



INFORMACIJSKI  
POOBLAŠČENEC



# Letno poročilo

Informacijskega pooblaščenca za leto 2021

## UVODNA BESEDA INFORMACIJSKE POOBLAŠČENKE

Spoštovani,

v letu 2021 so življenje v Sloveniji in Evropski uniji še naprej krojili zlasti ukrepi za zajezitev epidemije in njihove posledice. Ukrepi so močno zaznamovali tudi delo Informacijskega pooblaščenca pri uresničevanju obeh ustavnih pravic, nad katerima bdi – pravice do dostopa do informacij javnega značaja in pravice do varstva osebnih podatkov. Marsikatera skrb, ki bi jo pred leti uvrstili med teme znanstvenofantastičnih filmov, se je udejanjila v praksi. Odziv družbe kot celote pa je vnovič dokazal, da morajo države rešitve iz krize vedno iskati v ustreznem ravnovesju in sočasnem spoštovanju vseh človekovih pravic. Informacijski pooblaščenec je zato v okviru svojih pristojnosti vse napore usmeril v učinkovito naslavljanje skrbi in stisk posameznikov, podjetij, šol, novinarjev in drugih, ki so se znašli v zapletenem labirintu izvajanja ukrepov z resnimi posledicami tako za zasebnost kot tudi za transparentnost.

Vendar podatki o delu Informacijskega pooblaščenca v preteklem letu ne ponujajo le razlogov za skrb, ampak kažejo tudi na dobro delovanje družbe. V iskanju učinkovitih rešitev se je pokazala moč nevladnih organizacij, novinarjev ter moč povezovanja posameznikov in skupnosti na ravni pobud civilne družbe. Podatki dokazujejo, da posamezniki, novinarji in podjetja nadzorne organe, tudi Informacijskega pooblaščenca, doživljajo kot pomembne sogovornike in partnerje pri iskanju rešitev in uveljavljanju pravic. To potrjujejo tako vnovična rast skupnega števila pritožb v zvezi z zahtevami za dostop do informacij javnega značaja kot tudi število prijav in pobud za uvedbo inšpekcijskega nadzora ter število pritožb za uveljavljanje pravic posameznikov. Informacijski pooblaščenec je prejel tudi bistveno več zaprosil za mnenja oz. pojasnila. Na podlagi izkušenj preteklega leta si upam trditi, da sta obe pravici močno zasidrani v družbeni in pravni zavesti prebivalcev in prebivalk Slovenije.

Na področju transparentnosti delovanja države in učinkovitosti dostopa do informacij javnega značaja pa analiza podatkov glede delovanja državnih institucij ne kaže optimistične slike. Najbolj skrb vzbujajoča je ugotovitev, da se je kar za 37 % povečalo število pritožb zoper državne organe (leta 2021 je Informacijski pooblaščenec prejel 338 pritožb, medtem ko je bilo leto poprej takih pritožb 245), in sicer tako zoper zavrnilne odločitve kot zaradi molka organa. Znova opažamo visok delež pritožb zaradi molka v skupnem deležu vseh pritožb (38 %), na kar Informacijski pooblaščenec opozarja že nekaj let. Skrb vzbuja tudi povečevanje števila zadev, ki se nanašajo na dostop do informacij javnega značaja, v katerih so prosilci novinarji oziroma mediji, saj to kaže, da se zavezanci na zaprosila ne odzivajo ustrezno. Zato vse zavezance pozivamo, naj zahteve novinarjev obravnavajo v najkrajših rokih, naj ne zavlačujejo postopkov, ampak sledijo utečeni praksi Informacijskega pooblaščenca in Upravnega sodišča. Le v transparentni državi se namreč lahko razvija vključujoča in uspešna družba, kar še posebej velja v kriznih časih.

Na področju dostopa do informacij javnega značaja je sicer skupno število pritožb zoper občine ostalo na podobni ravni kot leto poprej (107 pritožb, v letu 2020 je bilo takih pritožb 115), pri čemer je razveseljiv vnovičen padec števila pritožb zaradi molka občin. Padlo je tudi število pritožb zoper poslovne subjekte pod prevladujočim vplivom oseb javnega prava. Leta 2021 je Informacijski pooblaščenec podal 301 pisni odgovor na zaprosila zavezancev, v okviru telefonskega dežurstva pa je odgovoril tudi na 948 zaprosil, kar je 50-odstotno povečanje glede na leto 2020. Primere iz prakse je redno objavljajal na svoji spletni strani.

Na področju varstva osebnih podatkov je Informacijski pooblaščenec v letu 2021 znova prejel rekordno število prijav kršitev (kar 1360 prijav) in pritožb v zvezi z uveljavljanjem pravic posameznikov (313 pritožb). Žal pri obravnavi teh pritožb Informacijski pooblaščenec ugotavlja, da je odzivnost upravljavcev pogosto neustrezna in da se marsikateri upravljavec ne zaveda svojih obveznosti, ki izhajajo iz ustavne pravice do seznanitve z lastnimi osebnimi podatki. Na področju inšpekcijskega nadzora pa se je vnovič kot najbolj nujna pokazala potreba po transparentnem obveščanju o obdelavah in jasnem zakonskem urejanju obveznosti v zvezi z ukrepanjem glede epidemije. Najbolj množične prijave so bile namreč povezane z ukrepi države, povezanimi z epidemijo. Informacijski pooblaščenec je v letu 2021 prejel tudi devet obvestil o kršitvah podatkov o pacientih na podlagi 46. člena Zakona o pacientovih pravicah ter 108 uradnih obvestil o kršitvi varnosti osebnih podatkov na podlagi člena 33 Splošne uredbe.

Povezovanje in čezmejno sodelovanje so zahteve epidemije še okrepile. Številni novi izzivi v letu 2021 so tudi na ravni Evropske unije (EU) in pri sodelovanju v okviru Evropskega odbora za varstvo podatkov (EOVP)

pokazali, kako pomembno je sodelovanje nadzornih organov. Med odmevnimi primeri pa niso bili le spletni velikani, ampak tudi drugi akterji, kot so ponudniki bančnih storitev, povezanih vozil ipd. S ciljem krepitev učinkovitosti čezmejnega sodelovanja v okviru evropskega odbora je ta leta 2021 pripravil smernice za sodelovanje nadzornih organov po členu 60 Splošne uredbe.

Na ravni Evropske unije je Informacijski pooblaščenec izvedel 154 postopkov medsebojne pomoči po členu 61 Splošne uredbe in aktivno sodeloval v 62 novo začelih postopkih čezmejnega sodelovanja po členu 60 Splošne uredbe v zvezi z upravljavci, ki izvajajo čezmejno obdelavo osebnih podatkov. V 75 postopkih se je opredelil za zadevni nadzorni organ (po členu 56 Splošne uredbe), v dveh primerih pa za vodilni nadzorni organ. 22 postopkov čezmejnega sodelovanja je Informacijski pooblaščenec sprožil na podlagi prejete prijave oz. pritožbe.

Informacijski pooblaščenec v svojih postopkih vedno znova ugotavlja, da večina zavezancev želi delovati skladno z zakoni, a potrebuje pomoč in jasna navodila. To se je tudi leta 2021 izkazalo zlasti v zvezi z ukrepi, povezanimi z obvladovanjem epidemije, na področju delovnih razmerij in izobraževanja. Žal se država in zakonodajalec tudi v preteklem letu nista odzvala na glasno izražene potrebe po jasnih predpisih in razumljivi opredelitvi obveznosti zavezancev in posameznikov, na katere že od začetka epidemije opozarja Informacijski pooblaščenec. Zakonodajalec tudi v letu 2021 ni izkoristil priložnosti, da bi na ustrezen način uredil materijo odzivanja na epidemijo in zadostil pozitivni obveznosti zagotavljanja pravice do zdravstvenega varstva, varovanja javnega zdravja in življenja vseh članov družbe, predvsem pa odpravil številna neskladja, ki jih je v letih 2020 in 2021 že ugotovilo Ustavno sodišče RS, in preprečil morebitna neustavna stanja v prihodnje. Z zakonodajnim pristopom urejanja vsebinsko raznolikih materij z enim zakonom se načinja institut pravne varnosti in spodkopava sistemsko ureditev področij, ki so sicer vsebinsko zaključene enote. Slovenija ob tem še vedno ni sprejela ključnega zakona za izvajanje Splošne uredbe.

Zato je tudi leta 2021 do hudih težav in stisk prihajalo prav zaradi nejasnih navodil, zaradi česar posameznih uradnih odločitev ni bilo mogoče izvajati v praksi. Informacijski pooblaščenec je zato tudi na tem področju varstva podatkov leta 2021 intenzivno deloval: svetoval je 3.647 posameznikom in pravnim osebam, in sicer je izdal 1.471 pisnih mnenj ter v okviru projekta iDecide, ki ga financira Evropska unija iz programa REC (Rights, Equality and Citizenship Programme), odgovoril na 2.176 telefonskih klicev. V ta namen je med drugim pripravil posebne smernice za zagotavljanje skladnosti IT rešitev v šolstvu, smernice za organizatorje dogodkov in vodnik po pravicah za posameznike. Zaradi izredno velikega števila prejetih vprašanj smo v okviru projekta iDecide pripravili posebne smernice glede vidikov varstva osebnih podatkov pri preverjanju pogoja PCT za delodajalce, posameznike in za šole. Posebno pozornost je Informacijski pooblaščenec namenil ponudnikom spletnega gostovanja, vrtcem, izvajalcem taksi služb in šolam, in sicer prek preventivnih aktivnosti za skladnost.

Uspešnost naslavljanja kriznih situacij je glede na izkušnje iz leta 2021 neposredno odvisna prav od transparentnega vodenja vseh sistemov države in spoštovanja človekovih pravic. V nasprotnem primeru posamezniki in družba ukrepov ne ponotranjijo, ti se ne izvajajo učinkovito in posledično se kriza pogloblja, kar vodi v nove težave in ima lahko resne, celo dolgoročne posledice za celotno družbo. Leto 2021 nam je nastavilo ogledalo, ki je pokazalo dobre in slabe strani, naša skupna naloga pa je, da se iz izkušenj učimo in se izzivov lotimo vsak v okviru svojih pristojnosti.

Informacijski pooblaščenec si bo zato z odlično ekipo strokovnjakov, ki je ob vseh izzivih krize leta 2021 pokazala, kako predana je pravicama, ki ju varuje, z aktivnim sodelovanjem z vsemi deležniki in z odprtostjo do posameznikov, podjetij ter vseh drugih organizacij tudi leta 2022 prizadeval učinkovito zavarovati obe pravici, ki sta mu zaupani.

Mojca Prelesnik, informacijska pooblaščenka



## STRNJEN PREGLED LETA 2021

### DOSTOP DO INFORMACIJ JAVNEGA ZNAČAJA

Informacijski pooblaščenec ugotavlja, da je na področju dostopa do informacij javnega značaja število pritožbenih zadev v letu 2021 naraslo na 639 pritožb (leta 2020 je obravnaval 565 pritožb). Informacijski pooblaščenec je delo na področju dostopa do informacij javnega značaja v letu 2021 kljub posebnim razmeram, povezanim z epidemijo covid-19, izvajal kot običajno.

Informacijski pooblaščenec je leta 2021 znova zaznal bistveno povečanje števila primerov, ki se nanašajo na zahteve po informacijah glede izvajanja epidemioloških ukrepov, javnega zdravja in s tem povezano porabo javnega denarja. Gre za informacije, ki so pogosto v širšem javnem interesu, zato Informacijski pooblaščenec zavezance vnovič poziva, da pri odločanju o teh zahtevah postopajo hitro ter pri presoji upoštevajo drugi odstavek 6. člena ZDIJZ, ki ureja test javnega interesa.

Število pritožb zaradi molka je bilo leta 2021 nekoliko višje (244) kot leto poprej (231). Razveseljivo je, da se je znova zmanjšalo število pritožb zoper molk občin (teh pritožb je bilo 46), skrb vzbujajoče pa je dejstvo, da se je krepko povečalo število pritožb zoper državne organe (338 pritožb). Informacijski pooblaščenec je zaznal bistven porast števila zadev, v katerih so prosilci mediji oziroma novinarji. Vodil pa je šest pritožbenih postopkov zoper poslovne subjekte pod prevladujočim vplivom, kar predstavlja le 0,9 % vseh pritožbenih zadev. Informacijski pooblaščenec ugotavlja, da število teh pritožb vsako leto pada in ostaja zelo nizko.

Informacijski pooblaščenec je leta 2021 v primerjavi z letom poprej v času telefonskega dežurstva prejel kar 50 % več zaprosil za mnenja oz. pojasnila s področja dostopa do informacij javnega značaja (948). Poleg tega je prejel 301 pisno prošnjo za mnenja in pojasnila. Informacijski pooblaščenec na področju dostopa do informacij javnega značaja kot pritožbeni organ sicer zavezancem in javnosti lahko svetuje le neformalno, na podlagi lastne prakse. Primere svoje prakse zato redno objavlja na spletni strani.

Informacijski pooblaščenec je na podlagi analize konkretnih primerov zaznal povečanje pritožb v zvezi z dostopom do podatkov o izplačilih plač javnim uslužbencem in različnih dodatkov za delo v času epidemije. Hkrati Informacijski pooblaščenec že tretje leto opaža številne postopkovne kršitve, katerih posledica so neustrezne obrazložitve odločitev zavezancev. Znova je skrb vzbujajoč visok delež pritožb zaradi molka; slednje so v letu 2021 predstavljale 38 % vseh pritožb.

Vse to kaže, da bi resorno Ministrstvo za javno upravo nujno moralo aktivneje pristopiti k usposabljanju zavezancev za uporabo ZDIJZ, k čemur Informacijski pooblaščenec poziva že več let. Prav tako bi ministrstvo moralo več napora vložiti v promocijo zakona. Informacijski pooblaščenec zavezance v zvezi s tem poziva, da pri obravnavi zadev natančno proučijo vse procesne vidike posamezne zadeve, da se ne izmikajo svojim obveznostim s sklicevanjem na neobstoje zahtevane informacije ter da posebej zahteve medijev in novinarjev obravnavajo v najkrajših rokih ter sledijo utečeni praksi Informacijskega pooblaščenca in Upravnega sodišča. V primeru zavrnitve morajo zavezanci svoje stališče skrbno obrazložiti in izjeme glede dostopa uporabiti skladno s prakso Informacijskega pooblaščenca ter upoštevajoč možnost uporabe testa javnega interesa, dokazno breme pa je v celoti na zavezancu.

### VARSTVO OSEBNIH PODATKOV

Informacijski pooblaščenec se je v letu 2021 na področju varstva osebnih podatkov vnovič 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 se je začel uporabljati v letu 2021. Vse to je povzročalo precej odprtih vprašanj tako na strani upravljavcev in obdelovalcev osebnih podatkov kot tudi na strani Informacijskega pooblaščenca.

V letu 2021 sta Višje sodišče (v primeru št. PRp 215/2021) in Vrhovno sodišče (v primeru IV Ips 2/2021) sprejela pomembni odločitvi za razrešitev nastale nevzdržne situacije po sodbah nižjih sodišč, po katerih Informacijski pooblaščenec ni smel izrekat sankcij niti za kršitve še veljavnih določb ZVOP-1. Z odločitvama

Višjega in Vrhovnega sodišča je bilo potrjeno stališče Informacijskega pooblaščenca in Ministrstva za pravosodje, da je prekrškovno sankcioniranje tistih določb ZVOP-1, ki niso v nasprotju s Splošno uredbo o varstvu podatkov in so kot take še vedno veljavne, skladno s slovenskim in evropskim pravnim redom.

Informacijski pooblaščenec zaradi odsotnosti ZVOP-2 tudi v letu 2021 zavezancem ni mogel izrekat sankcij za kršitve Splošne uredbe. 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, in 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, ki je zaradi odsotnosti ZVOP-2 za Informacijskega pooblaščenca močno oteženo.

Trend povečanega števila prijav, kršitev varstva osebnih podatkov in pritožb v zvezi z uveljavljanjem pravic posameznikov se je nadaljeval. Informacijski pooblaščenec je tako v letu 2021 prejel 1360 prijav oz. pobud za uvedbo inšpekcijskega postopka in 313 pritožb zaradi kršitev pravic posameznikov, kar je največ doslej. Poleg omenjenih prijav je Informacijski pooblaščenec obravnaval še devet primerov nedovoljenega sporočanja ali druge nedovoljene obdelave osebnih podatkov o pacientih na podlagi 46. člena Zakona o pacientovih pravicah (ZPacP). V okviru pritožbenih postopkov zaradi kršitev pravic posameznikov je Informacijski pooblaščenec obravnaval 226 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 174 pritožb vloženih zaradi molka upravljavca), tri pritožbe zaradi kršitve pravice do popravka osebnih podatkov po členu 16 Splošne uredbe in 29 pritožb zaradi kršitve pravice do izbrisa osebnih podatkov po členu 17 Splošne uredbe. Poleg tega je prejel še 13 pritožb zoper kršitve upravljavcev v zvezi z uveljavljanjem pravic po novem ZVOPOKD, 24 pritožb zaradi kršitev pri uveljavljanju pravic pacientov po 41. členu ZPacP, devet pritožb po 42. členu ZPacP ter štiri pritožbe zaradi kršitev upravljavca po 30. členu ZVOP-1. Vse to kaže, da se posamezniki vse bolj zavedajo svojih pravic, na strani upravljavcev pa opažamo precejšnje težave pri njihovem uresničevanju.

Številnim prijavam so botrovale pomanjkljive informacije, podane posameznikom s strani upravljavcev, ki osebne podatke zbirajo, zlasti v povezavi z obdelavami, ki so bile posredno ali neposredno povezane z ukrepi za obvladovanje epidemije. Upravljavci namreč posamezniku pogosto še vedno ne zagotovijo preglednih, razumljivih in lahko dostopnih informacij o obdelavi, kot jim to nalagata člena 12 in 13 Splošne uredbe. Izredno veliko število prijav je tako Informacijski pooblaščenec prejel zaradi obdelav osebnih podatkov vlagateljev prijave interesa za cepljenje proti covid-19 prek portala e-Uprava, zaradi obdelav, povezanih s pošiljanjem vabil k cepljenju proti covid-19, zaradi preverjanja izpolnjevanja pogoja PCT ter zaradi pošiljanja pisem vsem državljanov s strani predsednika Vlade Republike Slovenije.

Prijave, ki se niso nanašale na izvajanje ukrepov za preprečevanje in obvladovanje okužb s covid-19, so bile vložene iz podobnih razlogov kot v preteklih letih. Največ jih je bilo vloženih zaradi posredovanja osebnih podatkov neupravičenim osebam, izvajanja videonadzora, uporabe osebnih podatkov za namene neposrednega trženja, 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.

Informacijski pooblaščenec je prejel 108 uradnih obvestil o kršitvi varnosti osebnih podatkov na podlagi člena 33 Splošne uredbe. Obvestila o kršitvi varnosti osebnih podatkov 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).

Leto 2021 je zaznamovalo večje število zaprosil za mnenja, ki jih je Informacijski pooblaščenec prejel v zvezi z izvajanjem različnih ukrepov, povezanih z obvladovanjem epidemije. Informacijski pooblaščenec je svetoval 3.647 posameznikom in pravnim osebam. Izdal je 1.471 pisnih mnenj in napotitev na mnenja. Leta 2021 so državni nadzorniki v okviru projekta iDECIDE, ki ga financira Evropska unija iz programa REC (Rights, Equality and Citizenship Programme), odgovorili na 2.176 telefonskih klicev ter klicateljem svetovali glede vprašanj, povezanih z varstvom osebnih podatkov in pravicami posameznikov. Ne glede na posebne

okolščine je Informacijski pooblaščenec v tem letu izvedel 28 brezplačnih predavanj za zavezance, večinoma z uporabo spletnih orodij. Uspešno pa je izvajal tudi druge oblike ozaveščanja v projektu iDECIDE, v okviru katerega je za ozaveščanje treh ciljnih populacij (mladoletnikov, starejše populacije in delovne populacije) pripravil smernice o varstvu podatkov, prilagojene vsaki od omenjenih ciljnih skupin. Posebno pozornost je Informacijski pooblaščenec posvečal pooblaščenim osebam za varstvo osebnih podatkov – pripravil je nov spletni obrazec za poročanje podatkov o imenovanih pooblaščenih osebah za varstvo osebnih podatkov. Do zdaj je pooblaščen o sebo imenovalo že več kot 2500 zavezancev.

Zamujanje s sprejemom ZVOP-2 vpliva tudi na področje preventive in skladnosti, saj se zavezanci posledično – dokler ne bodo jasno opredeljeni pogoji v ZVOP-2 – ne morejo poslužiti certifikacije po Splošni uredbi.

Zavedanje o pomenu varstva osebnih podatkov in zasebnosti v družbi je bilo po izkušnjah Informacijskega pooblaščenca leta 2021 med splošno populacijo kljub izzivom na visoki ravni, s precej večjo zaskrbljenostjo pa Informacijski pooblaščenec spremlja spoštovanje teh temeljnih človekovih pravic pri odločevalcih. Nepoznavanje in nerazumevanje predpisov se je pokazalo zlasti v primeru predpisov, ki so bili sprejeti z namenom preprečevanja in obvladovanja okužb s covid-19, saj je pogosto prihajalo do sprejemanja nejasnih in ne dovolj premišljenih predpisov, ki so se poleg tega izredno hitro spreminjali in pri katerih je bila, glede na dosedanjo prakso Ustavnega sodišča v primeru predvidene obdelave osebnih podatkov, pogosto vprašljiva tudi njihova skladnost z Ustavo. Na to je Informacijski pooblaščenec vseskozi opozarjal predlagatelje; v letu 2021 je izdal 85 mnenj na predloge sprememb predpisov. Pri tem je Informacijski pooblaščenec opazal skrb vzbujajoč trend nesistemskega urejanja nekaterih resnih posegov v zasebnost ter poskuse 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 obvladovanjem epidemije.

Kot pomoč zavezancem in posameznikom je Informacijski pooblaščenec med drugim pripravil tri posebne smernice glede varstva osebnih podatkov v zvezi s preverjanjem pogoja PCT, prilagojene delodajalcem, šolam in posameznikom. Kot odziv na zaznane težave pri izvajanju šolanja in izobraževanja na daljavo je Informacijski pooblaščenec pripravil smernice za zagotavljanje skladnosti IT rešitev v šolstvu. Pripravil je tudi smernice za organizatorje dogodkov, vodnik po pravicah za posameznike ter posodobil smernice o prenosu osebnih podatkov v tretje države.

Informacijski pooblaščenec je nadaljeval s preventivnimi aktivnostmi za skladnost (angl. privacy sweep); naslovil je ponudnike spletnega gostovanja, vrtce, izvajalce taksi služb ter osnovne in srednje šole. Pri ponudnikih spletnega gostovanja se je izkazalo, da gre za sistemski problem razumevanja njihove vloge, zlasti glede obveznosti in dolžnosti, povezanih s pogodbeno obdelavo osebnih podatkov, kot izhajajo iz člena 28 Splošne uredbe. Vrtci so bili opozorjeni na problematiko pridobivanja soglasij staršev in ustreznega informiranja staršev o obdelavi podatkov. Na področju taksi služb je Informacijski pooblaščenec zaznal, da številne hranijo podatke o preteklih poteh svojih strank, ne da bi stranke o tem predhodno ustrezno informirali in pridobili njihovo soglasje. Na področju preventivnega delovanja Informacijski pooblaščenec sicer pogreša pogostejšo uporabo mehanizma izdelave predhodne ocene učinkov s strani upravljavcev v primeru načrtovanja novih obsežnih obdelav osebnih podatkov ali obdelav s pomembnimi vplivi na zasebnost in pravice posameznikov; posledično malo upravljavcev koristi s tem povezane možnosti predhodnega posvetovanja z Informacijskim pooblaščenecem.

Tudi delo Evropskega odbora za varstvo podatkov je leta 2021 v veliki meri zaznamovala pandemija covid-19, ki je botrovala nastanku evropskega digitalnega zelenega potrdila, ki naj bi omogočalo svobodno gibanje znotraj EU med pandemijo prek skupnega okvira za izdajanje, preverjanje in sprejemanje potrdila o tem, ali je bil posameznik cepljen in s katerim cepivom, ali je covid-19 že prebolel in kdaj oziroma ali izkazuje negativen rezultat testiranja. Evropski odbor za varstvo podatkov in Evropski nadzornik za varstvo podatkov sta ob tem poudarila, da mora biti delovanje zelenega potrdila skladno s Splošno uredbo o varstvu podatkov in da morajo biti ustrezno naslovljena tveganja za pravice posameznikov. Uporaba potrdila v državah članicah pa bi morala biti skladna z načelom sorazmernosti, učinkovitosti in nujnosti ustrezno urejena tudi z nacionalno zakonodajo.

V okviru čezmejnega sodelovanja nadzornih organov za varstvo osebnih podatkov v državah članicah EU in EGS (Islandija, Norveška in Lihtenštajn) po načelu »vse na enem mestu«, ki ga predvideva Splošna uredba, je Informacijski pooblaščenec leta 2021 sodeloval v 154 postopkih medsebojne pomoči med nadzornimi organi po členu 61 Splošne uredbe. Na temelju določitve vodilnega in zadevnih nadzornih organov 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 aktivno sodeloval v 62 novo začelih 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. V letu 2021 je bila sprejeta končna odločitev v postopku, ki ga je vodil irski nadzorni organ zoper ponudnika storitev WhatsApp, in sicer je bila podjetju odrejena globa 225 milijonov evrov zaradi neustreznega informiranja posameznikov (uporabnikov in neuporabnikov) glede obdelave njihovih osebnih podatkov in glede informiranja uporabnikov o tem, kako podatke uporabljajo Facebook in povezana podjetja. Sodelovanje v čezmejnih primerih pomeni velik izziv, saj zahteva dodatne resurse, tako finančne kot kadrovske. Izkušnje v tem letu 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. Čezmejni primeri pa niso zadevali le storitev popularnih spletnih velikanov, ki so v veliki meri še v teku (vodilni organ je na Irskem), temveč tudi neustrezna ravnanja z osebnimi podatki s strani raznolikih akterjev iz številnih držav članic EU.

Evropski odbor za varstvo podatkov in Evropski nadzornik za varstvo podatkov sta sprejela skupno mnenje glede predloga EU uredbe o enotnih pravilih za področje umetne inteligence. Mnenje pozdravlja enotno urejanje uporabe sistemov umetne inteligence v EU, hkrati pa nadzorni organi opozarjamo, da mora biti uredba usklajena s pravili na področju varstva osebnih podatkov ter da mora jasno določati, da ta veljajo tudi v primeru obdelave podatkov s pomočjo umetne inteligence.

V letu 2021 je pomembno sodbo v zvezi s čezmejnimi sodelovanjem po Splošni uredbi o varstvu podatkov sprejelo Sodišče EU, ki je proučevalo vprašanje, ali lahko nacionalni nadzorni organ, ki ni vodilni po določbah Splošne uredbe, sproži sodni postopek proti domnevemu kršitelju zaradi kršitve določb Splošne uredbe pred nacionalnim sodiščem v svoji matični državi članici. Razsodilo je, da je to mogoče le, če Splošna uredba nadzornemu organu, ki ni vodilni nadzorni organ, daje pristojnost odločanja o tem, ali določena obdelava osebnih podatkov posameznikov krši pravila iz Splošne uredbe, in če so spoštovani postopki sodelovanja in nadzora, določeni s Splošno uredbi. Sodišče EU je poudarilo pomen tesnega, lojalnega in učinkovitega sodelovanja.

Evropski odbor za varstvo podatkov aktivno pristopa k iskanju in oblikovanju enotnih rešitev izzivov, ki vznikajo 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 je leta 2021 pripravil osnutek smernic glede postopkov po členu 60. Odbor je aktivno prispeval k razlagam številnih drugih določb Splošne uredbe s smernicami in priporočili, med drugim glede vprašanj razmerja med členom 3 Splošne uredbe in obveznostmi upravljavcev in obdelovalcev pri prenosu osebnih podatkov v tretje države, glede omejitev pravice posameznikov po členu 23 Splošne uredbe, glede glasovnih pomočnikov in povezanih avtomobilov ter primerov kršitev varstva podatkov.

## KAZALO

<b>1 O INFORMACIJSKEM POOBLAŠČENCU – POD SVOJO STREHO ZDRUŽUJE DOSTOP DO INFORMACIJ JAVNEGA ZNAČAJA IN VARSTVO OSEBNIH PODATKOV . . . . .</b>	<b>1</b>
<b>1.1 NASTANEK IN OSEBNA IZKAZNICA INFORMACIJSKEGA POOBLAŠČENCA . . . . .</b>	<b>2</b>
1.1.1 ORGANIZIRANOST . . . . .	5
<b>1.2 KLJUČNA PODROČJA DELOVANJA IN PRISTOJNOSTI . . . . .</b>	<b>7</b>
<b>1.3 FINANČNO POSLOVANJE V LETU 2021 . . . . .</b>	<b>13</b>
<b>2 DOSTOP DO INFORMACIJ JAVNEGA ZNAČAJA – V IMENU LJUDI IN ZA LJUDI . . . . .</b>	<b>17</b>
<b>2.1 PRAVNA UREDITEV NA PODROČJU DOSTOPA DO INFORMACIJ JAVNEGA ZNAČAJA . . . . .</b>	<b>18</b>
<b>2.2 ŠTEVILO VLOŽENIH PRITOŽB IN REŠENIH ZADEV . . . . .</b>	<b>21</b>
2.2.1 PRITOŽBE ZOPER ZAVRNILNE ODLOČBE IN IZDANE ODLOČBE . . . . .	21
2.2.2 PRITOŽBE ZOPER MOLK . . . . .	23
<b>2.3 ŠTEVILO VLOŽENIH TOŽB IN PREJETIH SODB . . . . .</b>	<b>25</b>
<b>2.4 STORJENI PREKRŠKI PO ZDIJZ, ZInfP IN ZMed. . . . .</b>	<b>25</b>
<b>2.5 IZBRANI PRIMERI NA PODROČJU DOSTOPA DO INFORMACIJ JAVNEGA ZNAČAJA . . . . .</b>	<b>25</b>
<b>2.6 AKTIVNOSTI IZOBRAŽEVANJA IN OZAVEŠČANJA . . . . .</b>	<b>33</b>
2.6.1 DAN PRAVICE VEDETI . . . . .	33
2.6.2 MEDNARODNO SODELOVANJE . . . . .	34
<b>2.7 SPLOŠNA OCENA IN PRIPOROČILA . . . . .</b>	<b>35</b>
<b>3 VARSTVO OSEBNIH PODATKOV – VARSTVO TEMELJNE ČLOVEKOVE PRAVICE DO ZASEBNOSTI . . . . .</b>	<b>37</b>
<b>3.1 KONCEPT VARSTVA OSEBNIH PODATKOV V REPUBLIKI SLOVENIJI . . . . .</b>	<b>38</b>
<b>3.2 INŠPEKCIJSKI NADZOR V LETU 2021 . . . . .</b>	<b>40</b>
3.2.1 INŠPEKCIJSKI NADZOR V JAVNEM SEKTORJU . . . . .	42
3.2.2 INŠPEKCIJSKI NADZOR V ZASEBNEM SEKTORJU . . . . .	43
3.2.3 PRIJAVA KRŠITEV VARNOSTI OSEBNIH PODATKOV . . . . .	44
3.2.4 SODELOVANJE PRI ČEZMEJNIH INŠPEKCIJSKIH NADZORIH . . . . .	47
3.2.5 PREKRŠKOVNI POSTOPKI . . . . .	50
3.2.6 IZBRANI PRIMERI OBDELAVE OSEBNIH PODATKOV . . . . .	52
<b>3.3 DRUGI UPRAVNI POSTOPKI . . . . .</b>	<b>58</b>
3.3.1 DOPUSTNOST IZVAJANJA BIOMETRIJSKIH UKREPOV . . . . .	58
3.3.2 POVEZOVANJE ZBIRK OSEBNIH PODATKOV . . . . .	58
3.3.3 PRENOS OSEBNIH PODATKOV V TRETJE DRŽAVE . . . . .	61
3.3.4 PRAVICE POSAMEZNIKOV . . . . .	62
3.3.5 IZBRANI PRIMERI V ZVEZI Z OBRAVNAVANJEM PRAVIC POSAMEZNIKOV . . . . .	64
3.3.6 ZAHTEVA ZA OCENO USTAVNOSTI IN ZAKONITOSTI . . . . .	69
<b>3.4 PRIPRAVA MNENJ IN POJASNIL . . . . .</b>	<b>72</b>
3.4.1 SPLOŠNA POJASNILA . . . . .	72
3.4.2 MNENJA NA PREDPISE . . . . .	72
<b>3.5 SKLADNOST IN PREVENTIVA . . . . .</b>	<b>74</b>
3.5.1 OBVEZNOSTI UPRAVLJAVCEV . . . . .	75
3.5.2 PREVENTIVNE AKTIVNOSTI V ČASU IZREDNIH RAZMER . . . . .	75
3.5.3 OCENE UČINKOV NA VARSTVO OSEBNIH PODATKOV . . . . .	75
3.5.4 POOBLAŠČENE OSEBE ZA VARSTVO PODATKOV . . . . .	76
3.5.5 AKTIVNOSTI IZOBRAŽEVANJA IN OZAVEŠČANJA . . . . .	76
3.5.6 PREVENTIVNE AKTIVNOSTI ZA SKLADNOST . . . . .	79
<b>3.6 MEDNARODNO SODELOVANJE . . . . .</b>	<b>80</b>
3.6.1 SODELOVANJE V EVROPSKEM ODBORU ZA VARSTVO PODATKOV . . . . .	80
3.6.2 SODELOVANJE V DRUGIH NADZORNIH TELESIH EVROPSKE UNIJE . . . . .	82
3.6.3 SODELOVANJE V DRUGIH MEDNARODNIH TELESIH . . . . .	83
<b>3.7 SPLOŠNA OCENA STANJA VARSTVA OSEBNIH PODATKOV . . . . .</b>	<b>84</b>



## 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 pooblaščenju

**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

**ZJN-3** - Zakon o javnem naročanju

**ZIN** - Zakon o inšpekcijskem nadzoru

**ZP-1** - Zakon o prekrških

**ZTP** - Zakon o tajnih podatkih

**ZNPPol** - Zakon o nalogah in pooblastilih policije

**ZNDM-2** - Zakon o nadzoru državne meje

**ZODPol** - Zakon o organiziranosti in delu v policiji

**ZPND** - Zakon o preprečevanju nasilja v družini

**ZIPRS2122** - Zakon o izvrševanju proračunov Republike Slovenije za leti 2020 in 2021

**ZSPJS** - Zakon o sistemu plač v javnem sektorju

**ZZPPZ** - Zakon o zbirkah podatkov s področja zdravstvenega varstva

**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 pooblaščenču (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 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 pooblaščenčem ter nekatere prekrškovne določbe. Informacijski pooblaščenec je neodvisen in samostojen 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.

V okviru reforme varstva osebnih podatkov v EU ostaja neodvisnost Informacijskega pooblaščenca 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). Slednja je bila v slovenski pravni red prenesena z Zakonom o varstvu osebnih podatkov na področju obravnavanja kaznivih dejanj (ZVOPOKD), ki se je začel uporabljati v preteklem letu. Informacijski pooblaščenec tako kot nadzorni organ spremlja uporabo Splošne uredbe in ZVOPOKD, da se zaščitijo temeljne pravice in svoboščine posameznikov v zvezi z obdelavo osebnih podatkov ter se olajša prost pretok osebnih podatkov v Evropski uniji. Splošna uredba in ZVOPOKD 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.



47  
zaposlenih

## Varstvo osebnih podatkov



1127  
inšpekcijskih postopkov



prija



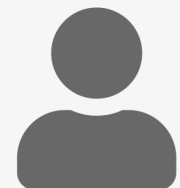
99  
prekrškovnih postopkov



mnenj n



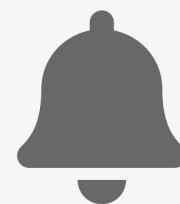
1471  
pisnih mnenj



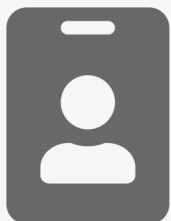
imenova  
za



2176  
ustnih mnenj



preve



77  
postopkov odločanja o  
vodilnem nadzornem organu



medna  
načelu



7  
novih smernic



2  
obrazec za zavezance



r



1  
infografike



65  
predavanj



# ŠTEVILKAH



2.287.193,00

EUR proračuna

## Informacije javnega značaja

108

kršitev varnosti



639

vloženih pritožb

6

prejete ocene učinka



397

izdanih odločb

2448

pooblaščenih oseb  
varstvo podatkov



168

pozivov zaradi molka

4

aktivna aktivnost za  
skladnost

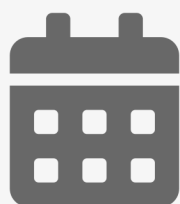


14

*in camera* ogledov

62

rodnih sodelovanj po  
"vse na enem mestu"



38 dni

povprečen čas reševanja  
pritožbenih zadev

154

postopkov vzajemne  
pomoči drugim  
nadzornim organom EU



301

pisnih prošenj za pojasnila

85

mnenj na predpise

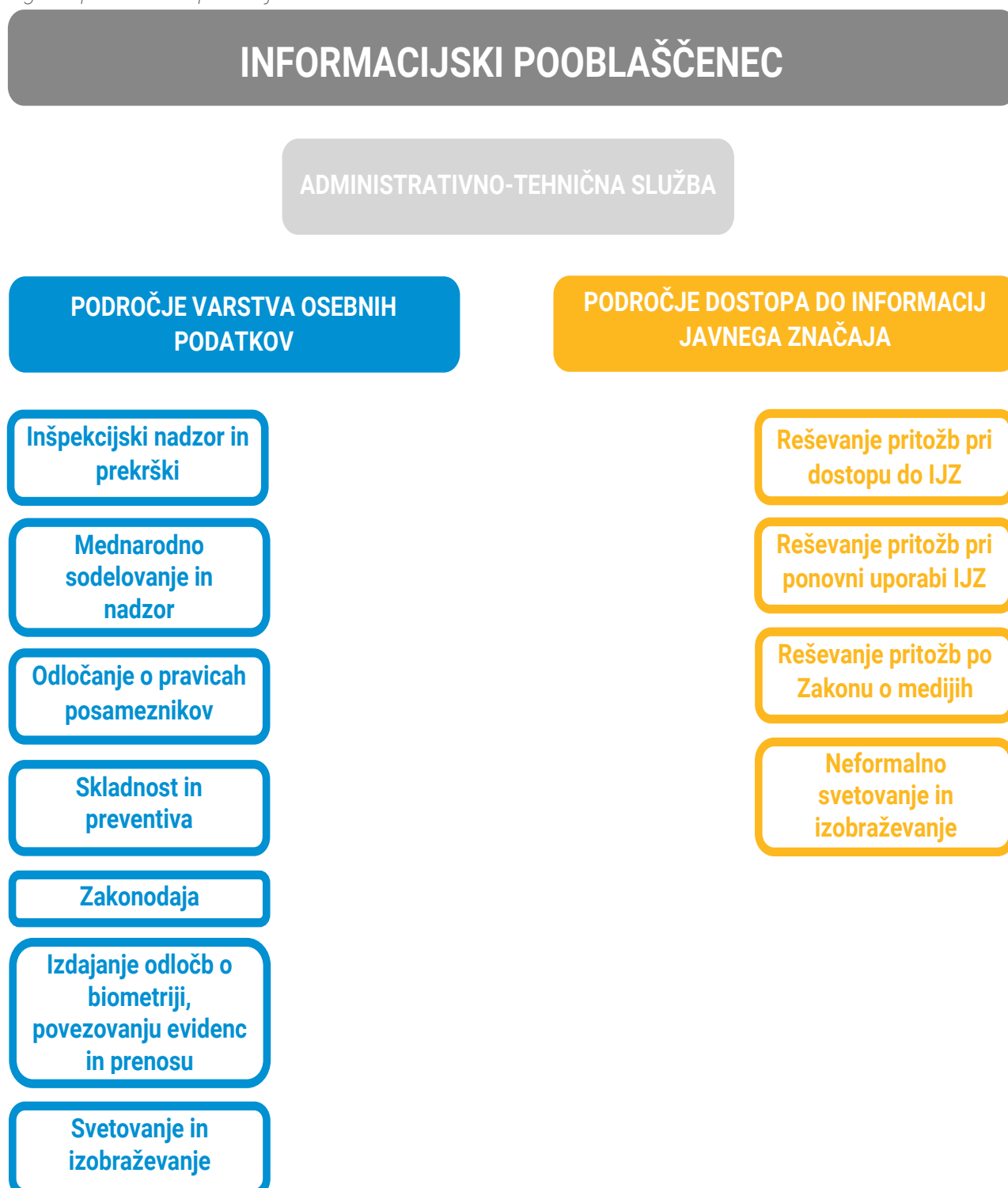
### 1.1.1 ORGANIZIRANOST

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



31. 12. 2021 je bil pri Informacijskem pooblaščenju zaposlen 1 funkcionar in 46 javnih uslužbencev. Izobrazbena struktura zaposlenih je razvidna iz spodnje preglednice.

Preglednica 1: Izobrazbena struktura zaposlenih pri Informacijskem pooblaščenju 31. 12. 2021.

	Srednja strokovna šola	Višja strokovna šola	Visoka strokovna šola, univerzitetni program	Univerzitetna izobrazba	Magisterij	Doktorat	Skupaj
Informacijska pooblaščenka				1			1
Namestniki informacijske pooblaščenke				2	2		4
Vodja mednarodnega sodelovanja in nadzora						1	1
Vodja nadzornikov					1		1
Generalna sekretarka					1		1
Državni nadzorniki za varstvo osebnih podatkov				10	5	1	16
Samostojni svetovalec pooblaščenca				1	1		2
Svetovalec pooblaščenca za dostop do informacij javnega značaja				5	1		6
Svetovalec pooblaščenca za varstvo osebnih podatkov				2	1		3
Svetovalec pooblaščenca za preventivo				1			1
Asistent svetovalca				2			2
Raziskovalec pooblaščenca			2				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
<b>Skupaj</b>	<b>2</b>	<b>2</b>	<b>5</b>	<b>24</b>	<b>12</b>	<b>2</b>	<b>47</b>

## 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 javnega značaja (peti odstavek 36.a člena ZDIJZ).

Na področju dostopa do informacij javnega značaja Informacijskemu pooblaščenecu 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 2021 ni bil sprejet.

**Splošna uredba** določa naloge Informacijskega pooblaščenca kot nadzornega organa v členu 57. Informacijski pooblaščenec:

- (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 pogodbeno določila in določbe iz člena 46(3);
- (s) odobri zavezujoča poslovna pravila v skladu s členom 47;
- (t) prispeva k dejavnostim Evropskega odbora za varstvo podatkov;
- (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 ugotovi zahtevi posameznika glede njegove pravice do seznanitve z zahtevanimi podatki, do izpisov, seznamov, vpogledov, potrdil, informacij, pojasnil, prepisovanja ali kopiranja po določbah zakona, ki ureja varstvo osebnih podatkov (pristojnost je določena v 2. členu ZInFP);
3. 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 ministrstvu, 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).

Informacijski pooblaščenec izvaja tudi pristojnosti skladno z **Zakonom o varstvu osebnih podatkov na področju obravnavanja kaznivih dejanj** (ZVOPOKD), ki je v slovenski pravni red prenesel Direktivo (EU) 2016/680 in Direktivo (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. Skladno z ZVOPOKD 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 skladno s 76. členom ZVOPOKD naslednje:

1. izvajanje inšpekcijskega nadzora nad izvajanjem določb ZVOPOKD in drugih zakonov, podzakonskih predpisov ali drugih splošnih aktov za izvrševanje javnih pooblastil glede obdelav osebnih podatkov s področij preprečevanja, preiskovanja, odkrivanja ali pregona kaznivih dejanj ali izvrševanja kazenskih sankcij;
2. odločanje v pritožbenem postopku ter v postopkih prijav prijaviteljev s posebnim položajem in izvajanje inšpekcijskega nadzora;
3. dajanje predhodnih mnenj ministrstvom, državnemu zboru, organom samoupravnih lokalnih skupnosti, drugim državnim organom in nosilcem javnih pooblastil o usklajenosti določb predlogov zakonov ter ostalih predpisov z zakoni in drugimi predpisi, ki urejajo osebne podatke s področij preprečevanja, preiskovanja, odkrivanja ali pregona kaznivih dejanj ali izvrševanja kazenskih sankcij;
4. izvajanje predhodnega posvetovanja;
5. dajanje neobveznih mnenj, pojasnil in stališč pristojnim organom in posameznikom o vprašanih glede varstva osebnih podatkov v zvezi z zakoni in povezanimi predpisi na področjih obravnavanja kaznivih dejanj;
6. spodbujanje ozaveščenosti in razumevanja javnosti o tveganjih, pravilih, zaščitnih ukrepih in pravicah v zvezi z obdelavo;
7. spodbujanje ozaveščenosti pristojnih organov, drugih upravljavcev in obdelovalcev o njihovih obveznostih na podlagi tega zakona;
8. sodelovanje z nadzornimi organi drugih držav ali mednarodnih organizacij;
9. sodelovanje pri delovanju Evropskega odbora za varstvo osebnih podatkov;
10. priprava letnega poročila o izvajanju zakona v skladu z določbami zakonov, ki urejata Informacijskega pooblaščenca in varstvo osebnih podatkov;
11. obveščanje pristojnega sodišča o kršitvah zakona oz. posredovanje mnenja sodišču o ugotovljenih kršitvah;
12. sodelovanje s pristojnimi organi, drugimi upravljavci in obdelovalci pri izvajanju nadzorov v skladu z določbami ZVOPOKD;
13. priprava obrazcev, ki olajšajo postopek vložitve prijav, pritožb, sporočil, pobud in drugih vlog v postopku inšpekcijskega nadzora glede varstva osebnih podatkov iz 27., 33. in 40. člena tega zakona;
14. izvajanje drugih nalog, določenih s tem zakonom.

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.

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

- 44. člena, ki opredeljuje pravico pacienta do zaupnosti osebnih podatkov ter pogoje za uporabo in drugo obdelavo osebnih podatkov za potrebe zdravljenja ali izven postopkov zdravstvene obravnave,
- 45. člena, ki določa dolžnost varovanja poklicne skrivnosti 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 **ZOlzk-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 ZOlzk-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 ZOlzk-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 odvratanja ravnanj, ki pomenijo nezakonito obdelavo osebnih podatkov, javno objavi informacije v zvezi z ukrepi nadzora in sankcijami zaradi prekrška, ki jih je izrekel.

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

## INFORMACIJSKI POOBLAŠČENEC

Splošna uredba o varstvu podatkov

Zakon o varstvu osebnih podatkov

Zakon o varstvu osebnih podatkov na področju obravnavanja kaznivih dejanj

Zakon o elektronskih komunikacijah

Zakon o pacientovih pravicah

Zakon o osebni izkaznici

Zakon o potnih listinah

Zakon o centralnem kreditnem registru

Zakon o potrošniških kreditih

Uredba o izvajanju Uredbe o drž. pobudi

Zakon o dostopu do informacij javnega značaja

Zakon o medijih

### 1.3 FINANČNO POSLOVANJE V LETU 2021

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 2021 **veljavni proračun na integralnih postavkah 2.330.548,50 EUR**, od tega na postavki plače 1.974.224,00 EUR, na postavki materialni stroški 312.969,00 EUR in na postavki investicije 43.355,50 EUR. Evidentiranih odredb na integralnih postavkah je bilo na dan 31. 12. 2021 2.325.964,73 EUR, od tega na postavki plače 1.974.218,39 EUR, na postavki materialni stroški 308.390,84 EUR in na postavki investicije 43.355,50 EUR.

