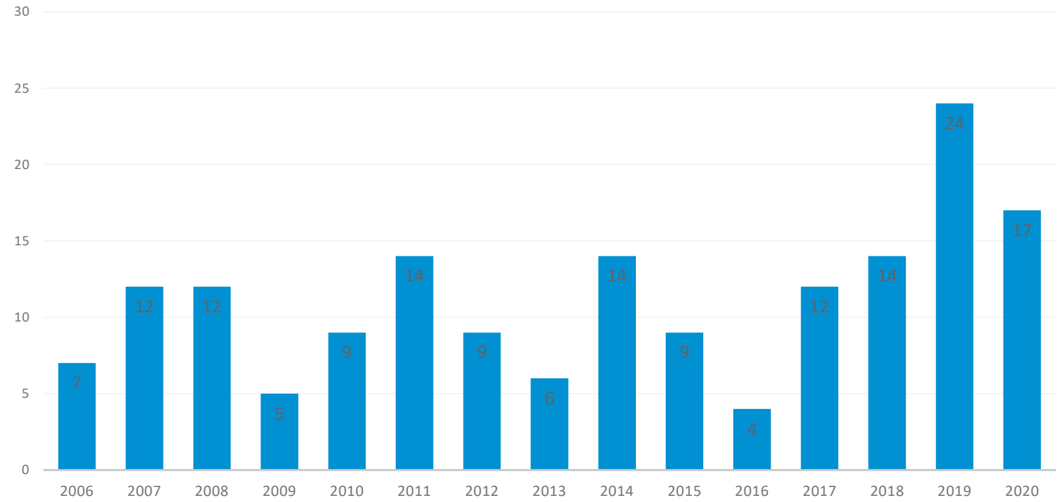
Informacijski pooblaščenec je leta 2020 prejel 17 vlog za pridobitev dovoljenja za povezovanje zbirk osebnih podatkov. Izdal je 15 odločb, in sicer 13 odločb, s katerimi je upravljavcem povezovanje zbirk osebnih podatkov

dovolil, ter dve odločbi, s katerima povezovanja zbirk osebnih podatkov ni dovolil. Dva vlagatelja sta vlogo umaknila, zato je Informacijski pooblaščenec postopka ustavil.

Izdane odločbe glede povezovanja javnih evidenc.

	Upravljavec 1	Zbirka osebnih podatkov 1	Upravljavec 2	Zbirka osebnih podatkov 2	Povezovalni znak
1.	Ministrstvo za infrastrukturo Republike Slovenije	Evidenca voznikov, ki so usposobljeni za vožnjo motornih vozil za prevoz potnikov ali blaga v cestnem prometu	Ministrstvo RS za notranje zadeve	Centralni register prebivalstva (CRP) Evidenca potnih listin Evidenca osebnih izkaznic	EMŠO
2.	Ministrstvo za izobraževanje, znanost in šport RS	Evidenčni in analitski informacijski sistem visokega šolstva RS Evidenca študentov in diplomantov (eVŠ – EŠD) Centralna evidenca udeležencev vzgoje in izobraževanja (CEUVIZ)	Študentski, d. o. o	Evidenca o dijakih in študentih, članih študentskega servisa	EMŠO
3.	Finančna uprava RS	Evidenca o odmeri davka na dediščine in darila Evidenca o odmeri davka na promet nepremičnin Evidenca o odmeri dohodnine od dohodka iz oddajanja premoženja v najem	Ministrstvo za okolje in prostor RS, Geodetska uprava RS	Evidenca vrednotenja nepremičnin	EMŠO
4.	Kapitalska družba pokojninskega in invalidskega zavarovanja, d. d.	Evidenca o zavarovancih – članih Sklada obveznega dodatnega pokojninskega zavarovanja Evidenca o obračunanih in plačanih prispevkih za poklicno zavarovanje	Finančna uprava RS	Evidenca o davkih	davčna številka
5.	Študentska organizacija Slovenije	Evidenca študentskega dela (EŠD)	Tevis, d. o. o.	Zbirka osebnih podatkov dijakov in študentov, ki so opravljali študentsko delo	EMŠO
6.	Agencija Republike Slovenije za javnopravne evidence in storitve	Register neposestnih zastavnih pravic in zarubljenih nepremičnin	Ministrstvo RS za notranje zadeve Finančna uprava RS, Generalni finančni urad Ministrstvo za infrastrukturo	Centralni register prebivalstva (CRP) Davčni register (DR) Evidenca registriranih vozil (MRVL)	EMŠO davčna številka VIN številka vozila
7.	Zavod RS za zaposlovanje	Zbirka osebnih podatkov po ZIUZEOP	Finančna uprava RS	Evidenca obračunov davčnega odtegljaja (REK obrazcev)	davčna številka
8.	Študentska organizacija Slovenije	Evidenca študentskega dela (EŠD)	Posavc, d. o. o.	Zbirka osebnih podatkov dijakov in študentov, ki so opravljali študentsko delo	EMŠO
9.	Ministrstvo za finance RS, Urad za preprečevanje pranja denarja	Evidenca podatkov o osebah in transakcijah iz 68. in 69. člena ZPPDFT-1 Evidenca o prejetih pobudah iz 99. in 100. člena ZPPDFT Evidenca obvestil in informacij iz 101. in 102. člena ZPPDFT-1 Evidenca mednarodnih zaprosil iz 105. in 106. člena ZPPDFT- 1	Agencija RS za javnopravne evidence in storitve	Poslovni register Slovenije (PRS)	davčna številka in/ali EMŠO
			Finančna uprava RS	Evidenca o davkih Evidenca finančnega nadzora Evidenca finančnih preiskav	davčna številka in/ali EMŠO
			Ministrstvo za okolje in prostor RS, Geodetska uprava RS	Evidenca vrednotenja (EVN)	davčna številka in/ali EMŠO
10.	Adecco H. R., kadrovsko svetovanje, d. o. o.	Evidenca dejavnosti obdelave podatkov v študentskem servisu	Ministrstvo za izobraževanje, znanost in šport RS	Evidenčni in analitski informacijski sistem visokega šolstva RS Evidenca študentov in diplomantov (eVŠ – EŠD) Centralna evidenca udeležencev vzgoje in izobraževanja (CEUVIZ)	EMŠO
11.	Finančna uprava RS	Evidenca davčnih blagajn	Študentska organizacija Slovenije	Evidenca študentskega dela	davčna številka
12.	Študentska organizacija Slovenije	Evidenca študentskega dela (EŠD)	Eurosplet, d. o. o.	Zbirka osebnih podatkov dijakov in študentov, ki so opravljali študentsko delo	EMŠO
13.	Študentska organizacija Slovenije	Evidenca študentskega dela (EŠD)	Atama, d. o. o.	Zbirka osebnih podatkov dijakov in študentov, ki so opravljali	EMŠO

Število vlog za izdajo odločbe glede povezljivosti zbirk osebnih podatkov med letoma 2006 in 2020.



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)).

Ob tem je treba opozoriti, da je Sodišče Evropske unije (SEU) v zadevi C-311/18, Schrems II (DPC Ireland proti Facebook Ireland Limited, Maximillian Schrems) odločbo Evropske komisije 2016/1250 o ustreznosti varstva osebnih podatkov, ki ga zagotavlja zasebnostni ščit EU-ZDA, razglasilo za neveljavno. Sodišče je hkrati potrdilo veljavnost standardnih pogodbenih klavzul, ki se še vedno lahko uporabljajo za prenose podatkov v tretje države, ki ne zagotavljajo ustreznega varstva osebnih podatkov. Več o tem v poglavju 3.6.

Informacijski pooblaščenec v letu 2020 ni prejel nobene vloge v zvezi s prenosom podatkov v tretje države.

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 do naslednjih dodatnih informacij:

- namen obdelave podatkov,
- vrste 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, ter za tovrstne zahteve zavezancem, ki niso zavezanci po Splošni uredbi, sta se tudi po 25. 5. 2018 še vedno uporabljala 30. in 31. člen ZVOP-1. ZVOPOKD, ki velja za obdelave osebnih podatkov, ki jih policija, državna tožilstva, Uprava Republike Slovenije za probacijo, Uprava Republike Slovenije za izvrševanje kazenskih sankcij in drugi državni organi Republike Slovenije, ki so zakonsko določeni kot pristojni za področja preprečevanja, preiskovanja, odkrivanja ali pregona kaznivih dejanj ali izvrševanja kazenskih sankcij, obdelujejo za namene izvrševanja teh pristojnosti, je namreč začel veljati šele z 31. 12. 2020. Bistvene razlike ureditve zgoraj navedenih pravic po ZVOP-1 so v ureditvi pritožbenega postopka, saj je Informacijski pooblaščenec v skladu s Splošno uredbo in ZVOPOKD pritožbeni organ za uveljavljanje vseh pravic, ne le pravice do seznanitve.

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.

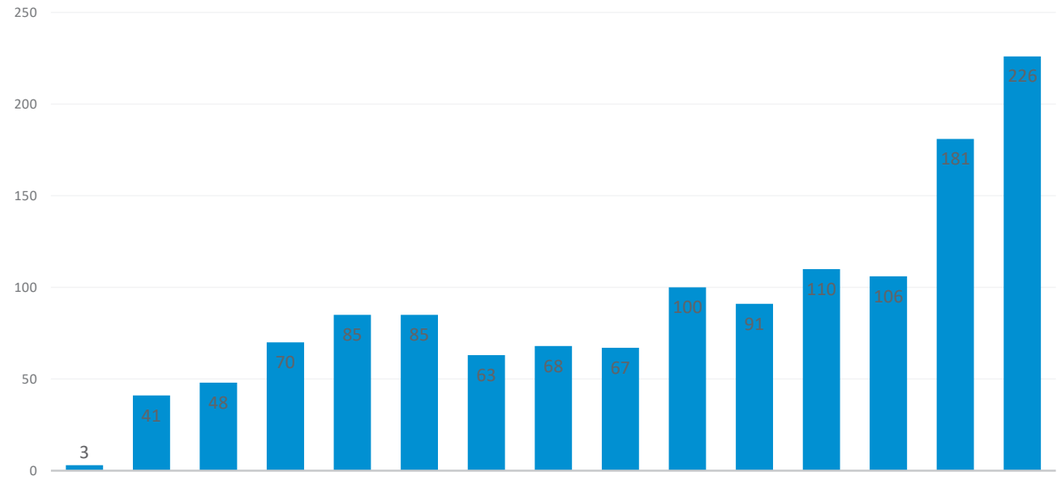
Informacijski pooblaščenec na pritožbeni stopnji odloča tudi o posebnih pravicah glede seznanitve z zdravstveno dokumentacijo po ZPacP, in sicer o:

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 v letu 2020 prejel 226 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. V primerjavi z letom 2019 je prejel 45 pritožb več (tj. 25 % več pritožb), na podlagi česar je mogoče zaključiti, da številni upravljavci osebnih podatkov ne izpolnjujejo svojih obveznosti in posameznikom ne omogočajo izvrševanja pravic, ki jim jih zagotavljajo različni predpisi. Informacijski pooblaščenec je zaznal skrb vzbujajoč trend neupravičenih primerov neodzivnosti ter zavrnitev pravice do seznanitve s strani delodajalcev, ko se želijo zaposleni seznaniti z različnimi lastnimi osebnimi podatki v zvezi z delovnim razmerjem.

Število pritožb v zvezi s pravico do seznanitve z lastnimi osebnimi podatki med letoma 2006 in 2020.



