



INFORMACIJSKI
POOBLAŠČENEC

2023

Letno POROČILO

☎ 01 230 97 30

✉ gp.ip@ip-rs.si

🌐 www.ip-rs.si

UVODNA BESEDA INFORMACIJSKE POOBLAŠČENKE

Spoštovani,

leto 2023 je na področju varstva osebnih podatkov zaznamoval začetek veljave težko pričakovanega novega Zakona o varstvu osebnih podatkov, hkrati pa je bilo to tudi leto pomembnih premikov v razvoju evropskih predpisov na področju zasebnosti in digitalizacije, na področju dostopa do informacij javnega značaja pa leto ratifikacije Konvencije Sveta Evrope o dostopu do uradnih dokumentov (Tromsø konvencija). To sicer ne pomeni novih zavez za Slovenijo, pomeni pa dolgoročno zavezo države k nadaljevanju prizadevanj za bolj odprto in bolj pregledno delovanje javnega sektorja. Slednjega v Sloveniji kljub zgledni zakonski ureditvi čakajo pomembni izzivi, saj se je število pritožb na tem področju, še posebej zaradi molka organov, v minulem letu močno povečalo.

Že več let vsako leto narašča skupno število pritožb v zvezi z zahtevami za dostop do informacij javnega značaja (v letu 2023 je Informacijski pooblaščenec prejel skupaj 704 pritožbe), visoko pa ostaja tudi število prijav in pobud za uvedbo inšpekcijskega nadzora (skupaj 1.146) na področju varstva osebnih podatkov, število čezmejnih primerov na tem področju, v katerih sodeluje Informacijski pooblaščenec (270), ter število pritožb za uveljavljanje pravic posameznikov glede varstva podatkov (skupaj 251). Na obeh področjih je Informacijski pooblaščenec prejel tudi veliko število zaprosil za mnenja oz. pojasnila. To kaže na visoko raven zavedanja posameznikov o obstoju obeh ustavnih pravic, hkrati pa tudi na številne izzive pri njunem učinkovitem izvajanju.

Zavezanci za dostop do informacij javnega značaja so se v primerjavi z letom poprej slabše odzivali na prejete zahteve za posredovanje informacij, stopnja transparentnosti se je posledično znižala. Največ pritožb je bilo vloženih zoper državne organe, tudi v zvezi z občinami pa je Informacijski pooblaščenec zaznal povečanje števila pritožb, pri čemer se je po nekaj letih upadanja žal vnovič povečalo število pritožb zaradi molka. Povečalo se je tudi število pritožb zoper poslovne subjekte pod prevladujočim vplivom oseb javnega prava. Žal pa Informacijski pooblaščenec po drugi strani vse pogosteje zaznava tudi posamezne primere zlorabe te pravice.

Po oceni Informacijskega pooblaščenca je povečanje števila pritožb po eni strani mogoče pripisati poenostavitvi uveljavljanja pravice dostopa do informacij javnega značaja, na katero zavezanci niso bili ustrezno pripravljene, po drugi strani pa je zaradi reorganizacije državne uprave pri zavezancih prihajalo do kadrovske spremembe in do menjav uradnih oseb, kar je vplivalo na slabšo odzivnost zavezancev. Dostop do informacij javnega značaja je v demokratični družbi pomembno orodje za spremljanje dela javne uprave, zato Informacijski pooblaščenec zavezance in pristojno Ministrstvo za javno upravo ponovno poziva, naj temu področju namenijo več pozornosti.

Na področju dostopa do informacij javnega značaja je v letu 2023 Informacijski pooblaščenec s ciljem krepitve tega področja podal 317 pisnih odgovorov na zaprosila zavezancev, odgovoril pa je tudi na 837 zaprosil v okviru telefonskega dežurstva. Primere iz prakse redno objavlja na svoji spletni strani.

Na področju varstva osebnih podatkov se je Informacijski pooblaščenec v letu 2023 ob velikem številu prijav in pritožb posvečal zlasti izzivom in novostim, ki jih je prinesel nov Zakon o varstvu osebnih podatkov. V marsičem zakon sledi že uveljavljenim rešitvam, na nekaterih področjih pa uvaja spremembe, katerih dolgoročno vzdržnost ter skladnost s predpisi EU bo pokazal čas. Zlasti nekatere postopkovne določbe novega zakona so v marsičem nejasne in povzročajo številne dileme pri izvajanju. Hkrati je nov zakon vendarle omogočil začetek prvih prekrškovnih postopkov zaradi kršitev Splošne uredbe, in sicer za kršitve, storjene po 26. 1. 2023. Na področju inšpekcijskega nadzora Informacijski pooblaščenec ugotavlja, da razlog za številne prijave ostaja neustrezna seznanjenost posameznikov s pravno podlago za obdelavo in informacijami o obdelavi.