*Proračun Informacijskega pooblaščenca 2015-2021.*

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
2021	2.330.548,50 EUR

Informacijski pooblaščenec je v letu 2021 razpolagal z namenskimi sredstvi v 7.317,92 EUR. Porabe namenskih sredstev v letu 2021 ni bilo.

V proračun leta 2022 je 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).

Na osnovi dopisa Ministrstva za finance številka 4103-1/2021/791 z dne 3. 12. 2021 je bilo na proračunsko postavko 7640 – Rezerva Republike Slovenije v skladu z drugim odstavkom 28. člena Zakona o izvrševanju proračunov Republike Slovenije za leti 2020 in 2021 (ZIPRS2122) z namenom zagotavljanja pravic porabe za oblikovanje in uporabo sredstev proračunske rezerve po 48. členu Zakona o javnih financah, prenesenih 152.765,50 EUR z integralnih proračunskih postavk Informacijskega pooblaščenca.

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

*Proračun Informacijskega pooblaščenca 2021.*

	Veljavni proračun v EUR	Prevzete obveznosti v EUR	Razpoložljiv proračun v EUR konec leta
<b>Informacijski pooblaščenec</b>	<b>2.430.553,75</b>	<b>2.417.902,41</b>	<b>12.651,34</b>
Podprogrami			
<b>OPRAVLJANJE DEJAVNOSTI</b>	<b>2.330.548,50</b>	<b>2.325.964,73</b>	<b>4.483,77</b>
PP 1267 Plače	1.974.224,00	1.974.218,39	5,61
PP 1271 Materialni stroški	312.969,00	308.390,84	4.578,16
PP 1273 Investicije	43.355,50	43.355,50	0,00
<b>NAMENSKA SREDSTVA</b>	<b>7.317,92</b>	<b>0,00</b>	<b>7.317,92</b>
7459 Namenska sr. kupnine	7.317,92	0,00	7.317,92
<b>Donacije – EU projekti</b>	<b>92.687,33</b>	<b>91.937,68</b>	<b>749,65</b>
PP 9958 Mednarodna spl. str.	0,14	0,00	0,14
PP130134 projekt Taiex	2,99	0,00	2,99
PP 190100 RAPID.si	16.907,20	16.167,13	740,07
PP200001 iDecide	75.777,00	75.770,55	6,45

**Za materialne stroške je bilo leta 2021 porabljenih 308.390,84 EUR**, in sicer za pisarniški in splošni material in storitve 66.774,64 EUR (pisarniški material, čiščenje poslovnih prostorov, storitve varovanja zgradb in prostorov, spremljanje medijev in arhiviranje, stroški prevajalskih storitev in lektoriranja, reprezentanca, revizija, tekoči obratovalni stroški ter drugi splošni material in storitve), za posebni material in storitve 5.484,54 EUR (nakup mask in testov za covid-19, nakup drobnega inventarja, zdravniški pregledi zaposlenih ter drugi posebni material in storitve), za energijo, vodo, komunalne storitve, pošto in komunikacijo 37.446,34 EUR (električna energija, ogrevanje, voda in komunalne storitve, odvoz smeti, stroški telefonov ter poštna storitve), za prevozne stroške in storitve 7.372,71 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 5.911,99 EUR (stroški, povezani s službenimi potovanji zaposlenih, dnevnice, nočnine, letalske karte, hotelske storitve in stroški prevozov), za tekoče vzdrževanje 9.268,04 EUR (tekoče vzdrževanje, povezano z najemom 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 135.825,82 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 40.306,76 EUR (stroški konferenc in seminarjev doma in v tujini, plačilo za delo prek študentskega servisa, 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 in stroški prevozov) od Evropske komisije na postavko prejel 355,95 EUR, dobropisa Generali zavarovalnice v znesku 61.98 EUR in vračilo preveč izplačane dnevnic v znesku 8,56 EUR. V letu 2021 je bila v oktobru s proračunske postavke materialni stroški izvedena prerazporeditev na proračunsko postavko investicije v znesku 16.000 EUR. Informacijski pooblaščenec je konec leta 2021 iz proračunske postavke materialni stroški prerazporedil proste pravice porabe na proračunsko postavko 7640 – Rezerva Republike Slovenije v znesku 39.476,00 EUR.

**Za investicije je bilo do konca leta 2021 porabljenih 43.355,50 EUR.** Sredstva so bila porabljena za nakup pisarniškega pohištva in pisarniške opreme v znesku 12.355,20 EUR (vgradne omare na hodniku in sedem pisarniških stolov), strojne računalniške opreme v znesku 11.911,20 EUR (sedem monitorjev, deset prenosnih računalnikov, dva skenerja in druga oprema), drugega pohištva v znesku 2.108,16 EUR (protivlomna vrata), strežnikov in diskovnih sistemov v znesku 1.050,42 EUR, druge opreme in napeljave v znesku 126,88 EUR (nadgradnja sistema za evidenco in kontrolo prisotnosti), nematerialnega premoženja v znesku 15.803,64 EUR (pet kosov avtomatske lektorice Amebis Besana, licenca HCL za 50 uporabnikov – nadgradnja poštnega strežnika domino strežnik in deset kosov Microsoft programske opreme). Konec leta 2021 je bilo stanje razpoložljivega proračuna na postavki investicije 0,00 EUR.

V letu 2021 so bile v oktobru s proračunske postavke materialni stroški izvedene prerazporeditve na proračunsko postavko investicije v znesku 16.000 EUR. S proračunske postavke investicije je Informacijski pooblaščenec konec leta 2021 prerazporedil proste pravice porabe na proračunsko postavko 7640 – Rezerva Republike Slovenije v znesku 2.644,50 EUR.

**Za plače zaposlenih je bilo porabljenih 1.974.218,39 EUR** oz. 99,99 % sredstev glede na veljavni proračun za leto 2021. Glede na predhodna leta se je poraba sredstev povečala zaradi 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, začetka izplačevanja redne delovne uspešnosti v skladu z določbami Zakona o sistemu plač v javnem sektorju (ZSPJS) in določbami Kolektivne pogodbe za javni sektor ter zaposlitev v skladu s kadrovskim načrtom in novimi pristojnostmi Informacijskega pooblaščenca na področju uveljavitev Splošne uredbe ter ZVOPOKD. Uveljavitev Splošne uredbe v Republiki Sloveniji je za Informacijskega pooblaščenca pomenila prevzem številnih novih nalog in zadalžitev, ki so zahtevale dodatne zaposlitve. Porabljena sredstva v višini 1.974.218,39 EUR so bila namenjena za osnovne plače in dodatke v znesku 1.546.444,56 EUR, za regres za letni dopust je bilo namenjenih 49.962,14 EUR, za povračila in nadomestila 52.925,88 EUR, sredstva za delovno uspešnost z naslova povečanega obsega dela zaradi povečanega pripada zadev in redne delovne uspešnosti so znašala 47.731,49 EUR, za druge izdatke zaposlenim je bilo porabljenih 1.884,16 EUR, za prispevke delodajalcev za pokojninsko in invalidsko zavarovanje 140.281,06 EUR, za prispevke za zdravstveno zavarovanje 113.198,40 EUR, za prispevke za zaposlovanje 990,76 EUR, za prispevek za starševsko varstvo 1.596,13 EUR, premije kolektivnega dodatnega pokojninskega zavarovanja na podlagi Zakona o kolektivnem dodatnem pokojninskem zavarovanju za javne uslužbenke pa so znašale

19.203,81 EUR. Informacijski pooblaščenec je leta 2021 od Zavoda za zdravstveno zavarovanje Slovenije z naslova refundacij bolnih in invalidnih prejel sredstva na postavko za plače v višini 23.236,14 EUR ter s strani Zavoda za zaposlovanje z naslova povračila nadomestila plač delavcem zaradi odrejene karantene in/ali odsotnosti zaradi višje sile v višini 2.142,72 EUR. S postavke plače je Informacijski pooblaščenec v letu 2021 prerazporedil proste pravice porabe na proračunsko postavko 7640 – Rezerva Republike Slovenije v znesku 110.645,00 EUR.

**Namenska sredstva kupnine** – v leto 2021 je bilo prenesenih 7.317,92 EUR finančnih sredstev kupnin. Leta 2021 na postavki ni bilo niti prilivov niti odlivov. Preostanek finančnih sredstev v višini 7.317,92 EUR se prenese v leto 2022.

**Mednarodna spletna stran info-commissioners.org** – iz leta 2020 je bilo prenesenih 0,14 EUR finančnih sredstev. Leta 2021 na tej postavki ni bilo porabe. Projekt se leta 2022 konča, preostanek sredstev (0,14 EUR) bo nakazan na podračun izvrševanja proračuna.

**Projekt Taiex** – iz leta 2020 je v leto 2021 prenesenih 2,99 EUR. Za projekt Taiex leta 2021 ni bilo niti prilivov niti odlivov. Projekt še vedno deluje v okviru EU. Preostanek finančnih sredstev (2,99 EUR) se prenese v leto 2022.

**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 leta 2020, in sicer je bilo oktobra oddano poročilo. Dne 18. 12. 2020 je bil Informacijskemu pooblaščenec nakazan končni priliv v znesku 16.907,80 EUR. V letu 2021 je bilo stanje veljavnega proračuna 16.907,20 EUR, prevzete obveznosti so znašale 16.167,13 EUR. Sredstva so bila porabljena za najem poslovnih prostorov za maj 2021 in obratovalne stroške za poslovne prostore za april 2021. Preostanek sredstev je konec leta znašal 731,20 EUR. Projekt se je leta 2022 zaključil, preostanek sredstev bo nakazan na podračun izvrševanja proračuna.

#### **Projekt iDecide – posamezniki odločajo**

Informacijski pooblaščenec je leta 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 2020–2024.

Projekt bo trajal 24 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 dvigovanje 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 24 mesecih trajanja projekta iz integralnih proračunskih sredstev zagotovil 48.586,56 EUR. Skupno bodo sredstva za izvedbo projekta torej znašala 242.932,80 EUR. Porabljena bodo 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, povezane s pripravo in izvedbo aktivnosti, ter za materialne stroške, ki jih bo s tem imel Informacijski pooblaščenec.

Večji del porabljenih stroškov v letu 2020 je bil namenjen za pokrivanje stroškov dela zaposlenih, del pa tudi za tisk brošur. Poraba leta 2020 za potrebe projekta je na proračunski postavki PP 200001 znašala 79.697,05 EUR, na postavki integralna sredstva PP 1271 materialni stroški pa 91,50 EUR.

Projekt se je v letu 2021 izvajal po predvidenem načrtu. Izvedenih je bilo pet izobraževalnih seminarjev za ciljne skupine, deloma prek spletnih platform zaradi omejevalnih ukrepov v zvezi s pandemijo koronavirusa in deloma v živo (sodelovanje na festivalu za 3. življenjsko obdobje in na Mreži znanja 2022). Strokovnjaki iz projektne skupine so nudili strokovno pomoč javnosti prek različnih kanalov: prek vzpostavljene telefonske linije za svetovanje splošni javnosti, izvedeno je bilo tudi strokovno svetovanje prek e-pošte. V okviru projekta so bile prek spletne strani [www.ip-rs.si](http://www.ip-rs.si) posredovane informacije ključnim javnostim ter izvedena izobraževalna predavanja na zunanjih dogodkih. Strokovnjaki iz projektne skupine so pripravili 16 člankov za različne revije in publikacije, s katerimi so širši javnosti predstavili teme iz priročnikov, ki so bili pripravljene v okviru projekta (npr. Dnevnik, revija Cool, Vzajemnost).

Veljavni proračun je ob koncu leta 2021 znašal 75.777,00 EUR. Poraba sredstev je bila v letu 2021 realizirana v višini 75.770,55 EUR, preostanek sredstev je znašal 6,45 EUR. Večji del prevzetih obveznosti je bil namenjen za pokrivanje stroškov dela zaposlenih, snemanju in montaži spletnih seminarjev in tisku nalepk.

Poraba leta 2021 za potrebe projekta je na postavki integralna sredstva PP 1271 materialni stroški znašala 7.339,82 EUR (potni stroški zaposleni, najem razstavnega prostora, priprava in montaža videoposnetkov in stroški dela zaposlenih).

Tip postavke 80 se ravna skladno s pravili Zakona o izvrševanju proračunov Republike Slovenije za leti 2021 in 2022 glede namenskih finančnih sredstev EU, kar pomeni, da se sredstva ne prenašajo v naslednja leta.

# 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).

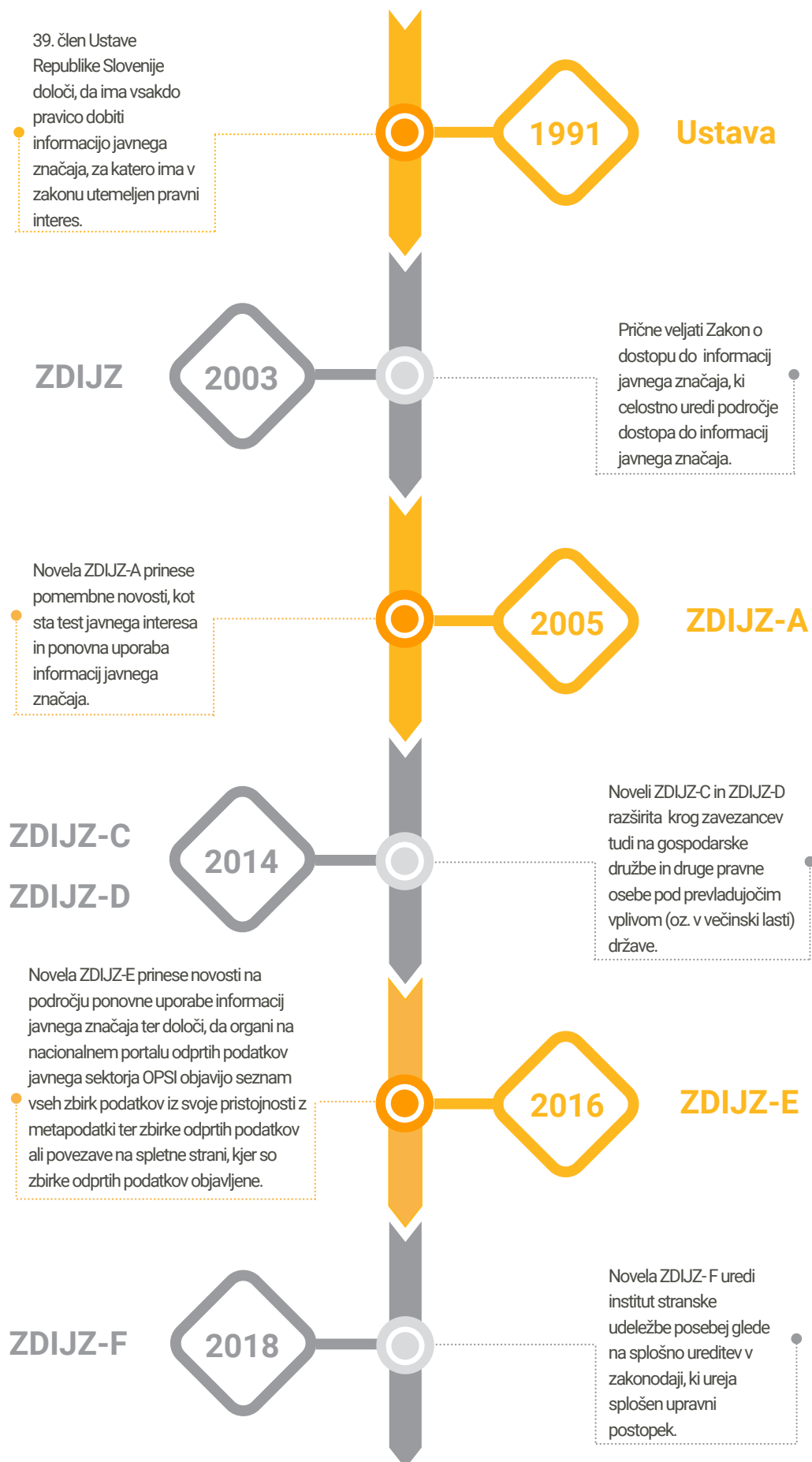
Leta 2005 je bil z novelo ZDIJZ-A narejen še korak naprej. Novela je namreč zožila možnost neupravičenega zapiranja dostopa do informacij in uvedla številne novosti, kot so ponovna uporaba informacij javnega značaja in pristojnosti upravne inšpekcije na področju izvajanja tega zakona. Najpomembnejša 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 krepi 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 informacije javnega značaja ali ponovne uporabe samo prosilec, če je predmet odločanja dostop do podatkov, za katere je z zakonom določeno, da so javni. S tem je uredila institut stranske udeležbe posebej glede na splošno ureditev v zakonodaji, ki ureja upravni postopek.

Časovnica razvoja Zakona o dostopu do informacij javnega značaja.



ZDIJZ zagotavlja dostop do informacij, ki so že ustvarjene, in sicer v kakršni koli obliki. S tem zakon zagotavlja preglednost porabe javnega denarja in odločitev javne uprave, saj ta dela v imenu ljudi in za ljudi.

### **Kdo so zavezanci za posredovanje informacij javnega značaja?**

Zavezanci za posredovanje informacij javnega značaja se delijo v dve skupini:

- **organi** (državni organi, organi lokalnih skupnosti, javne agencije, javni skladi in druge osebe javnega prava, nosilci javnih pooblastil in izvajalci javnih služb) ter
- **poslovni subjekti pod prevladujočim vplivom oseb javnega prava.**

Zavezanci so informacije javnega značaja dolžni zagotavljati na dva načina: z objavo na spletu in z omogočanjem dostopa na podlagi individualnih zahtev. Za vsako od skupin zavezancev je pojem »informacija javnega značaja« (torej informacija, ki jo morajo posredovati prosilcu) definiran drugače; pri zavezancih iz druge skupine je ožji. Medtem ko za organe na splošno velja, da so vsi dokumenti, zadeve, dosjeji, registri, evidence in dokumentarno gradivo, s katerim razpolagajo (ne glede na to, ali jih je organ izdelal sam, v sodelovanju z drugim organom ali jih je pridobil od drugih oseb), informacije javnega značaja, razen izjem, za poslovne subjekte pod prevladujočim vplivom oseb javnega prava 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 poslovnega 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 obveščeni. Vsak prosilec ima na zahtevo pravico pridobiti informacijo javnega značaja, in sicer tako, da jo dobi na vpogled ali da dobi njen prepis, fotokopijo ali elektronski zapis. Zavezanec mora o zahtevi odločiti v 20 delovnih dneh, organi lahko v izjemnih okoliščinah podaljšajo rok za največ 30 delovnih dni. Vpogled v zahtevano informacijo je brezplačen, 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 2021 je Informacijski pooblaščenec vodil 639 pritožbenih postopkov, od tega 389 postopkov zoper zavrnilne odločbe organov in 244 postopkov zaradi t. i. molka organa oz. neodzivnosti. Zoper poslovne subjekte pod prevladujočim vplivom je Informacijski pooblaščenec vodil šest pritožbenih postopkov, štiri zaradi zavrnitve dostopa ter dva zaradi molka.

Leta 2021 je Informacijski pooblaščenec odgovoril na 301 pisno prošnjo za neformalno pomoč ali mnenje, ki jih je prejel od zavezancev prve stopnje in prosilcev, odgovoril pa je tudi na 948 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.

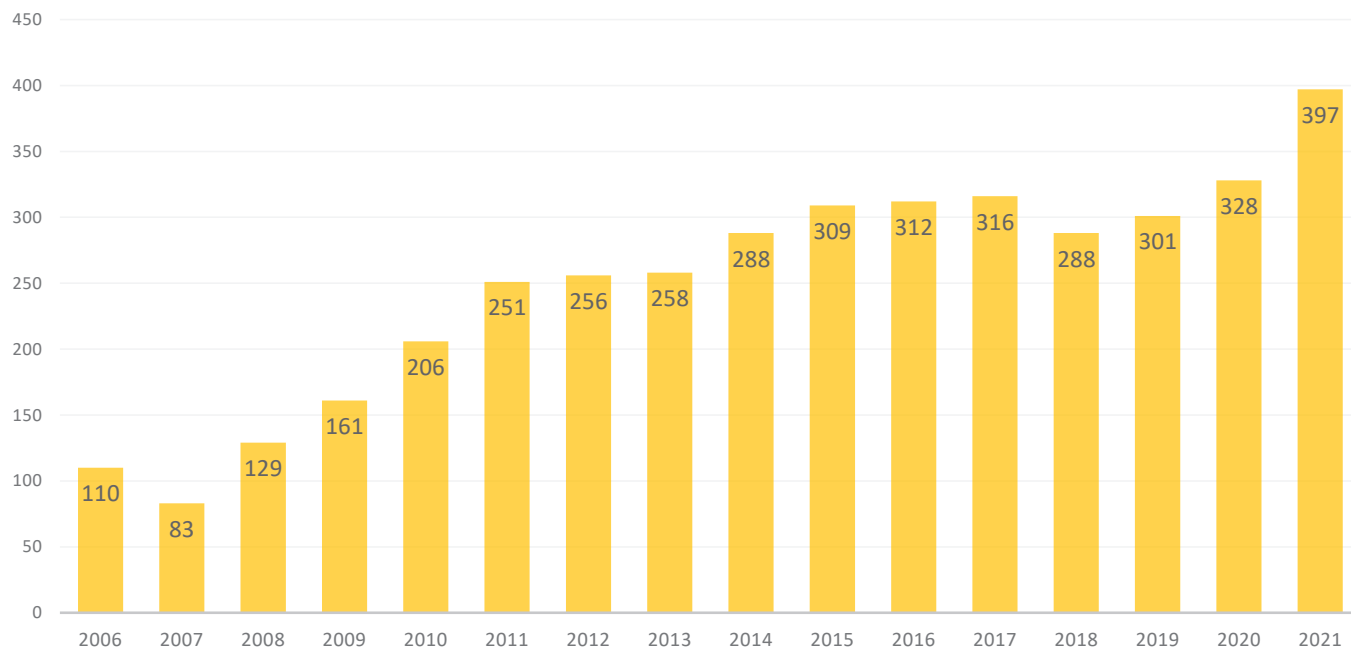
### 2.2.1 PRITOŽBE ZOPER ZAVRNILNE ODLOČBE IN IZDANE ODLOČBE

V okviru pritožbenih postopkov zoper odločbe, s katerimi so zavezanci zavrnili zahteve po dostopu do informacij javnega značaja, je Informacijski pooblaščenec v letu 2021 rešil 404 zadeve. Izdal je 397 odločb, tri pritožbe prosilcev je s sklepom zavrgel (pritožbe so bile nedovoljene), v štirih primerih pa je zaradi umika pritožbe prosilca izdal sklep o ustavitvi postopka. Informacijski pooblaščenec je izdal 353 odločb, ki so se nanašale na pritožbene postopke, začete v letu 2021, in 44 odločb, ki so se nanašale na postopke, začete pred letom 2021. Med reševanjem pritožb je na terenu opravil 14 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 (397):

- pritožbo zavrnil – 206,
- pritožbi delno ali v celoti ugodil oz. rešil zadevo v korist prosilca – 129,
- pritožbi ugodil in zadevo vrnil prvostopenjskemu organu v ponovno odločanje – 58,
- pritožbo zavrgel – 1,
- odločbo prvostopenjskega organa razglasil za nično – 3.

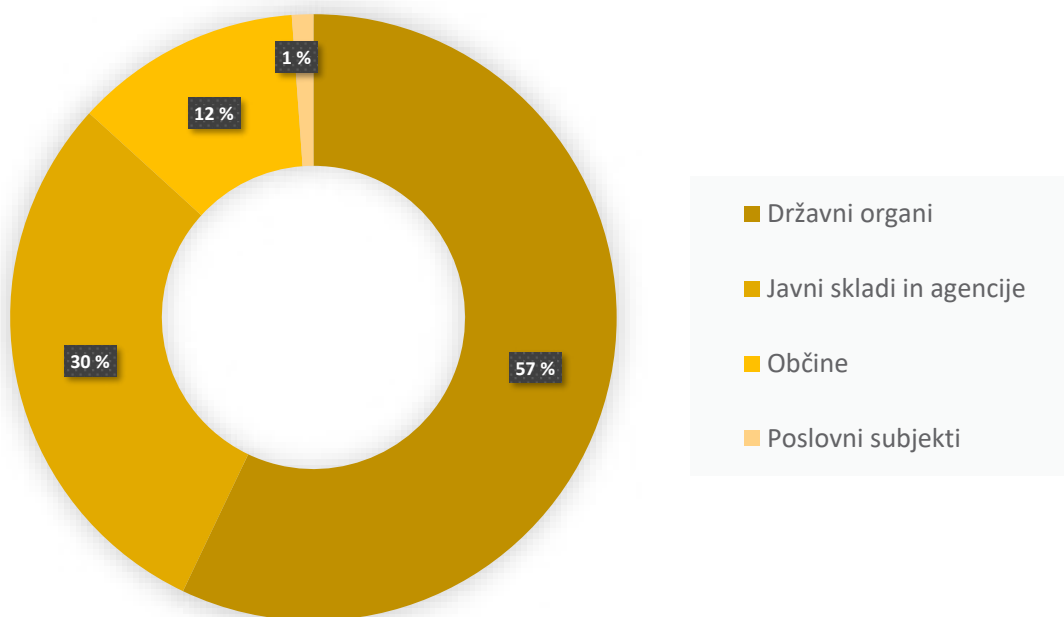
Število izdanih odločb na področju dostopa do informacij javnega značaja med letoma 2006 in 2021.



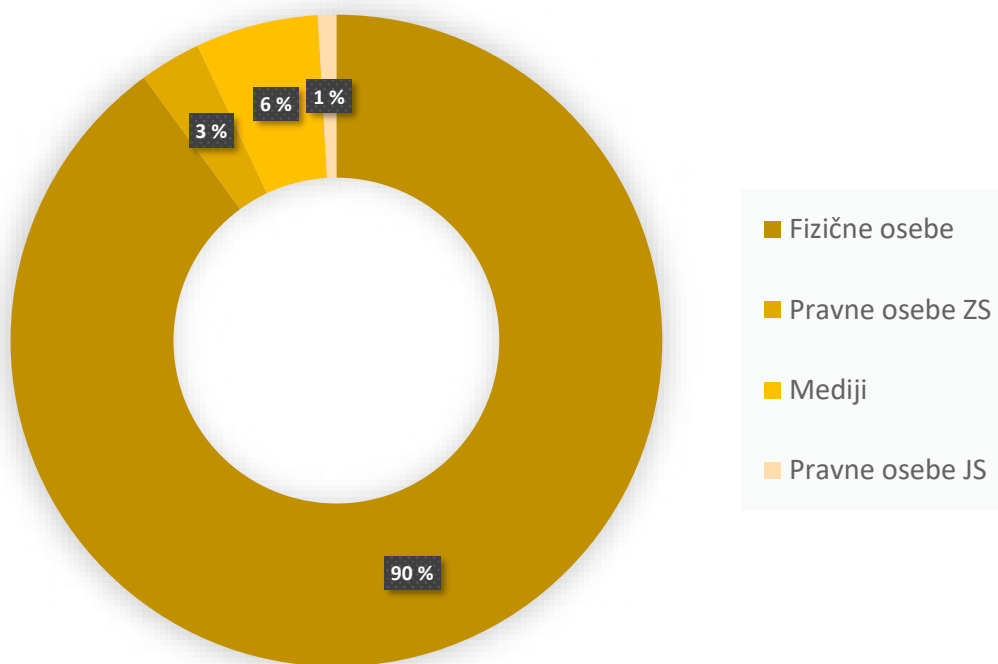
Pritožbe prosilcev zaradi zavrnitve dostopa do informacij javnega značaja, o katerih je Informacijski pooblaščenec odločil z odločbo, so zadevale naslednje skupine zavezancev:

- državni organi – 205, od tega ministrstva in organi v sestavi ter upravne enote 163, 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 – 130,
- občine – 57,
- poslovni subjekti pod prevladujočim vplivom države, občin ali drugih oseb javnega prava – 5.

Zoper katere zavezance so bile vložene pritožbe?



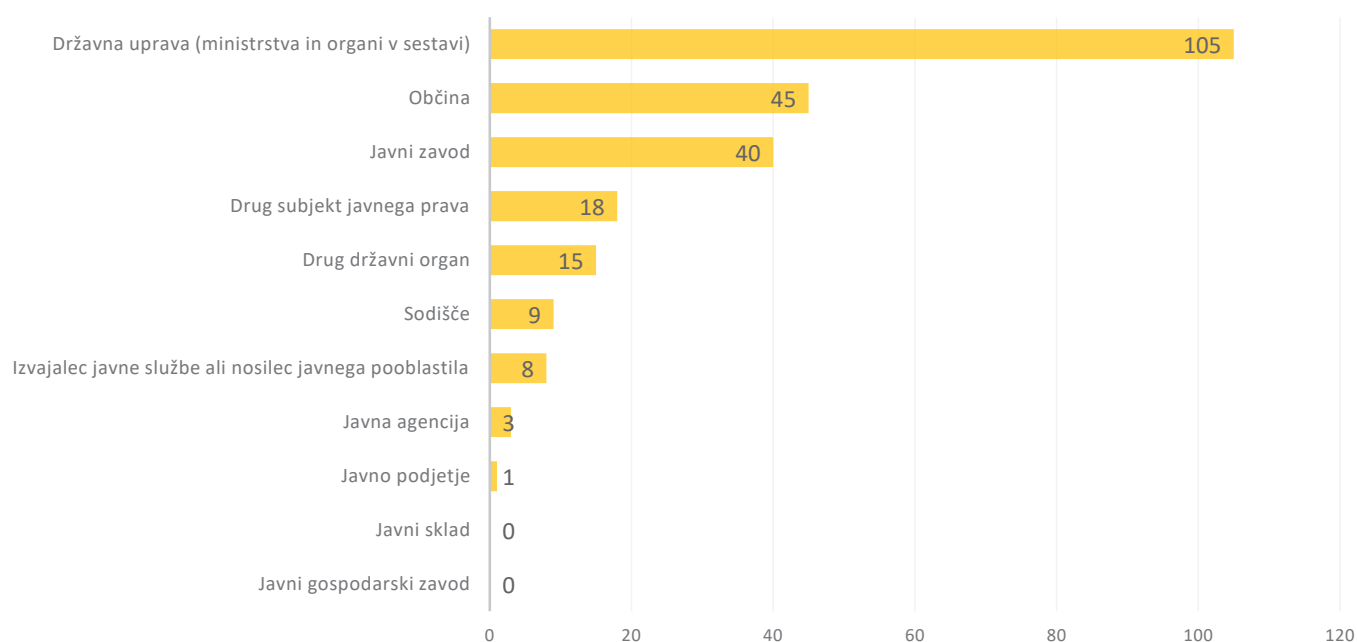
V 283 primerih so bili prosilci fizične osebe, v 61 primerih so se pritožile pravne osebe zasebnega sektorja, v 44 primerih novinarji in medijske hiše, devetkrat pa so se pritožile pravne osebe javnega sektorja.



## 2.2.2 PRITOŽBE ZOPER MOLK

Informacijski pooblaščenec je v letu 2021 prejel 244 pritožb zaradi molka organa in dve pritožbi zaradi neodziva poslovnih subjektov pod prevladujočim vplivom. Po podatkih je bilo največ primerov molka zaznati med organi državne uprave (ministrstva, organi v sestavi itd.), in sicer 105 (močno povečanje glede na leto 2020, ko je bilo zabeleženih 66 primerov molka organov državne uprave), sledile so občine (45 primerov) ter javni zavodi (40 primerov).

*Zoper katere zavezance so bile vložene pritožbe?*





Največ pritožb zoper molk organa je bilo vloženih s strani fizičnih oseb, in sicer kar 70,9 % vseh vloženih pritožb zaradi molka organa (173). V 16,8 % primerih (41) so pritožbo zaradi molka organa vložili novinarji oz. mediji. V 9,8 % primerih (24) je bila pritožba vložena s strani pravnih oseb zasebnega prava in v 2,5 % primerih (6) s strani pravnih oseb javnega prava.

Po preizkusu formalnih predpostavk Informacijski pooblaščenec v 74 primerih postopka zaradi molka ni uvedel, in sicer je v 16 primerih pritožbo s sklepom zavrgel, od tega v 15 primerih zaradi preuranjenosti, v enem primeru pa zato, ker pritožba ni bila dovoljena. V 11 primerih je prosilec tekom postopka pritožbo umaknil, saj je od zavezanca že prejel zahtevano informacijo. Informacijski pooblaščenec ni v nobenem primeru prevzel pritožbe v odločanje in sam meritorno odločil. V dveh zadevah je organ vloge odstopil na Upravno inšpekcijo (eno kot vlogo za uvedbo prekrškovnega postopka in eno kot prijavo organa zavezanca, ker nima imenovanega zakonitega zastopnika), v eni zadevi pa je organ z odločbo odločil, da zavezanec ni zavezan postopati po ZDIJZ.

V 44 primerih je Informacijski pooblaščenec postopek z molkom zaključil tako, da je prosilcu pojasnil:

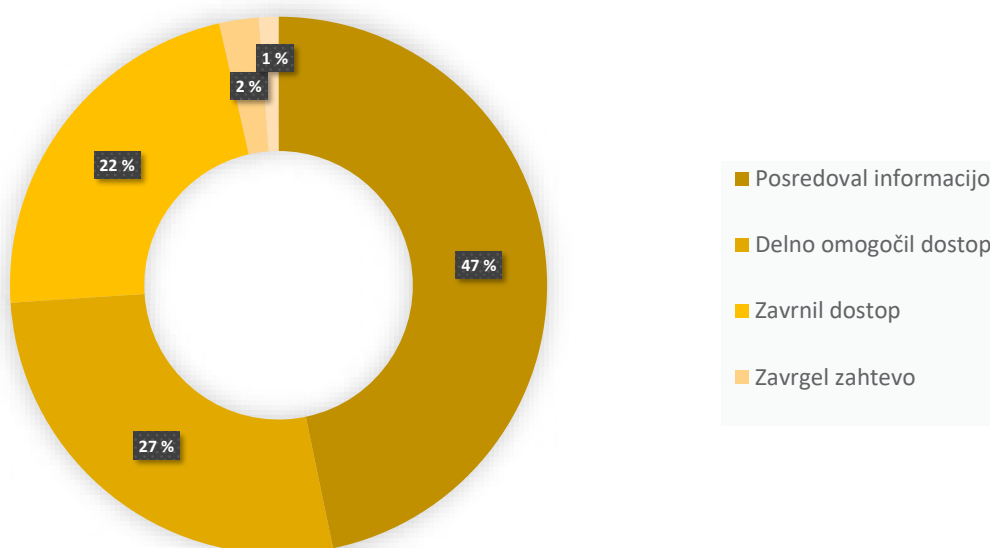
- da za reševanje njihove vloge ni pristojen, in mu svetoval, kako ravnati v zvezi z njegovo zahtevo,
- da vloga, ki jo je prosilec vložil pri zavezancu, ni formalno popolna,
- da zavezanec utemeljeno ni obravnaval njegove vloge po ZDIJZ, temveč na drugi pravni podlagi,
- da je bilo o njegovi vlogi že odločeno.

V pritožbenih postopkih je Informacijski pooblaščenec zaradi molka v 168 primerih zavezanca pozval, naj o zahtevi prosilca čim prej odločijo. Po pozivu Informacijskega pooblaščenca so zavezanci prosilcu v 78 primerih informacijo posredovali, v 38 primerih so prosilcu dostop zavrnil ter izdali zavrnilno odločbo, v 46 primerih pa so prosilcu delno omogočili dostop (določene podatke so zakrili oz. omogočili dostop le do določenih informacij, dostop do ostalih pa z odločbo zavrnil). V štirih primerih so zavezanci s sklepom zahtevo prosilca zavrgli, v dveh primerih pa so organi vlogo prosilca za dostop do dokumentov odstopili v reševanje drugemu organu.

Dve zadevi ima Informacijski pooblaščenec trenutno še odprti in v reševanju.

V okviru zahteve za dostop do informacij javnega značaja pri poslovnih subjektih pod prevladujočim vplivom je Informacijski pooblaščenec vodil dva pritožbena postopka zaradi molka zavezancev, in sicer je po pozivu Informacijskega pooblaščenca zavezanec v enem primeru prosilcu omogočil dostop, v drugem pa je prosilčevo zahtevo delno zavrnil z odločbo. Izmed 246 primerov molka je bilo 35 primerov povezanih z Zakonom o medijih, največkrat (v 18 primerih) je šlo za organe državne uprave.

*Kako so ravnali zavezanci po pozivu Informacijskega pooblaščenca zaradi molka?*



## 2.3 ŠTEVILO VLOŽENIH TOŽB IN PREJETIH SODB

Pritožba zoper odločbo Informacijskega pooblaščenca ni dopustna, mogoče pa je sprožiti upravni spor. Leta 2021 je bilo na Upravnem sodišču RS vloženi 49 tožb zoper odločbe Informacijskega pooblaščenca (zoper 12,34 % 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 2021 odločilo o 21 tožbah, ki so bile vložene zoper odločbe Informacijskega pooblaščenca, in:

- tožbo zavrnilo – 14,
- tožbi ugodilo, izpodbijano odločbo oz. del odločbe odpravilo in zadevo vrnilo Informacijskemu pooblaščenca v ponovno odločanje – 5,
- tožbi delno ugodilo tako, da je odločbo delno odpravilo in pritožbo prosilca zoper odločbo tožnika zavrnilo – 1,
- tožbo delno zavrglo, v preostalem delu zavrnilo – 1.

Leta 2021 je bila na Vrhovno sodišče RS vložena ena revizija zoper sodbo Upravnega sodišča.

## 2.4 STORJENI PREKRŠKI PO ZDIJZ, ZInFP IN ZMed

Leta 2021 je Informacijski pooblaščenec izdal eno odločbo o prekršku odgovorni osebi zavezanca zaradi kršitev določb ZDIJZ, in sicer odgovorna oseba ni posredovala zahtevanih informacij javnega značaja prosilcu oz. ni odločila o dostopu do zahtevanih informacij. Informacijski pooblaščenec je v zadevi pod opr. št. 090-112/2015 zoper Ekonomsko fakulteto v Ljubljani vodil postopek izvršbe s prisilitvijo, ker zavezanec, kljub temu da je odločba Informacijskega pooblaščenca postala pravnomočna in izvršljiva že leta 2016, prosilki še vedno ni želel posredovati informacij javnega značaja, kot mu je bilo naloženo.

## 2.5 IZBRANI PRIMERI NA PODROČJU DOSTOPA DO INFORMACIJ JAVNEGA ZNAČAJA

**Informacije, ki izkazujejo prejemke člana poslovnega organa oz. zakonitega zastopnika poslovnega subjekta, so absolutno javne.**

Prosilka je na Mrežni podjetniški inkubator Vrelec, d. o. o., naslovila zahtevo za dostop do kopij izstavljenih računov v določenem obdobju za subjekte, ki imajo v najemu prostore v objektu Vrelec 1 in Vrelec 2, kopije računov, ki se nanašajo na stroške obratovanja, kopije računov družbe Kartol, d. o. o., in podjetja Adinara skupaj s prilogami ter kopije obračunanih potnih nalogov za leto 2019. Zavezanec je prosilki odgovoril, da je na podlagi določb ZDIJZ zavezanec za posredovanje informacij javnega značaja kot poslovni subjekt pod prevladujočim vplivom oseb javnega prava. Zahtevo za dostop do zelenih informacij je zavrnil, ker je ocenil, da računi in potni nalogi ne predstavljajo informacije javnega značaja skladno s 4.a členom ZDIJZ, ker že pojmovno ne gre za pravne posle. Za razkritje podatkov, ki so nastali na podlagi pravnih poslov, pa je ocenil, da ni podan javni interes po drugem odstavku 6. člena ZDIJZ. Prosilka je s pritožbo oporekala odločitvi zavezanca. Navedla je, da Zakon o stvarnem premoženju države jasno opredeljuje pomen in vsebino upravljanja stvarnega premoženja. Zavezanec je za izvajanje dejavnosti podjetniškega inkubatorja od Občine Rogaška Slatina prejel v najem poslovne prostore. Prosilka je menila, da je ena glavnih dejavnosti zavezanca oddajanje teh istih poslovnih prostorov v podnajem, kar pa pomeni upravljanje s stvarnim premoženjem. Podobno kot izdani računi so tudi prejeti računi posledica upravljanja s stvarnim premoženjem, posledica tega pa je funkcionalna urejenost najetih prostorov. Ko pride do izplačila, razpolaganje s premoženjem predstavlja tudi vsak obračunan potni nalog. V pritožbenem postopku je Informacijski pooblaščenec ugotovil, da je družba Mrežni podjetniški inkubator Vrelec, d. o. o., kot poslovni subjekt pod prevladujočim vplivom oseb javnega prava zavezanec po prvem odstavku 1.a člena ZDIJZ. Pri teh zavezancih so informacije javnega značaja le tiste informacije, ki jih ZDIJZ navaja v 4.a členu, in sicer informacije iz sklenjenega pravnega posla, ki se nanašajo na pridobivanje, razpolaganje ali upravljanje s stvarnim premoženjem poslovnega subjekta ali izdatke poslovnega subjekta za naročilo blaga, gradenj, agentskih, svetovalnih ali drugih storitev ter sponzorskih, donatorskih in avtorskih pogodb in drugih pravnih poslov, s katerimi se dosega enak učinek. Informacijski pooblaščenec se je strinjal s pritožbeno

navedbo, da mora biti razpolaganje s stvarnim premoženjem države in samoupravnih lokalnih skupnosti transparentno, vendar pa je zakonodajalec pri poslovnih subjektih pod prevladujočim vplivom oseb javnega prava prosto dostopnost do podatkov omejil na »informacije iz sklenjenega pravnega posla«, torej na podatke iz konkretne pogodbe, med katere pa zahtevani računi v obravnavani zadevi ne sodijo, saj so del izvedbe pravnega posla. Z navedenim je Informacijski pooblaščenec sledil tudi svoji praksi (npr. odločbama št. 090-10/2017/5 in št. 090-37/2020/11). Glede računov podjetja Adinare je Informacijski pooblaščenec ugotovil, da gre v obravnavanem primeru za informacije, ki jih je mogoče obravnavati kot prejemke člana poslovnega organa, ki so v drugi alineji prvega odstavka 4.a člena opredeljene kot absolutno javne informacije. Informacijski pooblaščenec je menil, da bi bilo nesprejemljivo in v nasprotju s pravno varnostjo, da bi bilo izplačilo članu poslovnega organa oz. zakonitemu zastopniku zavezanca izvzeto iz prostega dostopa zgolj zato, ker se je plačilo prejemka ali bonitete izvedlo preko »računa«. To bi pomenilo obid zakonske določbe, kar je nedopustno. Sama »oblika« izplačila prejemka ali bonitete torej ne more vplivati na javnost podatkov. Pritožbi prosilke je Informacijski pooblaščenec delno ugodil in ji omogočil dostop do zneskov, izdajatelja, prejemnika ter datuma izdaje računov podjetja Adinare.

**KLJUČNE BESEDE:** Poslovni subjekt pod prevladujočim vplivom, ali gre za IJZ?, številka odločbe 09021-9/2020

### **Zaradi določil Aarhuške konvencije za okoljske informacije ne velja nobena izjema od prostega dostopa do informacij javnega značaja po ZDIJZ**

Prosilec je od Javnega podjetja Vodovod Kanalizacija Snaga, d. o. o., želel prejeti dopis organa, naslovljenega na Mestno občino Ljubljana, o pridobitvi lastninske pravice znotraj najožjega vodovarstvenega območja skupaj s tabelo morebitnih kršitev. Organ je dostop zavrnil s sklicevanjem na izjemo varstva upravnega postopka. Informacijski pooblaščenec je v pritožbenem postopku ugotovil, da iz izpodbijane odločbe (niti iz zahtevanih dokumentov) ni razvidno, da bi bil začet (kateri koli) upravni postopek, organ pa ni izkazal niti škode za njegovo izvedbo, zato je pritožbi ugodil in odločil, da mora organ prosilcu posredovati zahtevane informacije. Informacijski pooblaščenec je v pritožbenem postopku tudi ugotovil, da gre pri zahtevanih informacijah za podatke o emisijah v okolje. Zahtevani dokument s prilogo vsebuje zaznave kršitev na vodovarstvenih območjih z vidika kmetijske rabe. V obravnavani zadevi so zato zahtevane informacije absolutno prosto dostopne informacije javnega značaja na podlagi 2. alineje tretjega odstavka 6. člena ZDIJZ (okoljski podatki).

**KLJUČNE BESEDE:** okoljski podatki, varstvo upravnega postopka, številka odločbe 090-292/2020

### **Kadar je organ porabnik javnih sredstev, so informacije o ugotovitvah o pravilnosti in smotrnosti poslovanja organa pri porabi javnih sredstev prosto dostopne**

Prosilec je od Mestne občine Kranj zahteval dostop do analize ravnanja svetniških skupin z denarjem. Organ je ugotovil, da se zahteva nanaša na Poročilo o notranji reviziji izvrševanja proračuna Kabineta župana v Mestni občini Kranj na področju porabe sredstev za delo svetniških skupin. Dostop do zahtevanega dokumenta je zavrnil s sklicevanjem na notranje delovanje organa (11. točka prvega odstavka 6. člena ZDIJZ). Prosilec je odločitvi organa oporekal in v pritožbi poudaril, da je v interesu javnosti sleherna ugotovitev o porabi javnih sredstev. Informacijski pooblaščenec je v pritožbenem postopku ugotovil, da je bila revizija izvedena zato, da se preveri poslovanje organa na področju porabe sredstev za delo svetniških skupin organa, vse z namenom, da bi se sredstva za delo svetniških skupin porabljala pravilno in izključno za kritje stroškov, povezanih z izvrševanjem funkcije člana mestnega sveta. Glede izjeme notranjega delovanja morata biti izpolnjena dva pogoja hkrati, in sicer (1) podatek mora izhajati iz dokumenta, ki je bil sestavljen v zvezi z notranjim delovanjem oz. dejavnostjo organa, ter (2) razkritje takšnega podatka bi povzročilo motnje pri delovanju oz. dejavnosti organa. Kot je ugotovil Informacijski pooblaščenec, se je zahtevano poročilo nanašalo na pravilnost poslovanja proračunskega porabnika in že zato ne more predstavljati izjeme notranjega delovanja organa. Sredstva za delo svetniških skupin se namreč zagotavljajo v proračunu organa. Nedvomno torej ne gre za dokument, ki bi predstavljal informacije, namenjene za notranjo rabo organa in iz katerih bi izhajal postopek oz. način dela organa ali njegova notranja politika oz. občutljiva notranja navodila in načrti. Vsebina poročila se je obenem nanašala tudi na preverjanje skladnosti poslovanja organa z veljavnimi javnofinančnimi in organizacijskimi predpisi in tudi zato ne more predstavljati izjeme notranjega delovanja organa. Predmet zahteve so bili torej podatki o dejstvih ter ugotovitvah in priporočilih službe notranje revizije v zvezi s temi dejstvi, kar pa nedvomno ne predstavlja »notranjega razmišljanja« organa.