Vložene pritožbe so v 77 primerih zadevale upravljavce iz javnega sektorja (zlasti ministrstva in organe v njihovi sestavi, šole, javne zdravstvene zavode in centre za socialno delo), 149 pritožb pa se je nanašalo na upravljavce iz zasebnega sektorja (npr. banke, operaterje elektronskih komunikacij, gospodarske družbe, odvetnike in zasebne izvajalce zdravstvene dejavnosti). Le 19 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 82 primerih (torej v 36 %) 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 100 primerih, ki so se vodili zaradi molka upravljavca (vključno s postopki, ki so se začeli v letih 2018 in 2019), 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. 11 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 2020 je Informacijski pooblaščenec, vključno s postopki, začetimi v letih 2018 in 2019, izdal 64 upravnih odločb, kar je 68 % več kot leta 2019. V 30 odločbah je pritožbam posameznikov v celoti ugodil in upravljavcem naložil posredovanje določenih osebnih podatkov, v šestih primerih je pritožbam ugodil delno, z 28 odločbami pa je pritožbe posameznikov kot neutemeljene zavrnil. Trije posamezniki so zoper odločitve Informacijskega pooblaščenca sprožili upravni spor pred Upravnim sodiščem RS, dva zoper zavrnilno odločbo, izdano v letu 2020, eden pa zoper sklep o zavrženju vloge zaradi nepristojnosti, izdan v letu 2019.

Informacijski pooblaščenec je s sklepom zavrgel 16 pritožb, in sicer 15 pritožb zaradi postopkovnih pomanjkljivosti (nepopolna, prepozna ali preuranjena vloga, vloga se ni nanašala na pravico do seznanitve z lastnimi osebnimi podatki oz. Informacijski pooblaščenec za obravnavo ni bil pristojen) in eno pritožbo zato, ker je v postopku ugotovil, da je upravljavec zahtevi prosilca že v celoti ugodil, zaradi česar prosilec ni imel (več) pravnega interesa. Šestim posameznikom je Informacijski pooblaščenec posredoval predlog za ravnanje, štiri pritožbe pa je odstopil v reševanje pristojnim organom.

V letu 2020 je Informacijski pooblaščenec obravnaval tudi 5 pritožb zaradi kršitve pravice do popravka po členu 16 Splošne uredbe, 11 pritožb zaradi kršitve pravice do izbrisa po členu 17 Splošne uredbe in eno pritožbo zaradi kršitve pravice do omejitve po členu 18 Splošne uredbe. V dveh zadevah je bila pritožba zavržena (ker je bila nedovoljena oziroma prepozna), v dveh zavrnjena, v eni zadevi pa je bila pritožba odstopljena v reševanje pristojnemu organu. Posameznik je zoper zavrnilno odločbo Informacijskega pooblaščenca v zvezi s pravico posameznika do omejitve obdelave vložil tožbo pred Upravnim sodiščem RS. V eni zadevi se je pritožbeni postopek zaradi molka zaključil, ker je upravljavec v celoti odgovoril na zahtevo prosilca za izbris.

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 2020 je Informacijski pooblaščenec svetoval 3.183 posameznikom in pravnim osebam, ki so se nanj obrnili z vprašanji s področja varstva osebnih podatkov.

Informacijski pooblaščenec je izdal **1.331 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 6.000 mnenj**, ki so razvrščena v 65 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 2020 so državni nadzorniki sprejeli 1.852 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 2020 je Informacijski pooblaščenec izdal 85 mnenj na predloge sprememb zakonov ter na predloge novih zakonov in drugih predpisov, kar je nekoliko več kot leta 2019, ko jih je izdal 73. V preteklem letu je Informacijski pooblaščenec na področju priprave predpisov za obdelavo osebnih podatkov opažal skrb vzbujajoč trend nesistemskega urejanja nekaterih resnih posegov v zasebnost ter poskusov zniževanja že dosežene ravni varstva osebnih podatkov. 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. 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 visoke 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 se prepreči morebitne dodatne stroške ob njenem izvajanju.

Informacijski pooblaščenec je v letu 2020 podal mnenje, pripombe oz. je sodeloval pri pripravi naslednjih predpisov (v zvezi z nekaterimi je podal več mnenj):

- Mnenje glede uporabe zaščitnih ukrepov pri prenosu osebnih podatkov v tretje države in mednarodne organizacije s strani javnih organov,
- Predlog Zakona o spremembah in dopolnitvah Zakona o preprečevanju pranja denarja in financiranja terorizma,
- Predlog Zakona o spodbujanju rabe obnovljivih virov energije,
- Predlog Uredbe o uvedbi preverjanja državljanov tretjih držav na zunanjih mejah,
- Predlog Uredbe o izvajanju izvedbene uredbe Komisije (EU) o pravilih in postopkih za upravljanje brezpilotnih zrakoplovov,
- Predlog Zakona o interventnih ukrepih za omilitev posledic drugega vala epidemije COVID-19 (ZIUOPDVE; PKP6) iz pristojnosti Ministrstva za zdravje,
- Predlog Uredbe o e-zasebnosti DE PRED,
- Predlog ureditve aplikacije za sledenje stikom (PKP6),
- Predlog Letnega programa statističnih raziskovanj za leto 2021,
- Predlog Zakona o spremembah in dopolnitvah Zakona o bančništvu (ZBan-2B),
- Predlog Zakona o varstvu osebnih podatkov na področju obravnavanja kaznivih dejanj (ZVOPOKD),
- Predlog Sprememb in dopolnitev Letnega programa statističnih raziskovanj za 2020,
- Predlog Zakona o elektronskih komunikacijah,
- Predlog Zakona o spremembah in dopolnitvah Zakona o reševanju in prisilnem prenehanju bank (ZRPPB-B),
- Predlog Zakona o spremembah in dopolnitvah Zakona o lokalnih volitvah (ZLV-K),
- Zaprosilo za mnenje glede zakonodajnega predloga spremembe ZZdr,
- Predlog Protokola priporočenega ravnanja v primeru izvršitve odločb o odvzemu otroka z neposredno izvršitvijo,
- Predlog Zakona o spremembah in dopolnitvah Pomorskega zakonika,
- Predlog Zakona o začasnih ukrepih za omilitev in odpravo posledic COVID-19,
- Mnenje glede dveh členov Zakona o interventnih ukrepih za omilitev in odpravo posledic COVID-19 na področju zdravstva in dela (ZPZD),
- Predlog Uredbe o spremembah in dopolnitvah Uredbe o izvajanju ukrepa Sheme kakovosti za kmetijske proizvode in živila iz Programa razvoja podeželja Republike Slovenije za obdobje 2014–2020,
- Predlog Pravilnika o objavah prodaj v spletnem iskalniku in spletnih javnih dražbah v izvršilnih postopkih,
- Predlog o Zakona spremembah in dopolnitvah Zakona o državnem tožilstvu,
- Predlog Zakona o elektronski identifikaciji in storitvah zaupanja,
- Mnenje glede prenosa Direktive (EU) 2019/1151 Evropskega parlamenta in Sveta z dne 20. junija 2019 o spremembi Direktive (EU) 2017/1132 glede uporabe digitalnih orodij in postopkov na področju prava družb,
- Predlog Zakona o znanstvenoraziskovalni in inovacijski dejavnosti,
- Predlog Zakona o nagradi zlata čebela,
- Predlog Zakona o spremembah in dopolnitvah Zakona o kmetijstvu,
- Predlog Zakona o spremembah in dopolnitvah Zakona o sodnih taksah,
- Predlog Zakona o zaščiti otrok v kazenskem postopku in njihovi celostni obravnavi v hiši za otroke,
- Predlog Zakona o katastru nepremičnin,
- Predlog Pravilnika o spremembah in dopolnitvah Pravilnika o strokovnem usposabljanju, obdobnem izpopolnjevanju ter preizkusu znanja občinskih redarjev,
- Predlog Zakona o spremembah in dopolnitvah Zakona o cestninjenju,
- Predlog Zakona o spremembah in dopolnitvah Zakona o izvršbi in zavarovanju – delovno gradivo,
- Predlog Zakona o spremembah in dopolnitvah Zakona o mednarodni zaščiti,
- Predlog Pravilnika o registraciji motornih in priklopnih vozil,
- Predlog sprememb Zakona o osebni izkaznici,

- Predlog Zakona o interventnih ukrepih za pripravo na drugi val COVID-19,
- Predlog Zakona o spremembah in dopolnitvah Zakona o kazenskem postopku,
- Predlog Zakona o spremembah in dopolnitvah Zakona o tujcih,
- Predlog Uredbe o registru neposestnih zastavnih pravic in zarubljenih premičnin,
- Predlog Zakona o spremembah in dopolnitvah zakona o zavarovalništvu,
- Mnenje glede besedila 37. člena Predloga Zakona o interventnih ukrepih za omilitev posledic epidemije nalezljive bolezni SARS-CoV-2 (COVID-19) za državljane in gospodarstvo, sprejeto na 45. dopisni seji Vlade RS 20. 5. 2020,
- Predlog Uredbe o zasebnosti in elektronskih komunikacijah,
- Predlog Zakona o spremembah in dopolnitvah Zakona o referendumu in ljudski iniciativi,
- Predlog Zakona o interventnih ukrepih za zajezitev epidemije COVID-19 in omilitev njenih posledic za državljane in gospodarstvo,
- Predlog Zakona o spremembah in dopolnitvah Zakona o varstvu okolja,
- Predlog Zakona o spremembah in dopolnitvah Zakona o vrtcih,
- Mnenje glede pravne podlage za pridobivanje osebnih podatkov iz sistema e-sociala oz. ISCSD2 – priprava novega stanovanjskega zakona,
- Predlog Zakona o mladoletnih storilcih kaznivih dejanj,
- Predlog Zakona o interventnih dodatnih ukrepih zaradi afriške prašičje kuge pri divjih prašičih,
- Predlog Zakona o nadzoru vesoljskih dejavnosti,
- Predlog Pravilnika o elektronskem poslovanju v civilnih sodnih postopkih in v kazenskem postopku,
- Predlog novega Zakona o varstvu osebnih podatkov (ZVOP-2),
- Predlog Pravilnika o diplomatski, konzularni in službeni izkaznici.

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 pomočjo katerih lahko bolje razumejo in upoštevajo zahteve zakonodaje. Izmenjava informacij z zavezanci, preventivne aktivnosti za skladnost ter vzorčni dokumenti lahko zagotovo preprečijo marsikatero kršitev varstva osebnih podatkov in zmanjšajo potrebo po izvajanju inšpekcijskega nadzora.

Informacijski pooblaščenec je skozi čas razvil širok nabor orodij, s katerimi želi relativno kompleksno zakonodajo o varstvu osebnih podatkov približati zavezancem in splošnih javnosti. Med tovrstna orodja vsekakor sodijo smernice, mnenja, infografike, predavanja, srečanja s pooblaščenimi osebami za varstvo osebnih podatkov 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, koristna gradiva pa objavlja tudi na spletni strani upravljavec.si, ki je namenjana malim in srednje velikim podjetjem, ter tiodlocas.si, ki je namenjena posameznikom. Informacijski pooblaščenec nadaljuje tudi s širjenjem informacij, stališč in mnenj prek družbenih omrežij Facebook in LinkedIn, kjer predvsem objavlja povezave na pomembne novosti na področju varovanja zasebnosti.

Skladno z dolžnostmi, ki jih upravljavcem spletišč nalaga Zakon o dostopnosti spletišč in mobilnih aplikacij, je Informacijski pooblaščenec v letu 2020 po celovitem pregledu svojo spletno stran dopolnil z ustreznimi izjavami glede dostopnosti ter jo opremil z osnovnimi pojasnili v znakovnem jeziku.

Sektor za skladnost in preventivo podaja mnenja na prejete ocene učinkov glede varstva osebnih podatkov, pokriva področji kodeksov ravnanja in certifikacije ter, kjer to omogoča Splošna uredba, pripravlja vzročne dokumente za zavezance. Poudariti velja, da so bile v letu 2020 pripravljene standardne pogodbene klavzule, ki predstavljajo vzorčno pogodbo za ureditev pogodbene obdelave osebnih podatkov. Standardne pogodbene klavzule je potrdil Evropski odbor za varstvo osebnih podatkov.