Precej pozornosti na področju varstva osebnih podatkov je v letu 2023 Informacijski pooblaščenec namenil tudi podaji mnenj na pomembne nove predloge zakonskih sprememb ter mnenj na s tem povezane ocene učinkov. V tem delu je Informacijski pooblaščenec na področju omejevanja pravic posameznikov vložil zahtevo za presojo ustavnosti Zakona o pacientovih pravicah. Zlasti na področju sistematičnega zbiranja in obdelav osebnih podatkov s strani države so kakovostni predpisi predpogoj za obstoj pravice do zasebnosti in varstva podatkov. Z digitalizacijo se izzivi na tem področju tako v Sloveniji kot v EU eksponentno množijo, zato bo bistveno, da država strateško, modro in premišljeno uvaja in pripravlja zakonske rešitve, povezane s krepitvijo digitalizacije državnih sistemov in izvajanjem novih predpisov EU na področju digitalizacije družbe, kot sta uredba o evropskem upravljanju podatkov in akt o digitalnih storitvah, ki jim bodo v letih 2024 in 2025 sledili nov akt o umetni inteligenci, predpisi, povezani z digitalizacijo finančnega poslovanja, ter uredba o evropskem zdravstvenem podatkovnem prostoru.

Informacijski pooblaščenec je s ciljem lažje uporabe novega zakona in krepitve poznavanja predpisov na področju varstva podatkov v letu 2023 preko pisnih mnenj in telefonskega svetovanja svetoval 2.580 posameznikom in pravnim osebam. Izvedel je tudi 73 *pro bono* predavanj. V ta namen je Informacijski pooblaščenec celovito prenovil vsebine na spletni strani in pripravil številne smernice za zavezanca in posameznike. Pri krepitvi zavedanja in učinkovitega varstva podatkov so ključni sogovornik nadzornih organov pooblaščenec osebe za varstvo podatkov pri zavezancih, zato se je Informacijski pooblaščenec v okviru skupne akcije nadzora Evropskega odbora za varstvo podatkov (EOVP) posvetil prav njim. Akcija je pokazala, da jim bo treba tako na ravni samih organizacij kot na ravni nadzornih organov nameniti več pozornosti. Informacijski pooblaščenec je sodeloval tudi pri pripravi smernic in priporočil, ki jih je pripravil EOVP, med drugim glede tehničnega obsega 5. člena direktive o eZasebnosti in 37. člena direktive o varstvu podatkov s strani organov pregona ter mnenj skupaj z Evropskim nadzornikom za varstvo podatkov glede zakonodajnih aktov na ravni EU, npr. mnenja o predlogu uredbe o digitalnem evru.

Informacijski pooblaščenec se zlasti v okviru članstva v EOVP odziva na številne in vse bolj kompleksne izzive varstva podatkov na ravni EU, ki potrjujejo, da varstva osebnih podatkov ni brez čezmejnega sodelovanja. Med odmevnimi primeri rezultatov čezmejnega nadzora, ki jih je obravnaval EOVP, so bile visoke globe zaradi ugotovljenih kršitev s strani spletnih velikanov, izrečene na podlagi zavezujočih odločitev odbora. Prav čezmejno nadzorno sodelovanje in aktivnosti v okviru EOVP so tudi v letu 2023 predstavljale pomemben delež aktivnosti Informacijskega pooblaščenca v zvezi z upravljavci, ki izvajajo čezmejno obdelavo osebnih podatkov. Informacijski pooblaščenec je sodeloval v 277 postopkih čezmejnega sodelovanja po 60. členu Splošne uredbe, pri čemer je v 274 na novo začelih postopkih sodeloval kot zadevni nadzorni organ, v treh primerih pa je bil vodilni nadzorni organ. Poleg tega je Informacijski pooblaščenec sprožil 18 postopkov čezmejnega sodelovanja, in sicer na podlagi prejete prijave oz. pritožbe.

Velik obseg izzivov in zakonodajni premiki v EU v letu 2023 nakazujejo pot in pasti varstva zasebnosti v naslednjih letih. Tudi na področju transparentnosti pridobljene pravice ob kompleksnosti zahtev in digitalnega ustvarjanja informacij nikakor niso (več) samoumevne. Novega pooblaščenca ali pooblaščenko tako v letu 2024 čakajo pomembne naloge. Ne dvomim, da si bo Informacijski pooblaščenec enako kot doslej tudi z novim vodstvom z učinkovitim vodenjem pritožbenih in nadzornih postopkov, z nadaljevanjem aktivnega sodelovanja z vsemi deležniki in z odprtostjo do posameznikov, podjetij ter vseh drugih organizacij na obeh področjih varovanja ustavnih pravic tudi v prihodnje prizadeval učinkovito zavarovati obe pravici. Odlična ekipa strokovnjakov, ki je svojo strokovnost in predanost varstvu obeh ustavnih pravic v preteklih desetih letih dokazala ob številnih izzivih, je pomembno zagotovilo za to.