Poleg tega se je zahtevano revizijsko poročilo nanašalo na ugotavljanje pravilnosti in smotrnosti poslovanja organa pri porabi javnih sredstev, pri čemer so bili navedeni tudi konkretni podatki o njihovi porabi. Tako je v obravnavanem primeru dostop do zahtevanega poročila dopusten tudi na podlagi 1. alineje tretjega odstavka 6. člena ZDIJZ. Informacijski pooblaščenec je organu naložil, da prosilcu posreduje zahtevani dokument, pri čemer mora prekriti elektronske naslove javnih uslužbencev, ker gre za varovane osebne podatke (3. točka prvega odstavka 6. člena ZDIJZ).

KLJUČNE BESEDE: osebni podatek, notranje delovanje organa, številka odločbe 090-14/2021

### **Podatki o tem, kateri izdelki so bili dobavljeni, predstavljajo informacijo o porabi javnih sredstev**

Prosilec je od Zavoda za pokojninsko in invalidsko zavarovanje Slovenije zahteval dostop do določene dokumentacije v zvezi s postopkom oddaje javnega naročila »Dobava potrošnega materiala za tiskalnike«. Organ je zahtevo prosilca delno zavrnil. Pri zavrnitvi dostopa do izjave uradnega distributerja blagovne znamke Lexmark, serijskih številok dobavljenega potrošnega materiala, EAN kod in osebnih podatkov kontaktnih oseb v zahtevanih dobavninah in fakturah se je skliceval na varstvo poslovne skrivnosti (2. točka prvega odstavka 6. člena ZDIJZ) in varstvo osebnih podatkov (3. točka prvega odstavka 6. člena ZDIJZ). V pritožbi je prosilec izrazil prepričanje, da podatki, do katerih mu je bil dostop onemogočen, nikakor ne morejo predstavljati poslovne skrivnosti, saj gre za dokumente, vezane na postopek javnega naročanja. Stranski udeleženec, ki je prigljal udeležbo v postopku, je menil, da podatki, ki so bili zahtevani v konkretnem primeru (serijska številke oz. EAN koda ter izjava uradnega distributerja znamke Lexmark), ne predstavljajo javnih podatkov iz drugega odstavka 35. člena Zakona o javnem naročanju. Pri vseh pa je izkazoval poslovno skrivnost. Informacijski pooblaščenec je v pritožbenem postopku ugotovil, da informacij, tudi če posamezni podatki izpolnjujejo pogoje za obstoj poslovne skrivnosti, ne moremo določiti za poslovno skrivnost, če gre za informacije, ki so po zakonu javne, ali za informacije o kršitvi zakona ali dobrih poslovnih običajev. Gre za t. i. absolutno javne podatke, tj. podatke, na katerih razkritje volja »prizadetega« poslovne subjekta nima vpliva. Skladno z drugim odstavkom 35. člena ZJN-3 so vselej javni specifikacija ponujenega blaga, storitve ali gradnje in količina iz te specifikacije, cena na enoto, vrednost posamezne postavke in skupna vrednost iz ponudbe ter vsi tisti podatki, ki so vplivali na razvrstitev ponudbe v okviru drugih meril. Poleg tega je šlo v obravnavanem primeru za podatke izbranega ponudnika, ki je sklenil pogodbo z javnim zavodom, zato je bilo treba upoštevati tudi določbo 1. alineje tretjega odstavka 6. člena ZDIJZ, po kateri se ne glede na izjeme iz prvega odstavka 6. člena ZDIJZ dostop do zahtevane informacije dovoli, če gre za podatke o porabi javnih sredstev. Tudi Upravno sodišče je že večkrat potrdilo odločitev Informacijskega pooblaščenca, da so dokumenti iz ponudbe izbranega ponudnika, ki izkazujejo izpolnjevanje zahtevanih pogojev javnega naročila, prosto dostopne informacije javnega značaja na podlagi 1. alineje tretjega odstavka 6. člena ZDIJZ (npr. sodbe št. I U 1613/2009, št. I U 1911/2012, št. I U 1647/2017, št. II U 374/2018). Informacijski pooblaščenec je ugotovil, da Izjava uradnega distributerja blagovne znamke Lexmark odraža izpolnjevanje pogojev, določenih v razpisni dokumentaciji, zato je prosto dostopna. Kot prosto dostopne je določil tudi podatke o serijskih številkah in EAN kodah dobavljenega blaga, saj je šlo za podatke, ki identificirajo konkretne artikle, ki so bili v obravnavanem primeru dobavljeni organu kot naročniku, ki je javni zavod in kot tak porabnik javnih sredstev.

KLJUČNE BESEDE: poslovna skrivnost, javna naročila, številka odločbe 090-318/2020

### **Postopka za dostop do informacij javnega značaja ni mogoče voditi brez zahteve prosilca**

Prosilec je od Ministrstva za okolje in prostor zahteval dostop do kopije celotnega spisa v njegovi zadevi. Organ je, na podlagi določb ZDIJZ, izdal odločbo, s katero je zahtevo prosilca delno zavrnil in prosilca seznanil z zahtevano dokumentacijo, tako da je iz nje izločil varovane osebne podatke. Prosilec se je na izdano odločbo pritožil, češ da organ ni uporabil pravega temelja za izdajo odločbe. Informacijski pooblaščenec je v pritožbenem postopku ugotovil, da prosilec svoje zahteve ni vložil kot zahtevo za dostop do informacij javnega značaja, ampak kot zahtevo za dostop do dokumentov, ki se nanašajo na njega samega v njegovi zadevi v zvezi z zatrjevanim sporom glede določitve meje na konkretni parcelni številki. Po 128. členu Zakona o splošnem upravnem postopku je organ v zadevah, v katerih je po zakonu ali po naravi stvari za začetek upravnega postopka in za sam postopek potrebna zahteva stranke, pristojen začeti in voditi postopek samo, če je taka zahteva podana. ZDIJZ v drugem odstavku 5. člena določa, da ima vsak prosilec na svojo zahtevo pravico od organa pridobiti informacijo javnega značaja. Če organ izda odločbo brez zahteve stranke, je takšno odločbo treba na podlagi 249. člena Zakona o splošnem upravnem postopku izreči za

nično. Prošilec je v pritožbi navedel, da je organ odločil po zgrešenem temelju odločbe in napačno sklenil, da je Informacijski pooblaščenec pritožbeni organ v zvezi z njegovo zahtevo. Tudi iz sodne prakse (npr. sodba IU 388/2014) izhaja, da organ prvotnega zahtevka stranke ne more samoiniciativno spremeniti v zahtevek za dostop do informacij javnega značaja po ZDIJZ, ker se v takem primeru bistveno spremenijo pravila in postopki odločanja pred pristojnimi organi, lahko pa stranko, skladno z načelom varstva pravic strank iz 7. člena Zakona o splošnem upravnem postopku, opozori na različne podlage za uveljavitev določene pravice. Informacijski pooblaščenec je zaključil, da je bila izpodbijana odločba nična.

KLJUČNE BESEDE: kršitev postopka, ničnost, številka odločbe 090-63/2021

### **Zaradi širše javne razprave je javni interes za razkritje določenih delov dokumenta prevladal nad interesi varstva tajnih podatkov**

Prosilka je od Policije zahtevala kopijo poročila o opravljeni reviziji kriminalističnih preiskav na NPU. Organ je zahtevo zavrnil s sklicevanjem na varstvo tajnih podatkov (1. točka prvega odstavka 6. člena ZDIJZ), ker je dokument imel oznako INTERNO. Poleg tega so se podatki nanašali tudi na notranje delovanje organa (11. točka prvega odstavka 6. člena ZDIJZ) in razkritje dokumenta bi pri organu povzročilo motnje pri delovanju ali izvajanju nalog. Prosilka se je na odločitev pritožila in zahtevala umik stopnje tajnosti z dokumenta. V pritožbenem postopku je Informacijski pooblaščenec z namenom ugotovitve dejanskega stanja pri organu opravil ogled in camera. Na ogledu je organ pojasnil, da je poročilo, ki je predmet presoje v tem postopku, sestavljeno iz poročil oz. ugotovitev več nadzornikov, ki so po področjih dela izvajali strokovni nadzor, na podlagi katerega je vodja nadzora izdelal skupno poročilo. Tudi ocena škodljivih posledic je sestavni del skupnega poročila in se navezuje nanj, vključno z obema obrazcema. Pri izjemi tajnih podatkov je pomembno, da ZDIJZ kot izjemo dovoljuje samo tiste informacije, ki so ustrezno opredeljene kot tajne, na podlagi zakona, ki ureja tajne podatke, tj. Zakon o tajnih podatkih (ZTP). Informacijski pooblaščenec je ugotovil, da so bili glede zahtevanega poročila izpolnjeni tako materialni kot formalni pogoji za tajne podatke in je bila posledično tudi podana izjema varstva tajnih podatkov. To pa ni v celoti obveljalo za prilogi k poročilu, in sicer v delih, ki nimata vidne oznake stopnje tajnosti. Glede izjeme notranjega delovanja, po kateri organ prosilcu zavrne dostop do zahtevane informacije, če se zahteva nanaša na podatek iz dokumenta, ki je bil sestavljen v zvezi z notranjim delovanjem oz. dejavnostjo organov in katerega razkritje bi povzročilo motnje pri delovanju oz. dejavnosti organa, je Informacijski pooblaščenec ugotovil, da organ ni izpolnil svojega dokaznega bremena glede obstoja zatrjevane izjeme, saj je ni z ničemer izkazal. Posledično ta izjema ni bila podana. Ob izvedbi testa prevladujočega interesa javnosti je Informacijski pooblaščenec ugotovil, da je njegovo izvajanje v konkretnem primeru dovoljeno, saj je bilo poročilo označeno z najnižjo stopnjo tajnosti (Interno). Informacijski pooblaščenec je zaključil, da je treba do zahtevanega poročila o strokovnem nadzoru dovoliti delni dostop, saj javni interes za razkritje določenih delov dokumenta prevlada nad interesom varstva tajnih podatkov. K temu so ga vodile ugotovitve, da je bila tema deležna širše javne razprave o (ne)zakonitosti izvajanja policijskih pooblastil, o političnih pritiskih na delo policije, o očitkih, da je pri delovanju policije prišlo do nezakonitega oz. nestrokovnega ravnanja ter da je v konkretnem primeru prosilka novinarka, ki informacije zahteva v imenu medija. Da okoliščina, kdo podaja zahtevo za dostop do informacije javnega značaja, katero konkretno informacijo zasleduje in za kateri namen, pretehta v smeri širšega javnega interesa za dostop do zahtevanih dokumentov, izhaja tudi iz sodbe št. IU 1688/2016. Informacijski pooblaščenec je tako opravil presojo sorazmernosti in omogočil dostop le do tistih delov dokumenta, ki povzemajo zakonske podlage za delovanje policije in kažejo na splošno vsebino in potek izvedbe nadzora ter splošne ugotovitve.

KLJUČNE BESEDE: zahteva za umik stopnje tajnosti, test interesa javnosti, tajni podatki, številka odločbe 090-39/2021

### **Plače v javnem sektorju so javne v tem smislu, da se lahko za vsakega javnega uslužbenca poimensko ve, kakšno plačo ima**

Prošilec je od Univerzitetnega kliničnega centra Ljubljana zahteval poimenski seznam plač vseh zaposlenih na UKC Ljubljana. Organ je prosilcu posredoval podatke o redni plači, nadomestilu, dodatkih, delovni uspešnosti, nadurah in dežurstvu za december 2020, zavrnil pa je dostop do imen in priimkov javnih uslužbencev, na katere se ti podatki nanašajo. Navedel je, da Zakon o sistemu plač v javnem sektorju v 38. členu določa javnost plač in v prvem odstavku našteva, da so javnosti dostopni podatki o delovnem mestu, nazivu ali funkciji, o osnovnih plačah, o dodatkih ter delu plače za delovno uspešnost, razen dodatka za delovno

do. Ne določa pa, da je dostopen podatek o imenu in priimku javnega uslužbenca, zato je ta podatek varovan. Njegovo posredovanje bi pomenilo neutemeljen poseg v zasebnost zaposlenih. Prošilec se je zoper odločitev organa pritožil in zapisal, da je Informacijski pooblaščenec zavzel stališče, da je podatek o imenu in priimku javnega uslužbenca prosto dostopna informacija javnega značaja. Informacijski pooblaščenec je v pritožbenem postopku ugotovil, da je stališče organa, da bi posredovanje podatka o imenu in priimku javnega uslužbenca, skupaj s podatki o izplačani bruto plači, pomenilo kršitev varstva osebnih podatkov, zmotno. Pri presoji tega vprašanja je organ napačno uporabil materialno pravo ter spregledal obstoječo prakso Informacijskega pooblaščenca in sodno prakso na tem področju. Pri sklicevanju na 38. člen Zakona o sistemu plač v javnem sektorju je organ spregledal šesti odstavek navedenega člena, ki izrecno pravi, da so ne glede na določbo prvega odstavka tega člena javnosti po postopku, ki ga ureja ZDIJZ, dostopni individualni podatki o znesku celotne bruto plače vsakega javnega uslužbenca in vsakega funkcionarja brez zmanjšanja za morebitne odbitke iz naslova izvršbe, kreditov ali drugih osebnih obveznosti. Stališče, da je podatek o izplačani bruto plači skupaj z imenom in priimkom javnega uslužbenca javen, je že pred časom zavzelo tudi Upravno sodišče RS. V sodbi št. I U 1003/2010 je menilo, »da je bil namen zakonodajalca, da so plače v javnem sektorju javne v tem smislu, da se lahko za vsakega javnega uslužbenca poimensko ve, kakšno plačo ima, razen določenih omejitev, ki jih 38. člen ZSPJS določa«. Stališče je potrdilo tudi Vrhovno sodišče RS v sklepu št. X Ips 187/2011, pred tem tudi v odločbi št. X Ips 252/2009. To jasno izhaja tudi iz sodb I U 805/2012, I U 944/2015 in I U 1816/2016. Ker imajo pri organu zaposleni status javnih uslužbencev in se njihove plače zagotavljajo iz javnih sredstev, je šlo v obravnavanem primeru tudi za podatke v zvezi z delovnim razmerjem javnih uslužbencev in za podatke o porabi javnih sredstev, ki so prosto dostopni na podlagi 1. alineje tretjega odstavka 6. člena ZDIJZ. Stališče, da posamezni javni funkcionar oz. javni uslužbenec ni upravičen pričakovati zasebnosti glede svojega imena, naziva, položaja, plače, službenega naslova in vseh drugih podatkov, ki so povezani z opravljanjem javne funkcije ali delovnega razmerja javnega uslužbenca, izhaja iz obširne prakse Informacijskega pooblaščenca, npr. iz odločb Informacijskega pooblaščenca št. 090-109/2010/4, št. 090-204/2010/10, št. 090-89/2015, št. 090-211/2016, št. 090-55/2019/5 in št. 090-78/2019/9. Informacijski pooblaščenec je že večkrat zavzel stališče, da imajo osebe, ki so zaposlene v javnem sektorju, zaradi načela odprtosti javne uprave ter s tem povezanega načela transparentnosti bistveno zmanjšano pričakovanje zasebnosti v primerjavi z drugimi posamezniki, ko gre za podatke, ki so v zvezi z delovnim razmerjem javnega uslužbenca. Pri zahtevanih podatkih je torej šlo za podatke o porabi javnih sredstev in za podatke, povezane z opravljanjem javne funkcije ali delovnega razmerja javnega uslužbenca, zato je Informacijski pooblaščenec pritožbi prosilca ugodil.

KLJUČNE BESEDE: osebni podatek, javni uslužbenci in funkcionarji, številka odločbe 090-119/2021

### **Organ mora pred izdajo sklepa o stroških prosilca opozoriti na plačilo stroškov**

Informacijski pooblaščenec je v pritožbenem postopku št. 090-270/2020 odločil, da je javno podjetje CEROD, center za ravnanje z odpadki, d. o. o., prosilcem dolžno posredovati fotokopije vseh računov, ki jih je organ izdal za storitve izven okvirov izvajanja gospodarske javne službe, in sicer za leta 2017, 2018, 2019 ter 2020, na način, da v vseh dokumentih prekrije podatke o kupcu in stiku organa. Organ je prosilcem posredoval zahtevane dokumente ter jim s sklepom naložil plačilo materialnih stroškov za posredovanje fotokopij zahtevanih dokumentov. Prosilci so se na sklep o stroških pritožili in navedli, da je odmerjanje stroškov postopka pravno nevzdržno. Tiskanje skoraj 2500 kopij računov in pošiljanje le-teh po klasični pošti pooblaščenca strank je bilo popolnoma nepotrebno, saj je imel organ vse listine shranjene v elektronski obliki in bi jih lahko brezplačno posredoval elektronsko. Nesporno je, da lahko organ v skladu z drugim odstavkom 34. člena ZDIJZ zaračuna prosilcu stroške posredovanja zahtevanih informacij, torej za posredovanje prepisa, fotokopije ali elektronskega zapisa, vendar le v primeru, če pri tem izpolni oz. zadosti vsem zakonskim določbam, ki urejajo zaračunljivost stroškov posredovanja informacij. V pritožbenem postopku je bilo treba najprej ugotoviti, ali je organ zadostil zahtevam glede objave stroškovnika ter ali je organ prosilce opozoril na plačilo stroškov, kot to določa 36. člen ZDIJZ. Šteje se, da je enotni stroškovnik sprejet z Uredbo o posredovanju in ponovni uporabi informacij javnega značaja (17. člen), ki je javno objavljena in dostopna, tako da ima prosilec vedno možnost preveriti višino in način zaračunavanja stroškov. Glede opozorila na plačilo stroškov je Informacijski pooblaščenec ugotovil, da organ pred izdajo sklepa o stroških prosilcev ni opozoril na plačilo stroškov. Prosilci tako niso imeli možnosti, da bi se še pred izdajo sklepa o stroških odločili, da bi informacije zahtevali v manjšem obsegu, v drugi obliki (npr. elektronsko posredovanje) ali da jih sploh ne bi zahtevali. Tudi Informacijski pooblaščenec pred izdajo odločbe v zadevi št. 090-270/2020, s katero je organu naložil posredovanje fotokopij zahtevanih dokumentov, ni bil predhodno seznanjen z nastalimi materialnimi stroški. Informacijski pooblaščenec je ugotovil, da organ v obravnavanem primeru

ni zadostil zakonski predpostavki iz tretjega odstavka 36. člena ZDIJZ, saj prosilcev ni predhodno opozoril na plačilo stroškov, prav tako navedeno ne izhaja iz pravnomočne odločbe Informacijskega pooblaščenca. Zato je pritožbi prosilcev ugodil in izpodbijani sklep o stroških odpravil.

KLJUČNE BESEDE: stroški, številka odločbe 090-100/2021

### **Zaključene ankete ne morejo biti dokument v izdelavi, čeprav bodo njihovi podatki vključeni v dokument, ki šele nastaja**

Prosilec je od Občine Vodice zahteval dokumentacijo v zvezi z javnomnenjsko anketo o razvoju Vodice, ki jo je organ izvedel leto poprej. Organ je zahtevo zavrnil s sklicevanjem na izjemo po 9. točki prvega odstavka 6. člena ZDIJZ, tj. dokument v izdelavi. Kot je pojasnil v odločbi, bo zahtevana dokumentacija del dokumenta, ki je še v izdelavi. V pritožbi je prosilec zatrdil, da je anketa že končana in da dokumentacija v zvezi z njo predstavlja ločen in samostojen dokument. Informacijski pooblaščenec je v pritožbenem postopku ugotovil, da je organ v letu 2020 pristopil k izdelavi dokumenta z naslovom Razvojni program Občine Vodice za obdobje 2021–2031. V okviru priprave omenjenega dokumenta so (bile) predvidene tudi določene aktivnosti, kot je izvedba anket, s katerimi so (bodo) pridobili dodatne vhodne podatke za pripravo razvojnega programa. Glede izjeme dokumenta v izdelavi morajo biti izpolnjeni trije pogoji hkrati, in sicer (1) dokument mora biti še v postopku izdelave pri organu, (2) dokument mora biti še predmet posvetovanja v organu in (3) razkritje dokumenta bi povzročilo napačno razumevanje njegove vsebine (specifični škodni test), pri čemer je dokazno breme glede obstoja škode zaradi napačnega razumevanja vsebine dokumenta na organu. V obravnavani zadevi pogoji za obstoj navedene izjeme niso bili podani, ker dejstva, da bodo zahtevani podatki (tj. dokumentacija o javnomnenjski anketi) del dokumenta, ki je še v izdelavi (tj. Razvojni program Občine Vodice za obdobje 2021–2031), ni mogoče upoštevati kot argument, da gre za dokument v postopku izdelave. Izvedba javnomnenjske ankete je nesporno zaključena (anketa je bila aktivna med 12. in 20. novembrom 2020). Informacijski pooblaščenec je poudaril, da je mogoče o dokumentu v postopku izdelave govoriti, če gre za dokument, ki kot tak še ni v celoti napisan, izdelan kot zaključena celota in podpisan s strani uradne osebe, ki dokument pripravlja. Namen te izjeme je namreč zagotoviti nemotene postopke odločanja ter varstvo zaupnosti posvetovanja znotraj organov in med organi v času priprave zadeve. Če gre za dokument, ki je sam po sebi zaključena celota, s podpisom izdelovalca ali odgovorne osebe oz. na drugačen način zaključen dokument, ni več mogoče govoriti o tem, da gre za dokument v postopku izdelave. Pri tem je povsem irelevantno, ali je takšen dokument v nadaljevanju vključen v kak drug dokument oz. ali so podatki, ki jih vsebuje, uporabljeni kot vhodni podatki pri izdelavi drugih dokumentov. Poleg tega zahtevani podatki niso bili predmet posvetovanja v organu, saj dokumentacija v zvezi z javnomnenjsko anketo vsebuje podatke o že izvedeni anketi, njen vprašalnik in analizo odgovorov, ki jih je opravil zunanji izvajalec. Kakršno koli nadaljnje posvetovanje v organu, ki se bo zgodilo zaradi rezultatov že dokončnega dokumenta, ne more voditi v spremembe tega dokumenta, ampak je lahko zgolj povod za nastanek spoznanj, zaključkov oz. sklepov in ciljev, ki bodo vključeni in se bodo odražali v (povsem) novem dokumentu. Poleg tega organ v zvezi z zahtevanimi podatki ni opravil specifičnega škodnega testa in ni pojasnil, kako bi razkritje zahtevanih podatkov povzročilo napačno razumevanje njegove vsebine. Informacijski pooblaščenec je pritožbi prosilca ugodil v celoti.

KLJUČNE BESEDE: dokument v izdelavi, številka odločbe 090-114/2021

### **Stopnja razkrivanja osebnih podatkov, ki jo mora določena oseba trpeti, ko gre za izražanje o njej, je večja, če gre za javno osebo**

Novinarka je po Zakonu o medijih od Zdravniške zbornice Slovenije zahtevala informacijo, ali je že znana odločitev tožilca Zdravniške zbornice v zvezi s postopkom zoper tam navedenega zdravnika. Organ je odgovor na njeno vprašanje zavrnil s sklicevanjem na izjemo varstva osebnih podatkov (3. točka prvega odstavka 6. člena ZDIJZ). Zoper zavrnilni odgovor je prosilka vložila pritožbo, za katero je Informacijski pooblaščenec najprej ugotovil, da je dovoljena, saj odgovor na novinarkino vprašanje izhaja iz dokumenta, ki mu ga je organ poslal ob odstopu pritožbe. Informacijski pooblaščenec je v pritožbenem postopku ugotovil, da je podatek o tem, ali je konkretni posameznik v postopku pred tožilcem zbornice, osebni podatek, vendar pravno podlago za njegovo razkritje in za razkritje celotnega dokumenta (tj. odločitve tožilca zbornice) predstavlja javni interes, ki v obravnavani zadevi pretehta nad pravico posameznika do zasebnosti. Odločitev Informacijskega pooblaščenca je temeljila na presoji, da je šlo v obravnavi zadevi za relativno javno osebo, ki se je s svojim ravnanjem, ki je bilo predmet presoje tožilca, sama izpostavila javnosti. Ob tem je bilo

bistveno, da je posameznik izjave podal kot zdravnik, torej kot strokovnjak, ki opravlja izjemno odgovorno delo, ima visoka etična merila, njegovo delo pa ima tudi velik družbeni pomen. Izjave je podal v zvezi z epidemijo covid-19, torej s področjem javnega zdravja, ki se je dotikalo večjega števila državljanov in je predstavljalo aktualno temo v času epidemije, interes javnosti za teže besed strokovnjakov na področju zdravja pa je bil nedvomno velik. Informacijski pooblaščenec je, skladno s sodno prakso, pri svoji odločitvi upošteval tudi dejstvo, da je prosilka novinarka. Skladno z namenom pravice dostopa do informacij javnega značaja Informacijski pooblaščenec ni mogel mino dejstva, da je v času epidemije tema javnega zdravja ena od vodilnih tem javnih razprav. Zato je v javnem interesu, da javnost izve, kako zbornica obravnava primere svojih članov, ki so se v medijih javno izpostavili s svojimi stališči do reševanja aktualnega problema epidemije in z njo povezanih vprašanj. Po presoji Informacijskega pooblaščenca je nedvomno v javnem interesu, da se javnost seznaní, ali konkretne izjave in objave, ki jih poda zdravnik v medijih in na družabnih omrežjih in z njimi tangira splošno javnost, Odbor za etično-pravna vprašanja zbornice pa jih je prepoznal kot kršitve Zdravniškega kodeksa, pomenijo tudi kršitve pri opravljanju zdravniškega poklica. Upoštevajoč vse argumente je Informacijski pooblaščenec zaključil, da javni interes za razkritje zahtevanega dokumenta prevlada nad pravico posameznika do varstva zasebnosti, torej da je škoda, ki bi nastala z razkritjem osebnih podatkov, manjša kot javni interes po seznanitvi s temi podatki. Konkretni posameznik, na katerega se nanaša zahtevani dokument, tudi ni priglasil stranske udeležbe v postopku in ni izrecno nasprotoval posredovanju teh podatkov javnosti. Informacijski pooblaščenec je pritožbi prosilke ugodil v celoti.

KLJUČNE BESEDE: osebni podatek, test interesa javnosti, mediji, številka odločbe 090-178/2021

### **Dostopa do informacij javnega značaja ni moč odtegniti s sklicevanjem na podzakonski akt**

Prosilec je od Vlade Republike Slovenije zahteval dostop do mnenja Službe vlade za zakonodajo o Predlogu zakona o spremembah in dopolnitvah Zakona o izvrševanju proračunov Republike Slovenije za leti 2021 in 2022 ter o Predlogu Zakona o debirokratizaciji. Organ je dostop zavrnil s sklicevanjem na izjemo notranjega delovanja (11. točka prvega odstavka 6. člena ZDIJZ). Kot je pojasnil, so ta mnenja del delovnega procesa vlade, del njenega notranjega delovanja, in se posredujejo z namenom razprav, strokovnih usklajevanj in predhodnih posvetovanj znotraj medresorskega usklajevanja. Kot takšna so podlaga za to, da se vladna gradiva spreminjajo in dopolnjujejo, zato mnenja službe ne odražajo nujno gradiva, ki je sprejeto na vladi. Za podatke, ki so sestavljeni v zvezi z notranjim delovanjem, kaže šteti vso notranjo korespondenco med funkcionarji in uradniki vlade, ki je namenjena pripravi odločitve vlade. Če bi vsi dokumenti postali javni, potem bi resno ogrozili kritično in inovativno usklajevanje vladnih gradiv ter razpravo na sejah vlade. Prosilec je odločitvi oporekal in v pritožbi navedel, da gre pri zahtevanih dokumentih za strokovno pravno mnenje in ne za interno, politično komunikacijo, organ pa, da ni obrazložil, kakšne motnje pri delovanju naj bi zaradi razkritja mnenj nastale. Informacijski pooblaščenec je v pritožbenem postopku ugotovil, da je prosilec zahteval dostop do dveh dokumentov, ki sodita v proces sprejemanja predpisov. Po Poslovniku Vlade RS (10. člen) morajo biti namreč predlogi splošnih aktov in aktov poslovanja vlade vedno predhodno usklajeni s Službo vlade za zakonodajo. Glede izjeme notranjega delovanja organa morata biti izpolnjena dva pogoja hkrati, in sicer (1) podatek mora izhajati iz dokumenta, ki je bil sestavljen v zvezi z notranjim delovanjem oz. dejavnostjo organa, ter (2) razkritje takšnega podatka bi povzročilo motnje pri delovanju oz. dejavnosti organa. Informacijski pooblaščenec je sledil odločitvi organa, da je izpolnjen prvi pogoj zatrjevanje izjeme, saj sta zahtevani mnenji nastali v fazi medresorskega usklajevanja, ki je namenjena strokovnemu usklajevanju in predhodnemu posvetovanju, ko se vsebina predpisa dejansko šele pripravlja. Vendar pa organ ni uspel izkazati nastanka motenj zaradi razkritja zahtevanih mnenj, teh pa ni ugotovil niti Informacijski pooblaščenec. Po oceni Informacijskega pooblaščenca se s prostim dostopom do zahtevanih mnenj ne bi v ničemer poseglo v možnost kritičnega in inovativnega razmišljanja vlade oz. organa, saj iz samih mnenj ne izhaja niti vladna politika niti razmišljanje vlade ali interno, politično komuniciranje, ampak gre za strokovni pravni mnenji, ki predstavljata uradno strokovno stališče Službe Vlade RS za zakonodajo. Informacijski pooblaščenec je po uradni dolžnosti v okviru preizkusa pravilne uporabe materialnega prava ugotovil, da v obravnavani zadevi ni bila izkazana niti izjema dokumenta v izdelavi (9. točka prvega odstavka 6. člena ZDIJZ), ki jo je organ zatrjeval šele tekom pritožbenega postopka. Za obstoj navedene izjeme morajo biti izpolnjeni trije pogoji hkrati, in sicer (1) dokument mora biti še v postopku izdelave pri organu, (2) dokument mora biti še predmet posvetovanja v organu in (3) razkritje dokumenta bi povzročilo napačno razumevanje njegove vsebine. Informacijski pooblaščenec je ugotovil, da sta bili zahtevani mnenji Službe vlade RS za zakonodajo zaključeni celoti in podpisani s strani odgovorne osebe te službe ter odposlani izven službe, zaradi česar navedene izjeme ni bilo mogoče uporabiti. Sklicevanje organa na dopolnjen Poslovník Vlade RS z dne 15. 7. 2021, ki predpisuje, da pisna mnenja drugih ministrstev in vladnih služb



niso samostojna »informacija«, temveč pomenijo le prilogo k dokumentu – vladnemu gradivu, pa je bilo tudi neutemeljeno. Ne glede na to, da Poslovnik Vlade RS ureja sodelovanje javnosti pri pripravi predpisov, gre za določbe podzakonskega akta, ki ne morejo ožiti pogojev za dostop do informacij javnega značaja in pravice prosilcev, ki jih določata zakon in ustava. Informacijski pooblaščenec je pritožbi prosilca ugodil v celoti.

KLJUČNE BESEDE: dokument v izdelavi, notranje delovanje organa, številka odločbe 090-225/2021

**Namen avtorskoprnega varstva avtorja je v varstvu avtorja in njegove volje in ne v predpostavki, da avtor a priori prepoveduje vsakršno uporabo avtorskega dela**

Prošilec je na RTV Slovenija naslovil zahtevo za dostop do informacije javnega značaja, v kateri je zahteval posredovanje posnetka oddaje Nedeljski gost, ki je bila na sporedu 11. 7. 2021 na Valu 202, ter drugih dokumentov v zvezi z omenjeno oddajo. Organ je odločil, da se prošilec lahko seznaniti s posnetkom oddaje le z vpogledom, saj ima intervju Nedeljski gost z dne 11. 7. 2021 vse značilnosti avtorskega dela novinarja in intervjuvanca. Po 25. členu ZDIJZ pa se prosilcu omogoči seznanitev z informacijo tako, da mu jo organ da zgolj na vpogled, če je zahtevana informacija zavarovana skladno z zakonom, ki ureja avtorsko in sorodne pravice ter je imetnik pravic tretja oseba. Glede preostalih dokumentov je ugotovil, da z njimi ne razpolaga. Prošilec se z odločitvijo ni strinjal, ker so na spletni strani organa objavljeni številni drugi intervjuji, ki po tej logiki prav tako ne bi smeli biti objavljeni, saj prav za vse najbrž organ nima sklenjenih pogodb, s katerimi bi avtorji na organ prenesli svoje avtorske pravice. Informacijski pooblaščenec je v pritožbenem postopku ugotovil, da intervjuvanec ni soavtor intervjuja, zato mu ne gre avtorskopravno varstvo. Podrejeno je Informacijski pooblaščenec odločil, da bi moral organ, četudi je intervjuvanec soavtor, glede na ustavno skladno razlago drugega odstavka 25. člena ZDIJZ v okoliščinah obravnavanega primera izpolniti navedbeno in dokazno breme, da je avtor podal izrecno prepoved dostopa do posnetka. Avtor intervjuvanec je namreč sprejel povabilo za nastop na najbolj poslušani radijski postaji v državi, ki ima že dalj časa javno dostopen arhiv oddaj, pri čemer kot gost ni sklenil nobene avtorske pogodbe niti drugega podobnega dogovora, ki bi omejeval radijsko postajo pri njenem običajnem ravnanju z oddajami te vrste, v svojih odgovorih pa je izrecno izrazil stališče, da je njegov namen doseči čim več poslušalcev. Ker organ ni uspel izkazati izrecne prepovedi dostopa do posnetka, je Informacijski pooblaščenec odločil, da se pritožbi ugodi in da mora organ prosilcu posredovati posnetek. Glede drugih dokumentov v zvezi z oddajo je Informacijski pooblaščenec ugotovil, da organ razpolaga z določenimi dokumenti, ki so javno objavljeni in dostopni na njegovi spletni strani, zato je prosilca napotil nanje.

KLJUČNE BESEDE: ali dokument obstaja, avtorsko delo, številka odločbe 090-257/2021

**Prošilec lahko na podlagi določb ZDIJZ dostopa do posameznih dokumentov v postopku celovite presoje vplivov na okolje, še preden se navedeni upravni postopek zaključi**

Prošilec je od Mestne občine Koper zahteval dokumente, povezane s postopkom celovite presoje vplivov na okolje za namen izdelave občinskih prostorskih načrtov. Organ je kot dokumente zahteve prepoznal okoljsko poročilo, mnenja različnih državnih organov, ki so jih dali kot zakonsko obveznost na podlagi Zakona o varstvu okolja, ter dodatek za presojo sprejemljivosti vplivov izvedbe planov na varovana območja. Zahtevo je zavrnil s sklicevanjem na izjemo dokumenta v izdelavi (9. točka prvega odstavka 6. člena ZDIJZ). Za obstoj navedene izjeme morajo biti izpolnjeni trije pogoji hkrati, in sicer (1) dokument mora biti še v postopku izdelave pri organu, (2) dokument mora biti še predmet posvetovanja v organu in (3) razkritje dokumenta bi povzročilo napačno razumevanje njegove vsebine. Informacijski pooblaščenec je v pritožbenem postopku ugotovil, da pogoji za navedeno izjemo niso izpolnjeni, saj so vsi zahtevani dokumenti zaključene celote, podpisani in poslani izven organa, prav tako pa organ ni izkazal pogoja napačnega razumevanja njihove vsebine. Ob dejstvu, da celovita presoja vplivov na okolje predstavlja postopek in ne dokumenta, posameznih dokumentov, ki so že pripravljene in zaključene in se ne bodo več spreminjali, ne moremo šteti za dokumente v izdelavi, kljub temu da postopek sam še ni zaključen. Dokumenti, ki so še v postopku izdelave, so dokumenti, ki jih organ šele pripravlja in oblikuje, in ne verzije, ki so že pripravljene in oblikovane in posredovane v nadaljnje faze postopka. Postopek celovite presoje vplivov na okolje sestavlja več faz in dve izmed teh sta tudi faza priprave in izdelave okoljskega poročila. Ta faza je že zaključena, saj je bil predlog okoljskega poročila, ki ga je zahteval prošilec, posredovan MOP in dalje pristojnim organom in organizacijam, ki so podali mnenja o njegovi ustreznosti. Poleg tega je Informacijski pooblaščenec ugotovil še, da zahtevani dokumenti predstavljajo okoljske podatke, ki so absolutno javni (2. alineja tretjega odstavka 6. člena ZDIJZ). Zakon o varstvu okolja zelo široko opredeljuje, kaj je okoljski podatek (3. člen,

110. člen). Vse dokumente, ki so nastali v postopku celovite presoje vplivov na okolje pri pripravi občinskih prostorskih planov, je že po naravi stvari mogoče šteti med okoljske podatke (101. člen Zakona o varstvu okolja). Okoljski podatek je po določbah ZDIJZ absolutno javno dostopen podatek, glede katerega ne velja nobena izjema od prostega dostopa do informacij javnega značaja. Zato je Informacijski pooblaščenec organu naložil, da prosilcu posreduje zahtevane dokumente, pri tem pa prekrije varovane osebne podatke posameznikov, ki so navedeni na nekaterih od teh dokumentov, saj gre za zaposlene v zasebnih družbah, ki so pripravljali te dokumente po naročilu organa, niso pa zakoniti zastopniki teh družb.

KLJUČNE BESEDE: dokument v izdelavi, okoljski podatki, osebni podatek, številka odločbe 090-280/2021

### **Varstvo tajnosti vira ne preneha, ko se nadzorni postopek zaključi**

Prosilec je na Inšpektorat RS za okolje in prostor naslovil zahtevo za seznanitev z vsemi dokumenti iz inšpekcijskega postopka, glede katerega je prejel obvestilo, da se je postopek nadzora že zaključil. Organ je prosilcu posredoval določene dokumente, ostale pa zavrnil na podlagi izjeme varstva vira prijave (tretji odstavek 5. a člena ZDIJZ). Prosilec je zoper odločbo organa vložil pritožbo, v kateri je navedel, da je zahteval vse dokumente, vključno s spremnimi dopisi, ki so bili podlaga za obvestilo prijavitelju. Informacijski pooblaščenec je v pritožbenem postopku ugotovil, da se je zahteva prosilca razlikovala od tega, kar je prosilec v pritožbi navajal, da je zahteval. Informacijski pooblaščenec je pojasnil, da sta prvostopenjski in pritožbeni organ vezana na zahtevo prosilca in ne smeta odločati prek meja zahtevka. Takšno stališče je zavzelo tudi Upravno sodišče RS v sodbi št. I U 817/2015. Predmet pritožbenega postopka so bili tako le dokumenti, zahtevani s prvotno vlogo. Glede te zahteve je Informacijski pooblaščenec ugotovil, da prosilec z 21 dokumenti iz postopka že razpolaga, saj je šlo za njegove lastne vloge. Ker prosilec v postopku po ZDIJZ nima pravovarstvenega interesa, da bi od organa zahteval dokumente, s katerimi že razpolaga, je Informacijski pooblaščenec pritožbo prosilca v tem delu zavrnil kot neutemeljeno. Glede dveh dokumentov je Informacijski pooblaščenec ugotovil, da je podana izjema varstva vira prijave. Ta ne preneha s trenutkom, ko se postopek nadzora zaključi, zato je Informacijski pooblaščenec pritožbo prosilca tudi v tem delu zavrnil kot neutemeljeno.

KLJUČNE BESEDE: tajnost vira, številka odločbe 090-369/2021

## **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**

V zadnjem tednu septembra po vsem svetu potekajo aktivnosti, ki zaznamujejo svetovni dan pravice vedeti (28. september). Ta dan so leta 2002 razglasile nevladne organizacije, povezane v mrežo Freedom of Information Advokates Network (FOIANet), leta 2015 ga je za svetovni dan dostopa do informacij izglasovala Generalna konferenca UNESCO, temu pa je sledila 74. Generalna skupščina Združenih narodov, ki je ta dan leta 2019 razglasila za mednarodni dan univerzalne pravice dostopa do informacij.

V okviru dogodkov ob svetovnem dnevu pravice vedeti je Informacijski pooblaščenec 28. 9. 2021 organiziral **okroglo mizo** z naslovom **Dostop do informacij v času epidemije – vloga medijev in civilne družbe**; beseda je tekla o vlogi medijev in civilne družbe pri dostopu do informacij. Dogodek je potekal prek video povezave.

Dogodek je otvorila informacijska pooblaščenka Mojca Prelesnik z uvodnim nagovorom in predstavitvijo dela Informacijskega pooblaščenca na tem področju. Opozorila je na pomembno vlogo, ki jo imajo mediji pri dostopu do informacij. Tako Evropsko sodišče za človekove pravice kot Ustavno sodišče RS sta namreč medijem priznala posebno vlogo »javnih psov čuvajev«. Za demokratičen dialog je bistven hiter in celovit dostop javnosti do informacij, pri tem pa mediji igrajo ključno vlogo. To še zlasti velja za poročanje o temah, pri katerih je podan javni interes. Zaradi posebne družbene vloge medijev bi moralo biti njihovo delovanje v

času epidemije okrepljeno, pogoji za njihovo delovanje pa lažji. Žal pa statistika pritožbenih postopkov pred Informacijskim pooblaščenecem kaže ravno nasproten trend – od začetka epidemije leta 2020 do danes se je povečalo tako število pritožb v zvezi z dostopom do informacij javnega značaja kot število pritožb po Zakonu o medijih.

Udeleženci okrogle mize so se strinjali, da se vloga medijev in civilne družbe pri dostopu do informacij s časom spreminja, na kar med drugim vplivajo razvoj sodobnih tehnologij, hiter tempo življenja in tudi delovanje v posebnih družbenih razmerah, kot je npr. epidemija. Predstavili so svoje izkušnje pri dostopu do informacij v času epidemije in opozorili na številne izzive, s katerimi se v teh razmerah srečujejo tako mediji kot nevladne organizacije. Zaključili so, da veljavna zakonodaja že zdaj omogoča širok dostop do informacij, težave pa nastajajo v praksi. Ker dostop do informacij povečuje razumevanje aktualnih vsebin v javni razpravi in prispeva k odgovornejšemu delu javnega sektorja, so zavezance pozvali, naj tudi v praksi zagotovijo čim hitrejši dostop do informacij.

## 2.6.2 MEDNARODNO SODELOVANJE

*Srečanje Iniciative 2020, Bled, 3.–5. oktober 2021*



Septembra 2021 se je Informacijski pooblaščenec, na povabilo srbskega informacijskega pooblaščenca v okviru projekta USAID Government Accountability udeležil on-line foruma z naslovom Dostop do informacij v tožilskih in sodnih postopkih. V okviru dogodka so predstavniki urada srbskega informacijskega pooblaščenca, sodstva, tožilstva, nevladnih organizacij in novinarjev predstavili dileme glede dostopa do dokumentov iz tožilskih in sodnih postopkov v postopkih dostopa do informacij javnega značaja. Informacijski pooblaščenec je v okviru predstavitve mednarodnih izkušenj na tem področju sodeloval s prispevkom »Dostop do informacij v tožilskih in sodnih zadevah – izkušnje Republike Slovenije«.

Oktober 2021 se je Informacijski pooblaščenec na povabilo organizacije Regionalni dialog udeležil srečanja z uzbeško delegacijo Protikorupcijske agencije in ameriško ambasado iz Uzbekistana. Strokovni sodelavki Informacijskega pooblaščenca sta v okviru srečanja pripravili tri sklope predavanj z naslednjimi naslovi: »Introduction of the Institution of the Information Commissioner«, »The Competencies and Procedure in Handling Access to Information Complaints« in »Legal Basis and Important Cases of IC on Transparency Matters«. Predavanjem je sledila razprava, tej pa vprašanja udeležencev.

## 2.7 SPLOŠNA OCENA IN PRIPOROČILA

### Splošna ocena in priporočila na področju dostopa do informacij javnega značaja

Kljub temu da so tudi leto 2021 zaznamovale posebne razmere, povezane z epidemijo covid-19, je pri Informacijskem pooblaščenecu delo na področju dostopa do informacij javnega značaja potekalo kot običajno. Informacijski pooblaščenec je na tem področju obravnaval 940 zadev, v pritožbenih postopkih pa je izdal 404 odločitve (397 odločb in sedem sklepov), kar je največ od njegove ustanovitve.

Leta 2021 je Informacijski pooblaščenec zaznal znaten porast pritožbenih zadev, in sicer je naraslo tako število skupnih pritožb (639 glede na 565 v letu 2020) kot število pritožb zaradi molka organa (244 glede na 231 v letu 2020) in število pritožb zoper zavrnilne odločbe (389 glede na 320 v letu 2020). Ob tem je skrb vzbujajoča ugotovitev, da se je vnovič povečalo število pritožb zoper državne organe (338 glede na 245 v letu 2020, kar predstavlja 37-odstotni porast), in sicer tako zoper zavrnilne odločitve kot zaradi molka organa. Upadlo pa je skupno število pritožb zoper občine (107 glede na 115 v letu 2020), pri čemer je razveseljivo dejstvo, da je že drugo leto zapored upadlo število pritožb zaradi molka občin (46 glede na 56 v letu 2020). Upadlo je tudi število pritožb zoper poslovne subjekte pod prevladujočim vplivom oseb javnega prava: Informacijski pooblaščenec leta 2020 prejel 14 pritožb zoper to skupino zavezancev, leta 2021 pa je bilo teh pritožb le šest.

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 spletni strani, pri čemer se trudi, da je ta ažurna in da so objave pregledno dostopne, vse z namenom olajšati delo zavezancev in seznanjati javnost s pomenom te temeljne človekove pravice. Leta 2021 je Informacijski pooblaščenec prejel 301 pisnih prošenj za neformalno pomoč ali mnenje, odgovoril pa je tudi na 948 zaprosil v okviru telefonskega dežurstva, kar je 50-odstotno povečanje glede na leto 2020, ko je v okviru telefonskega dežurstva prejel 632 zaprosil.

V okviru pritožbenih postopkov zaradi molka organa je Informacijski pooblaščenec ugotovil, da se je delež teh pritožb glede na skupno število vseh pritožb sicer zmanjšal (v letu 2021 jih je bilo 35%, v letu 2020 pa 43 %), skrb vzbujajoč pa je podatek, da je naraslo število teh pritožb zoper državne organe. V to skupino zavezancev spadajo organi državne uprave ter drugi državni organi, ki bi morali biti glede na kadrovske in organizacijske vire, s katerimi razpolagajo, po 18 letih od uveljavitve ZDIJZ z zakonom in njegovo uporabo v praksi že dobro seznanjeni. Ker številna vprašanja, ki jih ti zavezanci naslavlajo na Informacijskega pooblaščenca, kažejo, da imajo pri izvajanju zakona v praksi še vedno težave, Informacijski pooblaščenec vnovič (kot že leto poprej) poziva Ministrstvo za javno upravo, ki je zadolženo za usposabljanje zavezancev za uporabo zakona v praksi, naj bolj aktivno pristopi k tej nalogi in temu področju nameni več pozornosti.

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

- Informacijski pooblaščenec je v letu 2021 zaznal bistven porast števila zadev, v katerih so bili prosilci mediji oz. novinarji. Kljub temu da so zavezanci leta 2021 delovali v posebnih pogojih zaradi epidemioloških razmer, povezanih s preprečevanjem širjenja bolezni covid-19, pa tega ne smejo izkoristiti v škodo prosilcev in za zmanjševanje transparentnosti. Ker imajo mediji v demokratični družbi posebno vlogo, Informacijski pooblaščenec zavezance poziva, naj zahteve medijev in novinarjev obravnavajo v najkrajših rokih (naj ne čakajo na iztek zakonskega roka) ter jim v skladu z načelom transparentnosti in načelom prostega dostopa posredujejo vse informacije, ki iz prostega dostopa niso izključene zaradi zakonskih izjem. Pri tem naj zavezanci, v izogib stroškom in zavlačevanju postopkov, sledijo utečeni praksi Informacijskega pooblaščenca in Upravnega sodišča RS.