Sektor za skladnost in preventivo nudi podporne dejavnosti ostalim sektorjem, tako glede informacijske tehnologije kot pomoči sektorju za inšpekcijski nadzor, med drugim je tako pripravil pregled zakonodaje o interventnih ukrepih (pregled novih in razširjenih zbirk osebnih podatkov), razvil nekatere interne aplikacije ter pripravil kontrolni seznam glede dolžnosti informiranja posameznikov po členih 13 in 14 Splošne uredbe

v bančnem sektorju, ki sta se izkazala kot učinkoviti orodji za izvajanje inšpekcijskega nadzora na tem področju. Sektor izvaja tudi interna izobraževanja in predstavitve novih mnenj Evropskega odbora za varstvo osebnih podatkov (npr. o pregledu ocen učinka, pametnih vozilih, kodeksih ravnanja).
Informacijski pooblaščenec je v letu 2020 nadaljeval z aktivnostmi projekta ozaveščanja RAPiD.Si, za katerega je pridobil evropska sredstva, začel pa je tudi izvajati nov projekt iDecide, ki je namenjen ozaveščanju treh ciljnih skupin, in sicer starejših od 65 let, delovne populacije ter starejših mladoletnikov.

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 Informacijski pooblaščenec vzpostavlja številne postopke ter pripravlja gradiva, kot je predstavljeno v nadaljevanju.

3.5.2 PREVENTIVNE AKTIVNOSTI V ČASU IZREDNIH RAZMER

Širjenje novega koronavirusa, sprejemanje številnih ukrepov in novih obdelav osebnih podatkov ter soočanje zavezancev z novimi razmerami na področju dela na daljavo ter šolanja na daljavo so sprožili vrsto novih vprašanj in izzivov, s katerimi smo se soočili vsi.

Informacijski pooblaščenec je prejel veliko število zaprosil za stališča, prevladujoče teme pa so bile:
- interventni zakoni in zbirke osebnih podatkov,
- posredovanje osebnih podatkov med Nacionalnim inštitutom za javno zdravje, policijo ter ministrstvom za zdravje,
- sledenje okuženim ter stikom z mobilnimi aplikacijami,
- obdelava osebnih podatkov pri šolanju na daljavo (videokonferenčni sistemi, dokazovanje opravljenih nalog, izpiti na daljavo ipd.),
- delodajalčevo spremljanje dela na domu z IT-programi,
- merjenje temperature ob vstopu v prostor (zaposlenim, strankam),
- javna dostopnost seznama upravičencev pomoči za samozaposlene,
- dopustnost nameščanja aplikacij na delavčev telefon ter programov za nadzor dela na daljavo,
- socialni inženiring, ribarjenja osebnih podatkov (angl. *phishing*), različne prevare,
- uporaba inteligentne videoanalitike,
- upravičenost delodajalčevega zbiranja izjav o nezmožnosti za delo zaradi pripadanja rizični skupini delavcev, okuženosti zaposlenih in družinskih članov itd.

Odgovore splošni in strokovni javnosti smo podajali z izjavami in sporočili za javnost ter na podstrani, oblikovani posebej za teme, povezane z varstvom osebnih podatkov v epidemiji (https://www.ip-rs.si/varstvo-osebnih-podatkov/varstvo-osebnih-podatkov-v-%C4%8Dasu-epidemije-koronavirusa-covid-19). Veliko angažmaja je terjala mobilna aplikacija za sledenje stikom #OstaniZdrav, v zvezi s katero smo podajali mnenja na ocene učinkov ter na predlagano zakonodajno ureditev, prav tako pa smo opozarjali na ustrezno ureditev spletnih strani za samoporočanje o okužbah, sistemov za merjenje telesne temperature, posredovanja podatkov o zdravju po elektronskih poteh in varnih kanalov za komunikacijo z bolniki, obveščanja javnosti prek SMS-sporočil ter opozarjali na številne druge teme.

3.5.3 OCENE UČINKOV NA VARSTVO OSEBNIH PODATKOV

Ocene učinkov na varstvo osebnih podatkov predstavljajo eno ključnih orodij načela odgovornosti; njihov namen je pravočasna identifikacija in obvladovanje tveganj v povezavi z varstvom osebnih podatkov, še zlasti pa so pomembne, kadar gre za nove projekte obdelave osebnih podatkov, ki predvidevajo množično obdelavo osebnih podatkov, še posebej v primeru, ko gre za uporabo modernih tehnologij, ranljive skupine posameznikov in za obdelavo posebnih vrst osebnih podatkov.

V letu 2020 je glede na epidemiološke razmere v prejetih ocenah učinka prevladovala tematika ukrepov v povezavi z obvladovanjem širjenja epidemije in sicer z uporabo sodobnih tehnoloških rešitev, kot so mobilne aplikacije za sledenje stikom, izvajanje videoidentifikacije na daljavo ter sistemov za merjenje telesne temperature.

V letu 2020 je Informacijski pooblaščenec v postopku predhodnega posvetovanja izdal mnenja o naslednjih ocenah učinkov:
- Mnenje glede ocene učinkov v zvezi z varstvom osebnih podatkov pri delovanju aplikacije COVID;
- Mnenje glede ocene učinkov v zvezi z varstvom osebnih podatkov sistema za avtomatsko merjenje telesne temperature z namenom odkrivanja oseb, potencialno okuženih z virusom SARS-CoV-2 in podobnimi nalezljivimi boleznimi;
- Mnenje glede ocene učinka na varstvo podatkov v zvezi predlogom Zakona o katastru nepremičnin;
- Mnenje glede ocene učinkov v zvezi z varstvom osebnih podatkov sistema ProbIS;
- Mnenje glede ocene učinkov v zvezi z Zakonom o spremembah in dopolnitvah Zakona o osebni izkaznici;
- Mnenje glede ocene učinka na varstvo podatkov v zvezi s projektom Videocheck.

Poleg naštetih ocen učinka je Informacijski pooblaščenec prejel tudi oceni učinka v okviru zakonodajnih predlogov, in sicer glede Zakona o elektronski identifikaciji in storitvah zaupanja ter glede Zakona o cestninjenju; mnenje Informacijskega pooblaščenca je bilo podano v sklopu mnenja na predloge zakonov, v obeh primerih pa je šlo po oceni Informacijskega pooblaščenca za kakovostni in celovito izdelani oceni učinka.

Ugotavljamo, da se znanje o izdelavi ocen učinkov počasi izboljšuje, s tem pa tudi kakovost izdelanih ocen, še vedno pa se premalo pozornosti posveča tveganjem, ki so povezana z uveljavljanjem pravic posameznika. Opozarjamo tudi na pravilno razumevanje vloge in pomena ocen učinka v zvezi z varstvom osebnih podatkov. Ocene učinka so namenjene pravočasni identifikaciji in obvladovanju tveganj glede varstva osebnih podatkov ter jih ni razumeti kot gradivo, ki popravlja predpise, utemeljuje potrebnost ali prednosti določenega projekta oziroma obdelave osebnih podatkov. Po naravi stvari se tako ocene učinkov osredotočajo na tveganja, na »negativne« vidike obdelav osebnih podatkov, ki jih želimo zmanjšati oziroma obvladovati. Ocene učinkov so predvsem v interesu upravljavcev, ki želijo pravočasno nasloviti tveganja, ne smemo pa jih enačiti s potrditvijo nadzornih organov, da je za varstvo osebnih podatkov ustrezno poskrbljeno.

Informacijski pooblaščenec ocenjuje, da bo treba v prihodnje preveriti, v kolikšni meri zavezanci izpolnjujejo dolžnosti glede izvedbe ocen učinka – tudi če ocene učinka ne pošljejo v predhodno mnenje Informacijskemu pooblaščencu, so jih glede na kriterije po Splošni uredbi in smernicah nadzornih organov dolžni izvesti, prav gotovo pa glede na epidemiološke razmere poteka veliko število projektov, ki vključujejo množično obdelavo posebnih vrst osebnih podatkov ter zato terjajo predhodne ocene učinka.

3.5.4 POOBLAŠČENE OSEBE ZA VARSTVO PODATKOV

Določitev pooblaščenih oseb za varstvo osebnih podatkov (angl. Data Protection Officer; DPO) je po oceni Informacijskega pooblaščenca eden najpomembnejših in hkrati najučinkovitejših mehanizmov za zagotavljanje skladnosti. 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. Ocenjujemo, da se delovanje pooblaščenih oseb izrazito izboljšuje, saj se s časom povečujejo tako izkušnje kot praksa glede njihovega delovanja.

Do konca leta 2020 je pooblaščeno osebo prijavilo 23.200 zavezancev. Pooblaščena oseba Informacijskega pooblaščenca je dostopna prek namenskega elektronskega predala dpo@ip-rs.si.

Informacijski pooblaščenec ocenjuje, da je pooblaščeno osebo prijavil pretežni del zavezancev, glede na informacije zunanjih izvajalcev storitev pooblaščenih oseb pa ugotavlja, da nekaj sto zavezancev (predvsem s področja zdravstva) še ni sporočilo podatkov svojih pooblaščenih oseb, zato bo to naslovljeno v eni od prihodnjih preventivnih aktivnosti za skladnost.

Pooblaščene osebe na neki način predstavljajo podaljšano roko Informacijskega pooblaščenca, zato smo jim v letu 2020 namenili več pozornosti, predvsem v smislu njihovega medsebojnega povezovanja, izmenjave izkušenj in prakse z upoštevanjem sektorske specifike. Maja 2020 je bilo načrtovano srečanje v živo s pooblaščenimi osebami za varstvo podatkov v šolstvu, a je bilo zaradi epidemioloških razmer odpovedano. Srečanja je Informacijski pooblaščenec preselil na splet in uspešno izvedel srečanje s pooblaščenimi osebami v bančnem in zavarovalniškem sektorju; ob sodelovanju Združenja bank Slovenije in Slovenskega zavarovalniškega združenja so bili izvedeni spletni posveti, na katerih so bile izmenjane izkušnje in predstavljeni primeri dobre prakse, pooblaščene osebe iz omenjenih združenj so predstavile statistične podatke glede reševanja zahtev posameznikov za uveljavljanje svojih pravic, opozorile pa so tudi na izzive, s katerimi se soočajo pri svojem delu. Tovrstna srečanja Informacijski pooblaščenec ocenjuje kot zelo koristna za obe strani, zato bo to prakso nadaljeval tudi v prihodnje.

Redno se Informacijski pooblaščenec srečuje s predstavniki zunanjih izvajalcev, ki nudijo zavezancem storitve pooblaščenih oseb za varstvo osebnih podatkov, saj na ta način pridobi koristne informacije iz prakse, hkrati pa nudi pojasnila glede določenih vprašanj o obveznostih po Splošni uredbi.

3.5.5 AKTIVNOSTI IZOBRAŽEVANJA IN OZAVEŠČANJA

Informacijski pooblaščenec je v letu 2020 nadaljeval aktivnosti na področju izobraževanja in ozaveščanja, ki vključujejo spletno mesto Informacijskega pooblaščenca (www.ip-rs.si), pripravo različnih gradiv, organizacijo in izvedbo dogodkov ter brezplačnih predavanj, sodelovanje z drugimi organizacijami in pri različnih projektih in prisotnost na družbenih omrežjih. Kljub številnim omejitvam, ki jih je prinesla epidemija, je Informacijski pooblaščenec uspešno izvajal različne aktivnosti izobraževanja in ozaveščanja.

Pooblaščenec je v letu 2020 izdal več gradiv. Poleg velikega števila mnenj med najpomembnejše sodijo smernice; izdane so bile naslednje:

- Smernice o varstvu osebnih podatkov v društvih,
- Smernice za delovno populacijo,
- Smernice za starejšo populacijo,
- Smernice za starejše mladoletnike.

Del smernic za starejše mladoletnike je tudi t. i. plonkceglc – povzetek ključnih informacij o varstvu osebnih podatkov za starejše mladoletnike, oblikovan kot plakat.

Pripravljeni so bili tudi novi obrazci v pomoč zavezancem, in sicer je Informacijski pooblaščenec pripravil vlogo za prenos osebnih podatkov v tretje države ali mednarodne organizacije, glede katerih je skladno z določbami Splošne uredbe o varstvu podatkov pred prenosom treba pridobiti dovoljenje nadzornega organa, v Sloveniji torej Informacijskega pooblaščenca. Obrazec je dostopen na spletni strani Informacijskega pooblaščenca.