Mojca Prelesnik, informacijska pooblaščenka

STRNJEN PREGLED LETA 2023

Dostop do informacij javnega značaja

Na področju dostopa do informacij javnega značaja je Informacijski pooblaščenec v letu 2023 obravnaval 1.021 zadev, kar je največ od ustanovitve (v letu 2022 je obravnaval 971 zadev), od tega 704 pritožb (kar glede na leto 2022 pomeni 10-odstotni porast).

Skrb vzbujajoče je zlasti to, da je za četrtno naraslo skupno število pritožb zaradi molka: v letu 2022 je bilo takih pritožb 241, v letu 2023 pa je Informacijski pooblaščenec prejel 302 taki pritožbi. To kaže na slabši odziv zavezancev na prejete zahteve za posredovanje informacij javnega značaja, hkrati pa to pomeni, da se je znižala stopnja transparentnosti. Največ prejetih pritožb je bilo vloženih zoper državne organe (državna uprava in drugi državni organi), pri katerih je glede na leto poprej naraslo tako število pritožb zoper zavrnilne odločbe kot zoper molk organa. Informacijski pooblaščenec je zaznal povišanje prejetih pritožb tudi v zvezi z občinami, pri čemer se je po nekaj letih upadanja žal vnovič povišalo število pritožb zaradi molka (v letu 2022 je bilo teh pritožb 44, v letu 2023 pa 67). V letu 2023 je na 16 naraslo tudi, sicer še vedno relativno nizko, število pritožb zoper odločitve poslovnih subjektov pod prevladujočim vplivom.

Po oceni Informacijskega pooblaščenca gre takšno stanje pripisati zlasti spremembi pravil in poenostavitvi upravnega poslovanja, ki sta prinesli povečanje števila zahtev in pospešen način komunikacije, na kar zavezanci niso bili ustrezno pripravljene (večina zahtev je bila namreč vložena po e-pošti). Obenem je zaradi reorganizacije državne uprave pri zavezancih prihajalo do kadrovske spremembe in do menjav uradnih oseb, ki so pristojne za to področje. Informacijski pooblaščenec zavezance zato poziva, naj temu področju namenijo več pozornosti, saj v praksi opaža, da s področjem še vedno niso dovolj seznanjeni. Hkrati Informacijski pooblaščenec vnovič poziva tudi Ministrstvo za javno upravo, naj nudi več podpore zavezanecem in prosilcem, npr. v obliki dodatnih brezplačnih usposabljanj, izdaje mnenj in smernic, objave predhodnih mnenj na svojih spletnih straneh. Informacijski pooblaščenec je s ciljem seznanjanja zavezancev in prosilcev s svojimi odločitvami pripravil tudi 317 odgovorov na njihova zaprosila ter opravil 837 svetovanj v okviru telefonskega dežurstva.

Deloma gre porast pritožbenih zadev pripisati tudi dejstvu, da se posamezniki pravnega varstva v pritožbenih postopkih pred Informacijskim pooblaščenecem poslužujejo pogosteje in hitreje, saj je ta postopek enostaven, hiter in brez posebnih stroškov (ni upravne takse), prosilci pa se običajno zastopajo sami. V letu 2023 je Informacijski pooblaščenec žal zaznal tudi več primerov zlorabe oz. neustreznih ravnanj prosilcev. Pravica dostopa do informacij javnega značaja kot temeljna ustavna pravica ne sme postati orodje v rokah prosilcev, da z namenom šikaniranja in zasipavanja zavezancev onemogočajo njihovo delo in ogrožajo njihovo javnopravno poslanstvo. Ob tem je treba upoštevati, da so se za opredelitev zlorabe pravice v praksi Informacijskega pooblaščenca in sodni praksi že razvili kriteriji, ki naj jim zavezanci, v izogib stroškom in zavlačevanju postopkov, v čim večji meri sledijo.

Varstvo osebnih podatkov

Področje varstva osebnih podatkov je v letu 2023 zaznamoval začetek veljave novega Zakona o varstvu osebnih podatkov (ZVOP-2), ki skupaj s Splošno uredbo o varstvu podatkov in Zakonom o varstvu osebnih podatkov na področju obravnavanja kaznivih dejanj (ZVOPOKD) predstavlja sklop sistemskih predpisov za področje varstva osebnih podatkov v Sloveniji. Pomembni premiki so se zgodili tudi na področju priprave in sprejema zakonodaje s področja digitalnega poslovanja in umetne inteligence, ki se vsi neposredno dotikajo varstva osebnih podatkov.