- Informacijski pooblaščenec je v letu 2021 znova zaznal povečanje števila primerov, v katerih so prosilci zahtevali informacije, ki se nanašajo na področje izvajanja epidemioloških ukrepov, javnega zdravja in s tem povezano porabo javnega denarja (npr. statistike o obolelosti in smrtnosti, nabava 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 ter 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.

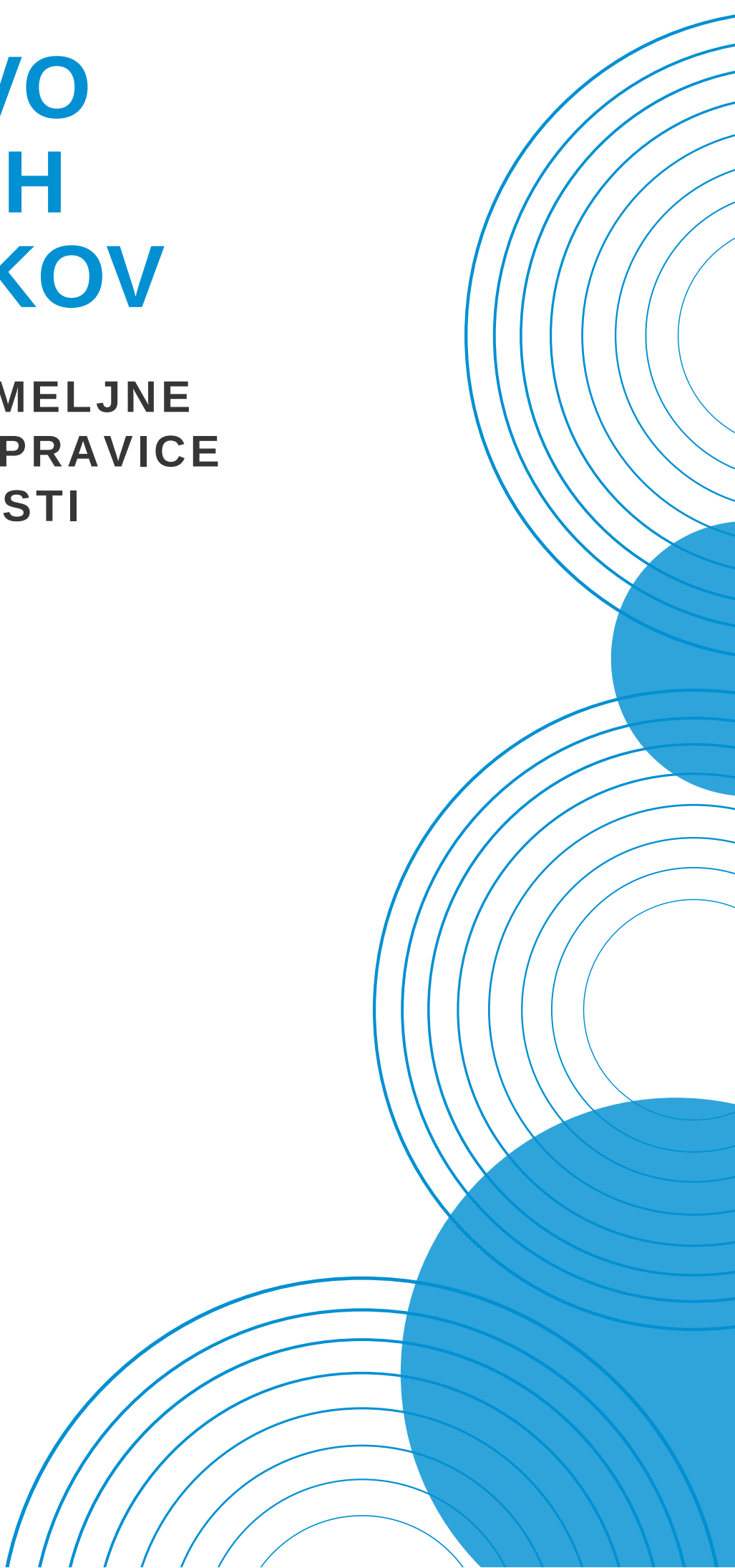
- Informacijski pooblaščenec je v letu 2021 prejel tudi več pritožb v zvezi z dostopom do podatkov o izplačilih plač javnim uslužbencem in različnih dodatkov za delo v epidemioloških razmerah. Več zavezancev je dostop do bruto plač in bruto izplačanih dodatkov zavrnilo, ob čemer so se sklicevali na varstvo osebnih podatkov. Zakonska ureditev, ki določa javnost plač v javnem sektorju, je povsem jasna, temu pa sledi tudi obsežna praksa Informacijskega pooblaščenca in Upravnega sodišča RS. Ti podatki, v skladu s prvo alinejo 3. odstavka 6. člena ZDIJZ in 38. členom ZSPJS, niso varovani osebni podatki, ker gre za podatke o porabi javnih sredstev in podatke v zvezi z delovnim razmerjem javnih uslužbencev. V izogib zavlačevanju postopkov Informacijski pooblaščenec zavezanca poziva, naj temu stališču sledijo.

- Informacijski pooblaščenec je, podobno kot v letih 2019 in 2020, tudi v letu 2021 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. Obrazložitve zavrnilnih odločb niso dovolj konkretizirane, predvsem pa iz njih ne izhaja, na podlagi katerih dejstev in izvedenih dokazov je organ sprejel odločitev. Informacijski pooblaščenec zato zavezancem predlaga, da pri obravnavi zahtev posebej natančno proučijo 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.

- Najpogostejši razlog zavrnitve v pritožbenih postopkih v letu 2021 ni bil obstoj izjeme varstva osebnih podatkov kot leto dni prej, temveč to, da zahtevana informacija ne obstaja. V zvezi s tem je Informacijski pooblaščenec ugotovil, da se zavezanci pogosto sklicujejo na neobstoj zahtevanih informacij tudi v primerih, ko bi s temi informacijami morali razpolagati oz. ko prosilci upravičeno pričakujejo, da z njimi razpolagajo. Iz definicije informacije javnega značaja, kot jo določa 4. člen ZDIJZ, sicer izhaja, da zavezanci za potrebe prosilca zahtevane informacije niso dolžni ustvariti oz. jo pridobiti, če v času odločanja o zahtevi z njo ne razpolagajo, vendar to ne pomeni, da se zavezanci s sklicevanjem na neobstoj informacije lahko izmikajo transparentnemu delovanju. Informacijski pooblaščenec zato zavezanca poziva, naj pri izdaji zavrnilne odločbe zaradi neobstoja informacij svoje stališče še posebej skrbno obrazložijo, pri čemer naj zlasti pojasnijo, na podlagi česa so zaključili oz. kako so preverili, da z dokumentom dejansko ne razpolagajo. Ker so zavrnilne odločbe pomanjkljivo obrazložene, prosilci tudi v primeru domnevnega neobstoja dokumenta želijo, da Informacijski pooblaščenec preveri dejansko stanje in ugotovi, ali informacija pri organu res ne obstaja.

# 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 njihovo zavarovanje. 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.

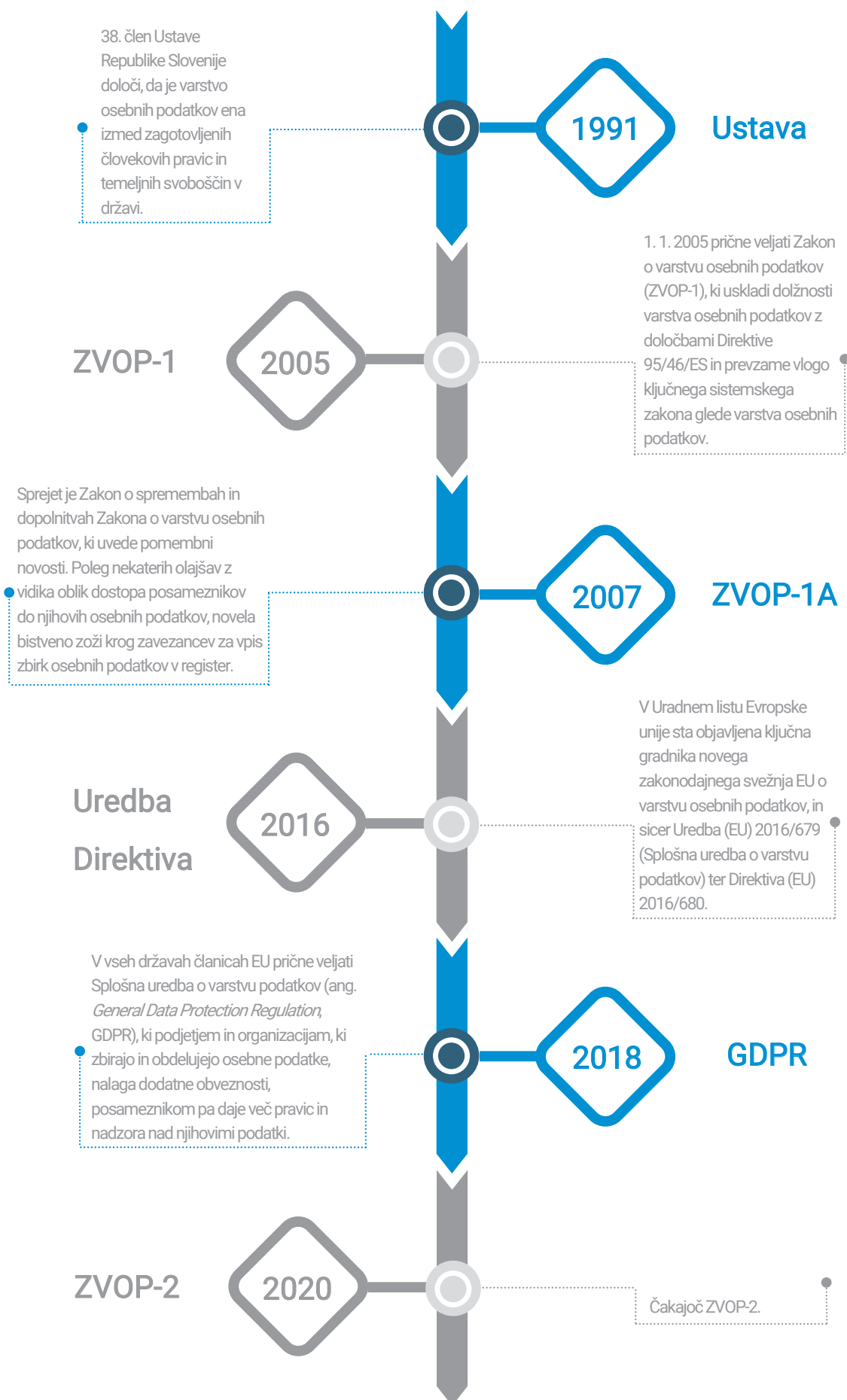
S Splošno uredbo so se okrepile pravice posameznika, poleg obstoječe pravice dostopa do osebnih podatkov ter pravice do popravka še pravica do pozabe, izbrisa, omejitve obdelave, ugovora in prenosljivosti podatkov. Precej večji poudarek je zdaj na transparentnosti obdelave, tj. glede zagotavljanja preglednih 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. Upravljalci 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 »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 27 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 2021

Postopek inšpekcijskega nadzora, ki ga izvaja Informacijski pooblaščenec oz. državni nadzorniki za varstvo osebnih podatkov, poleg Zakona o varstvu osebnih podatkov (ZVOP-1), Zakona o Informacijskem pooblaščenju (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, pooblaščenec 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 pooblaščenju 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:

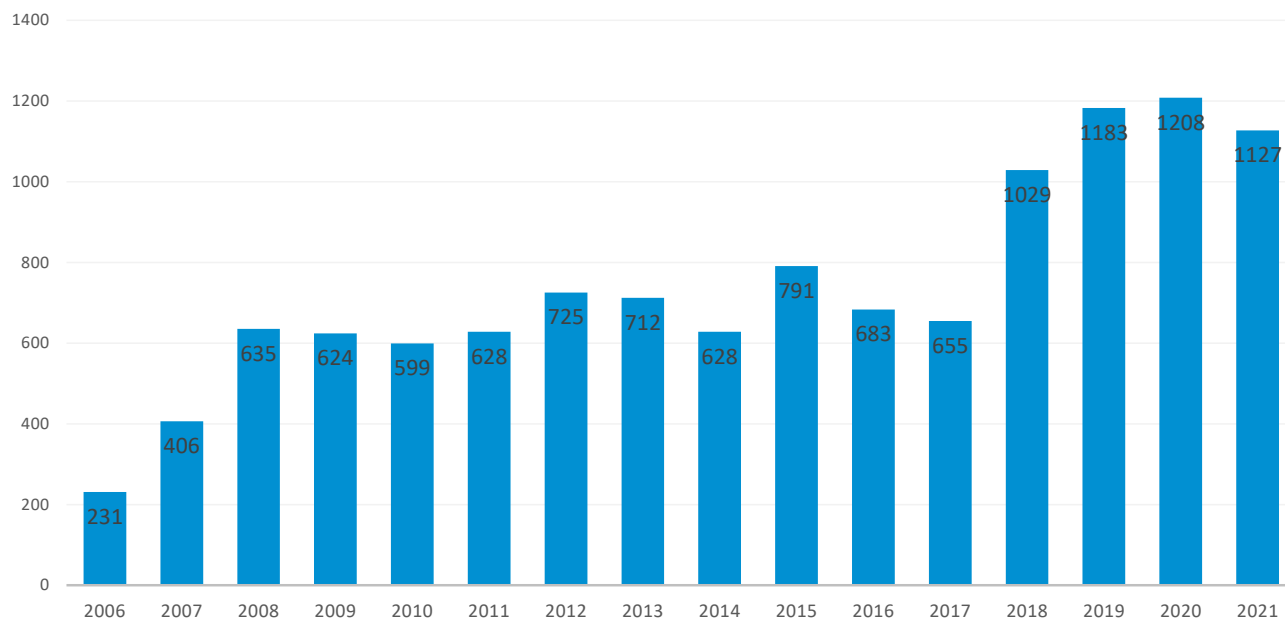
- da izda upravljavcu ali obdelovalcu opozorilo, da bi predvidena dejanja obdelave verjetno kršila določbe Splošne uredbe;
- da upravljavcu ali obdelovalcu izreče opomin, kadar so bile z dejanji obdelave kršene določbe Splošne uredbe;
- da upravljavcu ali obdelovalcu odredi, naj ugotovi zahteve posameznika, 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 2021 zaradi suma kršitev določb Splošne uredbe in/ali ZVOP-1 vodil 1.127 inšpekcijskih zadev, od tega 426 v javnem in 701 v zasebnem sektorju. V primerjavi z letom 2020, ko se je število inšpekcijskih zadev povečalo za 2 % glede na leto 2019, se je število inšpekcijskih zadev v letu 2021 sicer znižalo za 6,7 %, vendar je Informacijski pooblaščenec skupno obravnaval kar 1360 prijav,**

kar je največ doslej. Na podlagi prijav je Informacijski pooblaščenec uvedel 1036 inšpekcijskih postopkov.

V letu 2021 je Informacijski pooblaščenec obravnaval več t. i. žariščnih primerov, med katerimi so nekateri zadevali celotno prebivalstvo (npr. zadeva glede obdelave osebnih podatkov vlagateljev prijave interesa za cepljenje proti covid-19 preko portala e-Uprava, glede pošiljanja vabil k cepljenju proti covid-19, glede preverjanja izpolnjevanja pogoja PCT ter glede pošiljanja pisem vsem državljanov s strani predsednika Vlade RS) in so bili tudi medijsko zelo odmevni. V teh primerih je Informacijski pooblaščenec prejel po več kot 100 posameznih prijav, na podlagi katerih pa je potem vodil po en inšpekcijski postopek. Nekoliko manjše število uvedenih inšpekcijskih postopkov je pripisati tudi učinkovitemu preventivnemu delovanju Informacijskega pooblaščenca: na primer priprava smernic glede nekaterih perečih vprašanj (npr. smernic glede preverjanja pogoja PCT) je v določenem delu vplivala na število prejetih prijav, saj so smernice že vnaprej razjasnile določene dileme.

Število inšpekcijskih zadev med letoma 2006 in 2021.



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	278
Nezakonito zbiranje oz. zahtevanje osebnih podatkov	228
Nezakonito izvajanje videonadzora	140
Nezakonita obdelava osebnih podatkov pri izvajanju neposrednega trženja	98
Nezakonit vpogled v osebne podatke	54
Neustrezno zavarovanje osebnih podatkov	47
Hekerski napadi in vdori v informacijske sisteme	27
Kršitev pravice do informacij po členu 13	24
Piškotki	16
Obdelava osebnih podatkov v nasprotju z namenom zbiranja	15
Zavrnitev posredovanja osebnih podatkov	10
Zavrnitev izbrisa osebnih podatkov	6
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)	103

### 3.2.1 INŠPEKCIJSKI NADZOR V JAVNEM SEKTORJU

Zaradi suma kršitev določb Splošne uredbe in/ali ZVOP-1 je Informacijski pooblaščenec zoper zavezanca v javnem sektorju leta 2021 vodil 426 zadev, 396 jih je začel na podlagi prejetih prijav, 30 pa na lastno pobudo.

Informacijski pooblaščenec je 103 prijaviteljem pisno pojasnil, zakaj v prijavi opisano ravnanje ne pomeni kršitve zakonodaje s področja varstva osebnih podatkov, v 29 primerih pa je po proučitvi prijav zaključil, da uvedba inšpekcijskega postopka 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 11 kršiteljev uvedel postopke o prekršku oz. jim je izrekel ukrepe v skladu z Zakonom o prekrških (ZP-1), v 13 primerih je ocenil, da uvedba postopka o prekršku ne bi bila smotrna, ker je v prijavi opisano ravnanje predstavljalo prekršek neznatnega pomena, v enem primeru postopka ni uvedel zaradi zastaranja pregona, v enem primeru je ugotovil, da ravnanje zavezanca ni prekršek, v treh primerih pa prekrškovnega postopka ni uvedel, ker ZVOP-1 ne določa sankcije za kršitve določb Splošne uredbe (nesprejetje novega ZVOP-2). V 37 zadevah Informacijski pooblaščenec ni uvedel postopka, saj so bile zatrjevane nepravilnosti že odpravljene. 23 prijaviteljev je Informacijski pooblaščenec napotil na pravice posameznika po Splošni uredbi (predvsem pravice do seznanitve z lastnimi osebnimi podatki), v treh primerih pa ni uvedel postopka, ker iz prijave ni bilo razvidno, za kakšno kršitev naj bi šlo, prijavitelj pa po pozivu prijave ni dopolnil oz. v prijavi ni posredoval svojih podatkov, zaradi česar ga Informacijski pooblaščenec niti ni mogel pozvati k posredovanju dodatnih podatkov, ki bi bili potrebni za uvedbo inšpekcijskega postopka. V 49 zadevah prijavitelji pri utemeljevanju kršitve niso navedli ustreznih dokazov, v 36 zadevah pa je Informacijski pooblaščenec ugotovil, da za zatrjevane kršitve ni pristojen. V štirih zadevah je Informacijski pooblaščenec vlogo odstopil pristojnemu organu.

Informacijski pooblaščenec je leta 2021 zavezancem v javnem sektorju izdal 38 tako imenovanih predodločb<sup>1</sup> ter šest ureditvenih odločb, vse ostale kršitve so zavezanci sami prostovoljno odpravili takoj po pozivu državnega nadzornika za varstvo osebnih podatkov.

Leta 2021 je bilo v javnem sektorju 182 inšpekcijskih postopkov zaključenih z izdajo sklepa o ustavitvi postopka. Informacijski pooblaščenec je 71 postopkov ustavil, ker so zavezanci ugotovljene nepravilnosti odpravili, v 75 postopkih ni zaznal kršitev določb Splošne uredbe ali ZVOP-1, v sedmih primerih ni bilo predloženih dovolj dokazov za nadaljevanje postopka, 28 postopkov 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, v eni zadevi pa je ugotovil, da za zadevo ni pristojen.

<sup>1</sup> Informacijski pooblaščenec mora v primeru, ko ugotovi nezakonito obdelavo osebnih podatkov, pred izdajo odločbe, s katero odredi prenehanje takšne obdelave, zavezanca skladno z načelom zaslišanja stranke (9. člen ZUP) predhodno seznaniti s tem, zakaj po njegovem mnenju za predmetno obdelavo osebnih podatkov nima pravne podlage, ter ga seznaniti z argumenti, ki njegovo mnenje potrjujejo. Zavezancu je namreč glede na sodno prakso treba pred izdajo ureditvene odločbe dati možnost, da se izjavi do stališča Informacijskega pooblaščenca (načelo kontradiktornosti strank). To v praksi pomeni, da zavezanci po seznanitvi z argumenti Informacijskega pooblaščenca v večini primerov sami nehajo nezakonito obdelovati osebne podatke, zato izdaja ureditvene odločbe ni več potrebna.

### 3.2.2 INŠPEKCIJSKI NADZOR V ZASEBNEM SEKTORJU

Informacijski pooblaščenec je zoper zavezanca v zasebnem sektorju vodil 701 zadevo, od tega jih je 661 vodil na podlagi prejetih prijav, 18 postopkov je uvedel na lastno pobudo, preostali (22) pa so bili uvedeni po iniciativi drugih nadzornih organov v EU v okviru čezmejnega sodelovanja; v slednjih je Informacijski pooblaščenec sodeloval kot zadevni organ (več v poglavju 3.2.4.).

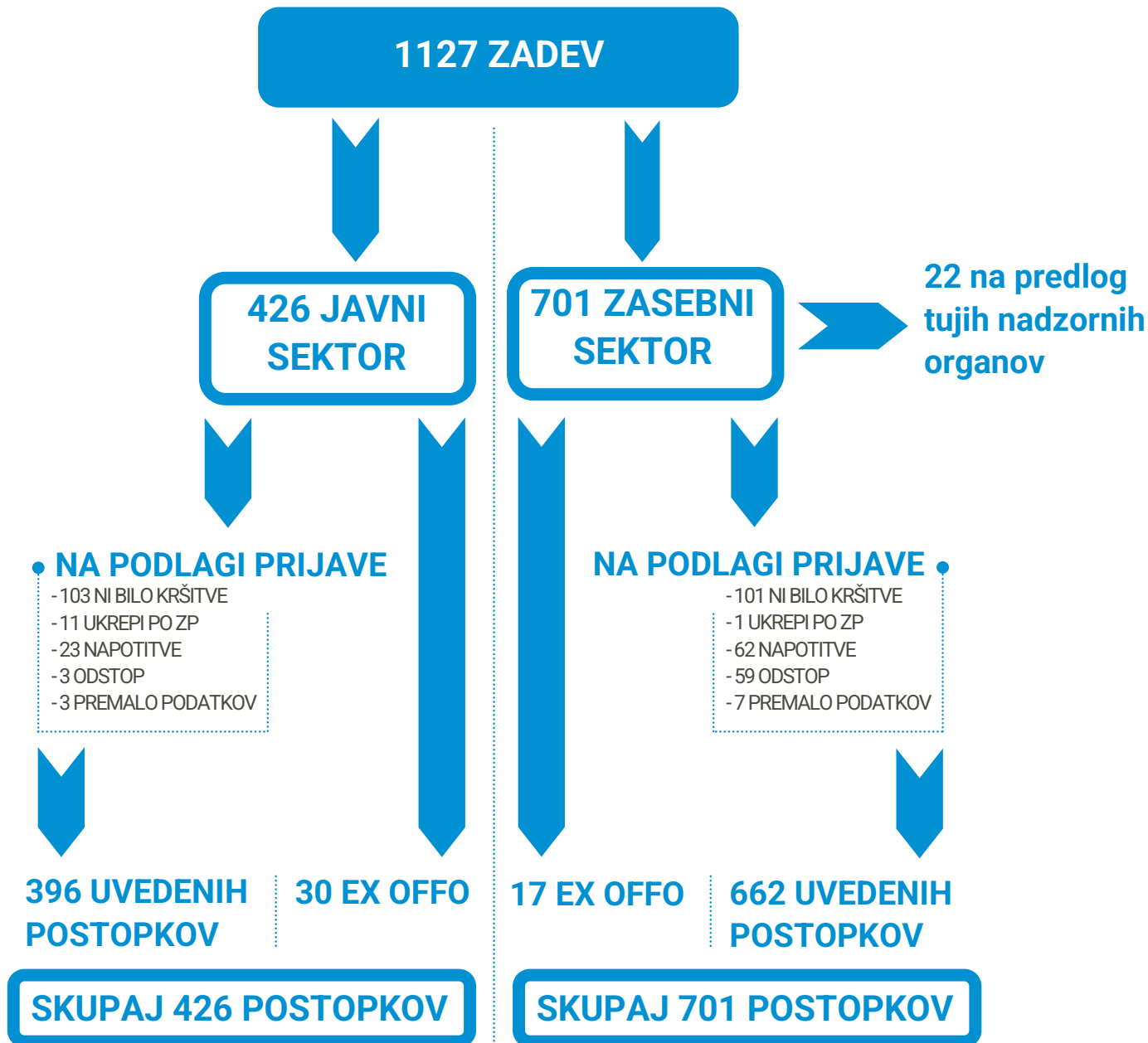
Po proučitvi prijav je Informacijski pooblaščenec 101 prijavitelja obvestil, da postopka inšpekcijskega nadzora ne bo uvedel, ker iz njegove prijave ne izhaja sum kršitev določb Splošne uredbe in ZVOP-1, 62 prijaviteljev pa je napotil na pravice, ki jih morajo pri upravljalcih osebnih podatkov uveljavljati sami, največkrat na pravico do seznanitve z lastnimi osebnimi podatki in pravico do ugovora. Informacijski pooblaščenec na podlagi 10 prijav inšpekcijskega postopka ni uvedel, ker je šlo za enkratna dejanja oz. kršitve varstva osebnih podatkov v preteklosti in teh kršitev 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 enemu kršitelju izrekel ukrep 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 pa uvedba prekrškovnega postopka ni bila dopustna zaradi zastaranja pregona. V 86 primerih Informacijski pooblaščenec ni uvedel postopka, ker niso bili predloženi ustrezni dokazi, ki bi zatrjevano kršitev utemeljevali, v 96 primerih pa za ukrepanje ni bil pristojen. Sedem prijav je vsebovalo premalo podatkov za uvedbo inšpekcijskega postopka, poleg tega so bile anonimne in Informacijski pooblaščenec prijaviteljev ni mogel pozvati k dopolnitvi. V 17 primerih inšpekcijski postopek ni bil uveden, ker je kršitelj nepravilnosti že odpravil, v 59 zadevah pa je Informacijski pooblaščenec vlogo odstopil pristojnemu organu.

Informacijski pooblaščenec je leta 2021 zavezancem v zasebnem sektorju izdal 74 tako imenovanih predodločb ter 11 ureditvenih odločb, vse ostale kršitve so zavezanci sami prostovoljno odpravili takoj po pozivu državnega nadzornika za varstvo osebnih podatkov.

Leta 2021 je Informacijski pooblaščenec pri zavezancih v zasebnem sektorju s sklepom ustavil 229 postopkov: 78 postopkov je ustavil, ker ni zaznal kršitev določb ZVOP-1, 116 postopkov je ustavil po tem, ko so zavezanci odpravili ugotovljene nepravilnosti, 25 postopkov je zaključil, ker v zvezi z ugotovljenimi prekrški ni bilo mogoče izreči inšpekcijskih ukrepov, saj je šlo za enkratna dejanja v preteklosti, v sedmih primerih ni bilo predloženih dovolj dokazov za nadaljevanje postopka, tri postopke pa je ustavil zaradi prenehanja zavezanca (pravne osebe).

Informacijski pooblaščenec je prejel dve sodbi Upravnega sodišča RS v zvezi s tožbama, vložanima leta 2017 in 2020 zoper ureditveno odločbo in zavrnilno odločbo v zvezi s pritožbo posameznika zoper odločitev upravljavca o pravici do izbrisa. Sodišče je obeh primerih tožbi zavrnilo in potrdilo pravilnost odločitev Informacijskega pooblaščenca.

Pregled inšpekcijskih zadev v javnem in zasebnem sektorju leta 2021.

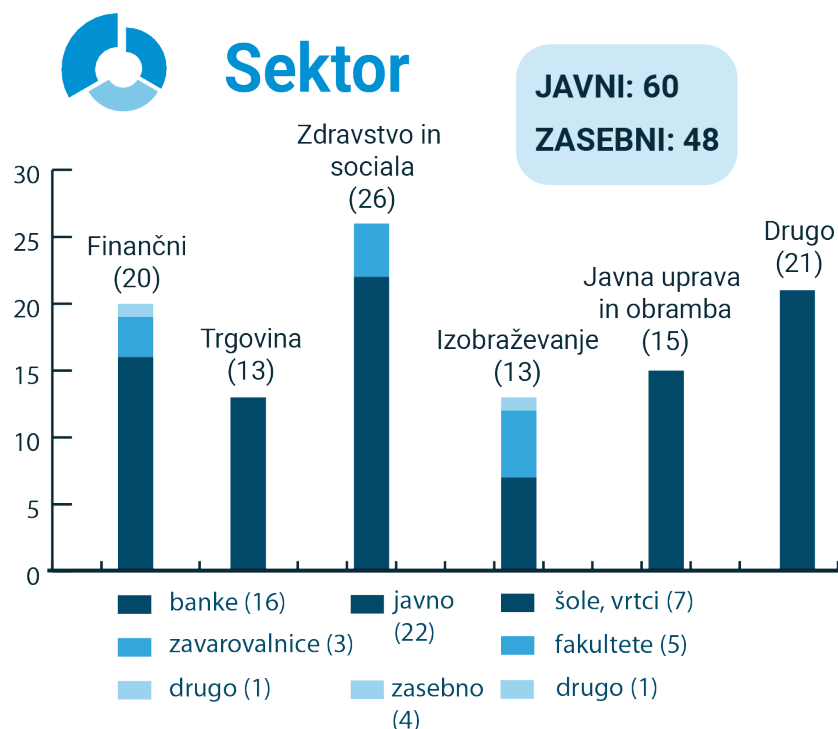


### 3.2.3 PRIJAVA KRŠITEV VARNOSTI OSEBNIH PODATKOV

Skladno s členom 33 Splošne uredbe so zavezanci nadzorni organ (Informacijskega pooblaščenca) dolžni obvestiti 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 posameznika, 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 2021 prejel 108 uradnih obvestil o kršitvi varnosti osebnih podatkov, t. i. samoprijav, ki so jih poslali zavezanci. 48 obvestil so poslali zavezanci iz zasebnega sektorja (npr. banke, trgovska podjetja, zavarovalnice), 60 pa zavezanci iz javnega sektorja (predvsem zdravstvene in izobraževalne ustanove).

Prijave kršitev varnosti glede na sektor.



Kršitve varnosti osebnih podatkov so se nanašale na:

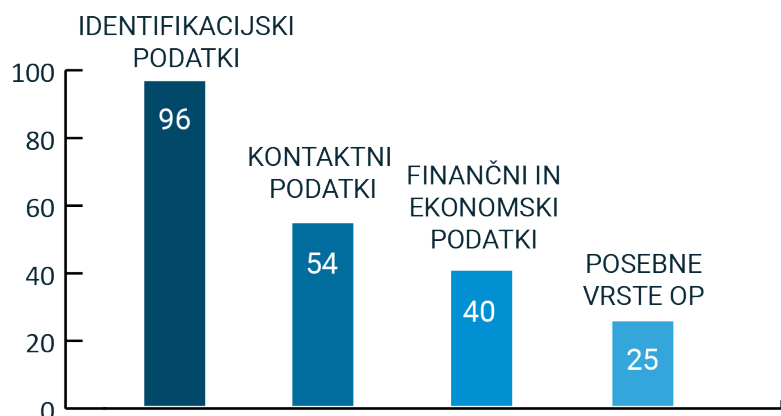
- nezakonito razkritje osebnih podatkov nepooblaščenim osebam – 24,
- posredovanje dokumentov z osebnimi podatki (npr. zdravniških izvidov, računov, dokumentov v upravnih postopkih, debetne kartice) napačnim osebam kot posledica nenamerne človeške napake ali netočnih podatkov v zbirkah osebnih podatkov (npr. e-naslovov strank) – 22,
- nepooblaščen dostop do osebnih podatkov oz. njihova obdelava s strani zaposlenih – 15,
- hekerski vdor – 11,
- neustrezno zagotavljanje varnosti osebnih podatkov – 9 (od tega na spletni strani 6),
- 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) – 7,
- nezakonito objavo osebnih podatkov na spletu – 6,
- pošiljanje zlonamerne e-pošte in objava lažne spletne strani (ang. phishing) – 4,
- razkritje osebnih podatkov zaradi napake v aplikaciji oz. tehnične napake – 3,
- nezakonita uporaba e-naslovov za druge namene – 3,
- izgubo ali krajo prenosnega računalnika ali drugih nosilcev osebnih podatkov (USB-ključek, zdravstveni karton, zvezek z osebnimi podatki strank) – 2,
- nezakonito izvajanje zvočnega snemanja – 1,
- nezakonito zbiranje osebnih podatkov za namene preverjanja pogoja PCT – 1 .

V največ primerih je bilo število prizadetih posameznikov v zvezi s posamezno kršitvijo med ena in deset (v 55 primerih) ter med 11 in 100 (v 21 primerih). Vrste osebnih podatkov, v zvezi s katerimi je Informacijski pooblaščenec prejel uradna obvestila o kršitvi varnosti, so bili: v 96 primerih identifikacijski podatki, v 54 primerih kontaktni podatki, v 40 primerih finančni in ekonomski podatki ter v 25 primerih posebne vrste osebnih podatkov.

Vrste osebnih podatkov.



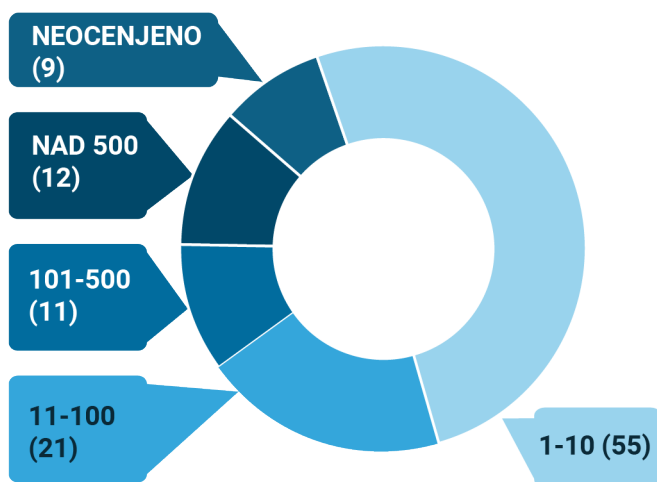
## Vrste osebnih podatkov



Število prizadetih posameznikov.



## Število prizadetih posameznikov



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](mailto: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).

### 3.2.4 SODELOVANJE PRI ČEZMEJNIH INŠPEKCIJSKIH NADZORIH

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

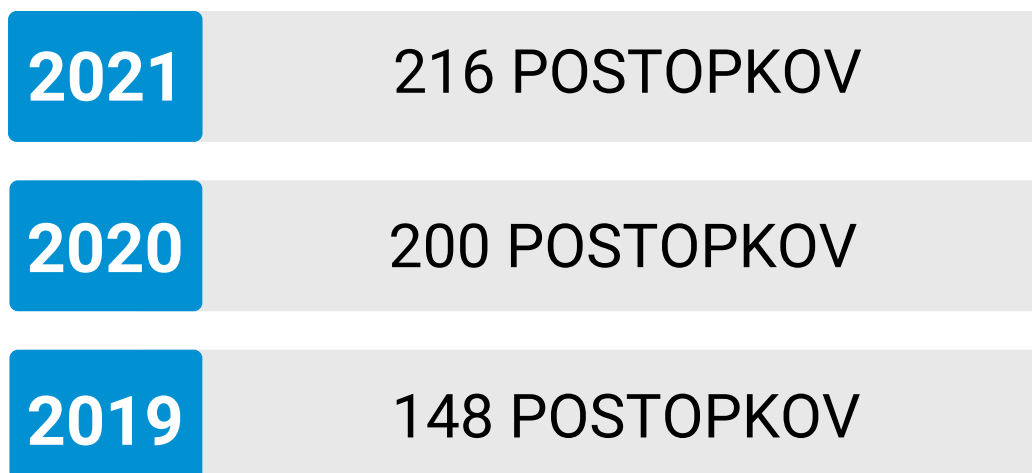
- **po načelu »vse na enem mestu« (angl. one stop shop)**, ki predvideva, da postopek nadzora v čezmejnem primeru obdelave osebnih podatkov vodi t. i. vodilni organ in pri tem sodeluje z drugimi organi za varstvo osebnih podatkov (člen 60 Splošne uredbe);
- **vzajemna pomoč** med organi za varstvo osebnih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

Sodelovanje po mehanizmu »vse na enem mestu« se lahko 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 pa se postopku nadzora priključijo kot zadevni organi, kadar ima upravljavec na njihovem ozemlju npr. podružnice ali poslovne enote oz. kadar obdelava osebnih podatkov pomembno vpliva na posameznike v teh državah članicah. Glavni organ v postopku inšpekcijskega nadzora vodi sodelovanje z drugimi organi ter pripravi osnutek odločbe, zadevni organi pa lahko izrazijo zadržke. V primeru nestrinjanja med vodilnim in zadevnimi organi o sporu odloči Evropski odbor za varstvo podatkov.

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

Leta 2021 je bil Informacijski pooblaščenec udeležen v 216 postopkih sodelovanja po členih 60 in 61 Splošne uredbe v zvezi z upravljavci, ki izvajajo čezmejno obdelavo osebnih podatkov; v 75 novih postopkih se je opredelil za zadevni nadzorni organ (po členu 56 Splošne uredbe) ter bil dvakrat v vlogi vodilnega nadzornega organa. V nadaljevanju so podrobneje predstavljeni različni postopki sodelovanja.

*Sodelovanje Informacijskega pooblaščenca v čezmejnih postopkih po členih 60 in 61*





## Opredelitve vodilnega in zadevnih nadzornih organov po členu 56 Splošne uredbe

### 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 75 tovrstnih postopkih leta 2021 se je Informacijski pooblaščenec opredelil za zadevni organ. 10 postopkov ugotavljanja je začel Informacijski pooblaščenec, in sicer na podlagi prijave domnevne kršitve varstva osebnih podatkov v čezmejnem primeru. 65 postopkov ugotavljanja je bilo začelih na iniciativo drugih organov v EU, Informacijski pooblaščenec pa se je opredelil za zadevni nadzorni organ predvsem:

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

Dvakrat je Informacijski pooblaščenec prevzel vlogo vodilnega nadzornega organa v zvezi s prijavi zoper zavezanca 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 leta 2021 **obravnaval 62 novih zadev** čezmejnega sodelovanja pri inšpekcijskem nadzoru nad podjetji, ki poslujejo čezmejno, poleg postopkov, začelih pred letom 2021, ki so še v teku. V teh postopkih je pričakovan sprejem odločitve nadzornih organov po členu 60 Splošne uredbe, po t. i. mehanizmu »vse na enem mestu«. Vodilni nadzorni organ v največ primerih predstavlja irski nadzorni organ, pogosto v tej vlogi nastopajo 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 prijave kršitev varstva osebnih podatkov ter pomanjkljivo zavarovanje osebnih podatkov, nezakonito obdelavo osebnih podatkov v okviru neposrednega trženja ter nesorazmerne zahteve po posredovanju osebnih podatkov. Primera, v katerih je Informacijski pooblaščenec sprejel vlogo vodilnega nadzornega organa, saj je sedež upravljavca v Sloveniji, sta zadevala zatrjevane nezakonnosti pri obdelavi osebnih podatkov v spletnih trgovinah.

40 tovrstnih postopkov je bilo začelih s strani drugih organov v EU in Informacijski pooblaščenec v teh postopkih sodeluje kot zadevni organ. Primeri niso zadevali le storitev priljubljenih spletnih velikanov (kot npr. Facebook, Google, Amazon itd.) temveč tudi neustrezna ravnanja z osebnimi podatki s strani raznolikih akterjev, ponudnikov bančnih storitev, spletnih ponudnikov različnih storitev, ponudnikov pretočnih storitev, povezanih vozil itd., iz številnih držav članic EU. Primeri spornih praks so vključevali pretirane zahteve po podatkih za identifikacijo strank pri spletnih igrah, posredovanje podatkov tretjim osebam, obdelavo osebnih podatkov brez ustrezne pravne podlage, neustrezno informiranje o obdelavi osebnih podatkov, pogosto so se primeri nanašali tudi na kršitve varnosti osebnih podatkov, med prizadetimi pa so bili tudi uporabniki iz Slovenije.

Leta 2021 je bilo v čezmejnih postopkih, v katerih je sodeloval Informacijski pooblaščenec, izdanih 26 osnutkov odločb po členu 60 Splošne uredbe. 22 postopkov je bilo končanih s končno odločbo po členu 60 Splošne uredbe. V okviru spletne strani Evropskega odbora za varstvo podatkov je dostopen 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](https://edpb.europa.eu/our-work-tools/consistency-findings/register-for-article-60-final-decisions_en).

Primeri čezmejnega sodelovanja se ne zaključijo nujno z izdajo končne odločbe; zakonodaja nekaterih držav članic EU v primerih, ko zavezanec prostovoljno izpolni zahteve prijaviteljev, namreč pozna tudi prijateljske poravnave. V teku ostajajo še številni postopki zoper velika multinacionalna podjetja; v večini teh primerov kot vodilni nastopa irski nadzorni organ.

Postopki po načelu »vse na enem mestu« v letu 2021.

## 62 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,
- 40 na iniciativo drugih nadzornih organov.

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

Informacijski pooblaščenec je leta 2021 **sodeloval tudi v 154 postopkih zagotavljanja medsebojne pomoči med nadzornimi organi** po členu 61 Splošne uredbe. Prejel je 136 zahtev drugih organov in se nanje, ko je bilo to potrebno, odzval, 18 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 razpredelnice.

Postopki zagotavljanja medsebojne pomoči.

## 151 postopkov prostovoljne medsebojne pomoči med nadzornimi organi po členu 61:

- 53 zahtev drugih organov za informacije in pojasnila,
- 80 obvestil drugih organov glede konkretnih postopkov v teku,
- 18 zahtev s strani Informacijskega pooblaščenca.

## 3 postopkov medsebojne pomoči med nadzornimi organi po členu 61:

- 3 odzivi na zahteve drugih organov.

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 krajeno pristojen obravnavati nadzorni organ v drugi državi članici. Postopki medsebojne pomoči pa običajno pomenijo zahtevo za izvedbo ukrepov zoper zavezance, ki izvajajo čezmejno obdelavo osebnih podatkov.

### Postopek spora po členu 65

Leta 2021 je bila sprejeta končna odločitev v primeru ponudnika storitev WhatsApp, in sicer v zvezi z neustreznim informiranjem posameznikov (uporabnikov in neuporabnikov) glede obdelave njihovih osebnih podatkov ter glede informiranja uporabnikov o tem, kako podatke uporablja Facebook in povezana podjetja, skladno s členi 12, 13 in 14 Splošne uredbe. Irski nadzorni organ je bil v vlogi vodilnega nadzornega organa, ki je obveščanje in prakso WhatsApp temeljito preiskal v postopku nadzora ter osnutek svoje odločitve delil z ostalimi zadevnimi organi iz drugih držav članic EU, tudi z Informacijskim pooblaščenecem, v skladu z določbami člena 60 Splošne uredbe, ki opredeljuje postopek sodelovanja pri čezmejnih zadevah. Zadevni organi so podali različne ugovore, zaradi česar je, skladno s členom 65 Splošne uredbe, o sporu odločil Evropski odbor za varstvo podatkov. V svoji zavezujoči odločitvi je Evropski odbor ugotovil dodatne pomanjkljivosti glede obveščanja uporabnikov WhatsApp, predvsem glede zakonitih interesov, na podlagi katerih WhatsApp obdeluje osebne podatke. Prav tako je ugotovil, da gre zaradi teže prekrškov v tem primeru tudi za kršitev načela 5(1)(a) Splošne uredbe, ki določa, da morajo biti osebni podatki obdelani zakonito, pošteno in na pregleden način. Prav tako je Evropski odbor ugotovil, da v tem primeru ne gre za anonimizirane osebne

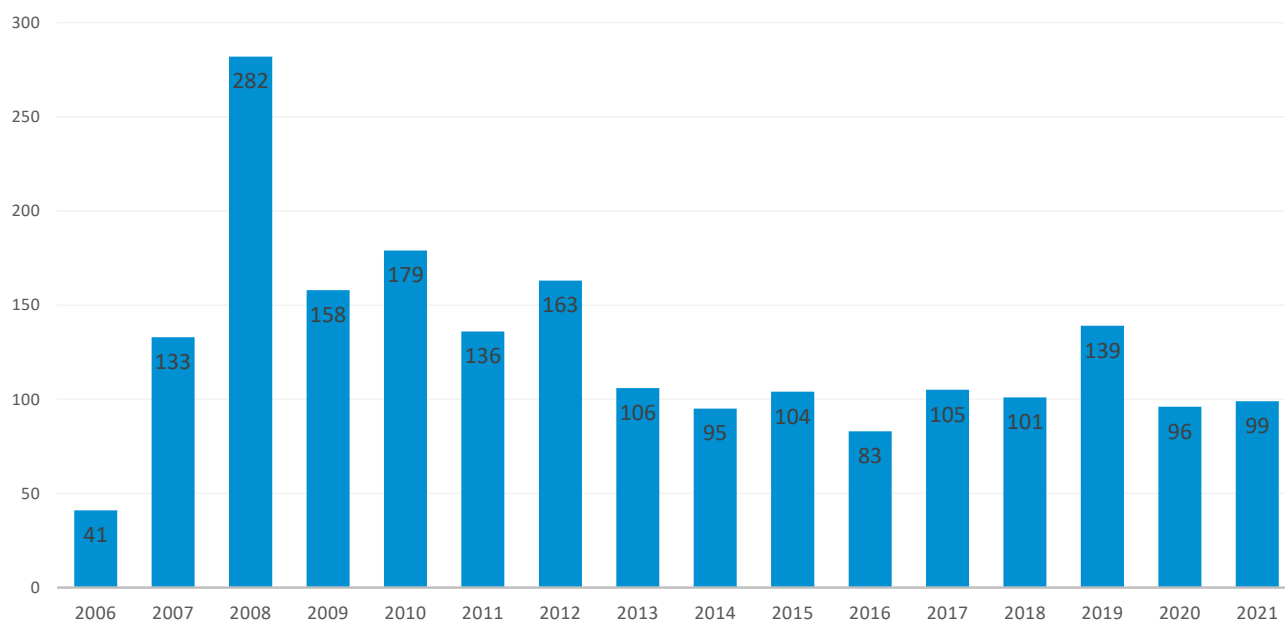
podatke, zato je irskemu nadzornemu organu naložil, da mora pri izreku sankcije upoštevati vsa merila iz člena 83 Splošne uredbe, da bo sankcija primerna in odvračalna, in da predlagano globo zaradi ugotovljenih kršitev zviša glede na vse okoliščine primera. Glede na to je irski nadzorni organ omrežju WhatsApp zaradi kršitev v zvezi z obveščanjem posameznikov o obdelavi njihovih osebnih podatkov naložil globo 225 milijonov evrov. Prav tako je omrežju WhatsApp naložil, da svojo prakso obveščanja in obdelave podatkov uskladi z določbami Splošne uredbe.