Med najpomembnejša orodja v pomoč zavezancem pa prav gotovo sodi vzorčna pogodba za ureditev

pogodbene obdelave osebnih podatkov (najemanje zunanjih izvajalcev storitev obdelave osebnih podatkov) oz. t. i. standardna pogodbena določila, ki jih lahko zavezanci z ustreznimi dopolnitvami uporabijo za ustrezno ureditev medsebojnega razmerja skladno z določbami člena 28 Splošne uredbe. Ta določa obsežen nabor zahtev tako za upravljavca kot za obdelovalce, zato je bila priprava primerne pogodbe zlasti za manjše zavezance velik izziv – vzorčna pogodba jim olajša delo in prinaša večjo gotovost. Poudariti velja, da je bil Informacijski pooblaščenec šele drugi nadzorni organ v Evropski uniji (za Dansko), ki je pripravil takšne standardne pogodbene klavzule – potrditi jih mora namreč Evropski odbor za varstvo osebnih podatkov.

Informacijski pooblaščenec je tudi v letu 2020 nadaljeval s pripravo infografik, ki so se izkazale za učinkovit in razumljiv način za izvajanje izobraževalnih aktivnosti in splošno razumevanje ključnih elementov zakonodaje o varstvu podatkov.

Infografika GDPR na kratko pojasnjuje glavne elemente Splošne uredbe, kot so temeljna načela varstva osebnih podatkov, pravne podlage, obveznosti zavezancev in pravice posameznikov. Infografika je lahko uporaben pripomoček za vse, ki izvajajo izobraževanja na področju varstva osebnih podatkov, saj kompleksno materijo uredbe predstavijo na grafičen in slušateljem bolj razumljiv način, predvsem pa je ta infografika lahko uporabno orodje za pooblaščene osebe za varstvo osebnih podatkov, ki izvajajo interna izobraževanja za zaposlene v svojih organizacijah.

Infografika o skupnih upravljavcih pojasnjuje določbe Splošne uredbe o skupnem upravljanju ter navaja primere za lažje razumevanje.

Splošna uredba uvaja dolžnost obveščanja nadzornega organa (Informacijskega pooblaščenca) o zaznanih kršitvah varnosti osebnih podatkov (npr. izguba USB-ključka z osebnimi podatki, vdor v informacijski sistem z bazami osebnih podatkov ipd.), 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. Če bi s kršitvijo varnosti nastala resna tveganja za posameznike, morajo zavezanci obvestiti tudi njih. Zavezanci morajo beležiti in hraniti vse zaznane kršitve varstva osebnih podatkov, ne glede na potrebo po uradnem obveščanju. V pomoč zavezancem pri razumevanju dolžnosti glede kršitev varnosti je Informacijski pooblaščenec objavil infografiko, ki na pregleden način predstavlja ključne dolžnosti v primeru kršitev varnosti. Grafično so predstavljeni tudi nekateri primeri iz statističnih podatkov o prejetih obvestilih o kršitvah varnosti osebnih podatkov v letu 2020 (glej poglavje 3.2.3).

Podajanje informacij z infografikami je posebej pohvalila Mreža pooblaščenih oseb za varstvo osebnih podatkov pri Evropskem odboru za varstvo podatkov (EDPB DPO Network).

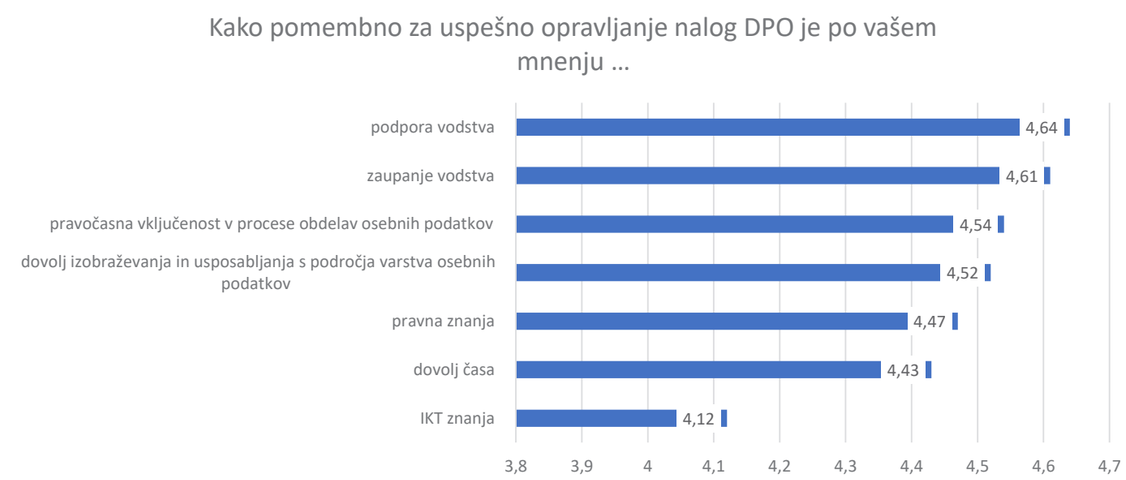
Evropski dan varstva osebnih podatkov je Informacijski pooblaščenec v letu 2020 posvetil izzivom, s katerimi so se tik pred drugo obletnico začetka uporabe Splošne uredbe o varstvu podatkov srečevale pooblaščene osebe za varstvo podatkov v javnem sektorju. Organiziral je okroglo mizo, na kateri so sodelovale pooblaščene osebe nekaterih največjih upravljavcev osebnih podatkov v javnem sektorju, kot so RTV Slovenija, Univerzitetni klinični center Ljubljana, Ministrstvo za pravosodje, Ministrstvo za javno upravo in Policija, ter predstavnik zunanjih ponudnikov storitev pooblaščenih oseb za varstvo podatkov.

Dogodek ob evropskem dnevu varstva osebnih podatkov.

Po mnenju udeležencev okrogle mize se v nekaterih primerih pooblaščene osebe za varstvo podatkov dojema kot edino odgovorno osebo za varstvo podatkov v organizaciji, kar ni namen ureditve v Splošni uredbi niti to v praksi ne zagotavlja učinkovitega varstva. Poudarjeno je bilo, da mora biti začetek vsakega dela temeljit pregled vseh procesov obdelave in popis zbirk ter ureditev razmerij z zunanjimi izvajalci, ki nastopajo kot pogodbenimi obdelovalci, za uspešnost pooblaščenih oseb pa je v praksi ključno vztrajno iskanje rešitev konkretnih problemov ter ustrezna struktura odločanja v organizaciji za uvajanje konkretnih ukrepov. Pooblaščene osebe za varstvo podatkov so v okviru ankete med ključne dejavnike uspešnosti izvajanja svojih nalog opredelile neposreden dostop do vodstva, zaupanje in podporo vodstva, seznanjenost zaposlenih z obstojem in nalogami pooblaščene osebe ter neodvisnost. Posebno predavanje je imela Vodja urada za varstvo podatkov pri EUROJUST, Diana Alonso Blas, ki je poudarila, da je za pooblaščene osebe nujno dobro poznavanje predpisov kot tudi seznanjenost z delovanjem informacijskih sistemov in same organizacije, uspešna pooblaščena oseba pa mora imeti tudi dobre pogajalske in komunikacijske sposobnosti, predvsem pa mora biti pragmatična ter ves čas spremljati področje.

V sklopu priprav na okroglo mizo smo konec leta 2019 med pooblaščenimi osebami za varstvo osebnih podatkov v javnem sektorju izvedli **anketo**, rezultate pa smo predstavili ob dnevu varstva podatkov, 28. 1. 2020. K izpolnjevanju ankete smo povabili 500 zavezancev v javnem sektorju. Odziv je bil visok, odzvalo se je 20 odstotkov povabljenih, zato smo pridobili koristne podatke o tem, kako delujejo pooblaščene osebe in katere dejavnike ocenjujejo kot najpomembnejše za svoj uspeh.

Izsek iz rezultatov ankete med pooblaščenimi osebami v javnem sektorju.



Že tradicionalno je Informacijski pooblaščenec ob tej priložnosti podelil priznanje ambasador zasebnosti. Za leto 2019 je priznanje prejel nacionalni center za odzivanje na omrežne incidente SI-CERT, ki s svojimi aktivnostmi ozaveščanja že vrsto let opozarja na varno rabo interneta in elektronskih omrežij ter pomaga organizacijam, ki so se znašle v težavah zaradi okužbe z virusi in ali zaradi drugih računalniških zagat. Z odmevnimi akcijami, med katerimi je na primer Varni na internetu, pomagajo tako posameznikom kot organizacijam k varni uporabi sodobnih tehnologij, s tem pa dvigujejo tudi ozaveščenost o varstvu osebnih podatkov in zasebnosti. SI-CERT kot dolgoletni partner Informacijskega pooblaščenca pomembno pripomore k temu, da so naši podatki bolj varni.

Informacijski pooblaščenec je, prav tako tradicionalno, podelil tudi priznanja prejemnikom mednarodnega certifikata za informacijsko varnost po standardu ISO/EIC 27001:2013, in sicer 17 organizacijam. Na ta način je poskrbel tudi za dodatno promocijo najbolj uveljavljenega mednarodnega standarda na področju informacijske varnosti.

Informacijski pooblaščenec je v letu 2020 kljub številnim omejitvam glede izvedb dogodkov (večinoma so ti potekali prek spleta) na področju varstva osebnih podatkov izvedel 34 brezplačnih predavanj za različne zbornice, združenja in druge javnosti po različnih dejavnostih v javnem in zasebnem sektorju.

Splošno in strokovno javnost je Informacijski pooblaščenec nagovarjal in obveščal tudi prek objav na družbenih omrežjih, in sicer je v letu 2020:

- objavil 79 sporočil na omrežju LinkedIn,
- delil 82 objav na omrežju Facebook ter
- poslal 12 novičnikov.

Informacijski pooblaščenec je v letu 2020 nadaljeval izvajanje projektov, sofinanciranih s strani EU: RAPiD.Si in iDecide.

Projekt RAPiD.Si

Informacijski pooblaščenec je leta 2020 uspešno končal dvoletni evropski projekt RAPiD.Si, ki je bil namenjen ozaveščanju in opolnomočenju posameznikov ter malih in srednje velikih podjetij o pomenu varstva osebnih podatkov. Projekt se je končal septembra 2020, do takrat so bile izvedene še zadnje projektne aktivnosti. V okviru aktivnosti, namenjenih malim in srednje velikim podjetjem, so člani projektne skupine nadaljevali pripravo in objavo **vsebin in animacij** za v okviru projekta vzpostavljeno spletno stran za mala in srednje velika podjetja www.upravljavec.si, nadaljevalo se je s pošiljanjem **mesečnega novičnika**, po več slovenskih mestih so bili izvedeni še preostali predvideni **strokovni seminarji**. V okviru aktivnosti, namenjenih posameznikom, pa so člani projektne skupine nadaljevali pripravo in objavo **vsebin in animacij** za v okviru projekta vzpostavljeno spletno stran za posameznike www.tiodlocas.si, na tedenski ravni so si sledile posebej tej ciljni skupini namenjene objave in zanimive **vsebine na Facebook profilu** Informacijskega pooblaščenca.

Primer objave na Facebook profilu Informacijskega pooblaščenca.

Zaključno projektno poročilo je bilo oddano v roku, in sicer 31. 10. 2020. Evropska komisija je v odzivu na zaključno poročilo pohvalila organizacijo projekta ter kot dobro prakso izpostavila organizacijo in izvedbo seminarjev po regijah širom Slovenije.

Projekt iDecide – posamezniki odločajo

Informacijski pooblaščenec je v letu 2020 začel izvajati projekt iDecide, »**Individuals Decide – Raising Awareness About Data Protection Rights (iDecide)**«, ki je financiran s strani Evropske komisije, in sicer v okviru Programa za pravice, enakost in državljanstvo 2020–2023.