ZVOP-2 je začel veljati 26. 1. 2023, bistvena novost na področju nadzora pa so nadzorni postopki, v okviru katerih Informacijski pooblaščenec obravnava prijave prijavitelja s posebnim položajem. V teh postopkih Informacijski pooblaščenec obravnava kršitve, ki jih v svojih zahtevah zatrjujejo posamezniki, ki menijo, da obdelava osebnih podatkov s strani upravljavca ali obdelovalca krši določbe Splošne uredbe, ZVOP-2 ali drugih zakonov, ki urejajo obdelavo ali varstvo osebnih podatkov.

Informacijski pooblaščenec je v letu 2023 prejel 1.146 prijav oz. pobud za uvedbo inšpekcijskega postopka in 251 prijav prijaviteljev s posebnim položajem po 77. členu Splošne uredbe ter 30. členu ZVOP-2 zaradi kršitev pravic posameznikov. Od tega je bilo 130 pritožb vloženih zaradi suma nezakonite obdelave osebnih podatkov pritožnika, 121 pa zaradi suma kršitve pravic pritožnika, in sicer 75 zaradi suma kršitve pravice dostopa do lastnih osebnih podatkov, 41 zaradi suma kršitve pravice do izbrisa, štiri zaradi suma kršitve pravice do popravka ter ena zaradi suma kršitve pravice do ugovora. Poleg tega je prejel devet pritožb zoper kršitve upravljavcev v zvezi z uveljavljanjem pravic po ZVOPOKD, 14 pritožb zaradi kršitev pri uveljavljanju pravic pacientov po 41. členu Zakona o pacientovih pravicah (ZPacP) in 12 pritožb po 42. členu ZPacP. Informacijski pooblaščenec je v 270 inšpekcijskih postopkih čezmejnega nadzora sodeloval kot zadevni nadzorni organ po 60. členu Splošne uredbe o varstvu podatkov (postopek čezmejnega sodelovanja).

Informacijskemu pooblaščenca je bila v četrtem odstavku 41. člena ZVOP-2 podeljena tudi pristojnost za odločanje o pritožbah vlagateljev, ki jim je upravljavec zavrnil posredovanje osebnih podatkov iz uradnih evidenc ali javnih knjig. V letu 2023 je obravnaval štiri takšne pritožbe. Poleg navedenih prijav in pritožb je Informacijski pooblaščenec v letu 2023 prejel še prijavo sedmih primerov nedovoljenega sporočanja ali druge nedovoljene obdelave osebnih podatkov o pacientih na podlagi 46. člena ZPacP ter 183 uradnih obvestil o kršitvi varnosti osebnih podatkov, ki so jih v tem času na podlagi 33. člena Splošne uredbe o varstvu podatkov na Informacijskega pooblaščenca poslali upravljavci osebnih podatkov.

Prijave za uvedbo inšpekcijskega postopka so bile tudi v letu 2023 vložene iz podobnih razlogov kot v preteklosti. Največ prijav je bilo vloženih zaradi nezakonitega razkrivanja in posredovanja osebnih podatkov neupravičenim osebam, izvajanja videonadzora, uporabe osebnih podatkov za namene neposrednega trženja, nezakonitega ali prekomernega zbiranja osebnih podatkov, nezakonitih vpogledov v zbirke osebnih podatkov ter neustreznega zagotavljanja varnosti osebnih podatkov. Veliko prijav se je nanašalo na izvajanje videonadzora s strani fizičnih oseb, ki so izvajale videonadzor s kamerami, ki so jih namestile na svoje objekte. V teh primerih se praviloma šteje, da posameznik izvaja videonadzor izključno za svoje lastne, domače namene in se Splošna uredba (na kar je vezana pristojnost Informacijskega pooblaščenca) načeloma ne uporablja, razen kadar posameznik videonadzor izvaja ob opravljanju poklicne ali komercialne dejavnosti, snema javni prostor, posnetke posameznikov nezakonito posreduje tretjim osebam ali jih objavi na spletu.

Tudi v letu 2023 je mogoče zaključiti, da so prijave v mnogih primerih vložene zaradi nerazumevanja določb Splošne uredbe o varstvu podatkov ter da so za vlaganje prijav še vedno pogosto krivi tudi sami upravljavci, ki ob zbiranju ali pridobitvi osebnih podatkov posamezniku ne zagotovijo vseh informacij, kot jim to nalagata 13. in 14. člen Splošne uredbe. Kljub ozaveščanju upravljavcev in kljub vzorcem takšnih obvestil, ki jih je Informacijski pooblaščenec objavil na svojih spletnih straneh, prav pomanjkljivo informiranje posameznikov ostaja ena od pogosto ugotovljenih kršitev.