Leta 2021 je pomembno sodbo v zvezi s čezmejnimi sodelovanjem po Splošni uredbi sprejelo tudi Sodišče EU, ki je preučevalo vprašanje, ali lahko nacionalni nadzorni organ, ki ni vodilni po določbah Splošne uredbe, sproži sodni postopek proti domnevni kršiteljki zaradi kršitve določb Splošne uredbe pred nacionalnim sodiščem v svoji matični državi članici. Razsodilo je, da je to mogoče le, če Splošna uredba nadzornemu organu, ki ni vodilni nadzorni organ, daje pristojnost odločanja o tem, ali določena obdelava osebnih podatkov posameznikov krši pravila iz Splošne uredbe in ali so spoštovani postopki sodelovanja in nadzora, določeni s Splošno uredbi. Sodišče EU je poudarilo pomen tesnega, lojalnega in učinkovitega sodelovanja. Pri izvrševanju svojih pristojnosti tako vodilni nadzorni organ ne sme prezreti stališč drugih nadzornih organov; vsak ustrezen in utemeljen ugovor enega od preostalih nadzornih organov tako začasno zaustavi sprejetje osnutka odločitve vodilnega nadzornega organa. Sodišče je tudi določilo, da lahko nacionalni nadzorni organ, ki ni vodilni, v določenih primerih odloči glede kršitev Splošne uredbe tudi sam (npr. pri obdelavi izključno lokalne pritožbe z lokalnimi učinki oz. pri izdaji začasnega ukrepa v skladu z nujnim postopkom po Splošni uredbi).

### 3.2.5 PREKRŠKOVNI POSTOPKI

Informacijski pooblaščenec je zaradi suma kršitev določb ZVOP-1 v letu 2021 uvedel 99 postopkov o prekršku, od tega je 39 postopkov uvedel zoper pravne osebe javnega sektorja in njihove odgovorne osebe, 24 zoper pravne osebe zasebnega sektorja in njihove odgovorne osebe, 36 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 9).

*Število uvedenih postopkov o prekršku med letoma 2006 in 2021.*



Za ugotovljeni prekršek lahko prekrškovni organ v skladu s 53. členom izreče opozorilo, če je storjeni prekršek neznamenit in če pooblaščenca uradna oseba oceni, da je glede na pomen dejanja opozorilo zadosten ukrep. V primeru hujšega prekrška 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 v eni zadevi postopka o prekršku ni uvedel, ker je pregon že zastaral, 54 postopkov o prekršku pa je ustavil.

**Informacijski pooblaščenec je v prekrškovnih postopkih v letu 2021 izdal:**

- 37 odločb o prekršku (18 glob in 19 opominov),
- 7 opozoril.

Poleg opozoril, ki so bila izrečena v prekrškovnih postopkih, je Informacijski pooblaščenec v skladu z načelom ekonomičnosti izrekel tudi 50 opozoril po 53. členu ZP-1 v okviru postopkov inšpekcijskega nadzora.

V zvezi s 37 odločbami, ki so po ZP-1 najprej izdane brez obrazložitve, je bilo na podlagi napovedi zahtev za sodno varstvo izdanih pet odločb z obrazložitvijo, pri čemer so vsi kršitelji po prejemu odločbe z obrazložitvijo vložili zahtevo za sodno varstvo. Kršitelji so torej zoper izdane odločbe o prekršku vložili pet zahtev za sodno varstvo (zoper 5,6 % 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.

Naslednja preglednica prikazuje, na katere kršitve so se nanašali uvedeni prekrškovni postopki v letu 2021.

*Kršitve varstva osebnih podatkov v letu 2021.*

Vrsta kršitve	Število kršitev (v okviru enega postopka je lahko več kršitev)
Nezakonita obdelava osebnih podatkov (8. člen ZVOP-1)	43
Neustrezno zavarovanje osebnih podatkov (24. in 25. člen ZVOP-1)	17
Kršitev določb v zvezi z izvajanjem videonadzora (74., 75., 76., in 77. člen ZVOP-1)	16
Neizpolnjevanje ukrepov, izrečenih v postopkih inšpekcijskega nadzora, kršitev drugega odstavka 29. člena ZIN	14
Kršitev določb glede roka hrambe osebnih podatkov (21. člen ZVOP-1)	5
Nezakonit namen zbiranja in nadaljnje obdelave osebnih podatkov (16. člen ZVOP-1)	1
Kršitev določb glede zavarovanja občutljivih osebnih podatkov (drugi odstavek 14. člena ZVOP-1)	1
Kršitve določb glede neposredovanja osebnih podatkov uporabnikom osebnih podatkov (prvi odstavek 22. člena ZVOP-1)	1
Kršitve določb glede obvestitve posameznika ob zahtevi za začasno ali trajno prenehanje uporaba osebnih podatkov za namen neposrednega trženja (prvi odstavek 73. člena 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). 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 ZVOP-1 velja v celoti.**

Nekaj dilem pa se je pojavilo tudi v luči sodbe Višjega sodišča v Ljubljani PRp 345/2019 z dne 18. 6. 2020 ter sodbe Okrajnega sodišča v Ljubljani ZSV 2045/2019 z dne 8. 3. 2021, ki sta odločila, da Informacijski pooblaščenec ne more več sankcionirati nobene kršitve določb ZVOP-1 in prekrška po tem zakonu, ki hkrati predstavlja tudi kršitev katere od določb Splošne uredbe in za kršitev katere Splošna uredba predpisuje upravno (in ne kaznovalno) sankcioniranje. Zaradi omenjenih sodb je Informacijski pooblaščenec začasno nehal z vodenjem prekrškovnih postopkov zaradi kršitev določb ZVOP-1, s prekrškovnimi postopki pa je nadaljeval šele po prejemu sodbe Vrhovnega sodišča IV Ips 2/2021 z dne 16. 3. 2021 ter po prejemu sklepa Višjega sodišča v Ljubljani št. PRp 215/2021 z dne 22. 6. 2021. Z tema odločitvama sodišč je bilo namreč potrjeno stališče Informacijskega pooblaščenca in Ministrstva za pravosodje, da je prekrškovno sankcioniranje tistih določb ZVOP-1, ki niso v nasprotju s Splošno uredbo o varstvu podatkov in so kot take še vedno veljavne, skladno s slovenskim in evropskim pravnim redom.

Leta 2021 je Informacijski pooblaščenec prejel šest sodb, s katerimi so okrajna sodišča odločila o zahtevah

za sodno varstvo, ki so jih storilci vložili zoper odločbe o prekrških, izdane v letih 2012, 2018, 2019 in 2020:

- zahteva za sodno varstvo je bila zavrnjena kot neutemeljena, odločba Informacijskega pooblaščenca pa potrjena – 3,
- zahtevi za sodno varstvo je bilo delno ugodeno tako, da se odločba Informacijskega pooblaščenca spremeni in se postopek zoper odgovorno osebo in pravno osebo oz. zoper pravne osebe ustavi – 2,
- zahtevi za sodno varstvo je bilo ugodeno tako, da se postopek o prekršku ustavi, ker je bil kršitelj za ista ravnanja že pravnomočno obsojen za kaznivo dejanje.

Informacijski pooblaščenec je prejel tudi eno sodbo, s katero je višje sodišče pritožbi zoper sodbo okrajnega sodišča ugodilo in sodbo sodišča prve stopnje v zvezi z odločitvijo Informacijskega pooblaščenca spremenilo tako, da se postopek zoper pravno osebo in odgovorno osebo pravne osebe ustavi zaradi zastaranja pregona.

### 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 2021 v povezavi z epidemijo covid-19.

#### **Videoposnetkov nadzorne kamere ni dopustno spremljati prek prenosnega računalnika ali mobilnega telefona**

V zvezi z videonadzorom ne glede na sprejetje Splošne uredbe še vedno veljajo določila ZVOP-1, in sicer ZVOP-1 poleg splošnih določb (74. člen) eksplicitno ureja le videonadzor dostopov v uradne službene oziroma poslovne prostore (75. člen), videonadzor v večstanovanjskih stavbah (76. člen) ter videonadzor delovnih prostorov (77. člen). Za vse druge oblike videonadzora mora imeti upravljavec osebnih podatkov, skladno s prvim odstavkom 6. člena Splošne uredbe, ustrezno pravno podlago.

Videonadzor v delovnih prostorih se tako lahko izvaja le v izjemnih primerih, ki so določeni z ZVOP-1, in sicer kadar je to nujno potrebno za varnost ljudi ali premoženja ali za varovanje tajnih podatkov ter poslovne skrivnosti, tega namena pa ni možno doseči z milejšimi sredstvi (prvi odstavek 77. člena ZVOP-1). Delodajalec mora zaposlene pred začetkom izvajanja videonadzora vnaprej pisno obvestiti o njegovem izvajanju, pred uvedbo videonadzora pa se mora posvetovati z reprezentativnim sindikatom (četrti in peti odstavek 77. člena ZVOP-1). Javni in zasebni sektor pa lahko izvajata tudi videonadzor dostopa v njihove uradne službene oz. poslovne prostore, če je to potrebno za varnost ljudi ali premoženja, zaradi zagotavljanja nadzora vstopa ali izstopa v ali iz službenih oziroma poslovnih prostorov ali če zaradi narave dela obstaja možnost ogrožanja zaposlenih. Odločitev sprejme pristojni funkcionar, predstojnik, direktor ali drugi pristojni oz. pooblaščen posameznik osebe javnega ali zasebnega sektorja. V pisni odločitvi morajo biti obrazloženi razlogi za uvedbo videonadzora. Uvedba videonadzora se lahko določi tudi z zakonom ali s predpisom, sprejetim na njegovi podlagi (prvi odstavek 75. člena ZVOP-1). Tudi v tem primeru zakon predpisuje obvezno obveščanje zaposlenih, in sicer je o izvajanju videonadzora treba pisno obvestiti vse zaposlene v osebi javnega ali zasebnega sektorja, ki opravljajo delo v nadzorovanem prostoru (tretji odstavek 75. člena ZVOP-1). Upravljavec mora pri izvajanju videonadzora upoštevati tudi druge določbe ZVOP-1 in Splošne uredbe, npr. objaviti mora obvestilo o izvajanju videonadzora skladno s 74. členom ZVOP-1 in osebne podatke ustrezno zavarovati (skladno s 24., 25. in 32. členom Splošne uredbe ter petim odstavkom 74. člena ZVOP-1).

V enem od inšpekcijskih postopkov je na primer Informacijski pooblaščenec ugotovil, da je upravljavec, ki opravlja dejavnost v prodajnem salonu in servisni delavnici, namestil kar devet videonadzornih kamer. Pet videonadzornih kamer je namestil na zunanjih površinah in štiri v notranjosti poslovnih prostorov – dve kameri v servisni delavnici ter dve v prodajnem salonu. Upravljavec je zatrjeval, da je v prodajnem salonu izvajal videonadzor z namenom zagotavljanja nadzora vstopa ali izstopa v ali iz službenih prostorov ter zaradi varovanja premoženja. Namen varovanja premoženja bi naj upravljavec dosegel s preventivnim delovanjem tako, da bi z videonadzorom odvrčal nezakonite namene obiskovalcev (morebitne poškodbe ali odtujitve delov razstavljenih avtomobilov oz. razstavljene dodatne opreme). Podobno je zatrjeval tudi glede videonadzora v servisni delavnici, ki se je izvajal z namenom varovanja ljudi in premoženja tako, da se je prek videonadzora spremljalo izvajanje servisnih storitev, pri katerih lahko pride do poškodb zaposlenih, pri čemer videonadzor zagotavlja boljšo odzivnost, na podlagi posnetkov je prav tako mogoče ugotoviti vzrok za poškodbe in odpravo vzrokov zanj. Videonadzor v servisnih delavnicah je bil nameščen tudi z

namenom odvrtačanja nezakonitih namenov serviserjev, strank ter morebitnega naknadnega ugotavljanja oškodovanja premoženja.

V inšpekcijskem postopku je Informacijski pooblaščenec ugotovil, da je upravljavec s kamerami, ki jih je namestil v notranjosti poslovnih prostorov, izvajal videonadzor nad delovnimi mesti, saj je s kamerami pokrival celotne prostore in ne zgolj premoženja, ki bi ga naj domnevno varoval v teh prostorih. Na podlagi slik, ki so jih prikazovale kamere, je bilo v postopku ugotovljeno, da se je videonadzor izvajal z namenom vsakokratnega spremljanja dogajanja v prostorih, kar pa ne ustreza dopustnim namenom iz ZVOP-1. Upravljavec ni izkazal, katero konkretno premoženje, poslovna skrivnost, tajni podatki ipd. naj bi se konkretno varovali s posamezno kamero, prav tako ni dokazal, da se teh namenov ne bi dalo doseči z drugimi, milejšimi ukrepi.

Upravljavec je ves čas spremljal živo sliko, ki so jo prikazovale kamere. Do žive slike je lahko dostopal direktor in od njega pooblaščen osebe, in sicer prek osebnega računalnika, prenosnega računalnika in mobilnega telefona. V kolikor je uvedba videonadzora v konkretnih okoliščinah zakonita, bi upravljavci načeloma lahko izvajali videonadzor v poslovnih prostorih s spremljanjem žive slike, vendar bi morali obdelavo osebnih podatkov upravičiti skozi dopustne namene, zaradi katerih je videonadzor dopustno izvajati. Spremljanje žive slike je torej dopustno zgolj v primeru, če bi to bilo nujno potrebno za varovanje premoženja ter zagotavljanja varnosti ljudi, kar pa bi bilo mogoče doseči le z neprekinjenim spremljanjem žive slike med delovnih procesom, in sicer s strani za to pooblaščen osebe, npr. varnostnika. Pregledovanje žive slike ne more biti prepuščeno npr. direktorju oz. drugim pooblaščenim osebam, ki lahko spremljajo dogajanje, ko imajo čas oz. so v prostoru, kjer jim je spremljanje videonadzora omogočeno. Prenos žive slike ali dostop do posnetkov izven delovnih prostorov, prek mobilnih telefonov, prenosnih računalnikov ipd., je nedopusten. Konkretno premoženje, ki bi ga upravljavec želel varovati v delovnih prostorih, bi lahko zavaroval s pomočjo videonadzora tako, da bi kamere namestil nad področji, kjer se konkretno premoženje dejansko nahaja (npr. v razstavnem prostoru, v skladišču, kjer se shranjujejo rezervni deli, itd.).

### **Spremljanje gibanja posameznikov po prostorih ni dopusten namen izvajanja videonadzora**

Upravljavec je namestil videonadzor nad celotno površino notranjosti in zunanosti gostinskega lokala, pa tudi nad javnimi površinami (nad deli cest in parkirišči). Pojasnil je, da je bil namen izvajanja videonadzora varovanje premoženja in stvari ter varnost gostov in osebja, kot je to opredeljeno v ZVOP-1. Skupno je namestil 16 kamer, ki so po njegovih navedbah pokrivalo npr. opremo v kavarni, šank z blagajno, opremo v restavraciji, zunanjo pokrito teraso restavracije in opremo, ki se zvečer ne pospravlja, dnevni trezor, kuhinjo, prehod v skladišče, zunanjo letno teraso, otroška igrala in parkirišče. Z videonadzorom je upravljavec nadzoroval vse vstopne in izstopne iz poslovnih prostorov, z namenom varovanja premoženja pa je bilo tudi omogočeno vpogledovanje v posnetke oz. spremljanje žive slike.

V postopku je Informacijski pooblaščenec ugotovil, da kamere prikazujejo celotne prostore, kjer se nahajajo gosti (notranji in zunanji deli lokala), ter prostore, v katerih delajo zaposleni (kuhinja, šank in zunanji ter notranji prostori za goste, kjer dela gostinsko osebje). Vzpostavljeni videonadzor je omogočal spremljanje gibanja posameznikov po prostorih, kar pa ni dopusten namen za vzpostavitev oz. izvajanje videonadzora v poslovnih prostorih. Varnost zaposlenih bi lahko upravljavec zagotovil z milejšimi ukrepi, npr. z obstoječim videonadzorom vstopov in izstopov iz poslovnih prostorov, s čimer ne bi posegal v področja delovnih mest zaposlenih, ki v teh prostorih opravljajo svoje delo. Varnost premoženja bi v konkretnih okoliščinah lahko zagotovil z videonadzorom tudi tako, da bi kamere pokrivalo zgolj območja, kjer se nahaja konkretno premoženje oz. delovna oprema, blagajna itd., ki ga ni mogoče varovati z milejšimi sredstvi. Takšen nadzor bi predstavljal bistveno manjši poseg v zasebnost zaposlenih in gostov. Z videonadzorom nad celotnimi prostori pa je upravljavec nadziral celotno gibanje in dogajanje v prostorih, kjer je namestil kamere, kar je z vidika določb Splošne uredbe in ZVOP-1 nedopustno.

Glede vpogledovanja v posnetke oz. živo sliko z namenom varovanja premoženja je Informacijski pooblaščenec poudaril, da pri tem nikakor ni dopustno nadzirati dela zaposlenih. Posnetke oz. živo sliko bi upravljavec lahko vpogledoval npr. v času, ko je lokal zaprt oz. ko gostinski prostori ne obratujejo ter v njih ni zaposlenih in gostov. Sprotno spremljanje žive slike pa bi moralo biti, kot je bilo že poudarjeno, namenjeno izključno varovanju premoženja ter zagotavljanju varnosti ljudi. Slednje bi bilo mogoče doseči le z neprekinjenim spremljanjem žive slike med delovnim procesom s strani pooblaščen osebe, npr. varnostnika, ki bi lahko ob zaznanem incidentu (npr. tatvina, pretep, poškodovanje stvari) ustrezno ukrepal

oz. o konkretnem incidentu obvestil za to pristojne organe (policijo, gasilce, reševalce ipd.).

### **Posredovanje vabila na cepljenje, starejšim od 50 let**

Splošna uredba med posebne vrste osebnih podatkov (po ZVOP-1 gre za t. i. občutljive vrste osebnih podatkov) šteje tudi podatke v zvezi z zdravjem. Skladno s točko 15 člena 4 Splošne uredbe pomenijo podatki o zdravstvenem stanju osebne podatke, ki se nanašajo na telesno ali duševno zdravje posameznika, vključno z zagotavljanjem zdravstvenih storitev, in razkrivajo informacije o njegovem zdravstvenem stanju.

Z namenom zagotovitve precepljenosti zadostnega števila populacije je Nacionalni inštitut za javno zdravje (NIJZ) na pobudo Ministrstva za zdravje RS in cepilnih centrov z dopisom pozval vse prebivalce, starejše od 50 let, ki še niso bili cepljeni, na cepljenje v cepilne centre ali mobilne cepilne enote. Podatki posameznikov so bili pridobljeni iz Centralnega registra podatkov. NIJZ se je v zvezi z obstojem pravne podlage za obdelavo osebnih podatkov skliceval na 14.b člen Zakona o zbirkah s področja zdravstvenega varstva (ZZPPZ) ter na člen 6(4) Splošne uredbe ter točki (d) in (e) člena 6(1) ter točko (i) člena 9(2) Splošne uredbe.

Informacijski pooblaščenec je poudaril, da med podatke o zdravstvenem stanju tako šteje tudi podatek o tem, ali je določena oseba cepljena ali ne. Obdelava posebnih vrst osebnih podatkov je skladno s členom 9(1) Splošne uredbe praviloma prepovedana, izjemoma je dopustna in zakonita, če je izpolnjen vsaj eden od pogojev, ki jih določa člen 9(2) Splošne uredbe. Informacijski pooblaščenec je odločil, da pride v konkretnem primeru v poštev točka (i) drugega odstavka člena 9 Splošne uredbe, ki določa, da je obdelava posebnih vrst osebnih podatkov dovoljena, kadar je obdelava potrebna iz razlogov javnega interesa na področju javnega zdravja, kot je zaščita pred resnimi čezmejnimi tveganji za zdravje ali zagotovitev visokih standardov kakovosti in varnosti zdravstvenega varstva ter zdravil ali medicinskih pripomočkov, na podlagi prava Unije ali prava države članice, ki zagotavlja ustrezne in posebne ukrepe za zaščito pravic in svoboščin posameznika, na katerega se nanašajo osebni podatki, zlasti varovanje poklicne skrivnosti. Relevantna določba prava države članice je, kot je izpostavil tudi NIJZ, določba 14.b člena ZZPPZ, ki določa, da je CRPP zbirka podatkov eZdravja o pacientih s stalnim ali začasnim prebivališčem v Republiki Sloveniji in o drugih pacientih, ki v Republiki Sloveniji prejmejo zdravstveno oskrbo. CRPP vsebuje naslednje podatke o pacientih iz prejšnjega odstavka: povzetek podatkov o pacientu in pacientovo zdravstveno dokumentacijo iz prvega odstavka 1. a člena tega zakona. Povzetek podatkov o pacientu vsebuje med drugim tudi pacientove zdravstvene podatke brez časovne omejitve, tudi podatke o cepljenjih. Namen obdelave osebnih podatkov v CRPP je določen v tretjem odstavku 14.b člena ZZPPZ, in sicer se osebni podatki v CRPP obdelujejo z namenom, da se izvajalcem v Republiki Sloveniji in v tujini omogoči dostop do podatkov in izmenjava podatkov za izvajanje zdravstvene oskrbe in mrliško pregledne službe ter z namenom ažuriranja podatkov zdravstvene dokumentacije. Kontaktno podatke pacienta iz CRPP lahko izvajalci in NIJZ uporabijo za obveščanje pacienta o spremembah podatkov v CRPP in drugih zbirkah eZdravja, posredovanje ključev za elektronsko identifikacijo pacienta, izvedbo stikov s pacientom pred načrtovano zdravstveno storitvijo, posredovanje informacij in navodil v povezavi z načrtovano zdravstveno storitvijo, vabilo pacienta na izvedbo zdravstvene storitve, izvajanje zdravstvene storitve na daljavo ter spremljanje izkušenj pacienta in izidov zdravstvene obravnave po izvedbi zdravstvene storitve, pri čemer je treba upoštevati predpise s področja varstva osebnih podatkov glede tehničnih ukrepov za zagotavljanje varnosti podatkov pri komunikaciji.

Na podlagi navedenega je Informacijski pooblaščenec presodil, da se je določba tretjega odstavka 14.b člena ZZPPZ v povezavi s točko (i) člena 9(2) Splošne uredbe šteje kot pravna podlaga, ki NIJZ skladno z njegovimi pristojnostmi dopušča, da uporabi kontaktno podatke pacienta iz CRPP, med drugim za pošiljanje vabil na izvedbo zdravstvene storitve, torej tudi za pošiljanje vabil k cepljenju proti covid-19.

Ob tem je Informacijski pooblaščenec izpostavil, da ima pacient možnost, da s pisno izjavo prepove vpogled v povzetek podatkov o pacientu (med katere spada tudi podatek o cepljenju), prav tako lahko pacient s pisno izjavo omeji uporabo svojih kontaktnih podatkov.

## Obveščanje zaposlenih o pozitivno testiranih sodelavcih na covid-19

Informacijski pooblaščenec je vodil več inšpekcijskih postopkov v zvezi z obravnavanjem dopustnosti obveščanja zaposlenih o sodelavcih, ki so prejeli pozitiven izvid po testiranju na covid-19. Tovrstno obveščanje zaposlenih se lahko vrši zgolj v primerih, ko obstaja ustrezna pravna podlaga za obdelavo posebnih vrst osebnih podatkov (v tem primeru podatkov o zdravstvenem stanju posameznika) skladno s členom 9 Splošne uredbe, npr. skladno s točko (h) člena 9(2) Splošne uredbe, če je obdelava potrebna za namene preventivne medicine ali medicine dela, oceno delovne sposobnosti zaposlenega, zdravstveno diagnozo, zagotovitev zdravstvene ali socialne oskrbe ali zdravljenja ali upravljanje sistemov in storitev zdravstvenega ali socialnega varstva na podlagi prava Unije ali prava države članice ali v skladu s pogodbo z zdravstvenim delavcem ter zanjo veljajo pogoji in zaščitni ukrepi iz odstavka 3, ob upoštevanju splošnih načel za obdelavo osebnih podatkov (člen 5 Splošne uredbe). Upravljevec mora posamezniku ob pridobitvi njegovih osebnih podatkov posredovati tudi informacije o obdelavi osebnih podatkov, kot to določa člen 13 Splošne uredbe. Upravljevec mora posamezniku zagotoviti npr. naslednje informacije: informacije o upravljavcu osebnih podatkov, namenih in pravni podlagi za obdelavo osebnih podatkov, uporabnikih oz. kategorijah uporabnikov osebnih podatkov, prenosu osebnih podatkov, roku hrambe, pravicah skladno s Splošno uredbo itd.

Informacijski pooblaščenec je med drugim vodil inšpekcijski postopek zoper upravljavca, ki je vsem zaposlenim, ki bi se lahko nahajali v objektu, v katerem ima zavezanec sedež, po elektronski pošti posredoval podatek o osebi, ki je zbolela za covid-19, in sicer njeno ime in priimek. V elektronskem sporočilu je upravljavec tudi pojasnil, kdaj je bil zaposleni zadnji dan v službi, kdaj je zbolel ter da nihče od zaposlenih nima oz. ni poročal o zdravstvenih težavah v zadevnem tednu. Prav tako je predstavnik NIJZ upravljavcu sporočil, da je preteklo več kot 48 ur od zadnjega stika, zaposleni pa zdravstvenih težav niso imeli, zato odreditev karantene za osebe, ki so z obolelim imele stik, ni bila potrebna. Elektronsko sporočilo je bilo poslano tudi drugima upravljavcema, in sicer upravljavcu, s katerim si deli prostore (skupni prostori, skupni hodniki, dvigalo ...), ter upravljavcu, katerega sodelavci vsakodnevno prihajajo na sedež upravljavca (hišnik, kurir ...).

Informacijski pooblaščenec je ugotovil, da bi upravljavec lahko z namenom zagotavljanja varnega in zdravega življenjskega okolja in varovanja javnega zdravja vsebino sporočila oblikoval brez navedbe imena in priimka zaposlenega, obvestil pa bi lahko zgolj osebe, ki so se 48 ur ali (upoštevajoč morebitno daljšo inkubacijsko dobo) do 15 dni pred tem nahajale v tej stavbi. Upravljevec skladno s takrat veljavnim protokolom za obvladovanje širjenja okužbe s SARS-CoV-2 na delovnih mestih v času razglašene epidemije, ki ga je pripravil NIJZ, namreč visoko tveganih stikov v konkretnem primeru ni iskal in tudi ni ugotovil, ali se je obolela oseba na sedežu upravljavca v času 48 ur (ali tudi 15 dni), preden je zbolela, sploh nahajala. Tudi ni pojasnjeno, kje na sedežu upravljavca, če sploh, se je zadnjega dne, ko je bila v službi, obolela oseba nahajala in ali je prišla v stik z drugimi posamezniki. Dodatno pa se je tudi NIJZ še pred pošiljanjem zadevnega elektronskega sporočila opredelil, da karantena drugih oseb, ki bi z obolelo osebo lahko prišle v stik ni potrebna (poteklo je namreč že več kot 48 ur od zadnjega morebitnega stika, nihče od drugih zaposlenih pa ni sporočil, da ima simptome).

Informacijski pooblaščenec je poudaril, da mora upravljavec pri obdelavi podatkov o zdravstvenem stanju zagotavljati iskanje t. i. visoko tveganega stika med zaposlenimi tako, da podatek o obolevnosti za covid-19 pri zaposlenem posreduje zgolj osebam, ki so z obolelo osebo prišle v visoko tvegan stik, in sicer upoštevajoč delovno okolje, naravo dela v konkretnih notranjih organizacijskih enotah in možne potencialne stike med zaposlenimi in drugimi obiskovalci prostorov. Na takšen način se v praksi upošteva načelo najmanjšega obsega podatkov ter vsakokratna navodila, priporočila in mnenja zdravstvene stroke.

V postopku je bilo tako ugotovljeno, da se je obveščanje zaposlenih z imenom in priimkom vršilo brez pravne podlage (nezakonita obdelava osebnih podatkov), upravljavec pa je kršil tudi načelo najmanjšega obsega podatkov, saj bi enak učinek in preventivni ukrep varovanja javnega zdravja lahko dosegel že s splošnim obvestilom brez navedbe imena in priimka, ki bi ga prav tako lahko poslal vsem deležnikom, v kolikor bi ugotovil, da je v določenih prostorih in v določenem obdobju lahko prišlo do t. i. visoko tveganega stika.

Informacijski pooblaščenec je prav tako ugotovil, da upravljavec zaposlenim in obolelim za boleznijo covid-19 ob zbiranju in posredovanju osebnih podatkov ni zagotovil informacij skladno z členom 13 Splošne uredbe. Informacije bi moral zagotoviti v jedrnatih, preglednih, razumljivih in lahko dostopnih oblikah ter jasnim in



preprostem jeziku, kot to zahteva člen 12 Splošne uredbe. Informacije je treba zagotoviti na način, ki je pri zavezancu sicer običajen način obveščanja zaposlenih, kot je npr. splošno obvestilo vsem zaposlenim prek e-pošte, na oglasni deski pri upravljavcu, na intranetni strani upravljavca itd.

Odgovorni osebi upravljavca je bila zaradi ugotovljenih kršitev izrečena globa v višini 830 EUR.

### **Neustrezno informiranje vlagateljev prijave interesa za cepljenje**

V Republiki Sloveniji je v letu 2021 prek portala eUprava potekalo obsežno zbiranje podatkov posameznikov o interesu za cepljenje. Posamezniki so pri oddaji vloge za sporočanje interesa za cepljenje prejeli nejasne in skope informacije, dodatne nejasnosti glede pomena same vloge pa so povzročala tudi nasprotujoča si tolmačenja posameznih govorcev na novinarskih konferencah Vlade RS. V javnosti je bilo mogoče večkrat zaslediti trditev, da se lahko posameznik uvrsti na seznam za cepljenje prek podane vloge na portalu eUprava, vendar pa posamezniku ta namen obdelave osebnih podatkov nikoli ni bil izrecno in nedvoumno sporočen. Informacijski pooblaščenec je s ciljem zaščite pravic posameznikov zavezancem, in sicer Ministrstvu za javno upravo RS, Ministrstvu za zdravje RS in NIJZ, dne 16. 3. 2021 izdal začasno odločbo, s katero jim je naložil obveznost zagotovitve jasnih, točnih in zanesljivih informacij iz člena 13 Splošne uredbe, med drugim podatkov o tem, kdo upravlja z osebnimi podatki, kakšni so nameni obdelave osebnih podatkov ter kakšna je pravna podlaga za obdelavo osebnih podatkov. Informacijski pooblaščenec je prav tako omejil nadaljnjo obdelavo zbranih osebnih podatkov. Ugotovljeno je bilo, da od začetka zbiranja podatkov (december 2020) do izdaje začasne odločbe do podatkov ni dostopal nihče, pristojni državni organi pa so posameznike pozivali k oddaji prijave za cepljenje le pri njihovih osebnih zdravnikih. To je pod vprašaj postavilo tako nujnost množičnega zbiranja podatkov kakor tudi njihovo ažurnost (glede na to, da je v zadevnem obdobju hkrati potekalo cepljenje po določenem vrstnem redu, skladno z nacionalno strategijo cepljenja).

Informacijski pooblaščenec je inšpekcijski postopek dne 26. 4. 2021 ustavil, saj je NIJZ posameznike obvestil o namenu zbiranja osebnih podatkov. Iz postopka izhaja, da so bili posamezniki zavedeni, saj se zaradi nasprotujočih si informacij, ki so jih prejeli, in različnih možnih poti prijave na cepljenje niso mogli ustvariti enotne in prave slike o sistemu prijavljanja na cepljenje.

### **Preverjanje zakonitosti obdelave osebnih podatkov slovenskih politikov in ustreznost zagotavljanja sledljivosti v zbirkah osebnih podatkov**

Informacijski pooblaščenec je po uradni dolžnosti uvedel inšpekcijski postopek zoper upravljavca Ministrstvo za notranje zadeve, Policija, z namenom preverjanja zakonitosti obdelave in ustreznosti zagotavljanja sledljivosti obdelave osebnih podatkov v elektronsko vodenih zbirkah osebnih podatkov s strani za to pooblaščenih oseb pri upravljavcu. V okviru inšpekcijskega postopka se je še posebej preverjalo, katere osebe so v obdobju od 1. 1. 2019 do 18. 2. 2020 v elektronskih zbirkah vpogledovale v osebne podatke predsednikov parlamentarnih strank, vodij poslanskih skupin ter nekaterih poslancev.

V postopku, ki ga je Informacijski pooblaščenec zaključil v začetku leta 2021, je bilo ugotovljeno, da lahko zaposleni pri upravljavcu dostopajo do evidenc policije, ki se vodijo na podlagi Zakona o nalogah in pooblastilih policije (ZNPPol), Zakona o prekrških (ZP-1), Zakona o nadzoru državne meje (ZNDM-2) in drugih predpisov, ki določajo naloge in pristojnosti policije. Dostopajo pa lahko tudi do zbirk drugih upravljavcev, do katerih ima policija po zakonu pravico do dostopa (npr. CRP, MRVL itd.). Dostop do informacijskega sistema policije je mogoč s pomočjo uporabniškega imena in gesla, uporabnik pa lahko dostopa zgolj do zbirk podatkov, za katere je pooblaščen glede na svoje delovne naloge in pristojnosti. Vsaka prijava v sistem se zabeleži v evidenco vpogledov, ki jo lahko pri upravljavcu pregledujeta zgolj dve osebi v vnosom uporabniškega imena in gesla.

Glede vpogledov v podatke predsednikov parlamentarnih strank, vodij poslanskih skupin ter nekaterih poslancev (skupno 45 oseb) je Informacijski pooblaščenec ugotovil, da je osebne podatke obdelovalo 700 zaposlenih na policiji. Eden od zaposlenih je obdeloval osebne podatke sedmih politikov, štirje zaposleni so obdelovali osebne podatke šestih politikov, sedem zaposlenih je obdelovalo osebne podatke petih politikov, osem zaposlenih je obdelovalo osebne podatke štirih politikov, preostali pa so večinoma obdelovali osebne podatke enega, redkeje tudi dveh ali treh politikov. Osebne podatke posameznih politikov je obdelovalo tudi po več kot 50 zaposlenih, in sicer v primerih, ko je policija v zvezi s posameznim dogodkom izvajala varovanje oseb. Kadar so zaposleni obdelovali podatke večjega števila politikov (štiri do največ sedem) so

obdelave osebnih podatkov večinoma izvajali zaradi sodelovanja pri varovanju oseb, in sicer tako, da so podatke v zvezi z varovanjem vnašali v evidence, kar se šteje kot zakonita obdelava osebnih podatkov. Pri tovrstnih obdelavah se praviloma ne vpogleduje v policijske in druge evidence, obdelava pa se kljub temu zabeleži v dnevniku obdelav in se prikaže na izpisu obdelav osebnih podatkov za določenega posameznika.

Uslužbenci policije (59), ki so izvajali obdelave osebnih podatkov vidnejših slovenskih politikov in sorodnika enega od njih, so osebne podatke obdelovali:

- na podlagi 121. člena ZNPPol s tem, ko so skrbeli za skladnost osebnih podatkov z ugotovitvami, informacijami in podatki, zbranimi pri opravljanju policijskih nalog;
- zaradi opravljanja nalog iz 112. in 123. člena v povezavi s 4. členom ZNPPol s tem, da so zbrane podatke vnesli v evidence policije;
- skladno s 84. členom Pravil policije s tem, ko so vpisovali sporočila, obvestila, naročila, ugotovitve in ukrepe v svoje poročilo ter dopolnjevali dnevnik dogodkov operativno komunikacijskega centra s časovnimi podatki o poteku posameznih dogodkov in izvedbi posameznih ukrepov;
- zaradi opravljanja nalog iz 112. člena v povezavi s 4. členom ZNPPol zaradi preprečevanja, odkrivanja in preiskovanja kaznivih dejanj;
- zaradi opravljanja nalog iz 112. člena v povezavi s 4. členom ZNPPol pri nadzoru državne meje;
- zaradi opravljanja nalog iz 112. člena v povezavi s 4. členom ZNPPol pri varovanju življenja, osebne varnosti in premoženja ljudi;
- zaradi opravljanja nalog iz 112. člena v povezavi s 4. členom ZNPPol zaradi preprečevanja, odkrivanja in preiskovanja prekrškov;
- zaradi opravljanja nalog iz 112. člena v povezavi s 4. členom ZNPPol in nalog iz 31. člena Zakona o organiziranosti in delu v policiji (ZODPol) pri preverjanju suma, da je policist neupravičeno obdeloval osebne podatke;
- zaradi opravljanja nalog iz 112. člena v povezavi s 4. členom ZNPPol pri varovanju določenih oseb, prostorov, objektov in okoliša objektov, varovanju določenih delovnih mest in tajnosti podatkov državnih organov;
- pri odrejanju nalog, ki jih morajo opraviti policisti in
- v enem primeru zaradi opravljanja nalog iz 112. člena v povezavi s 4. členom ZNPPol (obdelava osebnih podatkov občana z enakim imenom in priimkom, kot ga ima eden od slovenskih poslancev).

Informacijski pooblaščenec je opravil tudi pregled evidenc in dokumentacije v zvezi z obdelavo osebnih podatkov poslanca, ki je v javnosti zatrjeval, da so ga policisti preverjali malo pred polnočjo, dne 24. 12. 2019. V postopku je bilo ugotovljeno, da je zadevno obdelavo dne 24. 12. 2019 izvedel policist PP Murska Sobota, ki je v aplikacijo E-RISK vpisal iskalne parametre za osebo z imenom in priimkom, ki sta bila enaka imenu in priimku poslanca. V konkretni zadevi je namreč patrulja v okviru opravljanja policijske naloge obravnavala osebo z istim imenom in priimkom, kot ga ima poslanec, zato je bila opravljena poizvedba na podlagi iskalnih parametrov imena in priimka. Pri tem se pri takšni poizvedbi iz CRP pridobijo podatki o vseh osebah po iskalnem parametru in uporabnik pri tem vidi navedbo vseh oseb, ki ustrezajo poizvedbi (ime, priimek, EMŠO, datum rojstva, državo in kraj rojstva, prebivališče in državljanstvo). Na podlagi prikazanih podatkov se nato uporabnik odloči, od katere točno določene osebe potrebuje nadaljnje podrobnosti (npr. seznam naslovov, davčno številko, spremembo osebnega imena, seznam vozil, seznam listin itd.). V konkretnem primeru je torej uporabnik najprej napravil poizvedbo po imenu in priimku, nato pa je nadaljeval z vpogledom v osebne podatke osebe, ki je bila dejansko obravnavana, iz česar je bilo razvidno, da ni šlo za vpogled v osebne podatke poslanca, temveč za zakonito obdelavo osebnih podatkov posameznika z enakim imenom in priimkom.

Informacijski pooblaščenec v predmetnem postopku ni ugotovil nepravilnosti glede zagotavljanja sledljivosti obdelave osebnih podatkov v elektronsko vodenih zbirkah zavezanca, prav tako ni ugotovil sistematičnih nezakonitih vpogledov v osebne podatke politikov s strani uslužbencev policije. Sum nezakonitih vpogledov je Informacijski pooblaščenec zaznal zgolj pri dveh uslužbencih policije, in sicer je v enem primeru upravljavec sum nezakonite obdelave osebnih podatkov zaznal že pred uvedbo inšpekcijskega postopka in predlagal uvedbo postopka o prekršku, v drugem primeru pa je Informacijski pooblaščenec na podlagi ugotovitev v predmetnem postopku uvedel postopek o prekršku po uradni dolžnosti. Eden od teh postopkov je še v teku, drugi pa ustavljen, saj je bil kršitelj za ista ravnanja že pravnomočno obsojen za kazniva dejanja.

### 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 doseg 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 2021 prejel dve vlogi za izdajo dovoljenja za uvedbo biometrijskih ukrepov in izdal eno odločbo. Eno vlogo za izvajanje biometrijskih ukrepov je zavrnil, ker je vlagatelj želel uvesti biometrijske ukrepe z uporabo čitalnika prstnega odtisa zaradi dostopanja zaposlenih do strežniške sobe vlagatelja na njegovem sedežu. Izvajanje biometrijskih ukrepov je skladno z določbo prvega odstavka 80. člena ZVOP-1 v primeru, če vlagatelj izkaže, da je izvajanje teh ukrepov za varstvo ene od tam naštetih pravnih dobrin nujno potrebno. Vlagatelj v postopku ni navedel ali izkazal, na kakšen način bi lahko bile njegove poslovne skrivnosti ogrožene, če za kontrolo dostopa do strežniške sobe ne bi izvajal biometrijskih ukrepov. Prav tako ni konkretiziral nujne potrebnosti uporabe biometrijskih ukrepov za varstvo naštetih dobrin, temveč je podal zgolj splošno obrazložitev. V enem primeru je vlagatelj vlogo umaknil, zato je Informacijski pooblaščenec postopek ustavil.

#### 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. Informacijski pooblaščenec povezavo dovoli na podlagi pisne vloge upravljavca osebnih podatkov, če ugotovi, da upravljavec 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.

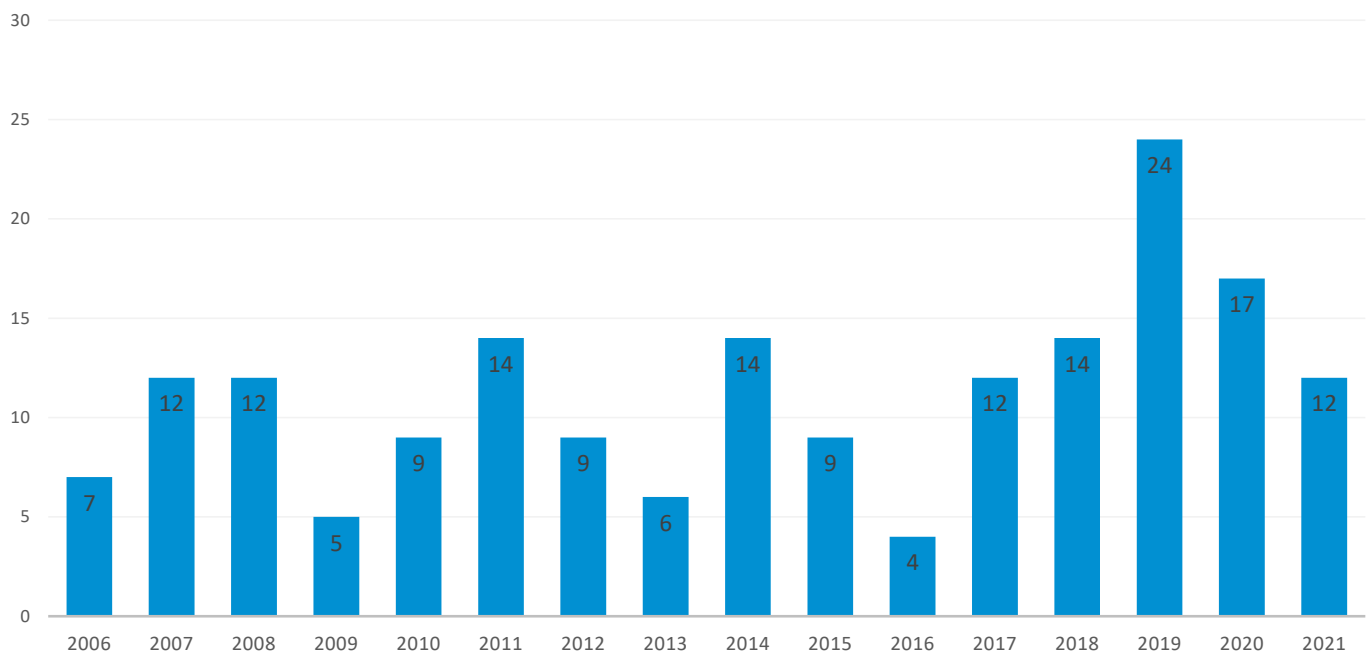
Informacijski pooblaščenec je leta 2021 prejel 19 vlog za pridobitev dovoljenja za povezovanje zbirk osebnih podatkov. Izdal je 12 odločb, in sicer 11 odločb, s katerimi je upravljavcem povezovanje zbirk osebnih podatkov dovolil, ter eno odločbo, s katero povezovanja zbirk osebnih podatkov ni dovolil. Trije vlagatelji so vlogo umaknili, zato je Informacijski pooblaščenec postopke ustavil, eno vlogo pa je zavrnil, saj vlagatelj v vlogi ni uveljavljal kakšne svoje pravice ali pravne koristi oziroma ni mogel biti stranka v postopku.

Izdane odobrene odločbe glede povezovanja javnih evidenc.

Upravljavec 1	Zbirka osebnih podatkov 1	U
1. Državna volilna komisija	Zbirka list kandidatov Zbirka predlaganih članov volilnih odborov in volilnih komisij	M
2. Olimpijski komite Slovenije – Združenje športnih zvez	Evidenca registriranih in kategoriziranih športnikov	M
3. Ministrstvo za infrastrukturo RS	Evidenca voznikov, ki so usposobljeni za vožnjo motornih vozil za prevoz potnikov ali blaga v cestnem prometu	M
4. Urad Vlade RS za varovanje tajnih podatkov	Informacijski sistem EUPP-UVTP za vodenje postopkov izdaje in preklica dovoljenj za dostop do tujih tajnih podatkov	M
5. Agencija RS za javnopravne evidence in storitve	Register transakcijskih računov	M F A
6. Finančna uprava RS	Evidenca o davčni izvršbi Evidenca o davkih	G N P U S T
7. Finančna uprava RS	Evidenca o davkih Evidenca motornih vozil finančne uprave	M
8. Onkološki inštitut Ljubljana	Register raka	N
9. Ministrstvo za notranje zadeve RS	Centralna evidenca o dovoljenjih za prebivanje in odpovedih prebivanja tujcem (Register tujcev)	F
10. Rekono, sistemske integracije, d. o. o.	Evidenca imetnikov kvalificiranih potrdil	M
11. Študentska organizacija Slovenije	Evidenca študentskega dela	T

<b>Upravitelj</b>	<b>Zbirka osebnih podatkov</b>	<b>Povezovalni znak</b>
Ministrstvo za notranje zadeve RS	Evidenca volilne pravice	EMŠO
Ministrstvo za notranje zadeve RS	Centralni register prebivalstva	EMŠO
Ministrstvo za infrastrukturo RS	Evidenca o voznških dovoljenjih	EMŠO
Ministrstvo za notranje zadeve RS	Centralni register prebivalstva	EMŠO
Ministrstvo za notranje zadeve RS	Centralni register prebivalstva	davčna številka
Finančna uprava RS	Davčni register	
Agenacija RS za javnopravne evidence in storitve	Poslovni register Slovenije Register dejanskih lastnikov	
Generali investments, d. o. o. ILB Skladi, d. o. o. Primorski skladi, d. o. o. Upravljanje z investicijskimi skladi, d. o. o. ava Infond, d. o. o. riglav Skladi, d. o. o.	Evidenca imetnikov investicijskih kuponov pri posameznih družbah za upravljanje	davčna številka
Ministrstvo za infrastrukturo RS	Evidenca registriranih vozil	VIN številka in EMŠO
NIJZ	Evidenca nalezljivih bolezni	EMŠO
Finančna uprava RS	Evidenca o davkih	EMŠO
Ministrstvo za notranje zadeve RS	Centralni register prebivalstva	davčna številka
ur servis, d. o. o.	Zbirka osebnih podatkov dijakov in študentov, ki so opravljali študentsko delo	EMŠO

Število vlog za izdajo odločbe glede povezljivosti zbirk osebnih podatkov med letoma 2006 in 2021.