Projekt bo predvidoma trajal 48 mesecev, osredotočal pa se bo na izobraževanje treh ciljnih skupin, starejših mladoletnikov (15–18 let), starejših (nad 65 let) in delovne populacije, in sicer o reformi zakonodajnega okvira na področju varstva osebnih podatkov in o temeljnih pravicah, ki jih zagotavlja zakonodaja s področja varstva osebnih podatkov. Cilj projekta iDecide je dvigovanje zavedanja o reformi okvira za varstvo osebnih podatkov v splošni javnosti v Sloveniji, še posebej glede pravic posameznikov.

V prvem letu izvajanja je Informacijski pooblaščenec pripravil **tri priročnike**, ki so namenjeni posameznikom različnih starostnih skupin: za starejše mladoletnike (*Moji podatki, moja stvar*), za delovno aktivne (*Kako so moji podatki varovani v delovnem razmerju*) in za starejše od 65 let (*Vi odločate o svojih podatkih*). Priročniki so dostopni na spletni strani, ker pa so bili natisnjeni v nakladi 8500 izvodov, bodo tudi distribuirani do ključnih ciljnih skupin. Priročniki obravnavajo tudi vprašanja, povezana z epidemijo covid-19, npr. v zvezi z obdelavo zdravstvenih osebnih podatkov in varno uporabo tehnologij pri učenju in delu od doma. V okviru projekta je bilo za namene strokovnega svetovanja vzpostavljeno dežurstvo po telefonu in elektronski pošti. Različne uporabne materiale in praktične napotke za splošno javnost, ki so bili razviti v okviru projekta, je Informacijski pooblaščenec objavil na svojih spletnih straneh, in sicer na www.ip-rs.si, www.tiodlocas.si in www.upravljavec.si.

Priročnik za varstvo osebnih podatkov za mlade: Moji podatki, moja stvar.

Med številnimi aktivnostmi v sklopu ozaveščanja v povezavi z epidemijo covid-19 je Informacijski pooblaščenec pripravil posebno covid-19 podstran, na kateri so za lažjo dostopnost zbrana aktualna mnenja in stališča glede dela na daljavo, šolanja na daljavo, sprejetih ukrepov za omejevanje širjenja koronavirusa in glede tehničnih rešitev. Opozarjali smo tudi na ustrezne ukrepe za zagotovitev varnosti osebnih podatkov, na primer s podajanjem priporočil, kot npr. *Kako zaščiti osebne podatke pri delu od doma?*.

3.5.6 PREVENTIVNE AKTIVNOSTI ZA SKLADNOST

Informacijski pooblaščenec je v letu 2020 zaradi zaostrenih razmer ob izvajanju ukrepov za omejevanje širjenja koronavirusa odložil izvajanje preventivnih aktivnosti za skladnost (ang. privacy sweep), saj so se praktično vsi zavezanci soočali s številnimi izzivi in so morali tako rekoč čez noč v pomembnem delu prilagoditi poslovanje, npr. zagotoviti ustrezno opremo za delo od doma, prilagoditi interne procese in pravilnike, prilagoditi varnostne postopke in ukrepe. Spričo novonastalih razmer, katerih posledica so bile izjemne obremenitve tako v javnem kot v zasebnem sektorju, izvajanje preventivnih aktivnosti za skladnost ni bilo sorazmerno, zato smo večji del naših preventivnih aktivnosti preusmerili v aktivnosti izobraževanja in ozaveščanja, kot smo jih opisali v predhodnem poglavju, saj je bilo to v težavnem letu 2020 bolj potrebno. Izvajanje preventivnih aktivnosti za skladnost je preloženo na leto 2021, ko bo na voljo več informacij, na katerih področjih lahko dosežemo, da zavezanci brez potrebe po uvajanju tako za zavezance kot za nadzorni organ stroškovno in časovno zahtevnih inšpekcijskih postopkov samostojno ocenijo lastno stanje na področju varstva osebnih podatkov ter zadostijo zahtevam zakonodaje, v pomoč pa so jim ustrezne informacije nadzornega organa. Med usmerjene aktivnosti bo prav gotovo sodilo področje varstva osebnih podatkov pri izvajanju dela na daljavo, vključno z uporabo zasebnih sredstev v službene namene, kar je posledica ukrepov za omejevanje epidemije, ter izpolnjevanje dolžnosti imenovanja pooblaščenih oseb za varstvo osebnih podatkov.

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 v zvezi s prenosi podatkov v tretje države; v zvezi z odobritvijo pogodbenih določil ali zavezujočih poslovnih pravil;
- reševanja sporov med nadzornimi organi (po členu 65 Splošne uredbe), npr. glede nasprotujočih si stališč o vsebini odločitve v čezmejnih primerih; o tem, kateri nadzorni organ je vodilni v določenem čezmejnem postopku; ter v primeru nespoštovanja mnenja odbora s strani posameznega nadzornega organa;
- reševanja nujnih postopkov (po členu 66 Splošne uredbe) s sprejemom začasnih ukrepov v izjemnih primerih, ko je ukrepanje potrebno zaradi varstva pravic in svoboščin posameznikov.

Delo odbora, ki se vsak mesec (v času pandemije koronavirusa pa tudi večkrat mesečno) sestaja na plenarni ravni, poteka tudi v 12 podskupinah strokovnjakov. V letu 2020 je dodatno delovalo 6 delovnih skupin in odborov, ki so se posvečali specifičnim temam. Te obravnavajo različna področja dela odbora, v njih pa sodelujejo predstavniki vseh nadzornih organov. Zaradi epidemičnih razmer je delo odbora od marca 2020 potekalo v spletnem okolju, v okviru spletne videorešitve, ki jo omogoča Evropski parlament in zagotavlja

varno komunikacijo. Odbor se je sestal na 27 plenarnih zasedanjih, strokovne in delovne skupine pa na 132 delovnih sestankih.

Predstavniki Informacijskega pooblaščenca tako 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.

Evropski odbor je v letu 2020 sprejel 12 smernic in priporočil po členu 70, 32 mnenj v okviru mehanizma skladnosti po členu 64, od tega eno na pobudo Informacijskega pooblaščenca (glede standardnih klavzul za prenos podatkov k pogodbenemu obdelovalcu), 19 drugih dokumentov in izjav ter eno zavezujočo odločitev po členu 65 Splošne uredbe.

Leto 2020 je zaznamovala epidemija novega koronavirusa, ki je narekovala pripravo izjave glede perečih vprašanj uporabe aplikacije za sledenje stikov z okuženimi in glede uporabe podatkov, ki jih obdelujejo operaterji elektronskih komunikacij za namene spremljanja razvoja epidemije, lokacij posameznikov, nadzora nad ukrepi za zajezitev. Sprejeta je bila tudi izjava o uporabi podatkov za namen raziskav v kontekstu epidemije covid-19, izjava glede obdelave osebnih podatkov v okviru ponovnega odpiranja meja po prvem valu epidemije ter izjava glede interoperabilnosti aplikacij za sledenje stikov z okuženimi v državah članicah EU.

Drugo polovico leta 2020 je zaznamovala tudi prelomna sodba Evropskega sodišča v primeru Schrems II, s katero je Sodišče EU razveljavilo odločitev Evropske komisije o ustreznosti varstva podatkov v okviru zasebnostnega ščita, ki je subjektom iz EU omogočal prenose podatkov iz EU v ZDA. Sodišče EU je svojo argumentacijo za razveljavitev zasebnostnega ščita utemeljilo na ugotovitvi, da varstvo osebnih podatkov, kot ga zagotavlja zakonodaja v ZDA, ni na primerljivi ravni z EU. Predvsem je opozorilo na premalo omejena pooblastila ameriških organov za dostope do prenesenih podatkov in na neučinkovito varstvo prek ombudsmana, ki naj bi v ZDA zagotavljal izvajanje pravic posameznikov. V tem kontekstu naj bi drugi mehanizmi za prenos podatkov, ki jih bodo morale uporabiti organizacije iz EU, npr. standardne pogodbene klavzule ali zavezujoča poslovna pravila, zagotavljali višjo raven varstva pravic posameznikov. Evropska podjetja, ki iznašajo osebne podatke, morajo glede na sodbo poskrbeti, da so pri vsakokratnem iznosu osebnih podatkov zajeta in spoštovana vsa načela evropskega varstva osebnih podatkov. Evropski odbor za varstvo podatkov je v odzivu na razveljavljeni zasebnostni ščit prejel več priporočil glede ustreznih dopolnilnih ukrepov za prenos podatkov v ZDA in kriterijev za ocenjevanje vpliva nacionalne zakonodaje v državi prejemnici na varstvo prenesenih podatkov.

Evropski odbor za varstvo podatkov je v letu 2020 aktivno prispeval tudi k razlagam številnih določb Splošne uredbe s smernicami in priporočili glede:
- konceptov upravljavca in obdelovalca,
- ciljanja uporabnikov na spletnih družbenih omrežjih,
- omejitev po členu 23 Splošne uredbe,
- glasovnih pomočnikov,
- povezanih avtomobilov ter
- primerov kršitev varstva podatkov.

Evropski odbor je pripravil številna pojasnila s področja prenosa podatkov v tretje države. S koncem leta 2020 se je končal tudi izstop Združenega Kraljestva iz EU in EDPB je v zvezi s prenosi podatkov v zdaj tretjo državo pripravil več dokumentov in pojasnil za izvoznike podatkov.

Sprejeta mnenja v okviru mehanizma skladnosti po členu 64 Splošne uredbe so predvsem zadevala certifikacijske in akreditacijske mehanizme v državah članicah EU. Informacijski pooblaščenec je v postopek pridobitve mnenja predložil standardne klavzule za pogodbeno obdelavo, ki so zdaj na voljo zavezancem kot vzorec, ki ga lahko uporabijo pri sodelovanju s pogodbenimi obdelovalci podatkov.

Evropski odbor je pojasnjeval procesna pravila čezmejnega sodelovanja, ki ga je vzpostavila Splošna uredba, in sicer so bila v ospredju vprašanja glede izvedbe sodelovanja »vse na enem mestu«, torej postopka po členu 60 Splošne uredbe, kadar na osnutek odločitve vodilnega nadzornega organa zadevni nadzorni organi podajo ustrezne in utemeljene razloge za ugovor taki odločitvi. Sprejete so bile Smernice 20/2020 o ustreznem in utemeljenem ugovoru po Splošni uredbi, ki vsebujejo pojasnila glede forme, vsebine in načina podaje tovrstnih ugovorov. Evropski odbor za varstvo podatkov pripravlja nadaljnje smernice glede postopkov po členih 60 in 65 Splošne uredbe.

V letu 2020 je bil prvič izveden postopek po členu 65(1)(a) Splošne uredbe, torej odločitev Evropskega odbora za varstvo podatkov v sporu med zadevnimi organi, ki so podali ustrezen in utemeljen ugovor osnutku odločitve vodilnega organa, ta pa je ugovore zavrnil kot neustrezne ali neutemeljene. V čezmejnem postopku člen 60(3) Splošne uredbe vodilnemu organu nalaga, da drugim zadevnim nadzornim organom brez odlašanja predloži osnutek odločitve, s čimer jih zaprosi za mnenje, ki ga ustrezno upošteva. Četrti odstavek zadevnim organom daje možnost, da v obdobju štirih tednov po opravljenem posvetovanju (izdaji osnutka odločbe) podajo ustrezne in utemeljene razloge za ugovor glede osnutka odločitve. Vodilni nadzorni organ zadevo predloži mehanizmu za skladnost, če se z ugovorom ne strinja ali meni, da ugovor ni ustrezen ali utemeljen. Člen 65 Splošne uredbe v točki (a) prvega odstavka določa, da odbor sprejme zavezujočo odločitev, da se zagotovi pravilna in dosledna uporaba te uredbe, in sicer med drugim v primeru, kadar je, v primeru iz člena 60(4), zadevni nadzorni organ dal ustrezen in utemeljen ugovor osnutku odločitve vodilnega organa ali če je vodilni organ zavrnil tak ugovor kot neustrezen ali neutemeljen. Zavezujoča odločitev velja za vse zadeve, na katere se nanaša ustrezen in utemeljen ugovor, zlasti kadar gre za kršitev te uredbe.