Podobno je v letu 2023 mogoče ugotoviti, da so se uradna obvestila o kršitvi varnosti osebnih podatkov v letu 2023 najpogosteje nanašala na nezakonito razkritje ali posredovanje osebnih podatkov nepooblaščenim ali napačnim osebam, nepooblaščen dostopanje do osebnih podatkov zaradi programske napake ali zlorabe pooblastil s strani zaposlenih ter izgube ali kraje nosilcev osebnih podatkov. V zadnjem času so vse pogostejša tudi obvestila o kršitvi varnosti osebnih podatkov zaradi kibernetkega napada oz. vdora v informacijski sistem z izsiljevalskim virusom.

Informacijski pooblaščenec je zato v letu 2023 redne in sistematične inšpekcijske nadzore izvedel na področjih preverjanja zakonitosti obdelave osebnih podatkov ter spoštovanja splošnih načel za obdelavo osebnih podatkov; ustreznosti postopkov in ukrepov za zagotavljanje varnosti osebnih podatkov; izvajanja določb Splošne uredbe glede informiranja posameznikov o obdelavi, o pogodbeni obdelavi osebnih podatkov ter o vodenju evidenc obdelave. V teh nadzornih postopkih je preverjal tudi zakonitost izvajanja videonadzora v delovnih prostorih ter s tem povezano zakonitost neposrednega spremljanja dogajanja pred kamerami.

Informacijski pooblaščenec je v letu 2023 pripravil obsežno vsebinsko prenovu svoje spletne strani, da bi s tem posameznikom in zavezancem pomagal lažje razumeti novosti, ki jih je prinesel ZVOP-2, ter razmerja med različnimi temeljnimi predpisi na področju varstva osebnih podatkov. Objavil je tudi prenovljene smernice za upravnike večstanovanjskih stavb, smernice o uporabi piškotkov in podobnih sledilnih tehnologij, smernice glede izvajanja videonadzora, smernice za organizatorje dogodkov, smernice glede biometrije po ZVOP-2 ter smernice glede prenosa osebnih podatkov v tretje države in mednarodne organizacije.

Informacijski pooblaščenec je aktivno deloval tudi na področju priprave predpisov s področja varstva osebnih podatkov – pripravil je 93 mnenj na predloge predpisov ter 13 mnenj na prejete zakonodajne ocene učinka, ki so večinoma sledile metodologiji, ki jo je Informacijski pooblaščenec pripravil za ta namen. V zvezi s tem Informacijski pooblaščenec opaža zlasti potrebo po dvigu ozaveščenosti o namenu in obveznosti glede priprave t. i. zakonodajne ocene učinka glede varstva osebnih podatkov, ki jo zahteva tretji odstavek 24. člena ZVOP-2. Namen zakonodajne ocene učinka je, da se še pred oblikovanjem dokončnega besedila členov pravočasno razmisli o tem, kako ustrezno upoštevati temeljna načela varstva osebnih podatkov pri določanju besedila zakona. V pomoč zavezancem je zato Informacijski pooblaščenec pripravil infografiko, ki pojasnjuje namen in proces priprave zakonodajne ocene učinka. Ocenjujemo, da zakonodajne ocene učinka glede varstva osebnih podatkov pozitivno pripevajo k pravočasnemu naslavljanju tveganj in s tem zlasti h kakovosti predpisov.

ZVOP-2 poleg zakonodajnih ocen učinka določa dodatne obveznosti tudi glede ocene učinka v zvezi z vodenjem dnevnikov obdelav (22. in 24. člen ZVOP-2), obdelavami osebnih podatkov za raziskovalne namene (69. člen ZVOP-2), videonadzorom cestnega prometa (80. člen ZVOP-2) in povezovanjem zbirk osebnih podatkov (87. člen ZVOP-2).

S sprejemom ZVOP-2 je pomemben zagon dobilo tudi področje potrjevanja (certifikacije) in s tem povezane akreditacije po Splošni uredbi, ki pred sprejemom ZVOP-2 nista bila možna. V skladu z ZVOP-2 bo akreditacijo teles, ki bodo izvajala certifikacijo (t. i. organi za potrjevanje oz. certifikacijska telesa), opravljala Slovenska akreditacija, dodatne zahteve za akreditacijska merila pa predpiše Informacijski pooblaščenec. Informacijski pooblaščenec je konec leta 2023 pripravil tovrstne zahteve in jih poslal v mnenje Evropskemu odboru za varstvo podatkov, za lažje razumevanje zadevnih postopkov pa je na spletni strani objavil posebno infografiko.