### 3.3.3 PRENOS OSEBNIH PODATKOV V TRETJE DRŽAVE

Splošna uredba ureja prenos podatkov v tretje države in mednarodne organizacije v V. poglavju. Prenos je dovoljen, če obstaja ena izmed naslednjih pravnih podlag:

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

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

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

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

**Informacijski pooblaščenec v letu 2021 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 bile v letu 2021 posodobljene in so dostopne na tej povezavi.

Leta 2021 je sta bili v zvezi s prenosi podatkov v tretje države sprejeti dve pomembni novosti. Evropska komisija je sprejela sklepa o ustreznosti ravni varstva osebnih podatkov (po Splošni uredbi in po Direktivi za organe kazenskega pregona) v Združenem kraljestvu Velike Britanije in Severne Irske, ki se je po t. i. brexitu uvrstilo med tretje države, s katerima je ugotovila, da Združeno kraljestvo zagotavlja raven varstva osebnih podatkov, ki je v bistvu enakovredna tej v EU. To v praksi pomeni, da subjektom iz EU (tudi EGP), ki podatke prenašajo drugim upravljavcem ali obdelovalcem v Združeno kraljestvo, ni treba vzpostaviti nobenih dodatnih orodij za prenos osebnih podatkov (npr. standardnih pogodbenih določil). Evropska komisija je leta 2021 sprejela tudi nove standardne pogodbene klavzule, ki služijo kot podlaga za prenos

osebnih podatkov v tretje države in so modularnega značaja, kar pomeni, da vključujejo različne scenarije obdelave osebnih podatkov oz. t. i. module, ki jih pogodbeni stranki izbereta glede na konkretne okoliščine prenosa: EU upravljavec – neEU upravljavec, EU upravljavec – neEU obdelovalec, EU obdelovalec – neEU obdelovalec in EU obdelovalec – neEU upravljavec). Nove klavzule krepijo pravice posameznikov, tako da jim omogočajo, da so obveščeni o postopkih obdelave njihovih podatkov, da imajo možnost vzpostaviti stik s tujimi upravljavci, da prejmejo kopijo sklenjenih klavzul, odškodnino za škodo, povzročeno v zvezi z njihovimi osebnimi podatki, itd. Več informacij o novih standardnih pogodbenih klavzulah je dostopnih v prenovljenih smernicah.

### 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 lahko ti podatki v enaki obliki vključijo oz. uporabljajo pri drugem upravljavcu. Lahko pa te podatke posameznik 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.

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 vložiti pritožbo pri Informacijskem pooblaščenca.

Za zahteve posameznikov, ki se nanašajo na področje preprečevanja, odkrivanja, preiskovanja in pregona kaznivih dejanj ter izvrševanja kazenskih sankcij, se uporablja ZVOPOKD. ZVOPOKD 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 navedenih pristojnosti. Skladno s Splošno uredbo in ZVOPOKD je Informacijski pooblaščenec pritožbeni organ za uveljavljanje vseh pravic, ne le pravice do seznanitve, kot je veljalo po ZVOP-1 (ki se je v letu 2021 še uporabljal za zahteve posameznikov, ki se nanašajo na področje preprečevanja, odkrivanja, preiskovanja in pregona kaznivih

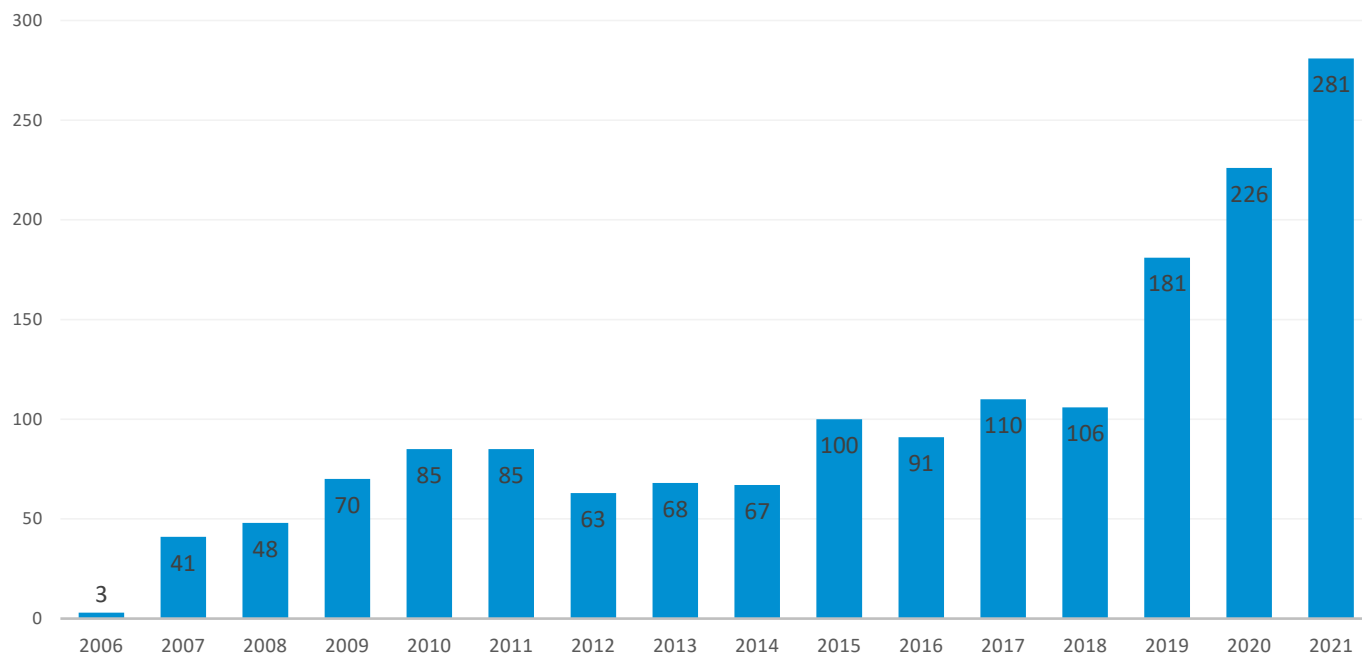
dejanj ter izvrševanja kazenskih sankcij, in sicer v zvezi z zahtevami, podanimi pred uveljavitvijo ZVOPOKD, ter za zahteve upravljavcem, ki niso zavezanci niti po Splošni uredbi niti po ZVOPOKD).

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 2021 prejel 281 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 2020 je prejel 55 pritožb več (tj. 24 % več). Zaključiti je mogoče, da se posamezniki vedno bolj zavedajo svoje ustavne pravice do seznanitve s svojimi osebnimi podatki, številni upravljavci pa še vedno ne izpolnjujejo svojih obveznosti in posameznikom ne omogočajo izvrševanja pravic, ki jim jih zagotavljajo različni predpisi.**

*Število pritožb v zvezi s pravico do seznanitve z lastnimi osebnimi podatki med letoma 2006 in 2021.*



Vložene pritožbe so v 101 primeru zadevale upravljavce iz javnega sektorja (zlasti ministrstva in organe v njihovi sestavi, šole, javne zdravstvene zavode in centre za socialno delo), 180 pritožb pa se je nanašalo na upravljavce iz zasebnega sektorja (npr. banke, zavarovalnice, operaterje elektronskih komunikacij, trgovska podjetja in druge gospodarske družbe). Le 33 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, ZVOPOKD oz. ZVOP-1. V 179 primerih (torej v 64 %) 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 zavrnil 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 176 primerih, ki so se vodili zaradi molka upravljavca (vključno s postopki, ki so se začeli pred letom 2021), so upravljavci po prejemu poziva Informacijskega pooblaščenca o zahtevah posameznikov odločili na način, da so jim posredovali zahtevane podatke in dokumente ali zahteve obrazloženo zavrnil 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 2021 je Informacijski pooblaščenec, vključno s postopki, začetimi v letih 2019 in 2020, izdal 102 upravni odločbi, kar je 59 % več kot leta 2020. V 27 odločbah je pritožbam posameznikov v celoti ugodil in upravljavcem naložil posredovanje določenih osebnih podatkov, v 22 primerih je pritožbam ugodil delno, s 53 odločbami pa je pritožbe posameznikov kot neutemeljene zavrnil. Dva posameznika sta zoper odločitve Informacijskega pooblaščenca sprožila upravni spor pred Upravnim sodiščem RS, in sicer eden zoper zavrnilno in eden zoper delno ugodeno odločbo, izdano v letu 2021.

Informacijski pooblaščenec je s sklepom zavrgel 10 pritožb, in sicer 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). 122 posameznikom je Informacijski pooblaščenec posredoval predlog za ravnanje, eno pritožbo pa je odstopil v reševanje pristojnim organom.

Leta 2021 je Informacijski pooblaščenec obravnaval tudi tri pritožbe zaradi kršitve pravice do popravka po členu 16 Splošne uredbe in 29 pritožb zaradi kršitve pravice do izbrisa po členu 17 Splošne uredbe. Vključno s postopki, začetimi v preteklih letih, je Informacijski pooblaščenec zaradi kršitve pravice do izbrisa in popravka izdal 11 odločb, in sicer je v osmih zadevah pritožbe zavrnil, trem pa je v celoti ugodil. Zoper eno zavrnilno in dve ugodilni odločbi so posamezniki vložili tožbo pred Upravnim sodiščem RS. V desetih zadevah je bila nadalje pritožba zavržena (ker je bila nedovoljena, prepozna, ni bila dopolnjena oz. posameznik ni uveljavljal kakšne svoje pravice oz. pravne koristi), v desetih je bil postopek ustavljen (v osmih zadevah zato, ker je upravljavec zahtevi ugodil in v dveh zaradi umika pritožbe), v dveh zadevah Informacijski pooblaščenec postopka ni uvedel, v eni zadevi je posamezniku podal predlog za ravnanje, v eni zadevi pa je bila pritožba odstopljena v reševanje pristojnemu organu.

V zvezi s pritožbami po ZVOPOKD je Informacijski pooblaščenec izdal pet odločb, in sicer je v dveh odločbah pritožbama posameznikov v celoti ugodil, v enem primeru je pritožbi ugodil delno, z dvema odločbama pa je pritožbi posameznikov kot neutemeljeni zavrnil. V treh zadevah je pritožbo zavrgel (iz postopkovnih oz. formalnih razlogov), v petih zadevah je postopek ustavil (v štirih primerih zato, ker upravljavec ni bil več v molku, in v eni zadevi zaradi umika pritožbe), v eni zadevi pa Informacijski pooblaščenec za odločanje ni bil pristojen.

### 3.3.5 IZBRANI PRIMERI V ZVEZI Z OBRAVNAVANJEM PRAVIC POSAMEZNIKOV

V nadaljevanju so predstavljeni nekateri primeri v zvezi s pritožbami, ki jih je obravnaval Informacijski pooblaščenec in se nanašajo na pravice posameznikov po Splošni uredbi.

#### **Pravica do seznanitve staršev z osebnimi podatki mladoletnih otrok v primerih centrov za socialno delo**

Pravice glede varstva osebnih podatkov v imenu otrok, dokler so ti mladoletni, praviloma uresničujejo starši (oz. zakoniti zastopniki). Pri nobeni pravici, ki se nanaša na obdelavo osebnih podatkov, Splošna uredba o varstvu podatkov ne določa, kdaj ali v kakšnih okoliščinah jo lahko uveljavljajo starši oz. kdaj in v kakšnih okoliščinah jih lahko v zvezi s svojimi osebnimi podatki uveljavlja otrok sam, pri tem pa mora upravljavec pri odločanju upoštevati tudi vprašanje zavarovanja največje koristi otroka.

V primeru, ki ga je obravnaval Informacijski pooblaščenec, je prosilec kot zakoniti zastopnik (starš, ki mu sicer ni bila odvzeta starševska skrb) zahteval določene podatke iz spisov centra za socialno delo (CSD), ki so se nanašali na njegovega mladoletnega otroka. CSD je zavrnil pravico prosilca do dostopa do zahtevanih osebnih podatkov in izpostavil, da je bil proti staršu, ki je podal zahtevo, v veljavi ukrep prepovedi približevanja, da je bil otrok obravnavan kot žrtev nasilja v družini po Zakonu o preprečevanju nasilja v družini (v nadaljevanju ZPND), dokumenti v spisu pa so zajemali tudi zapečateni dokumente.

V tem primeru je Informacijski pooblaščenec s ciljem zavarovanja pravic otroka pritrdil utemeljitvi centra za socialno delo, ki je zavzel strokovno stališče, da mora kot institucija omogočiti otroku zaupnost, če s tem zaščiti največjo korist otroka in mu zagotovi varen prostor, kjer se lahko otrok izrazi. Prav tako je Informacijski pooblaščenec potrdil stališče upravljavca, ki je v tehtanju pravic prosilca in njegovega otroka presodil, da imajo pravice in koristi mladoletnega otroka prednost pred koristmi in pravicami drugih

udeležencev v postopku, med drugim zaradi načela otrokove koristi ter posebnega varstva in skrbi za otroke, ki ga uteleša Konvencija o otrokovih pravicah ter ga zagotavlja 56. člen Ustave Republike Slovenije in Družinski zakonik. Tudi Informacijski pooblaščenec je v postopku opravil tehtanje med pravicami, in sicer med pravico prosilca (zakonitega zastopnika otroka) do seznanitve z lastnimi osebnimi podatki ter pravico otroka in drugega starša do zasebnega in družinskega življenja. Ugotovil je, da bi bil posameznik, ki je bil v obravnavi pred centrom za socialno delo zaradi stiske, v kateri se je znašel, v primeru razkritja njegovih osebnih podatkov neprimerno bolj oškodovan, poleg tega bi bil ogrožen sistem zaupnosti dela centra za socialno delo, porušena pa bi bila tudi zaupnost, ki je že bila vzpostavljena med konkretnim posameznikom in centrom za socialno delo. Toliko bolj to velja za primere, ki se obravnavajo skladno z ZPND. Informacijski pooblaščenec je poudaril, da Zakon o socialnem varstvu zavezuje strokovne delavce, da kot poklicno skrivnost varujejo podatke in okoliščine o materialnih in socialnih stiskah posameznika. Skladno s tem je treba varovati vsebino zapisov razgovorov z mladoletnim otrokom in z otrokom povezanih oseb ter zapise upravljalca, ki vsebujejo podrobnosti o otroku in njegovem življenju. Ne glede na to, da prosilcu ni bila odvzeta starševska skrb, mu torej ni bil omogočen dostop do določenih osebnih podatkov mladoletnega otroka iz drugih razlogov ter po tehtanju različnih pravic in interesov, ki so bili v koliziji.

### **Pravica do seznanitve z zdravstveno dokumentacijo in vprašanje omejitev po 22. členu ZPacP**

Pravica do seznanitve z zdravstveno dokumentacijo je urejena v 41. členu ZPacP. Skladno s prvim odstavkom 22. člena ZPacP, ki se na podlagi osmega odstavka 41. člena ZPacP uporablja tudi v zvezi s pravico do seznanitve z zdravstveno dokumentacijo, se sme pacientu le izjemoma zamolčati podatke o njegovem zdravstvenem stanju, če zdravnik glede na okoliščine oceni, da bi mu takšno obvestilo povzročilo resno zdravstveno škodo, razen kadar pacient, ki je sposoben odločanja v svojo največjo zdravstveno korist, izrecno zahteva, da je o svojem zdravstvenem stanju popolnoma obveščen.

Neustreznost obstoječe ureditve pa se je pokazala v eni izmed pritožbenih zadev. Pacient je pri izvajalcu zdravstvene dejavnosti vložil zahtevo za seznanitev z zdravstveno dokumentacijo, ki se nanaša nanj, ta pa je presodil, da bi seznanitev s to dokumentacijo pacientu povzročila resno zdravstveno škodo, zaradi česar je zahtevo zavrnil. Nato je pacient pri istem izvajalcu zdravstvene dejavnosti vložil še izrecno zahtevo za seznanitev z lastno zdravstveno dokumentacijo. Izvajalec zdravstvene dejavnosti je zahtevo vnovič zavrnil, tokrat z utemeljitvijo, da pacient ni sposoben odločanja v svojo korist, in sicer zaradi psihiatričnih izvidov, ki so zabeleženi v njegovem zdravstvenem kartonu. Informacijski pooblaščenec je ocenil, da takšna odločitev brez konkretnejše utemeljitve ne omogoča preizkusa izpodbijane odločitve, saj razlogi za zamolčanje niso bili dovolj določno navedeni. Zato je zadevo z napotki vrnil izvajalcu zdravstvene dejavnosti v ponovno odločanje. Poudaril je, da je treba izjemo od pravice do obveščeniosti pacienta (t. i. terapevtski privilegij oziroma obzirni molk zdravnika) v povezavi s pravico do seznanitve z zdravstveno dokumentacijo razlagati skrajno restriktivno, saj lahko preširoko tolmačenje te izjeme privede do hudega posega v pravico do samoodločanja, osebnega dostojanstva in varstva osebnih podatkov.

Težavo Informacijski pooblaščenec vidi predvsem v tem, da je odločanje na prvi stopnji prepuščeno zgolj enemu zdravniku, pri čemer je pravni standard »odločanja v svojo največjo zdravstveno korist« premalo določen ter posledično omogoča različne razlage, kar vodi v zmanjšano predvidljivost pravnega položaja pacientov. Kot se je izkazalo tudi v konkretni pritožbeni zadevi, v praksi zdravniki svojo odločitev oprejo zgolj na zakonsko določbo (tj. brez navezovanja na konkretno dejansko stanje) ali se pavšalno sklicujejo na splošno zdravstveno stanje pacienta brez konkretnejše obrazložitve, ki bi omogočala instančni preizkus. Pri tem se postavlja tudi vprašanje, ali je pogojevanje uresničitve pravice do seznanitve s sposobnostjo odločanja v svojo največjo zdravstveno korist res utemeljeno oziroma, če je utemeljeno, kdo je pristojen za opravo te presoje. Informacijski pooblaščenec je pisal tudi Ministrstvu za zdravje in Varuhu človekovih pravic ter podal pobudo za presojo ustreznosti obstoječe ureditve.

### **Uresničevanje pravice dostopa do osebnih podatkov pri delodajalcu**

Informacijski pooblaščenec je obravnaval 36 istovrstnih pritožb delavcev zaradi kršitve pravice do dostopa po členu 15 Splošne uredbe, saj delodajalec v predpisanem roku ni odgovoril na njihove zahteve. Ko je o zahtevah naknadno odločil, pa so delavci zoper odgovore vložili vsebinske pritožbe.

V teh pritožbenih postopkih se je kot bistveno izpostavilo vprašanje, na kakšen način lahko delodajalec izkaže, da zahtevane dokumentacije, ki naj bi predstavljala delavčeve osebne podatke, nima. Delodajalec je

namreč zatrjeval, da zahtevane dokumentacije ne hrani in je tudi ni dolžan hraniti, pritožniki pa so vztrajali, da delodajalec kot upravljavec s temi podatki razpolaga, kar so dokazovali s pisnimi izjavami delavcev kot tudi z vzorčnimi listinami. Zato je Informacijski pooblaščenec ugotavljal, ali iz zatrjevanih dejstev in predloženih dokazov izhaja, da delodajalec razpolaga oziroma bi bil vsaj dolžan razpolagati z osebnimi podatki, pri dostopu do katerih so vztrajali pritožniki. Ker je delodajalec logično in razumljivo pojasnil, zakaj z zahtevano dokumentacijo (vloge za vize in spremljajoča dokumentacija) ne razpolaga (prenehanje delovnih razmerij ter narava listin), pri čemer je bila njegova utemeljitev podprta s pisnimi izjavami nekaterih delavcev, je Informacijski pooblaščenec ocenil, da pritožniki niso uspeli dokazati, da delodajalec s spornimi podatki razpolaga. Ker niso izkazali niti, da bi bil delodajalec ob podaji zahtev dolžan hraniti takšne osebne podatke, ki se nanašajo na nanje, Informacijski pooblaščenec tudi ni izvedel oglada v prostorih delodajalca.

Informacijski pooblaščenec ugotavlja, da v posameznih primerih pravico do seznanitve z lastnimi osebnimi podatki vse pogosteje uveljavljajo tudi delavci, ki od delodajalca ne prejmejo podatkov ali listin, do katerih bi načeloma bili upravičeni že na podlagi delovnopravne zakonodaje. Informacijski pooblaščenec je v teh odločbah opozoril, da navedbe v zvezi s sumom ponarejanja dokumentov ter druga delovnopravna oziroma davčnopravna vprašanja ne morejo biti predmet presoje v okviru postopka uveljavljanja pravice do dostopa do osebnih podatkov.

### **Izbris osebnih podatkov, ki jih je zahteval posameznik**

Posameznik ima na podlagi 24. člena ZVOPOKD pravico od policije, državnega tožilstva, Uprave Republike Slovenije za probacijo, Uprave Republike Slovenije za izvrševanje kazenskih sankcij in drugih državnih organov, ki so zakonsko določeni kot pristojni za področja preprečevanja, preiskovanja, odkrivanja ali pregona kaznivih dejanj ali izvrševanja kazenskih sankcij, zahtevati podatek o tem, ali se obdelujejo njegovi osebni podatki, in kopijo ali izpis teh podatkov. Informacijski pooblaščenec je v okviru pritožbenih postopkov po ZVOPOKD odločal o pritožbi obsojenca, ki mu je zavod za prestajanje kazni zapora zavrnil zahtevo za pridobitev kopije videoposnetkov njegovega gibanja v določenih prostorih na določeni dan. Zahteva je bila zavrnjena, ker so bili zahtevani videoposnetki avtomatično izbrisani.

Podzakonski akti in interna pravila zavoda določajo največ enomesečni rok hrambe tovrstnih posnetkov. Toda v pritožbenem postopku je bilo ugotovljeno, da je obsojenec zahtevo vložil pravočasno, predpisani rok hrambe pa se je iztekel tekom odločanja o obsojenčevi zahtevi. To pomeni, da so bili videoposnetki uničeni po tem, ko je obsojenec že vložil zahtevo za seznanitev, in bi jih lahko pridobil, če bi zavod o zahtevi odločil takoj oziroma če bi z aktivnim ravnanjem preprečil njihovo uničenje. Do izbrisa videoposnetkov je prišlo kljub temu, da 16. člen ZVOPOKD določa, da zavod od seznanitve z uvedbo postopka (tj. od vložitve zahteve posameznika) ne sme izbrisati zahtevanih osebnih podatkov, ki so predmet postopka, ne glede na potek rokov hrambe, dokler o zadevi ni pravomočno odločeno. Ker se je izkazalo, da zahtevanih videoposnetkov ni več, je bila pritožba zavrnjena, zoper zavod pa je bil uveden prekrškovni postopek, ker ni preprečil avtomatskega uničenja videoposnetkov oziroma zaradi kršitve zakonske prepovedi izbrisa osebnih podatkov.

S podobnimi primeri avtomatskega ali namernega predčasnega uničenja zahtevanih osebnih podatkov v škodo posameznikov se je Informacijski pooblaščenec v preteklih letih že večkrat srečal. Izkazalo se je, da je zaradi uspešnega uresničevanja pravice do seznanitve zelo pomembno, da upravljavec takoj, ko prejme zahtevo posameznika, prepreči uničenje osebnih podatkov ter ustrezno zavaruje podatke, o katerih se odloča. To mora veljati ne glede na to, ali so v trenutku vložitve zahteve ali v času odločanja o zahtevi že pretekli predpisani ali notranje določeni roki hrambe, pa tudi, če notranje določenih rokov hrambe sploh ni. Posebno prepoved tovrstnega uničenja ima le ZVOPOKD, žal pa take določbe, ki bi veljale za vse upravljavce, ni v ZVOP-1. Zato bo pomembno, da se bo podobno določbo uvrstilo tudi v novi ZVOP-2.

### **Zahteva za dostop do podatkov v zvezi z obravnavo odškodninskega zahtevka in omejitve pravic**

Informacijski pooblaščenec je v okviru pritožbenih postopkov po ZVOPOKD odločal tudi o pritožbi obsojenca, ki mu je bilo zavrnjeno zaprosilo za vpogled v vso dokumentacijo v zvezi z izvrševanjem pripora in zapora. Zaprosilo je bilo zavrnjeno v delu, ki se nanaša na obsežno dokumentacijo v zvezi z reševanjem odškodninskega zahtevka zoper državo. Informacijski pooblaščenec je odločbo upravljavca odpravil in zadevo vrnil v ponovno odločanje zaradi bistvene kršitve postopka. V odločbi namreč ni bilo konkretno utemeljeno, zakaj se lahko pravilo o varstvu zaupnosti podatkov iz mediacijskega postopka po zakonu, ki ureja mediacijo, ter enako pravilo o varstvu zaupnosti podatkov iz predhodnega postopka mirne rešitve spora

po zakonu, ki ureja državno odvetništvo, uveljavlja nasproti oziroma v škodo osebi, ki je kot oškodovanec aktivni udeleženec teh postopkov. Nadalje ni bilo utemeljeno, zakaj naj bi se omenjeno pravilo nanašalo na prav vse dokumente, ki so po vsebini, izvoru in funkciji zelo različni. Upravljavec tudi ni utemeljil, kateri dokumenti se neposredno nanašajo na postopek mirnega reševanja sporov oziroma iz tam izvirajo, in zakaj se na to izjemo sploh lahko sklicuje upravljavec, ki v postopkih ni neposredno sodeloval kot stranka. Brez utemeljitve je ostalo tudi vprašanje, zakaj posameznik ni upravičen niti do dokumentov, ki jih je sodelujočim organom sam poslal ali jih je od teh organov že prejel.

V tej zadevi se je odprlo zanimivo vprašanje, ali in v kakšnem obsegu se lahko posamezniku zavrne dostop do lastnih osebnih podatkov, ki vsebujejo informacije o »notranjem razmišljanju« organov, ki sodelujejo ali odločajo o utemeljenosti in višini odškodnine v postopkih alternativnega reševanja sporov, zlasti če postopki še niso končani. Ni namreč izključeno, da bi se na tak način posameznik lahko seznanil z »internimi« informacijami, ki bi mu morda omogočile neuravnoteženo privilegiran pogajalski položaj, torej v škodo poštenega uresničevanja pravic in obveznosti. Vprašanje je še posebej zanimivo zato, ker zakonodaja za take primere ne določa jasne in izrecne omejitve pravice do seznanitve, kot to zahteva člen 23 Splošne uredbe in 25. člen ZVOPOKD.

### **Izbris nezakonito pridobljenih osebnih podatkov**

Splošna uredba med pravice posameznika uvršča tudi pravico do izbrisa oz. do pozabe, ki je določena v členu 17. Skladno s členom 17(1) Splošne uredbe ima posameznik, na katerega se osebni podatki nanašajo, pravico doseči, da upravljavec brez nepotrebne odlašanja izbriše osebne podatke v zvezi z njim, upravljavec pa ima obveznost osebne podatke brez nepotrebne odlašanja izbrisati, kadar: osebni podatki niso več potrebni za namene, za katere so bili zbrani ali kako drugače obdelani; posameznik, na katerega se osebni podatki nanašajo, prekliče privolitev, na podlagi katere poteka obdelava, in za obdelavo ne obstaja nobena druga pravna podlaga; posameznik, na katerega se osebni podatki nanašajo, 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 osebni podatki nanašajo, 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 izbriše 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.

Informacijski pooblaščenec je obravnaval pritožbo posameznika zaradi molka organa, ki naj ne bi odločil o njegovem zahtevku za izbris nezakonito pridobljenih, hranjenih oz. nadalje obdelanih osebnih podatkov v zbirkah podatkov, ki jih kot upravljavec vodi policija. Upravljavec je pojasnil, da naj bi se pritožnikovi osebni podatki obdelali ob zbiranju podatkov v zvezi s prometno nesrečo s pobegom. Pritožnik je po dogodku na policijsko postajo naslovil več elektronskih sporočil, v katerih je med drugim zahteval tudi izbris osebnih podatkov. V zvezi s pritožbami posameznika je bil izveden pomiritveni postopek, v okviru katerega bi naj bila pritožniku predstavljena zakonitost obdelave osebnih podatkov. Ker se posameznik z ugotovitvami pomiritvenega postopka ni strinjal, je pritožbo obravnaval Sektor za pritožbe zoper policijo, ki je prav tako potrdil zakonitost same obdelave. Upravljavec zahteve posameznika ni obravnaval kot zahtevo za izbris oz. je menil, da pritožnikove navedbe ne predstavljajo razloga za izbris, kot jih določa člen 17 Splošne uredbe.

Informacijski pooblaščenec je v postopku ugotovil, da je upravljavec obdeloval osebne podatke pritožnika v poročilu dežurnega policista in uradnem zaznamku, in sicer njegovo ime, priimek, datum rojstva in naslov stalnega prebivališča. Osebni podatki so bili pridobljeni v zvezi z obravnavo prometne nesreče. Policist je osebne podatke pritožnika prejel pri izvrševanju policijskega pooblastila iz 1. točke prvega odstavka 33. člena ZNPPol – zbiranje obvestil, ki je natančneje urejeno v 34. členu ZNPPol. Drugi odstavek 34. člena ZNPPol določa pogoje za obdelavo osebnih podatkov oseb, od katerih policisti zbirajo podatke, potrebne za opravljanje policijskih nalog. Določeno je, da ima oseba pravico do prostovoljnosti in anonimnosti ter da morajo policisti osebo o tej pravici tudi poučiti. V postopku je bilo ugotovljeno, da policist pritožnika o tej pravici na nobeni točki ni poučil in da je osebne podatke obdeloval tudi po tem, ko je pritožnik večkrat

izrazil željo oz. zahtevo, da se preneha z obdelavo njegovih osebnih podatkov. Informacijski pooblaščenec je na podlagi navedenega ugotovil, da je obstajal vsaj razlog za izbris iz točke (d) prvega odstavka člena 17 Splošne uredbe, ki določa, da ima posameznik pravico doseči, da upravljavec izbrise osebne podatke v zvezi z njim, upravljavec pa ima obveznost osebne podatke izbrisati, kadar so bili osebni podatki pridobljeni nezakonito. Po določbi drugega odstavka 34. člena ZNPPol je namreč posameznik tisti, ki lahko pri izvajanju policijskega pooblastila razpolaga s svojimi osebnimi podatki in se odloča o tem, ali bo policiji dovolil poseganje v njegovo ustavno pravico do varstva osebnih podatkov ali ne. V obravnavanem primeru upravljavec pritožniku takega razpolaganja ni omogočil, saj ga ni poučil v skladu z zakonom, poleg tega pa je njegove osebne podatke pridobival iz uradnih evidenc, ne da bi pritožnik to sploh vedel oz. ne da bi s tem soglašal. Informacijski pooblaščenec je odločil, da takšna obdelava osebnih podatkov ne predstavlja zakonite obdelave osebnih podatkov, zato je bila pritožnikova zahteva za izbris njegovih podatkov iz poročila dežurnega policista in uradnega zaznamka utemeljena.

### **Posameznik na podlagi pravice do izbrisa ne more doseči izbrisa svojih osebnih podatkov iz krstne knjige**

Informacijski pooblaščenec je obravnaval zadevo v zvezi z zahtevo za izbris osebnih podatkov iz krstne matične knjige, ki jo je posameznik vložil pri svoji župniji. Zatrjeval je, da že vrsto let ni več član Katoliške cerkve in da 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 ne bi Cerkev nikoli 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 prevladajo interes in temeljne pravice in svoboščine posameznika.

Informacijski pooblaščenec je odločil, da posameznik s sklicevanjem na pravico do izbrisa iz člena 17 Splošne uredbe ne more doseči izbrisa svojih osebnih podatkov iz krstne knjige, ki jo upravlja Rimskokatoliška cerkev (RKC). Zoper odločbo Informacijskega pooblaščenca je posameznik vložil tožbo na Upravno sodišče RS.

Informacijski pooblaščenec je v tej zadevi presojal določbo člena 17(3) Splošne uredbe, v skladu 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 statistične primere. Po ugotovitvah Informacijskega pooblaščenca, ki jih je potrdilo tudi upravno sodišče, gre pri vodenju osebnih podatkov v krstnih knjigah RKC za primer obdelave iz člena 17(3)(d) Splošne uredbe, torej za obdelavo, ki je potrebna za namene arhiviranja v javnem interesu. Ta določba Splošne uredbe sicer postavlja še dodaten pogoj za uporabo te omejitve pravice do izbrisa, in sicer da taka omejitev pride v poštev, če bi pravica do izbrisa lahko onemogočila ali resno ovirala uresničevanje namenov te obdelave. Informacijskem pooblaščenču in upravnemu sodišču izpolnjevanja tega pogoja ni bilo treba ugotavljati, saj je vprašanje razrešil že zakonodajalec v prvem odstavku 52. člena Zakona o varstvu dokumentarnega in arhivskega gradiva ter arhivih (ZVDAGA). Ta določa, da ima gradivo RKC lastnosti arhivskega gradiva po tem zakonu, zanj pa veljata načeli trajnosti in celovitosti. Test sorazmernosti med upravičenostjo do obdelave osebnih podatkov za namene arhiviranja v javnem interesu in posegom v pravico posameznika do informacijske zasebnosti je torej opravil že zakonodajalec. Informacijski pooblaščenec je zato zavrnil pritožbo posameznika zoper odločitev RKC, saj niso bili podani pogoji za izbris osebnih podatkov iz člena 17 Splošne uredbe, sodišče pa je njegovi odločitvi pritrdilo ter tožbo posameznika zoper njegovo odločbo zavrnilo.

Upravno sodišče je v odločitvi poudarilo tudi, da pri hrambi osebnih podatkov posameznika v matični krstni knjigi že po naravi stvari ne gre za primer, ko bi tožnik zaznaval izpovedovanje ali izvrševanje vere, ki bi pomenilo tako prisilno konfrontacijo z verskim prepričanjem, da bi pomenila poseg v njegovo versko svobodo. Z golo hrambo njegovih osebnih podatkov v krstni knjigi posameznik ni prisilno soočen z verskimi elementi ali prisiljen v sodelovanje pri izvrševanju vere, poleg tega pa se je v konkretnem primeru o izstopu oziroma izčlanitvi iz RKC v krstni knjigi napravil zaznamek, kar po stališču upravnega sodišča že samo po sebi predstavlja spoštovanje njegove pravice ne pripadati nobeni veri.

### **Pravica do popravka osebnih podatkov v anamnezi izvida**

Posameznik, na katerega se nanašajo osebni podatki, ima pravico doseči, da upravljavec brez nepotrebnega odlašanja popravi netočne osebne podatke, ki se nanašajo nanj. Posameznik, na katerega se nanašajo osebni podatki, ima ob upoštevanju namenov obdelave pravico do dopolnitve nepopolnih osebnih podatkov, vključno s predložitvijo dopolnilne izjave (člen 16 Splošne uredbe).

Informacijski pooblaščenec je obravnaval zadevo v zvezi z zahtevkom za popravilo osebnih podatkov, ki jo je vložila posameznica v okviru prve zahteve za prvo kršitev pacientov pravic zoper upravljavca (izvajalca zdravstvene dejavnosti) glede popravka navedb v anamnezi izvida. V originalnem zapisu je bilo v anamnezi izvida med drugim zapisano, da se je pritožnica naknadno še dvakrat vrnila v ambulanto in zahtevala, da se pod anamnezo vpiše njeno osebno mnenje v zvezi z načinom nastanka same poškodbe. Pritožnica je zahtevala popravilo teksta tako, da se izbriše del, ki po njenem mnenju ne sodi v izvid, in se navede zgolj relevanten tekst (v zvezi z nastankom poškodbe). Komisija za prvo obravnavo pri upravljavcu je opozorila na interna pravila s področja arhiviranja dokumentarnega gradiva, ki vsebujejo osebne podatke pacientov. Pravila zaradi zagotavljanja sledljivosti namreč prepovedujejo kakršno koli brisanje vsebine zdravstvene dokumentacije, ne da bi za to obstajala pravna podlaga. Nestrinjanje pacienta se lahko korigira zgolj tako, da se k obstoječi zdravstveni dokumentaciji doda navedbe pacienta oz. drugo besedilo, nikakor pa tako, da bi se že avtorizirani izvidi brisali oz. popravljali za nazaj. Komisija je poudarila tudi, da je nacionalna zakonodaja s področja arhiviranja dokumentarnega gradiva, ki vsebuje osebne podatke pacientov v razmerju do Splošne uredbe specialnejša (lex specialis), vendar kljub temu ni v nasprotju z določbo člena 16 Splošne uredbe, ki ureja pravico do popravka osebnih podatkov, saj ima posameznik ob upoštevanju namena obdelave osebnih podatkov pravico do dopolnitve nepopolnih osebnih podatkov, vključno s predložitvijo dopolnilne izjave. Obstoj nastanka poškodbe pa bo moral posameznik dokazovati z ustreznimi dokazili pri morebitnem uveljavljanju drugih pravic (npr. z naslova delovnega razmerja). Upravljavec je predlagal rešitev spora tako, da se v anamnezi doda zapis, da se na podlagi člena 16 Splošne uredbe doda besedilo o navedbah pacientke o nastanku poškodbe.

Informacijski pooblaščenec je ugotovil, da vsebina zahtevka pritožnice ni pravica do popravka po členu 16 Splošne uredbe, zaradi česar je njeno pritožbo zavrnil. Poudaril je, da pravica do popravka omogoča posamezniku, da od upravljavca zahteva, da popravi netočne osebne podatke, ki jih obdeluje o njem. Gre za pravico do popravka napačno zapisanih podatkov, kot so zapis imena, priimka, naslova, kontaktnih podatkov, datuma rojstva, davčne številke itd. S to pravico pa nikakor ni mogoče zahtevati popravka v smislu vsebinske interpretacije podatkov, saj namen pravice do popravka ni vsebinsko spreminjanje osebnih podatkov. Poudaril je tudi, da se lahko pacient in upravljavec prostovoljno dogovorita, da upravljavec izvede morebitne dopolnitve nepopolnih osebnih podatkov, vključno s predložitvijo dopolnilne izjave, toda tega pacient ne more doseči na prisiljujoč način prek pritožbenega postopka po členu 16 Splošne uredbe. Informacijski pooblaščenec je tudi dodatno pojasnil, da tako Splošna uredba kot veljavna zakonodaja s področja varstva dokumentarnega in arhivskega gradiva določata, da je hramba osebnih podatkov zakonita za izpolnjevanje pravnih obveznosti, izvajanje nalog v javnem interesu ali pri izvajanju javne oblasti, dodeljene upravljavcu, iz razlogov javnega interesa na področju javnega zdravja, za namene arhiviranja v javnem interesu, znanstveno-ali zgodovinskoraziskovalne namene ali statistične namene. Hramba dokumentarnega gradiva pa mora prav tako skladno z načelom celovitosti zagotavljati nespremenljivost in integralnost dokumentarnega gradiva oz. reprodukcijo njegove vsebine, urejenost dokumentarnega gradiva oz. njegove vsebine ter dokazljivost izvora dokumentarnega gradiva.

### 3.3.6 ZAHTEVA ZA OCENO USTAVNOSTI IN ZAKONITOSTI

Informacijski pooblaščenec lahko z zahtevo začne postopek za oceno ustavnosti oz. zakonitosti predpisov na podlagi 23.a člena Zakona o Ustavnem sodišču (ZUstS), če se pojavi vprašanje ustavnosti ali zakonitosti v zvezi s postopkom, ki ga vodi. Informacijski pooblaščenec je v letu 2021 vodil postopek inšpekcijskega nadzora nad ravnanjem upravljavca – Nacionalni inštitut za javno zdravje v zvezi z obdelavo osebnih podatkov s pomočjo aplikacije za preverjanje izpolnjevanja pogojev o prebolewnosti, cepljenosti ali testiranju glede bolezni covid-19.

V zvezi z navedenim postopkom je Informacijski pooblaščenec na Ustavno sodišče RS podal tri zahteve za oceno ustavnosti in zakonitosti, in sicer odlokov Vlade RS, ki so določali začasne omejitve izvajanja dejavnosti oz. način ugotavljanja izpolnjevanja t. i. pogoja PCT (pogoj prebolewnosti, cepljenosti ali testiranja), med drugim Odloka o načinu ugotavljanja izpolnjevanja pogojev prebolewnosti, cepljenosti in testiranja v zvezi z nalezljivo boleznijo COVID-19 (Uradni list RS, št. 126/2021), Odloka o začasnih omejitvah ponujanja in prodajanja blaga in storitev potrošnikom v Republiki Sloveniji (Uradni list RS, št. 122/21, 124/21, 126/21 in 129/21), Odloka o začasnih ukrepih za zmanjšanje tveganja okužbe in širjenja okužbe z virusom SARS-CoV-2 (Uradni list RS, št. 129/21) ter vseh ostalih odlokov, ki določajo omejitve izvajanja dejavnosti pod pogojem izpolnjevanja pogoja cepljenosti, prebolewnosti ali testiranja.

Skladno z vladnimi odloki je lahko posameznik izkazal izpolnjevanje pogoja PCT bodisi z digitalnim COVID potrdilom EU v digitalni ali papirnati obliki ali z drugim potrdilom oziroma dokazilom, ki je bil kot tak določen z odlokom vlade. Digitalno COVID potrdilo EU je enotno evropsko, splošno veljavno potrdilo o prebolewnosti, cepljenosti ali testiranju, določeno z Uredbo (EU) 2021/953 Evropskega parlamenta in Sveta z dne 14. 6. 2021 o okviru za izdajanje, preverjanje in priznavanje interoperabilnih potrdil o cepljenju, testu in preboleli boleznih v zvezi s COVID-19 (digitalno COVID potrdilo EU) za olajšanje prostega gibanja med pandemijo COVID-19 (Uredba (EU) 2021/953). Kot je pojasnjeno v nadaljevanju, se v primeru, ko posameznik kot dokazilo o izpolnjevanju pogoja PCT predloži digitalno COVID potrdilo EU v digitalni ali papirnati obliki, opremljeno s kodo QR, izpolnjevanje pogoja PCT preveri z aplikacijo za odčitavanje kode QR. Informacijski pooblaščenec z aplikacijo za preverjanje izpolnjevanja pogoja PCT ni bil seznanjen v nobeni fazi njene priprave in uveljavitve, z njenim obstojem se je seznanil šele iz poročanja medijev. Od seznanitve z informacijo o prvi verziji aplikacije za preverjanje pogoja PCT in do objave Odloka o načinu ugotavljanja izpolnjevanja pogoja prebolewnosti, cepljenosti ali testiranja v zvezi z nalezljivo boleznijo COVID-19 (Uradni list RS, št. 126/2021; v nadaljevanju: Odlok o načinu ugotavljanja izpolnjevanja PCT pogojev) je Informacijski pooblaščenec večkrat javno poudaril, da pravna podlaga za obdelavo osebnih podatkov obstaja le za uporabo digitalnih COVID potrdil EU za namene prehajanja meje med državami članicami EU, da pa morajo države članice, če bi želele ta potrdila uporabljati tudi za druge namene, sprejeti ustrezno nacionalno zakonodajo, ki bi to dopuščala (na to sta opozarjala tudi Evropski odbor za varstvo podatkov in Evropski nadzornik za varstvo podatkov)<sup>2</sup>.

Z vidika Splošne uredbe je treba poudariti, da digitalno COVID potrdilo EU vsebuje tudi posebne vrste osebnih podatkov, saj so podatki o cepljenju, testiranju in prebolewnosti v skladu s členom 9(1) Splošne uredbe nedvomno podatki, ki so povezani z zdravjem posameznika. Obdelava posebnih vrst osebnih podatkov je prepovedana, razen pri določenih izjemah, ki so določene v členu 9(2) Splošne uredbe. Tako točka (g) drugega odstavka člena 9 Splošne uredbe določa, da je obdelava posebnih vrst osebnih podatkov dopustna, kadar je obdelava potrebna iz razlogov bistvenega javnega interesa na podlagi prava Unije ali prava države članice, ki je sorazmerno z zastavljenim ciljem, spoštuje bistvo pravice do varstva podatkov ter zagotavlja ustrezne in posebne ukrepe za zaščito temeljnih pravic in interesov posameznika, na katerega se nanašajo osebni podatki točke. Kakršna koli obdelava podatkov o izpolnjevanju pogoja PCT, ki odraža zdravstveno stanje (da je oseba cepljena, testirana ali je prebolela covid-19), bi morala torej temeljiti zgolj in samo na pravu države članice (v Republiki Sloveniji je to lahko samo zakon), sorazmernosti z zastavljenim ciljem (tj. zagotavljanje javnega zdravja), pri čemer bi morala spoštovati bistvo pravice do varstva osebnih podatkov ter hkrati zagotoviti ustrezne in posebne ukrepe za zaščito temeljnih pravic in interesov posameznika.

Vlada RS je izdala Odlok o načinu ugotavljanja izpolnjevanja PCT pogojev, s katerim je določila način ugotavljanja izpolnjevanja PCT pogoja, kadar je ta določen z odlokom Vlade RS. V kolikor posameznik kot dokazilo o izpolnjevanju PCT pogoja predloži digitalno COVID potrdilo EU v digitalni ali papirnati obliki, opremljeno s kodo QR, pooblaščenca oseba, zadolžena za preverjanje, izpolnjevanje PCT pogoja preveri z aplikacijo za odčitavanje kode QR. Aplikacija je skladno s citiranim odlokom pri odčitavanju kode QR izpisala podatek o izpolnjevanju pogoja PCT tako, da iz podatka ni bilo razvidno, katerega od pogojev PCT oseba izpolnjuje, ter njeno osebno ime in letnico rojstva. Skladno z odlokom aplikacija ne sme omogočati hrambe ali druge obdelave osebnih podatkov iz prejšnjega odstavka in se ne sme povezovati z nobeno zbirko osebnih podatkov (3. člen odloka). Če pa se kot dokazilo o izpolnjevanju pogoja PCT predloži drugo potrdilo oziroma dokazilo v skladu z odloki, se izpolnjevanje pogoja PCT preveri z vpogledom v to potrdilo oziroma dokazilo.

Presoja ustavnosti in zakonitosti Odloka o načinu ugotavljanja izpolnjevanja pogoja PCT pa je po mnenju Informacijskega pooblaščenca neizogibno povezana s presojo ustavnosti in zakonitosti Odloka o začasnih omejitvah ponujanja in prodajanja blaga in storitev potrošnikom v Republiki Sloveniji (Uradni list RS, št. 122/21, 124/21, 126/21 in 129/21) ter vseh ostalih odlokov, ki določajo omejitve izvajanja dejavnosti pod pogojem izpolnjevanja pogoja prebolewnosti, cepljenosti ali testiranja, saj je Vlada RS z njimi določila zbiranje, obdelavo in namen uporabe osebnih podatkov. Pri tem se vsi navedeni odloki sklicujejo na Odlok o začasnih ukrepih za zmanjšanje tveganja okužbe in širjenja okužbe z virusom SARS-CoV-2 (Uradni list RS, št. 129/21), ki določa dokazila o izpolnjevanju pogoja prebolewnosti, cepljenosti ali testiranja.