Odločitev v sporu po členu 65 Splošne uredbe je zadevala primer družbe Twitter, ki je utrpela varnostni incident in s tem kršitev varstva osebnih podatkov, ki pa je ni pravočasno naznanila nadzornemu organu. Vodilni nadzorni organ iz Irske je svoj osnutek odločitve predložil zadevnim organom iz vseh članic EU, tudi slovenskemu. Na osnutek odločitve je prejel več ugovorov, ki pa jih je zavrnil in zato zadevo predal v postopek odločanja po členu 65 Splošne uredbe. Odločitev Evropskega odbora za varstvo podatkov po členu 65 Splošne uredbe je za vodilni nadzorni organ zavezujoča in jo mora upoštevati pri oblikovanju končne odločbe po členu 60. V zadevnem primeru je bilo vodilnemu organu naloženo, da mora v končni odločbi pri izreku sankcije upoštevati vsa merila iz člena 83 Splošne uredbe, da bo sankcija primerna in odvračalna.

3.6.2 SODELOVANJE V DRUGIH NADZORNIH TELESIH EVROPSKE UNIJE

Informacijski pooblaščenec je v letu 2020 na ravni EU aktivno sodeloval v šestih delovnih telesih, ki se ukvarjajo z nadzorom nad izvajanjem varstva osebnih podatkov v okviru velikih informacijskih sistemov EU, in sicer:
- v Europolovem Odboru 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 dolžan tesno sodelovati z nacionalnimi organi za varstvo osebnih podatkov),
- 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 VIS,
- na koordinacijskih sestankih EDPS in nacionalnih organov za varstvo osebnih podatkov za nadzor nad CIS,
- v Skupnem nadzornem organu za carino,
- na koordinacijskih sestankih EDPS in nacionalnih organov za varstvo osebnih podatkov za nadzor nad Eurodac.

Med pomembnejšimi dokumenti, ki so bili v letu 2020 sprejeti v okviru zgoraj naštetih delovnih teles, je bil v okviru Europolovega odbora za sodelovanje sprejet vodič za izvrševanje pravic posameznikov, ki vsebuje opis vrst podatkov in obsega izmenjave med Europolom in državami članicami, postopke za izvrševanje posameznih pravic ter pravna sredstva, ki jih ima posameznik na voljo pri njihovem izvrševanju. V okviru Europolovega odbora za sodelovanje je bil sprejet tudi vprašalnik o posredovanju osebnih podatkov Europolu, namenjen nacionalnim enotam Europola v posameznih državah članicah. V okviru nadzora nad obdelavo osebnih podatkov v CIS je bila sprejeta nova verzija vodiča za izvrševanje pravice posameznikov do dostopa do osebnih podatkov. V okviru nadzora nad obdelavo osebnih podatkov v SIS II je bilo pripravljeno pismo, s katerim je bil nadzorni organ države, iz katere je bil zaznano velikansko povečanje zahtev njenih državljanov

za seznanitev z osebnimi podatki v SIS II, zaprošen za podajo pojasnil v zvezi s tem.

3.6.3 SODELOVANJE V DRUGIH MEDNARODNIH TELESIH

POSVETOVALNI ODBOR T-PD

V okviru Sveta Evrope je predstavnik Informacijskega pooblaščenca tudi v letu 2020 sodeloval v Posvetovalnem odboru, ustanovljenem s Konvencijo Sveta Evrope o varstvu posameznikov glede na avtomatsko obdelavo osebnih podatkov (Konvencija št. 108), skrajšano Odbor T-PD. Namesto spomladanskega plenarnega zasedanja je bila organizirana tridnevna spletna konferenca z naslovom Data Protection Views from Strasbourg in Visio, ki je bila sestavljena iz šestih sklopov, namenjenih primarnim temam delovnega programa Odbora. Na plenarnem zasedanju novembra, ki je bil leta 2020 izjemoma organiziran le enkrat in je potekal na daljavo, je Odbor 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 2020 aktivno obravnaval aktualne teme, kot so varstvo osebnih podatkov v času epidemije covid-19, prepoznava obrazov, profiliranje, digitalna identiteta in obdelava osebnih podatkov v okviru političnih kampanj. Izdal je Smernice o varstvu osebnih podatkov otrok v izobraževalnih sistemih, Poročilo o razvoju po izdaji Priporočila o profiliranju, Poročilo o digitalnih rešitvah za boj proti covid-19, predsednica Odbora in pooblaščenec za varstvo podatkov Sveta Evrope pa sta podala več skupnih izjav v zvezi z epidemijo in sodbo Schrems II. Odbor je podelil tudi nagrado Stefano Rodotà, in sicer za projekt, osredotočen na izzive, ki se pojavljajo ob uveljavljanju pravice do pridobivanja informacij o »logiki« pri izključno avtomatiziranih odločitvah.

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

Informacijski pooblaščenec je tudi v letu 2020 aktivno deloval v Mednarodni delovni skupini za varstvo osebnih podatkov v telekomunikacijah (International Working Group on Data Protection in Technology (IWGDPT)), ki združuje predstavnike informacijskih pooblaščencev in organov za varstvo osebnih podatkov in zasebnosti s celega sveta. Delo skupine prepoznava tudi mednarodna konferenca informacijskih pooblaščencev.

Zaradi epidemioloških razmer sta bili v letu 2020 odpovedani zasedanji v Tel Avivu in Londonu, skupina pa je z delom nadaljevala na korespondenčni način. Sprejeta sta bila dokument o pravici do prenosljivosti osebnih podatkov ter dokument o tveganjih z naslova sledenja in ciljanega oglaševanja na spletu.

Dokument o prenosljivosti podatkov nakazuje, da pomen pravice do prenosljivosti osebnih podatkov prepoznavajo tudi v drugih delih sveta, kjer ta pravica še ni zakonodajno urejena, medtem ko je pravica do prenosljivosti že natančno opredeljena v EU v Splošni uredbi o varstvu podatkov. Pravica do prenosljivosti podatkov je ob široki digitalizaciji naših življenj čedalje bolj pomembna, saj posamezniku omogoča pridobitev lastnih podatkov v odprtih in strojno berljivih formatih; na ta način se omejuje vezanost posameznika na določene ponudnike informacijskih storitev, posamezniku pa ima večjo moč odločanja o lastnih podatkih (https://www.datenschutz-berlin.de/fileadmin/user_upload/pdf/publikationen/working-paper/2021/2021-IWGDPT-Working_Paper_Data_Portability.pdf).

IWGDPT v dokumentu o tveganjih z naslova sledenja in ciljanega oglaševanja na spletu opozarja na množično profiliranje posameznikov, ki se pogosto sploh ne zavedajo, da so njihovi osebni podatki predmet dražb med ponudniki oglaševanja (t. i. *real-time-bidding*), pri čemer oglaševalec z najvišjo ponudbo dobi možnost, da posamezniku prikaže ciljani oglas glede na njegov profil. Vtičniki družabnih omrežij in spletna analitika omogočajo zbiranje ogromnih količin podatkov o uporabnikih spleta, ki poteka večinoma slabo transparentno, kar pod vprašaj postavlja veljavnost privolitev posameznikov in otežuje dostop do lastnih osebnih podatkov ter spoštovanje ostalih temeljnih načel varstva osebnih podatkov. Pomemben del dokumenta predstavljajo priporočila zakonodajalcem glede ustreznih pristopov k regulaciji s tem povezanih tveganj za posameznike (https://www.datenschutz-berlin.de/fileadmin/user_upload/pdf/publikationen/working-paper/2021/2021-IWGDPT-Working_Paper_tracking_eco_system.pdf).

SVETOVNA SKUPŠČINA ZA ZASEBNOST

Svetovna skupščina za zasebnost (ang. Global Privacy Assembly (GPA)), ki povezuje prizadevanja več kot 130 nadzornih organov za varstvo zasebnosti in podatkov z vsega sveta, se je v preteklem letu posvečala zlasti izzivom za varovanje zasebnosti v povezavi z ukrepi za obvladovanje in zajezitev posledic svetovne zdravstvene epidemije. V ta namen je bila vzpostavljena posebna delovna skupina in organizirano posebno srečanje prek videopovezave ter videokonferenca v sodelovanju z Organizacijo za gospodarsko sodelovanje in razvoj, ki se je je udeležil tudi predstavnik Informacijskega pooblaščenca. V skladu s strateškimi usmeritvami, ki temeljijo na poudarjenih prizadevanjih za vzpostavitev mednarodnega okvira standardov varstva zasebnosti ter krepitev različnih oblik sodelovanja pri izvajanju nadzorov, je GPA spremljala zlasti dogajanje in izzive v zvezi s pandemijo v državah, iz katerih prihajajo člani GPA. V ta namen je bila razvita spletna platforma na spletni strani GPA, kjer se sproti objavljajo vse informacije o pristopih, izzivih in aktivnostih posameznih nadzornih organov za varovanje zasebnosti v času pandemije. Delo konference vodi izvršni odbor, ki mu trenutno predseduje britanska pooblaščenka Elizabeth Denham. Med pomembnejšimi resolucijami, sprejetimi na zadnji konferenci leta 2020, ki je potekala prek videopovezave, so resolucija, posvečena izzivom, povezanim s pandemijo, resolucija o varstvu zasebnosti v povezavi s tehnologijami za prepoznavo obrazov, resolucija o zagotavljanju varovanja zasebnosti pri zagotavljanju razvojne in humanitarne pomoči ter kriznem upravljanju ter resolucija o izzivih ob zagotavljanju odgovornosti pri razvoju in uporabi umetne inteligence.

3.7 SPLOŠNA OCENA STANJA VARSTVA OSEBNIH PODATKOV

Informacijski pooblaščenec je na področju varstva osebnih podatkov opravljal naloge, ki mu jih nalaga Splošna uredba o varstvu podatkov, ki se je začela uporabljati 25. 5. 2018 in katere določbe se morajo neposredno uporabljati v vseh državah članicah EU. Splošna uredba terja sprejem novega Zakona o varstvu osebnih podatkov (ZVOP-2), s katerim bi se v Republiki Sloveniji zagotovilo izvajanje te uredbe, vendar Republika Slovenija v letu 2020 tega še vedno ni sprejela, kar povzroča precej odprtih vprašanj tako pri upravljavcih in obdelovalcih osebnih podatkov kot tudi pri Informacijskem pooblaščencu.

To, da ZVOP-2 še ni bil sprejet, 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, pri čemer 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 tudi v letu 2020 glede na pretekla obdobja občutno povečalo število takih pritožb. Reševanje slednjih seveda terja določitev posebnih pravil, s katerimi bi se rešila posamezna vprašanja upravnega postopka oz. bi se določil postopek reševanja takšnih pritožb, in nesprejetje novega zakona o varstvu osebnih podatkov je pri vodenju takih pritožbenih postopkov povzročilo precej dilem.

Nesprejetje novega ZVOP-2 je še posebej negativno vplivalo na vodenje prekrškovnih postopkov in izrekanje glob za ugotovljene kršitve. Informacijski pooblaščenec je zaradi odsotnosti ZVOP-2 v primeru ugotovljenih kršitev določb Splošne uredbe ali določb ZVOP-1 lahko zavezancem v postopku inšpekcijskega nadzora odredil le odpravo ugotovljenih nepravilnosti, vzpostavitev zakonitega stanja ter prepovedal nezakonito obdelavo osebnih podatkov, postopek za prekrške pa je uvedel le v primeru, ko je šlo za kršitev tistih členov ZVOP-1, ki še veljajo. Informacijski pooblaščenec tako zaradi odsotnosti novega ZVOP-2 tudi v letu 2020 ni mogel izrekati sankcij za tiste kršitve, ki so določene v členu 83 Splošne uredbe. Zaradi tega je Informacijski pooblaščenec pristojno ministrstvo tudi v letu 2020 večkrat opozoril na nujnost sprejetja novega zakona ter 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. Evropski odbor za varstvo osebnih podatkov, 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 v različnih državah naj ne bi odstopale, kar še zlasti velja v primerih čezmejnega sodelovanja pri inšpekcijskem nadzoru.