Pomembni sogovorniki Informacijskega pooblaščenca, ki imajo ključno vlogo pri zagotavljanju načela odgovornosti in s tem skladnosti, so pooblaščenec osebe za varstvo osebnih podatkov, zato se jim je Informacijski pooblaščenec v letu 2023 posebej posvetil v okviru prve usklajene akcije sodelovanja (*Coordinated Enforcement Framework – CEF*) Evropskega odbora za varstvo podatkov (EOVP), v kateri smo k izpolnitvi usklajenega vprašalnika povabili vse pooblaščenec osebe s seznama Informacijskega pooblaščenca. Analiza odgovorov je pokazala, da bo v prihodnje treba več pozornosti nameniti predvsem vprašanju, ali so pooblaščenec osebe ustrezno podprte in izobražene, ali opravljajo predvidene naloge na področju nadzora, svetovanja ali ozaveščanja in ali so v morebitnem konfliktu interesov zaradi izvajanja nalog, ki ne sodijo med naloge pooblaščenih oseb. Informacijski pooblaščenec je zato okrepil sodelovanje s pooblaščenimi osebami za varstvo osebnih podatkov in konec leta 2023 organiziral posvet z vsemi pooblaščenimi osebami na ministrstvih, saj

so ta ključna za zagotavljanje učinkovitega varstva osebnih podatkov tako zaradi vodenja številnih velikih zbirk osebnih podatkov kot zaradi priprave sprememb zakonodaje.

Z vidika skladnosti in preventive je Informacijski pooblaščenec skozi leta razvil obširen nabor instrumentov in orodij, s katerimi (poleg že omenjenih) vpliva na raven ozaveščenosti in s tem spoštovanja zakonodaje. Zato bo tudi v prihodnje nadaljeval z izdajanjem smernic, infografik, mnenj, z rednim obveščanjem javnosti preko svoje spletne strani, družabnih omrežij in novičnikov, s sodelovanjem s partnerskimi organizacijami, podeljevanjem priznanj ob dnevu varstva osebnih podatkov ter z izvedbo brezplačnih predavanj in udeležbo na relevantnih strokovnih posvetih in konferencah. V letu 2023 je Informacijski pooblaščenec s pisnimi mnenji svetoval 1.011 posameznikom in organizacijam, 1.569 posameznikom in organizacijam je svetoval po telefonu, izvedel je tudi 73 *pro bono* predavanj.

Informacijski pooblaščenec sodeluje tudi v okviru različnih delovnih skupin EOVP in s tem prispeva k oblikovanju ključnih smernic, priporočil in odločitev v zvezi z varstvom osebnih podatkov. Njegovi predstavniki so v letu 2023 aktivno sodelovali v 11 rednih ekspertnih podskupinah ter v 12 posebnih delovnih ter koordinacijskih skupinah oz. odborih glede specifičnih tematik ter na 15 plenarnih; skupno so se udeležili 147 sestankov. EOVP je v letu 2023 prispeval k razlagam številnih določb Splošne uredbe s smernicami in priporočili, npr. s smernicami o tehničnem obsegu 5. člena direktive o eZasebnosti in s smernicami o 37. členu 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.

Na področju delovanja v okviru EU so bili v letu 2023 najpomembnejši premiki sprejem oz. priprava novih temeljnih evropskih aktov na področju digitalnega poslovanja in umetne inteligence, kot so uredba o evropskem upravljanju podatkov, akt o digitalnih storitvah, nov akt o umetni inteligenci, predpisi, povezani z digitalizacijo finančnega poslovanja, ter uredba o evropskem zdravstvenem podatkovnem prostoru. Na teh področjih je Informacijski pooblaščenec že dobil nekatere nove pristojnosti, ki se bodo s sprejemom novih aktov glede na razvoj področja nadzora digitalnega poslovanja in regulacije umetne inteligence še širila, zlasti sodeč po pristopu k regulaciji teh področij v drugih državah članicah. Informacijski pooblaščenec je v letu 2023 aktivno sodeloval kot član EOVP, med drugim tudi pri svetovanju Evropski komisiji v zvezi z vprašanji varstva podatkov in pri pripravi evropskih predpisov s področja varstva podatkov, in sicer je EOVP pripravil mnenje glede osnutka sklepa o ustreznosti okvira o zasebnosti podatkov EU-ZDA, ki izraža skrb glede izvajanja pravic posameznikov. Skupaj z Evropskim nadzornikom za varstvo podatkov je EOVP pripravil mnenje o predlogu uredbe o digitalnem evru kot digitalni valuti centralne banke, v katerem so poudarjeni vidiki varstva osebnih podatkov pri uporabi digitalnega evra in podana različna priporočila (med drugim naj bi posamezniki vedno imeli možnost izbire pri plačevanju z digitalnim evrom ali denarjem), ter mnenje o predlogu uredbe o določitvi dodatnih postopkovnih pravil v zvezi z izvrševanjem Splošne uredbe o varstvu podatkov. Sprejeta so bila tudi številna mnenja o postopkih skladnosti glede certifikacijskih in akreditacijskih mehanizmov.