<sup>2</sup>Glej npr. *Objavo Informacijskega pooblaščenca "Digitalno zeleno potrdilo za namen potovanja znotraj EU ne sme voditi v diskriminacijo posameznikov, uporaba mora biti jasno določena v zakonu in sorazmerna, po koncu pandemije mora ugasniti", ki je dostopna na: <https://www.ip-rs.si/novice/digitalno-zeleno-potrdilo-za-namen-potovanj-znotraj-eu-ne-sme-voditi-v-diskriminacijo-posameznikov-uporaba-mora-biti-jasno-dolo%C4%8Dena-v-zakonu-in-sorazmerna-po-koncu-pandemije-mora-ugasniti>*

Vlada je torej z odloki predpisala nekatere omejitve izvajanja dejavnosti tako, da so določene storitve posameznikom dostopne zgolj pod pogojem, da je posameznik prebolel covid-19, bil cepljen ali testiran, izpolnjevanje pogoja pa posameznik izkazuje bodisi z digitalnim COVID potrdilom EU (v digitalni ali papirnati obliki) ali drugim potrdilom oziroma dokazilom, ki je kot tak določen z odlokom vlade. Tako je npr. Odlok o začasnih omejitvah ponujanja in prodajanja blaga in storitev potrošnikom v Republiki Sloveniji določal, da so v igralnicah, igralnih salonih in pri posebnih igrah na srečo, v nastanitvenih obratih, v notranjih prostorih, v katerih se izvaja sejemska ali kongresna dejavnost, v gostinskih obratih, ki nudijo glasbo za ples oziroma družabni program, ter v prostorih, v katerih se izvaja gostinska dejavnost priprave in strežbe jedi in pijač, lahko samo potrošniki, ki izpolnjujejo pogoj PCT, kar dokazujejo z dokazili, določenimi v odloku, ki ureja začasne ukrepe za zmanjšanje tveganja okužbe z virusom SARS-Cov-2 (drugi odstavek 2. člena odloka).

Izkazovanje pogoja PCT je bilo torej določeno v Odloku o začasnih ukrepih za zmanjšanje tveganja okužbe in širjenja okužbe z virusom SARS-CoV-2. 4. člen tega odloka tako določa, da je pogoj PCT izpolnjen, če osebe razpolagajo z enim od spodaj navedenih dokazil, in sicer:

1. z dokazilom o negativnem rezultatu testa PCR, ki ni starejši od 72 ur od odvzema brisa, ali testa HAG, ki ni starejši od 48 ur od odvzema brisa;
2. z digitalnim COVID potrdilom EU v digitalni ali papirnati obliki, opremljenim s kodo QR;
3. z digitalnim COVID potrdilom tretje države v digitalni ali papirnati obliki, opremljenim s kodo QR, ki vsebuje vsaj enake podatke kot digitalno COVID potrdilo EU ter ga je pristojni zdravstveni organ tretje države izdal v angleškem jeziku;
4. z dokazilom o cepljenju zoper covid-19 (s katerim se izkazuje pretek časa za cepiva, določna s tem odlokom);
5. z dokazilom o pozitivnem rezultatu testa PCR, ki je starejši od deset dni, razen če zdravnik presodi drugače, vendar ni starejši od 6 mesecev;
6. s potrdilom zdravnika, da je oseba prebolela COVID-19 in od začetka simptomov ni minilo več kot 6 mesecev ali
7. z dokazilom iz citirane 5. ali 6. točke in so bile osebe v obdobju, ki ni daljše od 8 mesecev od pozitivnega rezultata testa PCR oziroma od začetka simptomov, cepljene z enim odmerkom cepiva iz 4. točke, pri čemer v primeru določenih cepiv iz te točke zadostuje en odmerek.

Odlok je obveznost preverjanja, ali uporabniki storitev izpolnjujejo zgoraj navedene pogoje, naložil ponudnikom blaga in storitev oz. odgovornim osebam, ki izvajajo ali organizirajo opravljanje dela. S tem, ko je bila ponudnikom storitev naložena obveznost preverjanja izpolnjevanja pogoja PCT, je bila določena tudi obdelava osebnih podatkov, saj je izpolnjevanje pogoja nemogoče preveriti, ne da bi s strani ponudnika storitve pooblaščenca oseba vpogledala v enega izmed dokazil, s katerim osebe zatrjujejo izpolnjevanje pogoja. Izkazovanje takšnega dokazila pa immanentno vključuje obdelavo osebnih podatkov, ki se na potrdilu oz. dokazilu nahajajo in s katerimi oseba izkazuje istovetnost oz. to, da se dokazilo nanaša nanjo, ter tudi, ali je bila ta oseba cepljena, testirana oz. je prebolela covid-19.

V kasneje izdanih odlokih (npr. v Odloku o začasnih ukrepih za preprečevanje in obvladovanje okužb z nalezljivo boleznijo COVID-19 (Uradni list RS, št. 174/21 in 177/21)) se je posameznik moral izkazati tudi z veljavnim osebnim dokumentom.

Glede na navedeno je Informacijski pooblaščenec vložil zahtevo za presojo ustavnosti in zakonitosti nekaterih odlokov, ki določajo omejitve, pogojene z izpolnjevanjem pogoja PCT, ker preverjanje izpolnjevanja pogoja predstavlja obdelavo osebnih podatkov. Informacijski pooblaščenec je tako v zahtevah za oceno ustavnosti poudaril, da je odlok Vlade RS, ki ponudnikom storitev nalaga obveznost preverjanja izpolnjevanja pogoja PCT (ki pomeni obdelavo osebnih podatkov), neustaven, saj bi smel takšno obdelavo v skladu z 38. členom Ustave RS določiti le zakonodajalec z zakonom. Pravica do varstva osebnih podatkov je namreč ustavno zagotovljena človekova pravica. Vsaka, še tako minimalna obdelava osebnih podatkov pomeni poseg v človekovo pravico (glede obdelave osebnih podatkov namreč velja, da je prepovedano vse, kar ni izrecno dovoljeno), poseg pa je lahko določen samo v zakonu in ne z odlokom vlade. Samo zakonodajni postopek, prek katerega se sprejema zakon, lahko zagotovi premišljeno odločitev, ali je obdelava osebnih podatkov za določen namen res nujna, potrebna in učinkovita. Postopek, prek katerega Vlada RS izdaja odloke, tega namreč ne zagotavlja in vsebina je prepuščena samovolji izdajatelja odloka. Določbe odlokov pa po mnenju Informacijskega pooblaščenca posegajo tudi v pravico do svobode gibanja (32. člen Ustave RS) ter pravico do svobode združevanja (42. člen Ustave RS).



Celotna besedila podanih zahtev za oceno ustavnosti in zakonitosti so na voljo na spletni strani Informacijskega pooblaščenca: <https://www.ip-rs.si/zakonodaja/zahteve-ip-za-presoj-ustavnosti-oz-zakonitosti-predpisov>.

### 3.4 PRIPRAVA MNENJ IN POJASNIL

#### 3.4.1 SPLOŠNA POJASNILA

Na podlagi člena 57 Splošne uredbe, 76. člena ZVOPOKD 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 2021 je Informacijski pooblaščenec svetoval 3.647 posameznikom in pravnim osebam, ki so se nanj obrnili z vprašanji s področja varstva osebnih podatkov.**

Informacijski pooblaščenec je izdal **1.471 pisnih mnenj in napotitev na mnenja**, in sicer največ s področja delovnih razmerij in v zvezi z obdelavo zdravstvenih osebnih podatkov. Če je posameznik zastavil vprašanje, na katerega je Informacijski pooblaščenec v preteklosti podobno že odgovoril, je posameznika le napotil na mnenje, objavljeno na spletni strani. Na spletni strani <https://www.ip-rs.si/vop/> je objavljenih več kot **6.000 mnenj**. 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. Slednja so razvrščena v kar 67 vsebinskih področij.

Informacijski pooblaščenec spodbuja svetovanje oz. posredovanje ustnih odgovorov na vprašanja, zato je bil v okviru projekta iDecide, ki ga je financirala Evropska unija iz programa REC (Rights, Equality and Citizenship Programme), v letu 2021 v uradu vsak dan na voljo dežurni državni nadzornik za varstvo osebnih podatkov, ki je na vprašanja odgovarjal po telefonu. **Leta 2021 so državni nadzorniki sprejeli 2.176 klicev.**

#### 3.4.2 MNENJA NA PREDPISE

Informacijski pooblaščenec podaja mnenja na predpise skladno s točko (c) člena 57 Splošne uredbe, 48. členom ZVOP-1 in 76. členom ZVOPOKD, ki določajo, da nadzorni organ svetuje državnemu zboru, vladi oz. ministrstvu ter drugim institucijam in organom o zakonodajnih in upravnih ukrepih v zvezi z varstvom pravic in svoboščin posameznikov pri obdelavi osebnih podatkov oz. daje predhodna mnenja, pojasnila in stališča o usklajenosti določb predlogov zakonov ter ostalih predpisov z zakoni in drugimi predpisi, ki urejajo osebne podatke ter vprašanjih glede varstva osebnih podatkov.

Leta 2021 je **Informacijski pooblaščenec izdal 85 mnenj na predloge sprememb zakonov ter na predloge novih zakonov in drugih predpisov**, kar je toliko kot leta 2020. Tudi v letu 2021 je Informacijski pooblaščenec na področju priprave predpisov za obdelavo osebnih podatkov opazal 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 predlagatelji v takih primerih 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, dodatnim nepredvidenim stroškom in težavam ob pripravi predpisa ter poskrbijo, da bo zakon dejansko skladen z načelom sorazmernosti z vidika posegov v zasebnost.

Informacijski pooblaščenec je leta 2021 med drugim podal mnenje, pripombe oz. je sodeloval pri pripravi naslednjih predpisov (v zvezi z nekaterimi je podal več mnenj):

- Predlog Pravilnika o spremembah in dopolnitvah Pravilnika o zaščiti podatkov policije,
- Predlog Zakona o spremembah in dopolnitvah Zakona o finančnem poslovanju, postopkih zaradi insolventnosti in prisilnem prenehanju,
- Predlog novega Zakona o preprečevanju pranja denarja in financiranja terorizma,
- Predlog Zakona o dodatnih ukrepih za preprečevanje širjenja, omilitev, obvladovanje, okrevanje in odpravo posledic COVID-19,
- Predlog Zakona o spremembah in dopolnitvah Zakona o gasilstvu,

- Predlog Zakona o spremembah in dopolnitvah Zakona o voznikih,
- Predlog novega Zakona o letalstvu,
- Predlog Zakona o dopolnitvah Zakona o interventnih ukrepih za pomoč gospodarstvu in turizmu pri omilitvi posledic epidemije COVID-19,
- Predlog Zakona o cestah,
- Predlog Zakona o izvajanju uredbe (EU) o evropskih ponudnikih storitev množičnega financiranja za podjetnike,
- Predlog Zakona o spremembah in dopolnitvah Zakona o izvrševanju kazenskih sankcij,
- Predlog Zakona o referendumu in o ljudski iniciativi (ZRLI-1),
- Predlog Zakona o spremembah in dopolnitvah Zakona o državnem odvetništvu,
- Predlog Zakona o spremembah in dopolnitvah Zakona o organizaciji in financiranju vzgoje in izobraževanja,
- Predlog Zakona o spremembah in dopolnitvah Zakona o nalogah in pooblastilih policije,
- Predlog Zakona o napotitvi oseb v mednarodne civilne misije in mednarodne organizacije,
- Predlog Zakona o spremembah in dopolnitvah Zakona o uveljavljanju pravic iz javnih sredstev,
- Predlog Zakona o spremembah in dopolnitvah Zakona o socialno varstvenih prejemkih,
- Predlog Direktive Evropskega parlamenta in Sveta o potrošniških kreditih,
- Predlog Zakona o oskrbi s plini,
- Predlog sprememb in dopolnitev Pomorskega zakonika (57. člen) s priloženo oceno učinkov,
- Predlog Zakona o varstvu potrošnikov,
- Predlog Zakona o bonitetnem nadzoru investicijskih podjetij,
- Predlog Zakona o spremembah in dopolnitvah Zakona o trgu finančnih instrumentov,
- Predlog Zakona o hipotekarni in komunalni obveznici,
- Predlog Pravilnika o spremembah in dopolnitvah Pravilnika o vsebini in formatu prošnje za izdajo vizuma za dolgoročno bivanje ter o vsebini in formatu garantnega pisma,
- Predlog Zakona o znanstvenoraziskovalni in inovacijski dejavnosti,
- Predlog Zakona o spremembah in dopolnitvah Zakona o kmetijskih zemljiščih,
- Predlog sprememb 33. člena Zakona o varstvu Zakona o varstvu kulturne dediščine,
- Predlog Pravilnika o spremembah in dopolnitvah Pravilnika o načinu izdaje dovoljenja za prebivanje, načinu zajemanja prstnih odtisov in načinu označitve prenehanja dovoljenja za prebivanje,
- Predlog novega Zakona o varstvu osebnih podatkov,
- Predlog Zakona o varstvu okolja,
- Predlog Zakona o spremembah Zakona o ureditvi določenih vprašanj zaradi končne rabsodbe arbitražnega sodišča na podlagi Arbitražnega sporazuma med Vlado Republike Slovenije in Vlado Republike Hrvaške,
- Predlog Sprememb in dopolnitev Pravil sistema izmenjave informacij o zadolženosti fizičnih oseb – SISBON na podlagi drugega odstavka 26. člena Zakona o centralnem kreditnem registru,
- Predlog Zakona o spremembah in dopolnitvah Zakona o investicijskih skladih in družbah za upravljanje,
- Predlog Zakona o spremembah in dopolnitvah Zakona o upravljavcih alternativnih investicijskih skladov,
- Predlog Zakona o oskrbi z električno energijo,
- Predlog Zakona o spremembah in dopolnitvah Zakona o zaščiti živali,
- Predlog Zakona o gostinstvu,
- Dopolnjen predlog Zakona o spremembah in dopolnitvah Zakona o kmetijstvu,
- Predlog Pravilnika o sofinanciranju šolskih tekmovanj,
- Dopolnjen predlog Zakona o spremembah in dopolnitvah Zakona o zadrugah,
- Predlog Zakona o spodbujanju rabe obnovljivih virov energije,
- Predlog Zakona o spremembah in dopolnitvah Zakona o referendumu in ljudski iniciativi,
- Predlog sprememb 7. člena Zakona o prijavi prebivališča,
- Predlog Zakona o spremembah in dopolnitvah Zakona o državnem tožilstvu,
- Predlog Zakona o spremembah in dopolnitvah Zakona o volitvah v državni zbor,
- Zakon o spremembah in dopolnitvah Zakona o osebni asistenci,
- Zakon o spremembah in dopolnitvah Zakona o revidiranju,
- Predlog Zakona o spremembah in dopolnitvah Zakona o organiziranosti in delu v policiji.

### 3.5 SKLADNOST IN PREVENTIVA

Splošna uredba za razliko od prejšnjih pravnih aktov, ki so urejali varstvo osebnih podatkov, bistveno več pozornosti namenja mehanizmom, ki jih lahko oz. jih morajo uporabiti zavezanci za zagotovitev skladnosti z zakonodajo. Gre za načelo odgovornosti (angl. accountability), v okvir katerega sodi:

- 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.

Nadzorni organi za varstvo osebnih podatkov so skozi čas prišli do podobnih ugotovitev kot nekateri drugi nadzorni organi, ki delujejo precej dalj časa, npr. finančni in davčni uradi, in sicer da si prevladujoči delež zavezancev želi delovati skladno z zakonodajo in si ne želi negativnega medijskega poročanja, izgube zaupanja strank in ne nazadnje sankcij. Po drugi strani pa se marsikateri zavezanec, zlasti mikro in mala podjetja ter organizacije, ob poplavi predpisov težko znajde in nima na voljo ustreznih kadrov in znanja, da bi skladnost tudi zagotovil. Ob upoštevanju, da praktično ni organizacije, ki ne bi obdelovala osebnih podatkov in bila posledično zavezana Splošni uredbi, precejšnje število zavezancev potrebuje pomoč pri razumevanju in implementaciji določb Splošne uredbe. Zato nadzorni organi za varstvo osebnih podatkov 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. Med bistvene preventivne dejavnosti Informacijskega pooblaščenca tako sodi telefonsko in pisno svetovanje, primerne informacije na spletnih straneh, izmenjava informacij z zavezanci, preventivne aktivnosti za skladnost, smernice, infografike, izobraževanja in komunikacija z mediji ter vzorčni dokumenti (obrazci, vzorčne pogodbe ipd.), ki lahko preprečijo marsikatero kršitev varstva osebnih podatkov in zmanjšajo potrebo po izvajanju inšpekcijskega nadzora.<sup>3</sup>

Informacijski pooblaščenec redno posodablja svojo spletno stran, na kateri je objavljen bogat nabor uporabnih gradiv, koristna gradiva pa objavlja tudi na spletnih straneh upravljavec.si, ki je namenjena malim in srednje velikim podjetjem, ter tiodlocas.si, ki je namenjena posameznikom. V letu 2021 so bili posodobljeni iskalniki na spletni strani (po mnenjih glede varstva osebnih podatkov in po odločbah o informacijah javnega značaja), ki omogočajo izbiro kategorij, časovnega obdobja, iskanje po polnem besedilu in izbiro kategorij; po začetku uporabe Splošne uredbe je na spletni strani objavljenih več kot 3000 mnenj.

Informacije, stališča in mnenja Informacijski pooblaščenec deli tudi prek družbenih omrežij Facebook in LinkedIn, kjer predvsem opozarja na pomembne novosti na področju varovanja zasebnosti ter objavlja povezave do relevantnih objav.

Sektor za skladnost in preventivo Informacijskega pooblaščenca nudi podporne dejavnosti drugim sektorjem, tako glede informacijske tehnologije kot pomoči sektorju za inšpekcijski nadzor; med drugim je tako pripravil izobraževanje o ribarjenju (angl. phishing) ter zgoščevanju podatkov (angl. hashing), razvil določene interne aplikacije, pripravil spletni obrazec za poročanje o pooblaščenih osebah za varstvo podatkov ter novo podstran o načelu preglednosti po Splošni uredbi.<sup>4</sup> Sektor izvaja tudi številne preventivne dejavnosti, ki so opisane v nadaljevanju.

Informacijski pooblaščenec je leta 2021 nadaljeval aktivnosti projekta ozaveščanja iDecide, ki je namenjen ozaveščanju treh ciljnih skupin, in sicer starejših od 65 let, delovne populacije ter starejših mladoletnikov.

<sup>3</sup>Iskalnik po mnenjih je dostopen na povezavi: <https://www.ip-rs.si/mnenja-gdpr/>

<sup>4</sup>Dostopno na: <https://www.ip-rs.si/zakonodaja/reforma-evropskega-zakonodajnega-okvira-za-varstvo-osebni-podatkov/klju%C4%8Dna-podro%C4%8Dja-uredbe/obve%C5%A1%C4%8Danje-posameznikov-o-obdelavi-osebni-podatkov>

### 3.5.1 OBVEZNOSTI UPRAVLJAVCEV

Kot je že bilo omenjeno, načelo odgovornosti od zavezancev terja določeno odgovornost in proaktivnost, v sklop mehanizmov za skladnost in upoštevanje načela odgovornosti pa sodijo različni mehanizmi, ki jih določa Splošna uredba. Z namenom ustreznega informiranja zavezancev in učinkovitega izvajanja teh obveznosti Informacijski pooblaščenec vzpostavlja številne postopke ter pripravlja gradiva, predstavljena v nadaljevanju.

### 3.5.2 PREVENTIVNE AKTIVNOSTI V ČASU IZREDNIH RAZMER

Širjenje koronavirusa in sprejemanje številnih ukrepov ter uvajanje novih obdelav osebnih podatkov je vplivalo tudi na način, obseg in doseg preventivnih aktivnosti. Srečanja s ciljnim publikami večino leta 2021 praktično niso bila mogoča, zato so se številne aktivnosti preselile na spletne komunikacijske kanale. Informacijski pooblaščenec je tako nadaljeval izdelavo ključnih gradiv in izvajanje aktivnosti za ozaveščanje, kot so:

- mnenja na vprašanja zavezancev,
- mnenja na predloge predpisov,
- mnenja na ocene učinkov,
- komunikacija s strokovno in splošno javnostjo,
- komunikacija s pooblaščenimi osebami za varstvo podatkov in vzdrževanje registra,
- smernice,
- infografike,
- ohranjanje aktualnosti spletne strani ter njeno vzdrževanje,
- objave vsebin na družabnih omrežjih,
- brezplačna predavanja za zavezance in cilje skupine.

### 3.5.3 OCENE UČINKOV NA VARSTVO OSEBNIH PODATKOV

Ocene učinkov na varstvo osebnih podatkov so eno ključnih orodij načela odgovornosti, katerih namen je pravočasna identifikacija in obvladovanje tveganj v povezavi z varstvom osebnih podatkov. Zlasti so pomembne, kadar gre za nove projekte, ki predvidevajo množično obdelavo osebnih podatkov, še posebej kadar gre za uporabo modernih tehnologij, za ranljive skupine posameznikov in za obdelavo posebnih vrst osebnih podatkov. V postopku predhodnega posvetovanja, kot ga opredeljuje člen 36 Splošne uredbe, lahko zavezanci svoje ocene učinka na varstvo osebnih podatkov pošljejo v predhodno mnenje Informacijskemu pooblaščenecu ter tako pridobijo stališča in priporočila glede izdelanih ocen učinka. Slednje so namreč zlasti pri velikih projektih, ki vključujejo obsežne obdelave osebnih podatkov, eno ključnih orodij, da se pravočasno in celovito naslovijo tveganja za morebitne kršitve varstva osebnih podatkov pri izvajanju projekta. Mnenje Informacijskega pooblaščenca na oceno učinka lahko opozori na neidentificirana tveganja ter pomanjkljive ukrepe za njihovo obvladovanje, pravočasno obvladovanje tveganja pa lahko zavezancem prinese izogib občutnim stroškom popravilnih ukrepov, potencialnim visokim sankcijam zaradi kršitev ter okrnitvi ali izgubi ugleda pri strankah in v javnosti.

Leta 2021 je Informacijski pooblaščenec glede na epidemiološke razmere prejel relativno malo ocen učinka v predhodno posvetovanje po členu 36 Splošne uredbe; te možnosti se je poslužilo le šest zavezancev. Na prejete ocene učinka je Informacijski pooblaščenec v postopku predhodnega posvetovanja izdal mnenja glede naslednjih tem:

- uvajanje avtomatiziranega branja registrskih tablic za upravljanje parkirnih površin,
- videonadzor priobalnih področij,
- videonadzor javnih površin v občini,
- uvajanje integralnega sistema za nadzor proizvodnje,
- obravnava bolnikov s kroničnimi stanji v osnovnem zdravstvenem varstvu,
- vključitev dodatnih podatkovnih virov v sistem poslovne analitike v državni upravi.

Poleg naštetih ocen učinka je Informacijski pooblaščenec prejel tudi ocene učinka v okviru zakonodajnih predlogov, na primer glede določenih rešitev (prepoznavna registrskih tablic, sistem za iskanje pogrešanih oseb) v okviru sprememb Zakona o nalogah in pooblastilih policije.

Od sprejema Splošne uredbe se znanje zavezancev o izdelavi ocen učinkov počasi izboljšuje, s tem pa se povečuje tudi kakovost izdelanih ocen. Kljub temu pa Informacijski pooblaščenec še vedno opaža pomanjkljive opredelitve metodologij ocene tveganja (zlasti način določanja skupne ravni tveganja) ter splošno prenizke ocene ravni tveganj. Tveganje pridobivanja nepopolnih ali neveljavnih privolitvev za obdelavo osebnih podatkov ne more biti ocenjeno nižje kot »visoko«, saj neveljavne privolitve pomenijo nezakonito obdelavo (vseh tako) pridobljenih osebnih podatkov. Ne glede na to pa po drugi strani številni zavezanci dobro poznajo Smernice Informacijskega pooblaščenca glede ocen učinka in jih dobro uporabljajo pri izdelavi svojih ocen.

Poudariti velja še, da mnenje Informacijskega pooblaščenca zavezancem omogoča praktično brezplačen pravni pregled ocene učinka in je zato – ob upoštevanju, da je ta pri projektih, ki vključujejo množično obdelavo osebnih podatkov, obvezna – nekoliko presenetljivo, da te možnosti ne izkoristi več zavezancev. Informacijski pooblaščenec bo zato v okviru svojih ozaveščevalnih aktivnosti izraziteje poudaril prednosti in koristi ocen učinkov ter možnost pridobitve predhodnega mnenja.

### 3.5.4 POOBLAŠČENE OSEBE ZA VARSTVO PODATKOV

Določitev pooblaščenih oseb za varstvo osebnih podatkov (angl. Data Protection Officer; DPO), predstavlja pomembno dolžnost zlasti večjih upravljavcev in obdelovalcev osebnih podatkov. Pooblaščen oseb naj bi izvajala svetovalne in nadzorne naloge na področju varstva osebnih podatkov ter delovala kot notranji revizor za varstvo osebnih podatkov, ki poleg nadzora tudi opozarja upravljavce in obdelovalce na njihove obveznosti, izobražuje in ozavešča zaposlene. Splošna uredba dopušča tudi imenovanje zunanjih pooblaščenih oseb, zato so se zlasti manjši zavezanci v javnem sektorju (npr. osnovne šole, javne knjižnice, manjši izvajalci zdravstvenih storitev tako v javnem kot v zasebnem sektorju), ki iz različnih razlogov ne razpolagajo z ustreznim kadrom znotraj svoje organizacije, odločili za pogodbeno imenovanje pooblaščenih oseb izven svoje organizacije. Slednje ima lahko določene prednosti (zunanji izvajalci imajo praviloma več izkušenj z različnih področij varstva osebnih podatkov), po drugi strani pa so seveda tudi med zunanjimi ponudniki razlike v kakovosti storitev in obsegu časa, ki ga zagotovijo strankam.

Z namenom lažjega izpolnjevanja dolžnosti zavezancev glede poročanja podatkov o imenovanih pooblaščenih oseb za varstvo osebnih podatkov, je Informacijski pooblaščenec pripravil spletni obrazec (na voljo je na povezavi: <https://www.ip-rs.si/pooblastcene-osebe>) s pomočjo katerega lahko zavezanci enostavno sporočijo podatke ali popravke o imenovanih pooblaščenih oseb. Zavezanci spletni način sporočanja podatkov uporabljajo, pri čemer se v zadnjem letu pretežni del nanaša na spremembe v imenovanju pooblaščenih oseb in le manjši del na prvo imenovanje.

**Do konca leta 2021 je pooblaščen oseb prijavilo 2448 zavezancev.**

Informacijski pooblaščenec je v stiku tudi s predstavniki zunanjih izvajalcev, ki nudijo zavezancem storitve pooblaščenih oseb za varstvo osebnih podatkov, saj na ta način pridobi koristne povratne informacije iz prakse o težavah sistemske narave, ki jih lahko naslovi s svojimi preventivnimi aktivnostmi.

### 3.5.5 AKTIVNOSTI IZOBRAŽEVANJA IN OZAVEŠČANJA

Zaradi velikega števila prejetih vprašanj o preverjanju pogoja PCT, je Informacijski pooblaščenec v drugem delu projekta iDecide izdal posebne smernice:

- [za delodajalce oz. upravljavce,](#)
- [za posameznike,](#)
- [za šole.](#)

Poleg njih so bile pripravljene tudi naslednje smernice :

- [smernice za zagotavljanje skladnosti IT rešitev v šolstvu,](#)
- [smernice za organizatorje dogodkov,](#)
- [vodnik po pravicah za posameznike](#) ter
- [posodobitev smernic o prenosu osebnih podatkov v tretje države.](#)

Smernice za zagotavljanje skladnosti IT rešitev v šolstvu je Informacijski pooblaščenec pripravil kot odziv na težave, ki so bile zaznane pri izvajanju šolanja in izobraževanja na daljavo. Posamezni vzgojno-izobraževalni zavodi so namreč ob odsotnosti enotnih in sistemskih navodil praktično vsak zase sprejemali hitre odločitve, katera orodja za izobraževanje na daljavo bodo uporabljali in katere osebne podatke bodo pri tem obdelovali; v nekaterih primerih so te odločitve sprejemali celo posamezni učitelji na nivoju posameznega razreda brez predhodnega razmisleka o zagotavljanju zasebnosti in varstva osebnih podatkov. To je vodilo v številne primere prekomernih obdelav osebnih podatkov in posegov v zasebnost, npr. za izkazovanje športnega udejstvovanja učencev, opravljenih nalog in opravljanja izpitov na daljavo. Smernice poleg številnih napotkov vsebujejo tudi kontrolni seznam za preverjanje skladnosti, s pomočjo katerega lahko vzgojno-izobraževalni zavodi vnaprej preverijo izpolnjevanje zahtev zakonodaje pri odločanju o uporabi IT rešitev.<sup>5</sup>

Informacijski pooblaščenec je leta 2021 posodobil infografiko o prenosu osebnih podatkov v tretje države zaradi t. i. sodbe »Schrems II«.

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 bodo 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. Grafično so predstavljeni tudi statistični podatki o prejetih obvestilih o kršitvah varnosti osebnih podatkov v letu 2021 (glej poglavje 3.2.3).

Evropski dan varstva osebnih podatkov je Informacijski pooblaščenec leta 2021 posvetil izzivom, ki jih je na področje obdelave osebnih podatkov in pravice do zasebnosti prinesla pandemija koronavirusa. Po nagovoru informacijske pooblaščenke ob evropskem dnevu varstva osebnih podatkov in podelitvi nagrade ambasador zasebnosti je Informacijski pooblaščenec v okviru evropskega projekta iDecide izvedel še spletni seminar za strokovnjake s področja sindikatov in delovnih združenj. Kako so moji podatki varovani v delovnem razmerju, ki se je prav tako dotikal tudi obdelave osebnih podatkov v času epidemije.

Informacijska pooblaščenka Mojca Prelesnik je v svoji predstavitvi uvodoma spomnila, da vsako leto 28. januarja obeležujemo evropski dan varstva osebnih podatkov, saj je bila na ta dan leta 1981 sprejeta Konvencija Sveta Evrope o varstvu posameznika glede na avtomatsko obdelavo osebnih podatkov (Konvencija št. 108); ta letos obeležuje že svojo 40-letnico.

Po kratkem pregledu statistike preteklega leta je informacijska pooblaščenka poudarila, da je bilo leto 2021 posebno predvsem zaradi pandemije novega koronavirusa. Ta je krojila tudi velik del aktivnosti Informacijskega pooblaščenca, saj je bilo v kontekstu obdelave osebnih podatkov v izrednih razmerah prejetih veliko število raznovrstnih vprašanj in prijav. Ta so se med drugim nanašala na obdelavo podatkov v okviru aplikacije za sledenje stikov, obdelavo osebnih podatkov pri šolanju na daljavo, ustreznost IT programov za spremljanje dela na domu, merjenje temperature (zaposlenim, strankam) ob vstopu v prostor, videonadzor s termo kamero kot obliko inteligentne videoanalitike itd. Informacijska pooblaščenka je poudarila, da je in da mora biti medicinska stroka tista, ki določa namen obdelave in nabor osebnih podatkov, ki je nujen za doseg namena varovanja javnega zdravja.

Že tradicionalno je Informacijski pooblaščenec na dogodku podelil priznanje ambasador zasebnosti. Za leto 2020 je priznanje prejel Inštitut za kriminologijo pri Pravni fakulteti v Ljubljani. Informacijska pooblaščenka je v utemeljitvi podelitve nagrade poudarila, da nagrajeni inštitut pod vodstvom dr. Aleša Završnika že vrsto let ozavešča in opozarja na pomen zasebnosti in varstva osebnih podatkov v sodobni družbi. V težavnem letu 2020 so organizirali številne posvete, konference, simpozije in okrogle mize, med drugim o aplikacijah za sledenje okužbam in kibernetičnih grožnjah v času covid-19. Splošno in strokovno javnost so s prispevki v različnih medijih opozarjali na posledice uvajanja interventnih ukrepov, na etične in pravne dileme uvajanja umetne inteligence ter na nevarnost drsenja v družbo nadzora. S svojim delom so nastavljali zrcalo sodobni družbi, osvetlili tehnološke, družbene in pravne izzive, s katerimi se soočamo, ter tako pomembno prispevali k bogatejšemu družbenemu dialogu o vplivu teh izzivov na temeljne človekove pravice.

<sup>5</sup>Smernice so dostopne na povezavi: <https://www.ip-rs.si/publikacije/priročnik-in-smernice/smernice-po-splošni-uredbi-o-varstvu-podatkov-gdpr/smernice-za-skladno-uporabo-informacijskih-rešitev-v-šolstvu>.

Po zaključku obeležitve dneva varstva osebnih podatkov je sledil strokovni seminar v okviru evropskega projekta iDecide, namenjen strokovnjakom s področja sindikatov in delovnih združenj z naslovom Kako so moji podatki varovani v delovnem razmerju?. Na dogodku je bil predstavljen tudi priročnik za delovno aktivno populacijo z odgovori na aktualne izzive obdelave osebnih podatkov v delovnih razmerjih. Evropski odbor za varstvo podatkov (EOVP) je pripravil kratko videopredstavitel, v kateri so vsi člani Evropskega odbora za varstvo podatkov vsak v svojem jeziku podali sporočilo ob evropskem dnevu varstva osebnih podatkov.<sup>6</sup>

Informacijski pooblaščenec je, prav tako tradicionalno, podelil tudi **priznanja prejemnikom mednarodnega certifikata za informacijsko varnost** po standardu ISO/EIC 27001:2013, in sicer 15 organizacijam, s čimer je poskrbel za dodatno promocijo najbolj uveljavljenega mednarodnega standarda na področju informacijske varnosti. Spodbudno je, da so se številne organizacije kljub zahtevnim razmeram zaradi epidemije, odločile za vlaganje resursov v sistemski pristop k varovanju informacij, ki ga zagotavlja omenjeni standard.

Informacijski pooblaščenec je leta 2021 kljub številnim omejitvam glede izvedb dogodkov (večinoma so ti potekali prek spleta) na področju varstva osebnih podatkov izvedel **65 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. V letu 2021 je tako:

- objavil 57 sporočil na omrežju LinkedIn,
- delil 51 objav na omrežju Facebook ter
- poslal 12 novičnikov.

Informacijski pooblaščenec je v letu 2021 nadaljeval izvajanje projekta za ozaveščanje »**Individuals Decide – Raising Awareness About Data Protection Rights (iDECIDE)**«, ki je sofinanciran s strani Evropske komisije, in sicer v okviru Programa za pravice, enakost in državljanstvo 2020–2023.

## Projekt iDECIDE

Projekt traja 48 mesecev, osredotoča pa se 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 povečanje zavedanja o reformi okvira za varstvo osebnih podatkov v splošni javnosti v Sloveniji, s poudarkom na pravicah posameznikov ob ustrezni prilagoditvi komunikacije in upoštevanju potreb različnih ciljnih skupin.

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). V letu 2021 se je izvajalo tudi strokovno svetovanje po telefonu in elektronski pošti ter izvajanje izobraževalnih in ozaveščevalnih dogodkov za ciljne publike, ki jih je Informacijski pooblaščenec pripravili v sodelovanju s sindikalnimi organizacijami, združenji na področju izobraževanja starejših ter mladoletnih. Na dogodkih, kot so Festival za tretje življenjsko obdobje<sup>7</sup> ter spletna seminarja za strokovnjake iz izobraževalnih zavodov za tretje življenjsko obdobje ter za srednješolske učitelje in strokovnjake s področja izobraževanja<sup>8</sup>, je bila zagotovljena tudi sprotne in naknadna distribucija gradiv, izdelanih v okviru projekta. Različne uporabne materiale in praktične napotke za splošno javnost je Informacijski pooblaščenec objavil tudi na svojih spletnih straneh, in sicer na [www.iprs.si](http://www.iprs.si), [www.tiodlocas.si](http://www.tiodlocas.si) in [www.upravljavec.si](http://www.upravljavec.si), izpostaviti pa velja troje smernic o preverjanju pogoja PCT za različne ciljne publike, in sicer za delodajalce oz. upravljavce<sup>9</sup>, za posameznike<sup>10</sup> in za šole.<sup>11</sup>

<sup>6</sup>[https://edpb.europa.eu/news/news/2021/edpb-celebrates-data-protection-day\\_sl](https://edpb.europa.eu/news/news/2021/edpb-celebrates-data-protection-day_sl)

<sup>7</sup><https://www.ip-rs.si/novice/vabilo-na-seminar-vi-odlo%20o%20date-o-svojih-podatkih-ki-bo-29-septembra-potekal-v-okviru-festivala-za-tretje-%20%C5%BEivljenjsko-obdobje>

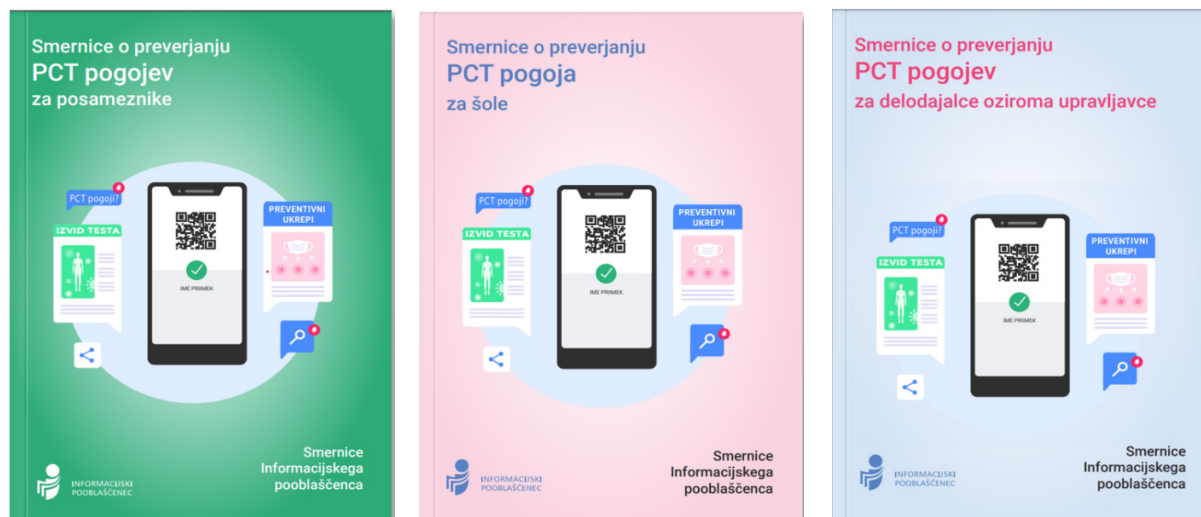
<sup>8</sup><https://www.ip-rs.si/novice/spletna-seminarja-o-varstvu-osebnih-podatkov-%E2%80%93-za-srednje-%C5%A1olske-u%C4%8Ditelje-in-strokovnjake-s-podro%C4%8Dja-izobra%C5%BEevanja-ter-za-strokovnjake-iz-izobra%C5%BEevalnih-zavodov-za-tretje-%C5%BEivljenjsko-obdobje>

<sup>9</sup><https://www.ip-rs.si/publikacije/prirocniki-in-smernice/smernice-po-splošni-uredbi-o-varstvu-podatkov-gdpr/smernice-o-preverjanju-pct-pogojev-za-delodajalce-oz-iroma-upravljavce>

<sup>10</sup><https://www.ip-rs.si/publikacije/prirocniki-in-smernice/smernice-po-splošni-uredbi-o-varstvu-podatkov-gdpr/smernice-o-preverjanju-pct-pogojev-za-posameznike>

<sup>11</sup><https://www.ip-rs.si/publikacije/prirocniki-in-smernice/smernice-po-splošni-uredbi-o-varstvu-podatkov-gdpr/smernice-o-preverjanju-pct-pogoja-za-šole>

Smernice o preverjanju pogoja PCT za različne ciljne publikе.



Projekt iDECIDE naj bi se končal v prvem kvartalu leta 2022.

Med številnimi aktivnostmi v sklopu ozaveščanja v povezavi z epidemijo covid-19 je Informacijski pooblaščenec nadaljeval objave na posebni »covid-19 podstrani«<sup>12</sup>, kjer so na voljo aktualna mnenja in stališča glede dela in šolanja na daljavo, sprejetih ukrepov za omejevanje širjenja koronavirusa ter drugih ukrepov glede tehničnih rešitev za boj z epidemijo. Informacijski pooblaščenec je na nekatere pereče probleme opozarjal tudi s priporočili, med drugim na to, da prepoved vpogleda v povzetek podatkov o pacientu ni povezana s preverjanjem izpolnjevanja pogoja PCT<sup>13</sup>, da je nedopustno preusmerjanje elektronske pošte delavcev, kar je potrdila tudi sodna praksa<sup>14</sup> ter glede novih pravil za uporabo brezpilotnih zrakoplovov (dronov)<sup>15</sup>. V začetku leta 2021 je namreč v veljavo stopila Izvedbena uredba Komisije (EU) 2019/947 z dne 24. 5. 2019 o pravilih in postopkih za upravljanje brezpilotnih zrakoplovov (C/2019/3824), ki določa pravila in postopke za upravljanje brezpilotnih zrakoplovov in se neposredno uporablja v vseh državah članicah EU.

### 3.5.6 PREVENTIVNE AKTIVNOSTI ZA SKLADNOST

Pri izvajanju preventivnih aktivnosti za skladnost je Informacijski pooblaščenec leta 2021 zaradi novonastalih epidemioloških razmer večji poudarek namenil izobraževalnim in ozaveščevalnim aktivnostim, ki so jih terjale razmere ob uvedenih ukrepih za obvladovanje epidemije. Informacijski pooblaščenec je tudi leta 2021 nadaljeval izvajanje preventivnih aktivnosti (angl. privacy sweep). V praksi so se pokazala področja, na katerih lahko zavezanci brez uvajanja stroškovno in časovno zahtevnih inšpekcijskih postopkov samostojno ocenijo stanje na področju varstva osebnih podatkov ter zadostijo zahtevam zakonodaje, v pomoč pa so jim ustrezne informacije nadzornega organa in ustrezna orodja.

Informacijski pooblaščenec je leta 2021 naslovil naslednje skupine zavezancev:

- ponudnike spletnega gostovanja,
- vrtce,
- osnovne in srednje šole ter
- izvajalce taksi služb.

Pri ponudnikih spletnega gostovanja se je kazal sistemski problem razumevanja njihove vloge. Mnogi se namreč niso zavedali, da pri ponujanju svojih storitev sodijo med pogodbeno obdelovalce osebnih podatkov in da morajo posledično s svojimi naročniki ustrezno urediti obveznosti in dolžnosti, kot izhajajo iz člena 28 Splošne uredbe. Informacijski pooblaščenec je pri tem opozoril na možnost uporabe standardizirane pogodbe, ki jo lahko uporabijo upravljavci in obdelovalci za ureditev medsebojnega razmerja, pravic ter obveznosti.<sup>17</sup>

<sup>12</sup><https://www.ip-rs.si/varstvo-osebni-podatkov/varstvo-osebni-podatkov-v-%C4%8Dasu-epidemije-koronavirusa-covid-19>

<sup>13</sup><https://www.ip-rs.si/novice/prepoved-vpogleda-v-povzetek-podatkov-o-pacientu-ni-povezana-s-preverjanjem-izpolnjevanja-pogoja-pct>

<sup>14</sup><https://www.ip-rs.si/novice/6051f21930eff>

<sup>15</sup><https://www.ip-rs.si/novice/6051f21930cca>

<sup>16</sup><https://eur-lex.europa.eu/legal-content/SL/TXT/?uri=CELEX%3A32019R0947>

<sup>17</sup>Standardizirana pogodba je na voljo na povezavi: [https://www.ip-rs.si/fileadmin/user\\_upload/doc/Standardna\\_pogodbena\\_dolocila\\_-\\_clen\\_28\\_15jul2020.docx](https://www.ip-rs.si/fileadmin/user_upload/doc/Standardna_pogodbena_dolocila_-_clen_28_15jul2020.docx)



Na podlagi informacij iz prakse je bilo razvidno, da v vrtcih obstaja sistemska problematika pridobivanja soglasij staršev za obdelavo osebnih podatkov otrok in ob tem ustreznega informiranja o namenih obdelave osebnih podatkov, rokih hrambe in ostalih informacijah, na podlagi katerih lahko starši sprejmejo informirane odločitve o tem, katere obdelave osebnih podatkov svojih otrok bodo dovolili (npr. objave na družabnih omrežjih ipd.). Vrtci pogosto uporabljajo storitev zunanjih pooblaščenih oseb za varstvo osebnih podatkov, izvajalci teh storitev pa so po preliminarnih analizah odziva k reševanju pristopili zelo aktivno. Informacijski pooblaščenec zato ocenjuje, da se bo ta preventivna aktivnost izkazala za zelo uspešno – končni rezultati bodo znani leta 2022, vrtci pa naj bi posodobljene obrazce začeli uporabljati s šolskim letom 2022/2023.

Na področju taksi služb se je v praksi izkazalo, da številni ponudniki taksi prevozov očitno hranijo podatke o preteklih poteh svojih strank, ne da bi stranke o tem predhodno ustrezno informirali in pridobili njihovo soglasje. Informacijski pooblaščenec je zato na podlagi podatkov iz poslovnega registra RS na ponudnike storitev taksi prevozov naslovil poziv za ureditev stanja ter priložil povezave na uporabne vire, kot je obrazec za informiranje.

Ravnatelje osnovnih in srednjih šol je Informacijski pooblaščenec v sodelovanju z resornim ministrstvom opozoril na problematiko obdelave osebnih podatkov zvezi s preverjanjem pogoja PCT. Dopustno je namreč obdelovati samo toliko osebnih podatkov posameznikov, kolikor je v konkretnem primeru nujno potrebno za izpolnitev namena, torej za preverjanje izpolnjevanja pogoja PCT. Sporno bi namreč bilo obdelovati tiste osebne podatke, ki za izpolnitev namena niso nujno potrebni, npr. podatke o vrsti cepiva, o izvajalcu cepljenja ipd., na kar so nakazovale informacije iz prakse. Ravnatelji so bili prav tako opozorjeni na nedopustnost vodenja centralnih seznamov oziroma evidenc glede izpolnjevanja pogoja PCT učencev ali dijakov na ravni šole (npr. v okviru informacijskih rešitev za upravljanje podatkov o šolajočih) ter na to, da šola nima pravne podlage za hrambo dokazil glede izpolnjevanja pogoja PCT učencev ali dijakov, lahko pa šola (prek pooblaščenih oseb) v takšna dokazila vpogleda.

## 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 čezmejnimi 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 na mesec) sestaja na plenarni ravni, poteka tudi v 12 podskupinah strokovnjakov. V letu 2021 je dodatno delovalo tudi sedem 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 potekalo v spletnem okolju, in sicer v okviru spletne video rešitve, ki jo omogoča Evropski parlament in zagotavlja varno komunikacijo. Odbor se je sestel na 15 plenarnih zasedanjih, strokovne in delovne skupine pa na 175 delovnih sestankih.

Predstavniki Informacijskega pooblaščenca 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 pripravljajo smernice in mnenja odbora za svoje področje ter obravnavajo aktualne izzive, s katerimi se srečujejo posamezni nadzorni organi in so pomembni v širšem evropskem prostoru, bodisi zaradi čezmejne obdelave podatkov bodisi zaradi pomembnih vprašanj enotnega tolmačenja evropskih predpisov.