Republika Slovenija je zamujala tudi z implementacijo Direktive (EU) 2016/680 ter Direktive (EU) 2016/681 v delu, ki se nanaša na položaj in naloge pooblaščenih oseb za varstvo osebnih podatkov. Ti direktivi sta bili v pravni red Republike Slovenje preneseni z Zakonom o varstvu osebnih podatkov na področju obravnavanja kaznivih dejanj (ZVOPOKD), ki je začel veljati 31. 12. 2020.

Trend povečevanja števila prijav kršitev varstva osebnih podatkov se je nadaljeval tudi v letu 2020. Število takih prijav se je v primerjavi s preteklimi obdobji še nekoliko povečalo: Informacijski pooblaščenec je prejel 1018 prijav oz. pobud za uvedbo inšpekcijskega postopka, kar je največ doslej.

Poleg omenjenih prijav je Informacijski pooblaščenec v letu 2020 prejel in obravnaval še pet primerov nedovoljenega sporočanja ali druge nedovoljene obdelave osebnih podatkov o pacientih, ki so mu jih na podlagi 46. člena Zakona o pacientovih pravicah (ZPacP) poslali izvajalci zdravstvene dejavnosti, 12 pritožb zoper odločitev upravljavca po 41. členu ZPacP, sedem pritožb zoper odločitev upravljavca po 42. členu ZPacP, 36 pritožb zaradi kršitev upravljavca po 30. členu ZVOP-1, 171 pritožb posameznikov zaradi kršitev pravice do vpogleda v lastne osebne podatke po členu 15 Splošne uredbe in odločitve upravljavca v zvezi s tem (od tega je bilo 82 pritožb vloženih zaradi molka upravljavca), pet pritožb zaradi kršitve pravice do popravka osebnih podatkov po členu 16 Splošne uredbe, 11 pritožb zaradi kršitve pravice do izbrisa osebnih podatkov po členu 17 Splošne uredbe ter eno pritožbo zaradi kršitve pravice do omejitve obdelave osebnih podatkov po členu 18 Splošne uredbe. Število pritožb zaradi kršitev navedenih pravic, ki jih posameznikom zagotavlja Splošna uredba, se je v letu 2020 glede na pretekla obdobja precej povečalo, kar kaže na to, da se posamezniki svojih pravic vse bolj zavedejo.

Informacijski pooblaščenec je v letu 2020 od upravljavcev in obdelovalcev osebnih podatkov prejel 120 uradnih obvestil o kršitvi varnosti osebnih podatkov. Kot kažejo dosedanje ugotovitve, se upravljavci in obdelovalci osebnih podatkov vse bolj zavedajo svoje dolžnosti prijavljanja varnostnih incidentov in Informacijskemu pooblaščencu vse bolj dosledno pošiljajo uradna obvestila o kršitvi varnosti osebnih podatkov, kot jim to nalaga člen 33 Splošne uredbe. Upravljavci in obdelovalci osebnih podatkov so uradna obvestila o kršitvi varnosti osebnih podatkov Informacijskemu pooblaščencu najpogosteje pošiljali zaradi posredovanja osebnih podatkov nepooblaščenim ali napačnim osebam, nepooblaščenega dostopanja do osebnih podatkov zaradi programske napake ali zlorabe pooblastil s strani zaposlenih, napada na informacijski sistem z izsiljevalskim virusom in kriptiranjem podatkov s CryptoLockerjem, objave osebnih podatkov strank upravnega postopka na oglasni deski portala e-Uprava ter izgube ali kraje nosilcev osebnih podatkov (npr. osebnih računalnikov in USB-ključkov).

Informacijski pooblaščenec je pri obravnavi uradnih obvestil o kršitvi varnosti osebnih podatkov ugotovil, da so se v letu 2020 občutno povečali napadi na informacijski sistem z izsiljevalskim virusom in kriptiranjem podatkov s CryptoLockerjem, kar je upravljavcem osebnih podatkov, ki niso izvajali ustreznih tehničnih in organizacijskih ukrepov za zagotavljaje varnosti obdelave osebnih podatkov, povzročilo velike stroške ter težave pri zagotavljanju zmožnosti pravočasne povrnitve razpoložljivosti in dostopnosti osebnih podatkov.

Pri obravnavi prijav posameznikov Informacijski pooblaščenec ugotavlja, da so te v mnogih primerih še vedno vložene zaradi nerazumevanja določb Splošne uredbe, kar velja zlasti v primeru obdelave osebnih podatkov na podlagi privolitve posameznika, na katerega se osebni podatki nanašajo, ter v primerih, ko gre za obdelavo osebnih podatkov, ki jo fizična oseba izvaja med potekom popolnoma osebne ali domače dejavnosti in za katero se Splošna uredba o varstvu podatkov ne uporablja. Prijavitelji pogosto še vedno ne razumejo, da je privolitev posameznika zgolj ena od šestih enakovrednih pravnih podlag, ki jih v zvezi z zakonitostjo obdelave osebnih podatkov določa člen 6 Splošne uredbe, pri čemer pa so za vlaganje takšnih prijav pogosto krivi tudi upravljavci, ki osebne podatke zbirajo, posamezniku pa ne zagotovijo preglednih, razumljivih in lahko dostopnih informacij, kot jim to nalagata člena 12 in 13 Splošne uredbe.

Zagotavljanje jedrnatih, preglednih, razumljivih in lahko dostopnih informacij iz člena 13 in 14 Splošne uredbe je bila kljub ozaveščanju upravljavcev in kljub vzorcem takšnih obvestil, ki jih je Informacijski pooblaščenec pripravil in objavil na svojih spletnih straneh, tudi v letu 2020 še vedno ena od najpogosteje ugotovljenih kršitev. Vrste informacij, ki jih je treba zagotoviti posamezniku ob zbiranju njegovih osebnih podatkov, so določene v členih 13 in 14 Splošne uredbe o varstvu podatkov, 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 njegovih osebnih podatkov, koliko časa se podatki hranijo itd.

Prijave, ki jih je v letu 2020 prejel in obravnaval Informacijski pooblaščenec, so bile vložene iz podobnih razlogov kot v preteklih letih. Največ prijav je bilo vloženih zaradi posredovanja osebnih podatkov neupravičenim osebam, uporabe osebnih podatkov za namene neposrednega trženja, izvajanje videonadzora, nezakonitega ali prekomernega zbiranja osebnih podatkov, uporabe osebnih podatkov za namene, ki so v nasprotju z namenom njihovega zbiranja, nezakonitih vpogledov v zbirke osebnih podatkov ter neustreznega zagotavljanja varnosti osebnih podatkov.

Leto 2020 je zaznamovalo tudi večje število prijav in zaprosil za mnenja v zvezi z varstvom osebnih podatkov v času epidemije koronavirusa (covid-19). Informacijski pooblaščenec je zato na svoji spletni strani pripravil posebno podstran, na kateri je objavljal vsa mnenja, stališča in priporočila, ki se nanašajo na varstvo osebnih podatkov v času epidemije.

Posebne okoliščine, ki so zaznamovale leto 2020, so vplivale tudi na področje skladnosti in preventive. Na splošno se je bistveno zmanjšal obseg strokovnih posvetov, konferenc, izobraževanj in usposabljanj na vseh področjih, tudi na področju izobraževanja zaposlenih glede varstva osebnih podatkov. Ne glede na posebne okoliščine pa je Informacijski pooblaščenec v letu 2020 izvedel 34 brezplačnih predavanj za zavezance, večinoma z uporabo spletnih orodij. Informacijski pooblaščenec je uspešno izvajal projekt iDECIDE, ki ga financira EU, namenjen pa je ozaveščanju treh ciljnih populacij: mladoletnikov, starejše populacije in delovne populacije. V okviru projekta iDECIDE smo za vsako od populacij izdali prilagojeno brošuro z informacijami o njihovih pravicah, izvajali svetovanje v obliki telefonskih in pisnih mnenj, načrtovani seminarji pa so bili zaradi epidemije prestavljeni v leto 2021.

Leto 2020 je tudi na tem področju terjalo nekatere prilagoditve – kot smo opisali v predhodnem poročilu predstavljajo pomemben institut pooblaščene osebe za varstvo osebnih podatkov, komunikacija Informacijskega pooblaščenca s temi osebami pa ima lahko pomembne multiplikativne učinke. Zaradi omejitev glede srečevanja v živo je Informacijski pooblaščenec z nekaterimi združenji pooblaščenih oseb za varstvo osebnih podatkov, kot sta združenji na področju zavarovalništva in bančništva, izvedel posvet prek spleta; udeleženci posveta so izmenjali informacije in predstavili primere dobre prakse. Pooblaščeno osebo je imenovalo že več kot 2300 zavezancev, nekaj sto pa je po oceni Informacijskega pooblaščenca takih, ki te obveznosti še niso izpolnili, zato bo to predmet posebne preventivne aktivnosti za skladnosti.

Zamujanje s sprejemom ZVOP-2 se kaže tudi na področju preventive in skladnosti, saj zavezanci – dokler ne bodo jasno opredeljeni pogoji v ZVOP-2 – ne morejo uporabiti certifikacije po Splošni uredbi, ki bi lahko v določenem segmentu učinkovito delovala v smeri skladnosti.

Med pomembnejšimi dosežki v letu 2020 na področju skladnosti in preventive velja poudariti, da je Slovenija šele druga država, ki je uspešno pripravila standardne pogodbene klavzule za ureditev pogodbene obdelave osebnih podatkov skladno s členom 28 Splošne uredbe. Glede na določbe Splošne uredbe mora namreč takšne standardne pogodbene klavzule – vzorčno pogodbo, ki jo lahko uporabijo upravljavci podatkov za najem storitev pogodbenih obdelovalcev – potrditi Evropski odbor za varstvo osebnih podatkov, šele potem so lahko dana na voljo zavezancem. Standardne pogodbene klavzule so na voljo na spletni strani Informacijskega pooblaščenca, zavezanci pa jih lahko z ustreznimi dopolnitvami uporabijo kot pogodbo za zunanjo obdelavo osebnih podatkov, kot so npr. obračun plač, izvajanje oglaševanja, uporaba storitev klicnih centrov, vzdrževanje podatkovnih baz ipd.

Informacijski pooblaščenec ugotavlja, da je zavedanje pomena varstva osebnih podatkov in zasebnosti v družbi kljub izzivom v letu 2020 med splošnim prebivalstvom ostalo na visoki ravni, s precej večjo zaskrbljenostjo pa spremlja upoštevanje teh temeljnih človekovih pravic pri odločevalcih. Razumljivo je sicer, da je treba v času epidemije določene ukrepe pogosto sprejeti zelo hitro, kar pa ne sme biti opravičilo za neupoštevanje mnenj, stališč in opozoril Informacijskega pooblaščenca. Zlasti v povezavi z uvajanjem mobilne aplikacije za sledenje stikom so bila ta večinoma preslišana in ocenjujemo, da je prav zaradi neustreznega komuniciranja, vztrajanja pri obvezni uporabi aplikacije in drugih nejasnostih prišlo do padca zaupanja v takšno rešitev, kar pa je ključno za njeno uporabo in s tem uspešnost. Na drugi strani lahko namreč Informacijski pooblaščenec navede primere dobrih praks, na primer uvajanje e-vinjete; predlagatelj je v tem primeru pravočasno pridobil stališča Informacijskega pooblaščenca, jih vgradil v določbe zakonodaje, sam sistem pa zato z vidika varstva osebnih podatkov ne v strokovni ne v splošni javnosti praktično ni bil deležen niti pomislekov niti polemik. Opisana primera lepo izkazujeta, da je pravočasno upoštevanje načel vgrajenega in privzetega varstva osebnih podatkov in upoštevanje pripomb Informacijskega pooblaščenca bistveno za zaupanje v načrtovane projekte obdelav osebnih podatkov.