Srečanja in s tem sodelovanje vseh nadzornih organov v EOVP so bistveni za zagotavljanje doslednega izvajanja Splošne uredbe po vsej EU in za učinkovit nadzor na področju varstva osebnih podatkov. EOVP je tako pripravil izjavo o tesnejšem sodelovanju nadzornih organov pri izvajanju strateških nadzornih primerov. V okviru svoje strategije za intenzivnejše sodelovanje med nadzornimi organi je EOVP ustanovil podporno skupino strokovnjakov (t. i. *Support Pool of Experts*), katere cilj je zagotoviti vsebinsko podporo članicam EOVP pri njihovih nadzorih. EOVP je v letu 2023 ustanovil tudi novo delovno skupino ChatGPT, katere namen je usklajevanje pri vprašanih skladnosti tega ponudnika generativne umetne inteligence s Splošno uredbo.

KAZALO

1 O INFORMACIJSKEM POOBLAŠČENCU	1
1.1 NASTANEK IN OSEBNA IZKAZNICA INFORMACIJSKEGA POOBLAŠČENCA	1
1.1.1 ORGANIZIRANOST	4
1.2 KLJUČNA PODROČJA DELOVANJA IN PRISTOJNOSTI	6
1.3 FINANČNO POSLOVANJE V LETU 2023	13
2 DOSTOP DO INFORMACIJ JAVNEGA ZNAČAJA.....	17
2.1 PRAVNA UREDITEV NA PODROČJU DOSTOPA DO INFORMACIJ JAVNEGA ZNAČAJA	17
2.2 ŠTEVILO VLOŽENIH PRITOŽB IN REŠENIH ZADEV.....	22
2.2.1 PRITOŽBE ZOPER ZAVRNILNE ODLOČBE IN IZDANE ODLOČBE.....	22
2.2.2 PRITOŽBE ZOPER MOLK	24
2.3 ŠTEVILO VLOŽENIH TOŽB IN PREJETIH SODB	25
2.4 STORJENI PREKRŠKI PO ZDIJZ, ZInfP IN ZMed.....	26
2.5 IZBRANI PRIMERI NA PODROČJU DOSTOPA DO INFORMACIJ JAVNEGA ZNAČAJA	26
2.6 AKTIVNOSTI IZOBRAŽEVANJA IN OZAVEŠČANJA.....	37
2.6.1 Dan pravice vedeti.....	37
2.6.2 Mednarodno sodelovanje	38
2.7 SPLOŠNA OCENA IN PRIPOROČILA	40
3 VARSTVO OSEBNIH PODATKOV	42
3.1 KONCEPT VARSTVA OSEBNIH PODATKOV V REPUBLIKI SLOVENIJI	42
3.2 NADZOR V LETU 2023	45
3.2.1 INŠPEKCIJSKI NADZOR	45
3.2.2 INŠPEKCIJSKI NADZOR V JAVNEM SEKTORJU	46
3.2.3 INŠPEKCIJSKI NADZOR V ZASEBNEM SEKTORJU.....	47
3.2.4 PRIJAVE KRŠITEV VARNOSTI OSEBNIH PODATKOV.....	49
3.2.5 PRITOŽBENI POSTOPKI PO 77. ČLENU SPLOŠNE UREDBE	49
3.2.6 PRAVICE POSAMEZNIKOV	51
3.2.7 OSTALI PRITOŽBENI POSTOPKI	53
3.2.8 SODELOVANJE PRI ČEZMEJNIH INŠPEKCIJSKIH NADZORIH	54
3.2.9 PREKRŠKOVNI POSTOPKI	57
3.2.10 IZBRANI PRIMERI OBDELAVE OSEBNIH PODATKOV.....	59
3.3 DRUGI UPRAVNI POSTOPKI	69
3.3.1 DOPUSTNOST IZVAJANJA BIOMETRIJSKIH UKREPOV	69
3.3.2 POVEZOVANJE ZBIRK OSEBNIH PODATKOV	70
3.3.3 PRENOS OSEBNIH PODATKOV V TRETJE DRŽAVE	72
3.4 PRIPRAVA MNENJ IN POJASNIL	74
3.4.1 SPLOŠNA POJASNILA	74
3.4.2 MNENJA NA PREDPISE	74
3.4.3 ZAHTEVA ZA OCENO USTAVNOSTI IN ZAKONITOSTI	76
3.5 SKLADNOST IN PREVENTIVA	79
3.5.1 NOVE OBVEZNOSTI UPRAVLJAVCEV PO ZVOP-2	79
3.5.2 OZAVEŠČANJE OB SPREJEMU ZVOP-2	85
3.5.3 OCENE UČINKOV NA VARSTVO OSEBNIH PODATKOV	85
3.5.4 POOBLAŠČENE OSEBE ZA VARSTVO PODATKOV	89
3.5.5 AKTIVNOSTI IZOBRAŽEVANJA IN OZAVEŠČANJA.....	89