Leto 2021 je v veliki meri zaznamovala pandemija covid-19, ki je botrovala tudi nastanku evropskega digitalnega zelenega potrdila, ki naj bi omogočalo svobodno gibanje znotraj EU med pandemijo covid-19 prek skupnega okvira za izdajanje, preverjanje in sprejemanje potrdila o tem, ali je bil posameznik cepljen in s katerim cepivom, ali je covid-19 že prebolel in kdaj oziroma ali izkazuje negativen rezultat testiranja. Evropski odbor za varstvo podatkov in Evropski nadzornik za varstvo podatkov (EDPS) sta ob tem poudarila, da mora biti delovanje zelenega potrdila skladno s Splošno uredbo o varstvu podatkov in da morajo biti ustrezno naslovljena tveganja za pravice posameznikov. Kljub temu da zeleno potrdilo lahko pripomore k varnejšim potovanjem in izvajanju pravice do svobode gibanja, lahko na drugi strani obdelava podatkov za ta namen pomeni tveganje za neenako obravnavo posameznikov zaradi različnih možnosti dostopa do cepiv, testiranja ter potrdil o preboleznosti. Uporaba digitalnega potrdila bi morala biti tudi v posameznih državah članicah ustrezno določena v njihovi zakonodaji, ki mora upoštevati načela učinkovitosti, nujnosti in sorazmernosti. Tovrstne pravne podlage bi morale jasno opredeliti najmanj obseg obdelave podatkov, natančen namen, kategorije prejemnikov podatkov in varovalke za preprečevanje zlorab pravic posameznikov, še posebej če gre za avtomatizirano obdelavo in obdelavo občutljivih osebnih podatkov. Nove pravne podlage za nadaljnjo obdelavo potrdila bi tako morale biti skladne s prvotnim namenom obdelave na ravni EU, tj. namen omogočanja svobode gibanja v EU. Evropski odbor in EDPS sta poudarila, da ne sme nastajati centralizirana zbirka osebnih podatkov na ravni EU, podatki pa se ne smejo obdelovati dlje, kot je nujno potrebno. Po koncu pandemije covid-19 se ti podatki ne smejo več obdelovati.

Evropski odbor za varstvo podatkov in Evropski nadzornik za varstvo podatkov sta sprejela tudi skupno mnenje glede predloga EU uredbe o enotnih pravilih za področje umetne inteligence. Mnenje pozdravlja enotno urejanje uporabe sistemov umetne inteligence v EU, hkrati pa nadzorni organi opozarjamo, da mora biti uredba usklajena s pravili na področju varstva osebnih podatkov ter da mora jasno določati, da ta veljajo tudi v primeru obdelave podatkov s pomočjo umetne inteligence. Jasno mora biti opredeljen nadzor nad uredbo in vloga organov za varstvo osebnih podatkov. Nadzorni organi pozivamo k splošni prepovedi uporabe sistemov umetne inteligence za namen prepoznave posameznikov in njihovih značilnosti na javnih krajih, npr. z uporabo tehnologij za prepoznavo obrazov, prstnih odtisov, DNK, glasu, in drugih biometričnih ali vedenjskih značilnosti. Prav tako priporočamo prepoved tovrstnih sistemov za namen razvrščanja posameznikov v skupine glede na njihove etnične značilnosti, spol in druge značilnosti, ki lahko vodijo v diskriminacijo. Svarimo tudi pred sistemi, ki omogočajo prepoznavo čustvenih stanj, razen v zelo omejenih okoliščinah zdravstvene narave.

Evropski odbor za varstvo podatkov je leta 2021 aktivno prispeval tudi k razlagam številnih določb Splošne uredbe s smernicami, priporočili in drugimi dokumenti glede:

- omejitev, kot jih določa člen 23 Splošne uredbe,
- dopolnilnih ukrepov pri prenosu podatkov v tretje države,
- pravne podlage za hranjenje podatkov o kreditnih karticah,
- virtualnih glasovnih pomočnikov,
- primerov obvestil o kršitvah varstva osebnih podatkov,
- kodeksov ravnanja kot instrumenta za prenos podatkov v tretje države,

- odnosa med členom 3 Splošne uredbe in določbami glede prenosa podatkov v tretje države,
- potencialne uvedbe digitalnega evra,
- evalvacije implementacije Direktive o varstvu posameznikov pri obdelavi osebnih podatkov, ki jih pristojni organi obdelujejo za namene preprečevanja, preiskovanja, odkrivanja ali pregona kaznivih dejanj ali izvrševanja kazenskih sankcij, ter o prostem pretoku takih podatkov.

Sprejeta mnenja v okviru mehanizma skladnosti po členu 64 so predvsem zadevala certifikacijske in akreditacijske mehanizme v državah članicah EU ter sprejem zavezujočih poslovnih pravil.

Evropski odbor je pojasnjeval procesna pravila čezmejnega sodelovanja, ki ga je vzpostavila Splošna uredba, in sicer so bila v ospredju predvsem vprašanja glede izvedbe sodelovanja »vse ne 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 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 tudi nadaljnje usmeritve glede postopkov po členih 60 in 65.

Evropski odbor je prvič odločal v postopku po členu 66 in sprejel svojo prvo nujno zavezujočo odločitev, in sicer na zahtevo nadzornega organa iz Hamburga, ki je sprejel začasne ukrepe na podlagi člena 66(1) zoper Facebook, ker je ta spremenil svoje pogoje uporabe, ki se nanašajo na evropske uporabnike, in sicer tako da obdeluje določene podatke uporabnikov WhatsApp. Evropski odbor je odločil, da v konkretnem primeru ni bila izkazana nujnost in obstoj kršitve, ki bi narekovala, da mora irski nadzorni organ zoper Facebook sprejeti nujne ukrepe. Je pa zaradi verjetnosti obstoja kršitve Evropski odbor od irskega nadzornega organa zahteval, da prioriteto izvede preiskavo, ali so kršitve dejansko prisotne, in da pridobi dodatne informacije o tem, na kakšen način Facebook in WhatsApp obdelujeta in kombinirata podatke uporabnikov.

Na področju prenosa podatkov v tretje države je treba omeniti, da je Evropska komisija je v letu 2021 sprejela sklepa o ustreznosti ravni varstva osebnih podatkov v Združenem kraljestvu Velike Britanije in Severne Irske, ki se je po t. i. brexitu uvrstilo med tretje države. S sklepoma je ugotovila, da Združeno kraljestvo zagotavlja raven varstva osebnih podatkov, ki je v bistvu enakovredna tej v EU. To v praksi pomeni, da subjektom iz EU (in tudi EGP), ki podatke prenašajo drugim upravljavcem ali obdelovalcem v Združeno kraljestvo, ni treba vzpostaviti nobenih dodatnih orodij za prenos osebnih podatkov (npr. standardnih pogodbenih določil). Evropska komisija je sprejela tudi nove standardne pogodbene klavzule, ki služijo kot podlaga za prenos osebnih podatkov v tretje države in so modularnega značaja, kar pomeni, da vključujejo različne scenarije obdelave osebnih podatkov oz. t. i. module, ki jih pogodbeni stranki izbereta glede na konkretne okoliščine prenosa: EU upravljavec – neEU upravljavec, EU upravljavec – neEU obdelovalec, EU obdelovalec – neEU obdelovalec in EU obdelovalec – neEU upravljavec). Nove klavzule krepijo pravice posameznikov, tako da jim omogočajo, da so obveščeni o postopkih obdelave njihovih podatkov, da imajo možnost vzpostaviti stik s tujimi upravljavci, da prejmejo kopijo sklenjenih klavzul, odškodnino za škodo, povzročeno v zvezi z njihovimi osebnimi podatki, itd.

### 3.6.2 SODELOVANJE V DRUGIH NADZORNIH TELESIH EVROPSKE UNIJE

Informacijski pooblaščenec je leta 2021 na ravni EU aktivno sodeloval v šestih delovnih telesih, ki se ukvarjajo z nadzorom nad obdelavo osebnih podatkov v okviru velikih informacijskih sistemov EU, in sicer:

- v Evropolovem Odboru za sodelovanje (za nadzor nad obdelavo osebnih podatkov v okviru Europol je po Uredbi o Europolu primarno pristojen Evropski nadzornik za varstvo osebnih podatkov – EDPS, ki pa je pri tem dolžan tesno sodelovati z nacionalnimi organi za varstvo osebnih podatkov),
- 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 leta 2021 sprejeti v okviru zgoraj navedenih delovnih teles, je bil v okviru nadzora nad obdelavo osebnih podatkov v CIS sprejet vprašalnik v zvezi z izvajanjem usposabljanj s področja varstva podatkov za osebe, ki dostopa do CIS. V okviru nadzora nad obdelavo osebnih podatkov v VIS je bil sprejet vprašalnik v zvezi s predčasnim izbrisom podatkov, ki ga ureja 25. člen Uredbe (ES) št. 767/2008 Evropskega parlamenta in Sveta z dne 9. 7. 2008 o vizumskem informacijskem sistemu (VIS) in izmenjavi podatkov med državami članicami o vizumih za kratkoročno prebivanje. Sprejeto je bilo tudi skupno pismo v okviru skupin za nadzor nad SIS II in nad VIS, s katerim je bila Evropska komisija seznanjena s skupnimi stališči obeh skupin glede predloga Uredbe o vzpostavitvi in delovanju ocenjevalnega in spremljevalnega mehanizma za preverjanje uporabe schengenskega pravnega reda in razveljavitvi Uredbe (EU) št. 1053/2013.

### 3.6.3 SODELOVANJE V DRUGIH MEDNARODNIH TELESIH

#### POSVETOVALNI ODBOR T-PD

V okviru Sveta Evrope je predstavnik Informacijskega pooblaščenca tudi leta 2021 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. To leto je zaznamovala že 40. obletnica Konvencije št. 108. Odbor je junija in novembra na plenarnih zasedanjih, ki sta potekali na daljavo, 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 informacije, podane s strani nadzornih organov ob dnevu varstva osebnih podatkov. Odbor je leta 2021 aktivno obravnaval aktualne teme, kot je digitalna identiteta. Izdal je Smernice o varstvu posameznikov v zvezi z obdelavo osebnih podatkov s strani političnih kampanj in za politične kampanje, Smernice o prepoznavi obrazov, Mnenje o Poročilu 2185 (2020) Parlamentarne skupščine Sveta Evrope »Umetna inteligenca v zdravstvu: zdravstveni, pravni in etični izzivi pred nami«, Mnenje o osnutku drugega dodatnega protokola k Budimpeški konvenciji, Poročilo o posledicah mehanizmov za meddržavno izmenjavo podatkov za preprečevanje pranja denarja/proti financiranju terorizma in davčne namene na varstvo podatkov, Poročilo o financiranju organov za varstvo podatkov, podal pa je tudi razlago nekaterih določb Konvencije 108+. Odbor je podelil nagrado Stefano Rodotà, in sicer za delo, ki se nanaša na analitiko oseb v zasebnih delovnih razmerjih in varstvo osebnih podatkov.

#### MEDNARODNA DELOVNA SKUPINA ZA VARSTVO OSEBNIH PODATKOV V TEHNOLOŠKIH ZADEVAH (IWGDPT)

Informacijski pooblaščenec je tudi leta 2021 aktivno deloval v Mednarodni delovni skupini za varstvo osebnih podatkov v tehnoloških zadevah (International Working Group on Data Protection in Technology (IWGDPT)), ki združuje predstavnike informacijskih pooblaščenecv in organov za varstvo osebnih podatkov in zasebnosti s celega sveta. Delo skupine prepoznava tudi mednarodna konferenca informacijskih pooblaščenecv.

Zaradi epidemioloških razmer sta bili v letu 2021 odpovedani zasedanja v živo in je skupina delo nadaljevala prek videokonference. Na videokonferenčnem sestanku je bil obravnavan osnutek mnenja o obdelavi osebnih podatkov v okviru pametnih mest, ki bo predvidoma sprejet na naslednjem zasedanju v letu 2022. Številna mesta in samoupravne lokalne skupnosti po svetu v zadnjem času s pridom izkoriščajo potencialne, ki jih nudi internet stvari, da bi tako dosegle boljše upravljanje sredstev in virov ter zagotovile storitve na lokalni ravni. Pri tem se zbirajo podatki o posameznikih in napravah ter podatki z različnih senzorjev, podatki pa se nato analizirajo in uporabljajo za nadzor uporabe lokalnih storitev, kot so promet, energetika, upravljanje z odpadki, za nadzor pojavljanja kriminalitete ter za številne druge namene. Ob številnih legitimnih ciljih pa lahko za to potrebno obsežno zbiranje podatkov, ki vključuje podatke o registrskih tablicah vozil, uporabi brezžičnih omrežij, porabi energentov, lokaciji in gibanju posameznikov, predstavlja poseg v pravice posameznikov, zato je treba veliko pozornosti nameniti predvsem transparentnemu uvajanju tovrstnih rešitev. Zagotoviti je treba ustrezno pravno podlago ter upoštevati preostala temeljna načela varstva osebnih podatkov, kot je vgrajeno in privzeto varstvo podatkov. Tema je relevantna tudi v Republiki Sloveniji in Informacijski pooblaščenec pozorno spremlja aktivnosti, ki jih na lokalni ravni načrtujejo nekatera naša mesta.

## INITIATIVE 20i7

Pobuda Initiative 20i7 je nastala leta 2017 na predlog Informacijskega pooblaščenca. Njen namen je izmenjava prakse in znanj nadzornih organov za varstvo osebnih podatkov z območja nekdanje Jugoslavije, saj se ti soočajo s podobnimi strokovnimi vprašanji in izzivi.

Ker epidemiološke razmere tudi leta 2021 niso dopuščale izvedbe v živo, je Informacijski pooblaščenec gostil spletno srečanje nadzornih organov, na katerem je Informacijski pooblaščenec predstavil aktivnosti posameznih organov, stanje na področju zakonodaje o varstvu osebnih podatkov ter izzive iz prakse, s katerimi se je srečeval v času epidemije covid-19. Nadzorni organi za varstvo osebnih podatkov smo se soočali s podobnimi izzivi, od zbiranja in deljenja zdravstvenih podatkov, dela in šolanja na daljavo do uvajanja aplikacij in tehnoloških rešitev za obvladovanje epidemije, pa tudi z obsežnim sprejemanjem vladnih odločitev in ukrepov, pogosto brez ustreznega upoštevanja temeljnih načel varstva osebnih podatkov. Udeleženci srečanja so izmenjavo praks ocenili kot zelo koristno ter izrazili pripravljenost, da bi v pobudi Initiative 20i7, ki se kaže kot zgleden primer povezovanja v regiji, sodelovali tudi v prihodnje.

### 3.7 SPLOŠNA OCENA STANJA VARSTVA OSEBNIH PODATKOV

Informacijski pooblaščenec je na področju varstva osebnih podatkov opravljal naloge, ki mu jih nalagata Splošna uredba o varstvu podatkov in novi Zakon o varstvu osebnih podatkov na področju obravnavanja kaznivih dejanj (ZVOPOKD). Splošna uredba o varstvu podatkov se od 25. 5. 2018 neposredno uporablja v vseh državah članicah Evropske unije, a je za njeno učinkovito izvajanje v Republiki Sloveniji nujen sprejem novega Zakona o varstvu osebnih podatkov (ZVOP-2), ki še vedno ni sprejet, zato je Evropska komisija februarja 2022 Sloveniji poslala uradni opomin, s čimer se začne postopek zaradi kršitve evropske zakonodaje.

Z uveljavitvijo Splošne uredbe o varstvu podatkov se je glede na obstoječi ZVOP-1 občutno povečal obseg pravic posameznika, na katerega se osebni podatki nanašajo, ter s tem povezane pristojnosti Informacijskega pooblaščenca kot pritožbenega organa. Reševanje takšnih pritožb posameznika, katerih število se je v letu 2021 glede na pretekla leta še povečalo, pa terja določitev posebnih pravil, s katerimi bi se rešila posamezna vprašanja upravnega postopka oz. določil postopek reševanja takšnih pritožb. Prav nesprejetje novega zakona o varstvu osebnih podatkov je Informacijskemu pooblaščenцу povzročilo precej težav in dilem pri vodenju pritožbenih in inšpekcijskih postopkov.

Odsotnost izvedbenega zakona je zelo vplivala zlasti na vodenje prekrškovnih postopkov in izrekanje glob za ugotovljene kršitve, bistveno manj pa na inšpekcijske postopke, saj se v primeru slednjih Splošna uredba o varstvu podatkov uporablja neposredno. Informacijski pooblaščenec lahko torej v primeru ugotovljenih kršitev določb Splošne uredbe o varstvu podatkov, ZVOPOKD ali določb ZVOP-1 zavezancu v postopku inšpekcijskega nadzora odredi odpravo vseh ugotovljenih nepravilnosti ter prepove obdelavo osebnih podatkov ali njihovo blokiranje, medtem ko lahko postopek za prekrške uvede le, če gre za kršitev ZVOPOKD ali tistih členov ZVOP-1, ki še veljajo. Informacijski pooblaščenec torej do sprejetja novega ZVOP-2 ne more izrekat glob za kršitve Splošne uredbe o varstvu podatkov. Na postopkovne nejasnosti in različna tolmačenja zaradi odsotnosti izvedbenega zakona za izvajanje Splošne uredbe pri vodenju prekrškovnih postopkov zaradi kršitev veljavnih določb ZVOP-1 je pokazala tudi sodna praksa. Okrajno in Višje sodišče v Ljubljani (pravnomočna sodba PRp 345/2019 z dne 18. 6. 2020) sta namreč v postopku za prekršek, ki je bil storjen še pred začetkom uporabe Splošne uredbe o varstvu podatkov, zavzela stališče, da Informacijski pooblaščenec ne more več sankcionirati nobene kršitve določb ZVOP-1, ki hkrati predstavlja tudi kršitev določb Splošne uredbe o varstvu podatkov, za katere Splošna uredba o varstvu podatkov v členu 83 predpisuje upravno (in ne kaznovalno) sankcioniranje. Slovenska zakonodaja namreč ne določa postopka za izrekanje upravnih glob, kot jih predpisuje Splošna uredba o varstvu podatkov. Zato bi moral Informacijski pooblaščenec po mnenju sodišča kot prekrškovni organ v vseh primerih, ko prekršek po ZVOP-1 pomeni tudi katero od kršitev določb člena 83 Splošne uredbe o varstvu podatkov, z vidika prekrškovnega prava kot kaznovalnega prava upoštevati Splošno uredbu o varstvu podatkov, ki je po mnenju sodišča za storilca milejši predpis, ter v prekrškovnem postopku uporabiti načelo zakonitosti iz drugega odstavka 2. člena ZP-1. Enakemu stališču se je v svoji zahtevi za varstvo zakonitosti zoper pravnomočno odločbo o prekršku, ki jo je izdal Informacijski pooblaščenec, pridružilo tudi Vrhovno državno tožilstvo Republike Slovenije.

Podobno stališče je v sodbi ZSV 2045/2019 z dne 8. 3. 2021 zavzelo tudi Okrajno sodišče v Ljubljani v

zvezi s prekrškom, ki je bil storjen po začetku uporabe Splošne uredbe o varstvu podatkov (25. 5. 2018), s to razliko, da je sodišče tu zavzelo stališče, da očitano ravnanje po Splošni uredbi o varstvu podatkov ni več prekršek, saj je zanj predpisano upravno sankcioniranje, zato se kršitelju skladno s prvim odstavkom 2. člena ZP-1 ne more izreči globe za prekršek po ZVOP-1. Splošna uredba o varstvu podatkov se namreč v državah članicah uporablja neposredno in kršitev ZVOP-1 ne določa več kot prekršek, pač pa za takšno kršitev predpisuje upravno globo in ne kaznovalno sankcioniranje.

Z navedenimi sodbami, zoper katere je Informacijski pooblaščenec sicer uporabil vsa razpoložljiva pravna sredstva, je nastala pravno povsem nevzdržna situacija, ki je Informacijskemu pooblaščenecu onemogočala tudi izrekanja sankcij za kršitve še veljavnih določb ZVOP-1. Informacijski pooblaščenec je moral zaradi teh sodb začasno nehati z vodenjem prekrškovnih postopkov zaradi kršitev določb ZVOP-1. S prekrškovnimi postopki je nadaljeval šele po prejemu sodbe Vrhovnega sodišča RS IV Ips 2/2021 z dne 16. 3. 2021, ki se nanaša na prekrške, storjene pred uveljavitvijo Splošne uredbe o varstvu podatkov, ter po prejemu sklepa Višjega sodišča v Ljubljani št. PRp 215/2021 z dne 22. 6. 2021, ki se nanaša na prekrške, storjene po uveljavitvi Splošne uredbe o varstvu podatkov. Šele s tema sodnima odločitvama je bilo potrjeno stališče Informacijskega pooblaščenca in Ministrstva za pravosodje, da je prekrškovno sankcioniranje tistih določb ZVOP-1, ki niso v nasprotju s Splošno uredbi o varstvu podatkov in so kot take še vedno veljavne, skladno s slovenskim in evropskim pravnim redom. Bistveni zaključek, ki izhaja iz zadnjih dveh sodnih odločitev, je, da Splošna uredba o varstvu podatkov državam članicam prepušča razmeroma široko polje pri urejanju nacionalnih pravil, s katerimi naj se sankcionirajo kršitve pravil o varstvu osebnih podatkov po Splošni uredbi o varstvu podatkov, zato tudi upravne globe, ki jih ta predpisuje v členu 83, niso edina možna sankcija za kršitve varstva osebnih podatkov. V takem polju diskrecije držav članic pri urejanju sankcioniranja kršitev se po odločitvi Vrhovnega sodišča Republike Slovenije nahajajo tudi določbe ZVOP-1, ki določajo nezakonito ravnanje z osebnimi podatki in predpisujejo sankcijo zanj, po odločitvi Višjega sodišča v Ljubljani pa tudi določbe ZVOP-1, ki določajo kršitve zavarovanja (varnosti) osebnih podatkov in zanje predpisujejo sankcije. Taka ureditev v ZVOP-1 po mnenju sodišč ni v nasprotju s pravili Splošne uredbe o varstvu podatkov, ampak ostaja v njenih mejah. Iz obeh odločitev sodišč tako izhaja, da Splošne uredbe o varstvu podatkov ni mogoče šteti kot kasnejši predpis, ki je za storilca milejši, Informacijski pooblaščenec pa lahko tudi po začetku veljavnosti Splošne uredbe še vedno vodi prekrškovne postopke in izreka sankcije kršiteljem, ki nezakonito obdelujejo osebne podatke ali opustijo postopke in ukrepe za zavarovanje teh podatkov ter s tem storijo prekršek po ZVOP-1, ne glede na to, ali je bil konkretni prekršek storjen pred ali po uveljavitvi Splošne uredbe.

Postopkov o prekršku in izrečenih sankcij je bilo zaradi opisanih zapletov v zvezi s pristojnostjo Informacijskega pooblaščenca za izrekanje prekrškovnih sankcij v letu 2021 bistveno manj kot v preteklih letih in tudi manj, kot bi jih bilo v primeru, če bi Informacijski pooblaščenec lahko izrekal tudi sankcije za ugotovljene kršitve določb Splošne uredbe o varstvu podatkov. Informacijski pooblaščenec je zato pristojno ministrstvo večkrat opozoril na nujnost sprejetja ZVOP-2 in nujnost uskladitve prekrškovnih določb z določbami Splošne uredbe o varstvu podatkov. Informacijski pooblaščenec mora namreč pri izrekanju sankcij slediti Evropskemu odboru za varstvo podatkov, ki 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 o varstvu podatkov. Namen mehanizma je prav usklajevanje prakse različnih nadzornih organov in s tem zagotavljanje, da izrečene globe za podobne prekrške v primerljivih okoliščinah v različnih državah ne bi odstopale, kar je še zlasti pomembno v primerih čezmejnega sodelovanja pri inšpekcijskem nadzoru.

Število prijav, ki jih je leta 2021 prejel Informacijski pooblaščenec, se je glede na pretekla leta sicer še nekoliko povečalo, saj je prejel kar 1360 prijav oz. pobud za uvedbo inšpekcijskega postopka, kar je največ doslej. Informacijski pooblaščenec je na podlagi prijav uvedel 1036 inšpekcijskih postopkov, saj je v medijsko bolj odmevnih zadevah prejel večje število prijav, na podlagi katerih pa je zoper istega zavezanca uvedel le en postopek. Takšne prijave so bile npr. prijave zaradi obdelave osebnih podatkov vlagateljev prijave interesa za cepljenje proti covid-19 prek portala e-Uprava, prijave zaradi pošiljanja vabil k cepljenju proti covid-19, prijave zaradi preverjanja izpolnjevanja pogoja PCT ter prijave zaradi pošiljanja pisem vsem državljanov s strani predsednika Vlade Republike Slovenije.

Poleg prijav, ki so se nanašale na izvajanje ukrepov za preprečevanje in obvladovanje okužb s covid-19, so bile preostale prijave vložene iz podobnih razlogov kot v preteklih letih. Največ jih je bilo vloženi zaradi posredovanja osebnih podatkov neupravičenim osebam, izvajanja videonadzora, uporabe osebnih podatkov

za namene neposrednega trženja, 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.

V zvezi z uveljavljanjem pravic posameznikov je Informacijski pooblaščenec leta 2021 prejel 313 pritožb, pri čemer se je največji delež nanašal na neodzivanje upravljavcev na zahteve posameznikov za seznanitev z lastnimi osebnimi podatki. Informacijski pooblaščenec ugotavlja, da se posamezniki vse bolj zavedajo svoje ustavne pravice do seznanitve z obdelavami njihovih osebnih podatkov, žal pa je odzivnost upravljavcev pogosto neustrezna in seznanjenost z obveznostmi v tem delu slaba.

Informacijski pooblaščenec je prejel in v okviru inšpekcijskih postopkov obravnaval tudi devet primerov nedovoljenega sporočanja ali druge nedovoljene obdelave osebnih podatkov o pacientih, ki so jih na podlagi 46. člena Zakona o pacientovih pravicah poslali izvajalci zdravstvene dejavnosti, ter 108 uradnih obvestil o kršitvi varnosti osebnih podatkov, ki so jih na podlagi člena 33 Splošne uredbe o varstvu podatkov poslali upravljavci osebnih podatkov. Slednja so se najpogosteje nanašala na posredovanje osebnih podatkov nepooblaščenim ali napačnim osebam, nepooblaščenost dostopanje do osebnih podatkov zaradi programske napake ali zlorabe pooblastil s strani zaposlenih, objave osebnih podatkov strank upravnega postopka na oglasni deski portala e-Uprava ter na izgube ali kraje nosilcev osebnih podatkov (npr. osebnih računalnikov in USB-ključkov). Pogosta so bila tudi obvestila o kršitvi varnosti osebnih podatkov zaradi napada oz. vdora v informacijski sistem z izsiljevalskim virusom, kar je upravljavcem osebnih podatkov, ki niso izvajali ustreznih tehničnih in organizacijskih ukrepov za zagotavljanje varnosti obdelave osebnih podatkov, povzročilo velike stroške ter probleme pri zagotavljanju zmožnosti pravočasne povrnitve razpoložljivosti in dostopnosti do osebnih podatkov.

Informacijski pooblaščenec pri obravnavi prijav, prejetih s strani posameznikov, ugotavlja, da so te v mnogih primerih še vedno vložene zaradi nerazumevanja določb Splošne uredbe o varstvu podatkov ter da so za vlaganje prijav in pritožb pogosto odgovorni tudi upravljavci, ki ob zbiranju ali pridobitvi osebnih podatkov posamezniku ne zagotovijo preglednih, razumljivih in lahko dostopnih informacij, kot jim to nalagajo členi 12, 13 in 14 Splošne uredbe. Prav tako številni upravljavci nimajo izdelanih postopkov za obravnavo zahtev posameznikov za uveljavljanje pravic.

Podobno kot v letu 2020 je tudi leto 2021 zaznamovalo večje število prijav in zaprosil za mnenja. Informacijski pooblaščenec je pripravil 1.471 pisnih mnenj in v okviru projekta iDECIDE, ki ga sofinancira EU, izvedel 2.176 svetovanj po telefonu. Veliko se jih je nanašalo na varstvo osebnih podatkov v zvezi z ukrepi zaradi epidemije koronavirusa (covid-19).

Informacijski pooblaščenec pri izvajanju inšpekcijskih nadzorov ugotavlja, da so ugotovljene nepravilnosti ali pomanjkljivosti v številnih primerih še vedno posledica nepoznavanja oz. nerazumevanja predpisov, ki urejajo obdelavo osebnih podatkov, kar je v veliki meri tudi posledica dejstva, da ZVOP-2, ki bi jasneje določil posamezna pravila v zvezi z izvajanjem Splošne uredbe o varstvu podatkov, še vedno ni sprejet. Nepoznavanje in nerazumevanje predpisov se je tudi v letu 2021 pokazalo zlasti v primeru predpisov, ki so bili sprejeti z namenom preprečevanja in obvladovanja okužb s covid-19. Pogosto je namreč prihajalo do sprejemanja nejasnih in ne dovolj premišljenih predpisov, ki so se poleg tega tudi izredno hitro spreminjali, v primeru predvidene obdelave osebnih podatkov pa je bila glede na dosedanjo prakso Ustavnega sodišča pogosto vprašljiva tudi skladnost predpisov z Ustavo, na kar je Informacijski pooblaščenec predlagatelj veseskozi opozarjal.

Podobno kot v preteklosti so bile ugotovljene kršitve v letu 2021 pogosto tudi posledica malomarnega ali neustreznega zagotavljanja varnosti osebnih podatkov ter namerne nezakonite obdelave osebnih podatkov s strani vodstva ali zaposlenih pri upravljavcih osebnih podatkov. To se je kazalo zlasti z nezakonitimi vpogledi v zbirke osebnih podatkov, s sporno obdelavo osebnih podatkov za namene neposrednega trženja ter z neupravičenim izvajanjem videonadzora v delovnih prostorih z namenom nadzora nad zaposlenimi.

Tudi v letu 2021 je Informacijski pooblaščenec posebno pozornost namenil pooblaščenim osebam za varstvo osebnih podatkov in poenostavil način poročanja.

Informacijski pooblaščenec že vse od začetka uporabe Splošne uredbe ugotavlja, da ostaja zagotavljanje jedrnatih, preglednih, razumljivih in lahko dostopnih informacij iz člena 13 in 14 Splošne uredbe kljub

ozaveščanju upravljavcev še vedno ena najpogosteje ugotovljenih kršitev. Informacijski pooblaščenec je zato poleg že pripravljenih obrazcev za informiranje posameznikov pripravil tudi posebno podstran, kjer so zavezancem na voljo vse informacije o zagotavljanju načela preglednosti.<sup>18</sup>

Posebne okoliščine v povezavi z epidemijo koronavirusa so vplivale tudi na področje skladnosti in preventive. Bistveno se je zmanjšalo število 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 leta 2021 izvedel 28 brezplačnih predavanj za zavezance, večinoma seveda z uporabo spletnih orodij, uspešno pa je izvajal tudi projekt iDECIDE, sofinanciran s strani EU in namenjen ozaveščanju treh ciljnih populacij: mladoletnikov, starejših in delovno aktivne populacije. Zaradi velikega števila prejetih vprašanj o preverjanju pogoja PCT, je Informacijski pooblaščenec v drugem delu projekta iDECIDE izdal posebne smernice:

- [za delodajalce oz. upravljavce](#)<sup>19</sup>,
- [za posameznike](#)<sup>20</sup>,
- [za šole](#)<sup>21</sup>.

Informacijski pooblaščenec je pripravil tudi smernice za zagotavljanje skladnosti IT rešitev v šolstvu, smernice za organizatorje dogodkov, vodnik po pravicah za posameznike ter posodobitev smernic o prenosu osebnih podatkov v tretje države. Smernice za zagotavljanje skladnosti IT rešitev v šolstvu je Informacijski pooblaščenec pripravil kot odziv na zaznane težave pri izvajanju šolanja in izobraževanja na daljavo in željo, da se prepreči prekomerne obdelave osebnih podatkov in posege v zasebnost zaradi nespoštovanja zakonodaje pri odločanju o uporabi IT rešitev.

Informacijski pooblaščenec je nadaljeval tudi s preventivnimi aktivnostmi za skladnost (angl. privacy sweep) in v letu 2021 naslovil naslednje skupine zavezancev:

- ponudnike spletnega gostovanja,
- vrtce,
- izvajalce taksi služb ter
- osnovne in srednje šole.

Pri ponudnikih spletnega gostovanja se je kazal sistemski problem razumevanja njihove vloge, saj se mnogi niso zavedali, da pri ponujanju svojih storitev sodijo med pogodbene obdelovalce osebnih podatkov in da morajo posledično s svojimi naročniki ustrezno urediti obveznosti in dolžnosti, kot izhajajo iz člena 28 Splošne uredbe. Vrtce in taksiste je Informacijski pooblaščenec opozoril na bistvene obveznosti glede varstva podatkov, kot so zahteve pri pridobivanju soglasij in informiranje posameznikov o obdelavi. Ravnatelje osnovnih in srednjih šol pa je Informacijski pooblaščenec v sodelovanju z resornim ministrstvom opozoril na problematiko obdelave osebnih podatkov zvezi s preverjanjem pogoja PCT. Skladno z načelom minimizacije obdelave je namreč dopustno obdelovati samo toliko osebnih podatkov posameznikov, kolikor je v konkretnem primeru nujno potrebno za izpolnitev namena (preverjanje izpolnjevanja pogoja PCT). Nezakonito bi bilo torej obdelovati tiste osebne podatke, ki niso nujni za izpolnitev namena (npr. podatke o vrsti cepiva, o izvajalcu cepljenja ipd.). Poudarjeno je bilo tudi, da nikakor ni dovoljeno voditi centralnih seznamov oz. evidenc glede izpolnjevanja pogoja PCT učencev ali dijakov na ravni šole ter da šola nima pravne podlage za hrambo dokazil glede izpolnjevanja pogoja PCT učencev ali dijakov, temveč lahko šola (prek pooblaščenca osebe) v takšna dokazila le vpogleda.

Informacijski pooblaščenec ugotavlja, da je zavedanje pomena varstva osebnih podatkov in zasebnosti v družbi kljub izzivom v letu 2021 med splošnim prebivalstvom ostalo na visoki ravni, zavezanci pa bi lahko bolje izkoristili nekatera orodja za skladnost, ki jih predvideva že sama Splošna uredba. Eno od njih je postopek predhodnega posvetovanja, v okviru katerega lahko zavezanci svoje ocene učinka na varstvo osebnih podatkov pošljejo v predhodno mnenje Informacijskemu pooblaščenecu in tako pridobijo stališča in

<sup>18</sup><https://www.ip-rs.si/zakonodaja/reforma-evropskega-zakonodajnega-okvira-za-varstvo-osebnih-podatkov/klju%C4%8Dna-podro%C4%8Dja-uredbe/obve%C5%A1%C4%8Ddanje-posameznikov-o-obdelavi-osebnih-podatkov>

<sup>19</sup><https://www.ip-rs.si/publikacije/priročniki-in-smernice/smernice-po-spolšni-uredbi-o-varstvu-podatkov-gdpr/smernice-o-preverjanju-pct-pogojev-za-delodajalce-ozroma-upravljavce>

<sup>20</sup><https://www.ip-rs.si/publikacije/priročniki-in-smernice/smernice-po-spolšni-uredbi-o-varstvu-podatkov-gdpr/smernice-o-preverjanju-pct-pogojev-za-posameznike>

<sup>21</sup><https://www.ip-rs.si/publikacije/priročniki-in-smernice/smernice-po-spolšni-uredbi-o-varstvu-podatkov-gdpr/smernice-o-preverjanju-pct-pogoja-za-šole>



priporočila glede ocen učinka. Slednje so namreč zlasti pri velikih projektih, ki vključujejo obsežne obdelave osebnih podatkov, eno ključnih orodij, da se pravočasno in celovito naslovijo tveganja za morebitne kršitve varstva osebnih podatkov pri izvajanju projekta. Žal se je te možnosti v letu 2021 poslužilo le šest zavezancev, ki so pridobili stališča na svoje ocene učinka, projekti pa so bili zelo različne narave: uvajanje avtomatiziranega branja registrskih tablic za upravljanje parkirnih površin, videonadzor priobalnih področij ter videonadzor javnih površin v občini, uvajanje integralnega sistema za nadzor proizvodnje, obravnava bolnikov s kroničnimi stanji v osnovnem zdravstvenem varstvu ter vključitev dodatnih podatkovnih virov v sistema poslovne analitike v državni upravi. Mnenje Informacijskega pooblaščenca na oceno učinka lahko opozori na neidentificirana tveganja ter pomanjkljive ukrepe za njihovo obvladovanje, s pravočasnim obvladovanjem tveganja pa se lahko zavezanci izognejo občutnim stroškom popravilnih ukrepov, potencialnim visokim sankcijam zaradi kršitev ter okrnitvi ali izgubi ugleda pri strankah in v javnosti.

Splošna uredba je formalizirala postopek sodelovanja nadzornih organov za varstvo osebnih podatkov v državah članicah EU in EGS (Islandija, Norveška in Lihtenštajn) pri čezmejnih primerih po načelu »vse na enem mestu«, ki predvideva, da postopek nadzora v čezmejnem primeru obdelave osebnih podatkov vodi t. i. vodilni organ, ki pri tem sodeluje z drugimi organi za varstvo osebnih podatkov; Splošna uredba je uvedla mehanizme vzajemne pomoči in skupnega ukrepanja organov za varstvo osebnih podatkov v državah članicah EU. Informacijski pooblaščenec je leta 2021 sodeloval v kar 154 postopkih medsebojne pomoči med nadzornimi organi po členu 61 Splošne uredbe, pri čemer je prejel 136 zahtev drugih organov, 18 zaprosil za sodelovanje pa je poslal drugim organom v EU. V 75 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, v dveh postopkih pa je prevzel vlogo vodilnega nadzornega organa. Na temelju postopkov določitve vodilnega in zadevnih nadzornih organov je Informacijski pooblaščenec leta 2021 aktivno sodeloval v 62 novo začelih postopkih čezmejnega sodelovanja pri inšpekcijskem nadzoru nad podjetji, ki poslujejo čezmejno, še naprej pa je tudi sodeloval v primerih, začelih še pred letom 2021. V teh postopkih je pričakovan sprejem odločitve nadzornih organov po členu 60 Splošne uredbe, po t. i. mehanizmu »vse na enem mestu«. 40 tovrstnih postopkov so začeli drugi organi v EU; Informacijski pooblaščenec v njih sodeluje kot zadevni organ.

Primeri niso zadevali le storitev priljubljenih spletnih velikanov (Facebook, Google, Amazon itd.), temveč tudi 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 pri spletnih igrah, posredovanje podatkov tretjim osebam, obdelavo osebnih podatkov brez ustrezne pravne podlage, neustrezno informiranje o obdelavi osebnih podatkov, pogosto so se primeri nanašali tudi na kršitve varnosti osebnih podatkov, med prizadetimi pa so bili tudi uporabniki iz Slovenije.

Kar 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 prijave kršitev varstva osebnih podatkov ter pomanjkljivo zavarovanje osebnih podatkov, nezakonito obdelavo osebnih podatkov v okviru neposrednega trženja ter nesorazmerne zahteve po posredovanju osebnih podatkov. Primera, v katerih je Informacijski pooblaščenec sprejel vlogo vodilnega nadzornega organa, saj je sedež upravljavca v Sloveniji, sta zadevala zatrjevane nezakonnosti pri obdelavi osebnih podatkov v spletnih trgovinah.

Leta 2021 je bilo v čezmejnih postopkih, v katerih je sodeloval Informacijski pooblaščenec, izdanih 26 osnutkov odločb po členu 60 Splošne uredbe. 22 postopkov je bilo končanih s končno odločbo po členu 60 Splošne uredbe. V okviru spletne strani Evropskega odbora za varstvo podatkov je na voljo 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](https://edpb.europa.eu/our-work-tools/consistency-findings/register-for-article-60-final-decisions_en).

V letu 2021 je bila sprejeta končna odločitev skladno s členom 65 Splošne uredbe v zvezi z neustreznim informiranjem posameznikov glede obdelave njihovih osebnih podatkov v primeru ponudnika storitev WhatsApp in povezanih podjetij. V svoji zavezujoči odločitvi je Evropski odbor ugotovil dodatne pomanjkljivosti glede obveščanja uporabnikov poleg pomanjkljivosti, ki jih je v prvem osnutku ugotovil Irski nadzorni organ kot vodilni nadzorni organ. Evropski odbor je zato slednjemu med drugim naložil, da mora pri izreku sankcije upoštevati vsa merila iz člena 83 Splošne uredbe. Glede na to je irski nadzorni organ omrežju WhatsApp na podlagi te odločitve zaradi kršitev naložil globo 225 milijonov evrov.

Sodelovanje v čezmejnih primerih inšpekcijskega nadzora 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. Evropski odbor za varstvo podatkov aktivno pristopa h grajenju enotnih rešitev izzivov, ki nastajajo zaradi razlik v nacionalnih procesnih pravilih v državah članicah EU ter pripravlja nadaljnje smernice glede postopkov po členih 60 in 65 Splošne uredbe.

Leta 2021 je pomembno sodbo v zvezi s čezmejnimi sodelovanjem po Splošni uredbi o varstvu podatkov sprejelo tudi Sodišče EU, ki je proučevalo vprašanje, ali lahko nacionalni nadzorni organ, ki po določbah Splošne uredbe ni vodilni, sproži sodni postopek proti domnevemu kršitelju zaradi kršitve določb Splošne uredbe pred nacionalnim sodiščem v svoji matični državi članici. Razsodilo je, da je to mogoče le, če Splošna uredba nadzornemu organu, ki ni vodilni nadzorni organ, daje pristojnost odločanja o tem, ali določena obdelava osebnih podatkov posameznikov krši pravila iz Splošne uredbe, in če so spoštovani postopki sodelovanja in nadzora, določeni s Splošno uredbi. Sodišče EU je poudarilo pomen tesnega, lojalnega in učinkovitega sodelovanja. Pri izvrševanju svojih pristojnosti tako vodilni nadzorni organ ne sme prezreti stališč drugih nadzornih organov, temveč ima vsak ustrezen in utemeljen ugovor enega od preostalih nadzornih organov učinek začasne blokade sprejetja osnutka odločitve vodilnega nadzornega organa.

Leto 2021 je v veliki meri zaznamovala pandemija covid-19, ki je botrovala tudi nastanku evropskega digitalnega zelenega potrdila, ki naj bi omogočalo svobodno gibanje znotraj EU med pandemijo ter naj bi predstavljalo skupni okvir za izdajanje, preverjanje in sprejemanje potrdila o tem, ali je bil posameznik cepljen in s katerim cepivom, ali je covid-19 že prebolel in kdaj oziroma ali izkazuje negativen rezultat testiranja. Evropski odbor za varstvo podatkov in Evropski nadzornik za varstvo podatkov sta ob tem poudarila, da mora biti delovanje zelenega potrdila skladno s Splošno uredbi o varstvu podatkov in da morajo biti ustrezno naslovljena tveganja za pravice posameznikov. Kljub temu da zeleno potrdilo lahko pripomore k varnejšim potovanjem in izvajanju pravice do svobode gibanja, lahko na drugi strani obdelava podatkov za ta namen pomeni tveganje za neenako obravnavo posameznikov zaradi različnih možnosti dostopa do cepiv, testiranja ter potrdil o prebolelnosti. Uporaba digitalnega potrdila bi morala biti v državah članicah ustrezno določena v domači zakonodaji, ki mora upoštevati načela učinkovitosti, nujnosti in sorazmernosti. Tovrstne pravne podlage bi morale jasno opredeliti najmanj obseg obdelave podatkov, natančen namen, kategorije prejemnikov podatkov, opredeliti pa bi morale tudi varovalke za preprečevanje zlorab pravic posameznikov, še posebej če gre za avtomatizirano obdelavo in obdelavo občutljivih osebnih podatkov. Nove pravne podlage za nadaljnjo obdelavo potrdila bi tako morale biti skladne s prvotnim namenom obdelave na ravni EU, tj. z namenom omogočanja svobode gibanja v EU. Evropski odbor in evropski nadzornik sta poudarila, da ne sme nastajati centralizirana zbirka osebnih podatkov na ravni EU ter da se podatki ne smejo obdelovati dlje, kot je nujno potrebno. Po koncu pandemije se ti podatki ne smejo več obdelovati oz. hraniti.

Evropski odbor za varstvo podatkov in Evropski nadzornik za varstvo podatkov sta sprejela skupno mnenje glede predloga EU uredbe o enotnih pravilih za področje umetne inteligence. Mnenje pozdravlja enotno urejanje uporabe sistemov umetne inteligence v EU, hkrati pa nadzorni organi opozarjamo, da mora biti uredba usklajena s pravili na področju varstva osebnih podatkov in da mora jasno določati, da ta pravila veljajo tudi v primeru obdelave podatkov s pomočjo umetne inteligence. Jasno mora biti opredeljen nadzor nad uredbi in vloga organov za varstvo osebnih podatkov. Nadzorni organi pozivamo k splošni prepovedi uporabe sistemov umetne inteligence za prepoznavo posameznikov in njihovih značilnosti na javnih krajih, npr. z uporabo tehnologij za prepoznavo obrazov, prstnih odtisov, DNK, glasu in drugih biometričnih ali vedenjskih značilnosti. Priporočamo tudi prepoved tovrstnih sistemov za namen razvrščanja posameznikov v skupine glede na njihove etnične značilnosti, spol in druge značilnosti, ki lahko vodijo v diskriminacijo, ter svarimo pred sistemi, ki omogočajo prepoznavo čustvenih stanj, razen v zelo omejenih okoliščinah zdravstvene narave.

Evropska komisija je leta 2021 sprejela sklepa o ustreznosti ravni varstva osebnih podatkov v Združenem kraljestvu Velike Britanije in Severne Irske, ki se je po t. i. brexitu, uvrstilo med tretje države. S sklepoma je ugotovila, da Združeno kraljestvo zagotavlja raven varstva osebnih podatkov, ki je v bistvu enakovredna tej v EU, zato subjektom iz EU (tudi EGP), ki podatke prenašajo drugim upravljavcem ali obdelovalcem v Združeno kraljestvo, ni treba vzpostaviti nobenih dodatnih orodij za prenos osebnih podatkov (npr. standardnih pogodbenih določil). Evropska komisija je sprejela tudi nove standardne pogodbene klavzule, ki služijo kot podlaga za prenos osebnih podatkov v tretje države. Nove klavzule krepijo pravice posameznikov, tako da jim omogočajo, da so obveščeni o postopkih obdelave njihovih podatkov, da imajo možnost vzpostaviti stik s

tujimi upravljavci, da prejmejo kopijo sklenjenih klavzul, da se jim izplača odškodnina za škodo, povzročeno v zvezi z njihovimi osebnimi podatki, itd.

**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  
**Manja Resman**, svetovalca Pooblaščenca II  
**Grega Rudolf**, asistent svetovalca  
**mag. Andrej Tomšič**, namestnik informacijske pooblaščenke  
**Maja Wondra Horvat**, svetovalca Pooblaščenca II

**OBLIKOVANJE:**

**Darko Mohar**  
**Tomaž Brodgesell**

**LEKTORIRALA:**

**Katja Klopčič Lavrenčič**

**Informacijski pooblaščenec Republike Slovenije**

Dunajska cesta 22  
1000 Ljubljana  
[www.ip-rs.si](http://www.ip-rs.si)  
[gp.ip@ip-rs.si](mailto:gp.ip@ip-rs.si)

ISSN 2670-5788  
Ljubljana, maj 2022