Opozoriti velja tudi na pomen koordiniranega pristopa k varstvu osebnih podatkov na določenih področjih, kar se še toliko bolj pokaže v kriznih časih. Omenjeno je bilo zlasti izrazito na področju šolanja in izobraževanja, kjer so posamezni zavodi, ob odsotnosti enotnih navodil, praktično vsak zase sprejemali hitre odločitve, katera orodja za izobraževanje na daljavo bodo uporabljali in kateri osebni podatki bodo pri tem obdelovani. Zaradi parcialnosti pristopov smo zasledili številne primere prekomernih obdelav osebnih podatkov, npr. za izkazovanje športnega udejstvovanja učencev, opravljenih nalog in opravljanja izpitov na daljavo. Do podobnih situacij je prihajalo tudi v delovnih okoljih, kjer ni bilo dovolj jasnih usmeritev pristojnih organov, npr. glede (obveznega) merjenja telesne temperature, zbiranja in posredovanja podatkov o okužbah ter glede izvajanja dela na daljavo. Razumljivo, je, da smo bili mnogi prisiljeni sprejemati ukrepe v zelo kratkem času, a predvsem na področju šolstva pomanjkanje enotnih usmeritev ni težava, ki bi se pojavila šele z epidemijo.

O čezmejnih primerih

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. Omogočila in formalizirala je postopek sodelovanja po načelu »vse na enem mestu«, ki predvideva, da postopek nadzora v čezmejnem primeru obdelave osebnih podatkov vodi t. i. vodilni organ in pri tem sodeluje z drugimi organi za varstvo osebnih podatkov, uvedla mehanizme vzajemne pomoči in skupnega ukrepanja organov za varstvo osebnih podatkov v državah članicah EU.
Informacijski pooblaščenec je v letu 2020 sodeloval v 123 postopkih medsebojne pomoči med nadzornimi

organi po členu 61 Splošne uredbe, pri čemer je prejel 96 zaprosil drugih organov in se nanje odzval, 27 zaprosil za sodelovanje pa je poslal drugim organom v EU. V 104 postopkih ugotavljanja vodilnega organa po členu 56 Splošne uredbe se je Informacijski pooblaščenec opredelil za zadevni organ, ki sodeluje v postopku čezmejnega postopka nadzora pri zavezancu. 101 postopek ugotavljanja je bil začet na iniciativo drugih organov v EU, tri je začel Informacijski pooblaščenec. Na temelju postopkov določitve vodilnega in zadevnih nadzornih organov je Informacijski pooblaščenec v letu 2020 aktivno sodeloval v 77 postopkih čezmejnega sodelovanja pri inšpekcijskem nadzoru nad podjetji, ki poslujejo čezmejno. Štirje tovrstni primeri so zadevali pravico do vpogleda v lastne osebne podatke. V teh postopkih je pričakovan sprejem odločitve nadzornih organov po členu 60 Splošne uredbe, po t. i. mehanizmu »vse na enem mestu«. 55 tovrstnih postopkov so začeli drugi organi v EU, Informacijski pooblaščenec v njih sodeluje kot zadevni organ.

Primeri niso zadevali le storitev priljubljenih spletnih velikanov, ki so v veliki meri še v teku (vodilni organ je na Irskem), temveč tudi neustrezna ravnanja z osebnimi podatki s strani različnih akterjev, letalskih družb, ponudnikov bančnih storitev, spletnih ponudnikov različnih storitev itd. iz številnih držav članic EU. Primeri spornih praks so vključevali pretirane zahteve po podatkih za identifikacijo strank, za namen izbrisa podatkov, neustrezno izvrševanje pravice do dostopa, posredovanje podatkov tretjim osebam (npr. v oglaševalski sitem omrežja Facebook brez privolitve posameznika). Pogosto so se primeri nanašali na kršitve varnosti osebnih podatkov, med prizadetimi pa so bili tudi uporabniki iz Slovenije. V tem okviru je Informacijski pooblaščenec kot zadevni nadzorni organ sodeloval v postopkih nadzora v zvezi s kršitvijo varstva osebnih podatkov pri podjetjih, kot so Nintendo, TicketMaster, Marriot Hotels, Twitter, National Australia Bank, British Airways itd., ki so bili zaključeni v letu 2020.

22 postopkov čezmejnega 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 EU oz. so dejanja obdelave osebnih podatkov zadevala posameznike iz različnih držav članic EU. Med drugim so ti postopki zadevali pritožbe o spornih praksah spletnih družbenih omrežij, ki podatke svojih uporabnikov delijo z nepreglednim številom oglaševalskih partnerjev, in to ob nezadostnem obveščanju in ukrepih za zavarovanje podatkov. Informacijski pooblaščenec je ob sodelovanju španskega nadzornega organa obravnaval primer pilotnega projekta vkrcavanja potnikov z uporabo biometrije na ljubljanskem letališču, ki ga je izvajala španska družba Amadeus; ugotovil je kršitve določb ZVOP-1 o biometriji.

V letu 2020 je bilo v postopkih sodelovanja »vse na enem mestu« izdanih 38 osnutkov odločb po členu 60 Splošne uredbe. 29 postopkov je bilo končanih s končno odločbo po členu 60 Splošne uredbe. V okviru spletne strani Evropskega odbora za varstvo podatkov je nastal tudi javni register končnih odločb v postopkih čezmejnega sodelovanja po členu 60: https://edpb.europa.eu/our-work-tools/consistency-findings/register-for-article-60-final-decisions_en.

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. Seveda pa tako sodelovanje za Informacijskega pooblaščenca, pa tudi za druge nadzorne organe, predstavlja velik izziv v smislu dodatnih potrebnih resursov, tako finančnih kot kadrovskih. Ključno je odlično poznavanje angleškega jezika, saj je angleščina v čezmejnih postopkih operativni jezik. Dodatne resurse zahteva že samo administriranje sodelovanja prek platforme IMI, ki jo je moral Informacijski pooblaščenec organizacijsko integrirati v svoje procese obravnave inšpekcijskih primerov in primerov odločanja o pravici do seznanitve z osebnimi podatki.

Izkušnje v letu 2020 so pokazale tudi na druge izzive sodelovanja po poglavju 7 Splošne uredbe, in sicer so bila v ospredju vprašanja glede izvedbe postopka po členu 60 Splošne uredbe, kadar na osnutek odločitve vodilnega nadzornega organa zadevni nadzorni organi podajo ustrezne in utemeljene razloge za ugovor taki odločitvi. Različne interpretacije konceptov in norm sodelovanja, ki ga kot novost uvaja Splošna uredba, so Evropski odbor za varstvo podatkov spodbudile k sprejemu Smernic 20/2020 o ustreznem in utemeljenem ugovoru po Splošni uredbi, ki vsebujejo pojasnila glede forme, vsebine in načina podaje tovrstnih ugovorov.

Nadaljnji izziv na področju čezmejnega sodelovanja je bila v letu 2020 izvedba prvega odločanja Evropskega odbora za varstvo podatkov v postopku po členu 65(1)(a) Splošne uredbe v sporu med zadevnimi organi, ki so podali ustrezen in utemeljen ugovor osnutku odločitve vodilnega organa, ta pa je ugovore zavrnil kot neustrezne ali neutemeljene. Odločitev v sporu po členu 65 Splošne uredbe je zadevala primer družbe Twitter, ki je utrpela varnostni incident in s tem kršitev varstva osebnih podatkov, vendar tega ni pravočasno

naznanila nadzornemu organu. Odločitev Evropskega odbora za varstvo podatkov po členu 65 Splošne uredbe je za vodilni nadzorni organ zavezujoča in jo mora upoštevati pri oblikovanju končne odločbe po členu 60 Splošne uredbe. V zadevnem primeru je bilo vodilnemu organu naloženo, da mora v končni odločbi pri izreku sankcije upoštevati vsa merila iz člena 83 Splošne uredbe, da bo sankcija primerna in odvračalna. Vodilni nadzorni organ iz Irske je v končni odločbi po členu 60 Splošne uredbe zavezancu Twitter naložil globo v znesku 450.000 EUR. Evropski odbor za varstvo podatkov aktivno pristopa h grajenju enotnih rešitev izzivov, ki nastajajo zaradi 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) ter pripravlja nadaljnje smernice glede postopkov po členih 60 in 65 Splošne uredbe.

Nekaj poudarkov o delu EDPB

Leta 2020 je bila sprejeta sodba v primeru Schrems II, s katero je Sodišče EU razveljavilo odločitev Evropske komisije o ustreznosti varstva podatkov v okviru zasebnostnega ščita, ki je subjektom iz EU omogočal prenose podatkov iz EU v ZDA. Sodišče EU je argumentacijo za razveljavitev zasebnostnega ščita utemeljilo na ugotovitvi, da varstvo osebnih podatkov, kot ga zagotavlja zakonodaja v ZDA, ni na primerljivi ravni z EU. Predvsem je opozorilo na premalo omejena pooblastila ameriških organov za dostope do prenesenih podatkov in na neučinkovito varstvo prek ombudsmana, ki naj bi v ZDA zagotavljal izvajanje pravic posameznikov. V tem kontekstu naj bi drugi mehanizmi za prenos podatkov, ki jih bodo morale uporabiti organizacije iz EU, npr. standardne pogodbene klavzule ali zavezujoča poslovna pravila, zagotavljali višjo raven varstva pravic posameznikov. Evropska podjetja, ki iznašajo osebne podatke, morajo glede na sodbo poskrbeti, da so pri vsakokratnem iznosu osebnih podatkov zajeta in spoštovana vsa načela evropskega varstva osebnih podatkov. Evropski odbor za varstvo podatkov je v odzivu na razveljavljeni zasebnostni ščit sprejel več priporočil glede ustreznih dopolnilnih ukrepov za prenos podatkov v ZDA in kriterijev za ocenjevanje vpliva nacionalne zakonodaje v državi prejemnici na varstvo prenesenih podatkov.

Evropski odbor za varstvo podatkov je v letu 2020 aktivno prispeval k razlagam številnih določb Splošne uredbe s smernicami in priporočili glede konceptov upravljavca in obdelovalca, glede ciljanja uporabnikov na spletnih družbenih omrežjih, glede omejitev po členu 23 Splošne uredbe, glede glasovnih pomočnikov in povezanih avtomobilov ter primerov kršitev varstva podatkov. Ob začetku epidemije covid-19 sta bili pripravljani izjavi glede takrat najbolj perečih vprašanj uporabe aplikacije za sledenje stikov z okuženimi in glede uporabe podatkov, ki jih obdelujejo operaterji elektronskih komunikacij za namene spremljanja razvoja epidemije, lokacij posameznikov, nadzora nad ukrepi za zajezitev. Sprejeta je bila tudi izjava o uporabi podatkov za namen raziskav v kontekstu epidemije covida-19. Smernice in priporočila Evropskega odbora so zadevali tudi področje prenosa podatkov v tretje države in procesnih pravil čezmejnega sodelovanja, ki ga je vzpostavila Splošna uredba. Sprejeta so bila številna mnenja v postopkih skladnosti glede certifikacijskih in akreditacijskih mehanizmov. Informacijski pooblaščenec je postopku pridobitve mnenja predložil standardne klavzule za pogodbeno obdelavo; standardne klavzule so zdaj na voljo zavezancem kot vzorec, ki ga lahko uporabijo pri sodelovanju s pogodbenimi obdelovalci podatkov.

ODGOVORNA UREDNICA:
Mojca Prelesnik, informacijska pooblaščenka

AVTORJI BESEDIL:
Jože Bogataj, namestnik informacijske pooblaščenke
dr. Jelena Burnik, vodja mednarodnega sodelovanja in razvoja
Tina Ivanc, svetovalka Pooblaščenca za varstvo osebnih podatkov
Alenka Jerše, namestnica informacijske pooblaščenke
mag. Eva Kalan Logar, vodja državnih nadzornikov
mag. Kristina Kotnik Šumah, namestnica Informacijske pooblaščenke
Karolina Kuševič, svetovalka Pooblaščenca II
Barbara Pirš, svetovalka Pooblaščenca za preventivo
Grega Rudolf, študent
Matej Sironič, svetovalec Pooblaščenca za varstvo osebnih podatkov
Polonca Štrekelj, nadzornica pooblaščenca II
Mateja Telič, državna nadzornica
mag. Andrej Tomšič, namestnik informacijske pooblaščenke

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 2021