3.5.6 PREVENTIVNE AKTIVNOSTI ZA SKLADNOST	90
3.6 MEDNARODNO SODELOVANJE	92
3.6.1 SODELOVANJE V EVROPSKEM ODBORU ZA VARSTVO PODATKOV	92
3.6.2 SODELOVANJE V DRUGIH NADZORNIH TELESIH EVROPSKE UNIJE	98
3.6.3 SODELOVANJE V DRUGIH MEDNARODNIH TELESIH.....	99
3.7 SPLOŠNA OCENA STANJA VARSTVA OSEBNIH PODATKOV	102

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 – Zakon o varstvu osebnih podatkov (veljavnost od 26. 1. 2023)

ZInfP – Zakon o Informacijskem pooblaščenču

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-2 – Zakon o elektronskih komunikacijah

ZCKR – Zakon o centralnem kreditnem registru

ZPotK-2 – Zakon o potrošniških kreditih

ZBan-3 – Zakon o bančništvu

ZUstS – Zakon o Ustavnem sodišču

ZJN-3 – Zakon o javnem naročanju

ZIN – Zakon o inšpekcijskem nadzoru

ZP-1 – Zakon o prekrških

ZSPJS – Zakon o sistemu plač v javnem sektorju

ZKP – Zakon o kazenskem postopku

ZPPDFT-2 – Zakon o preprečevanju pranja denarja in financiranja terorizma

ZKSNKB – Zakon o kupcih in serviserjih nedonosnih kreditov bank

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 pooblaščenecu (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 pooblaščencom 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 Evropski uniji (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). Direktiva (EU) 2016/680 je bila v slovenski pravni red prenesena z Zakonom o varstvu osebnih podatkov na področju obravnavanja kaznivih dejanj (ZVOPOKD), ki se je začel uporabljati 31. 12. 2020. Splošna uredba pa je terjala sprejem novega Zakona o varstvu osebnih podatkov, s katerim bi se v Republiki Sloveniji zagotovilo celovito izvajanje navedene uredbe, vključno s sankcioniranjem kršitev. Novi Zakon o varstvu osebnih podatkov (ZVOP-2) je bil sprejet 15. 12. 2022 in se je začel uporabljati 26. 1. 2023.

Informacijski pooblaščenec tako kot nadzorni organ spremlja uporabo Splošne uredbe, ZVOP-2 in ZVOPOKD, da se zaščitijo temeljne pravice in svoboščine posameznikov v zvezi z obdelavo osebnih podatkov ter se olajša prost pretok osebnih podatkov v EU. Splošna uredba, ZVOP-2 in ZVOPOKD določajo naloge Informacijskega pooblaščenca kot nadzornega organa ter pri tem opredeljujejo njegova pooblastila. Z navedenimi predpisi je okrepjeno tudi sodelovanje med nadzornimi organi v EU, še posebej s sodelovanjem Informacijskega pooblaščenca v okviru Evropskega odbora za varstvo podatkov (EOVP).

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

LETO 2023 V ŠTEVILKAH



48
zaposlenih



2.674.238,00
EUR proračuna

Varstvo osebnih podatkov



686
inšpekcijskih postopkov



251
pritožb po 77. členu
Splošne uredbe



111
prekrškovnih postopkov



1569
ustnih mnenj



1011
pisnih mnenj



6
novih smernic



93
mnenj na predpise



3
infografike



73
predavanj



183
prijav kršitev varnosti



29
mnenj na prejete ocene učinka



3340
imenovanih pooblaščenih oseb
za varstvo podatkov



3
preventivne aktivnosti za
skladnost



277
mednarodnih sodelovanj po
načelu "vse na enem mestu"



247
postopkov vzajemne
pomoči drugim
nadzornim organom EU



274
postopkov odločanja o
vodilnem nadzornem organu

Informacije javnega značaja



704
vložene pritožbe



389
izdanih odločb



232
pozivov zaradi molka



35
in camera ogledov



28 dni
povprečen čas reševanja
pritožbenih zadev



317
pisnih prošenj za pojasnila

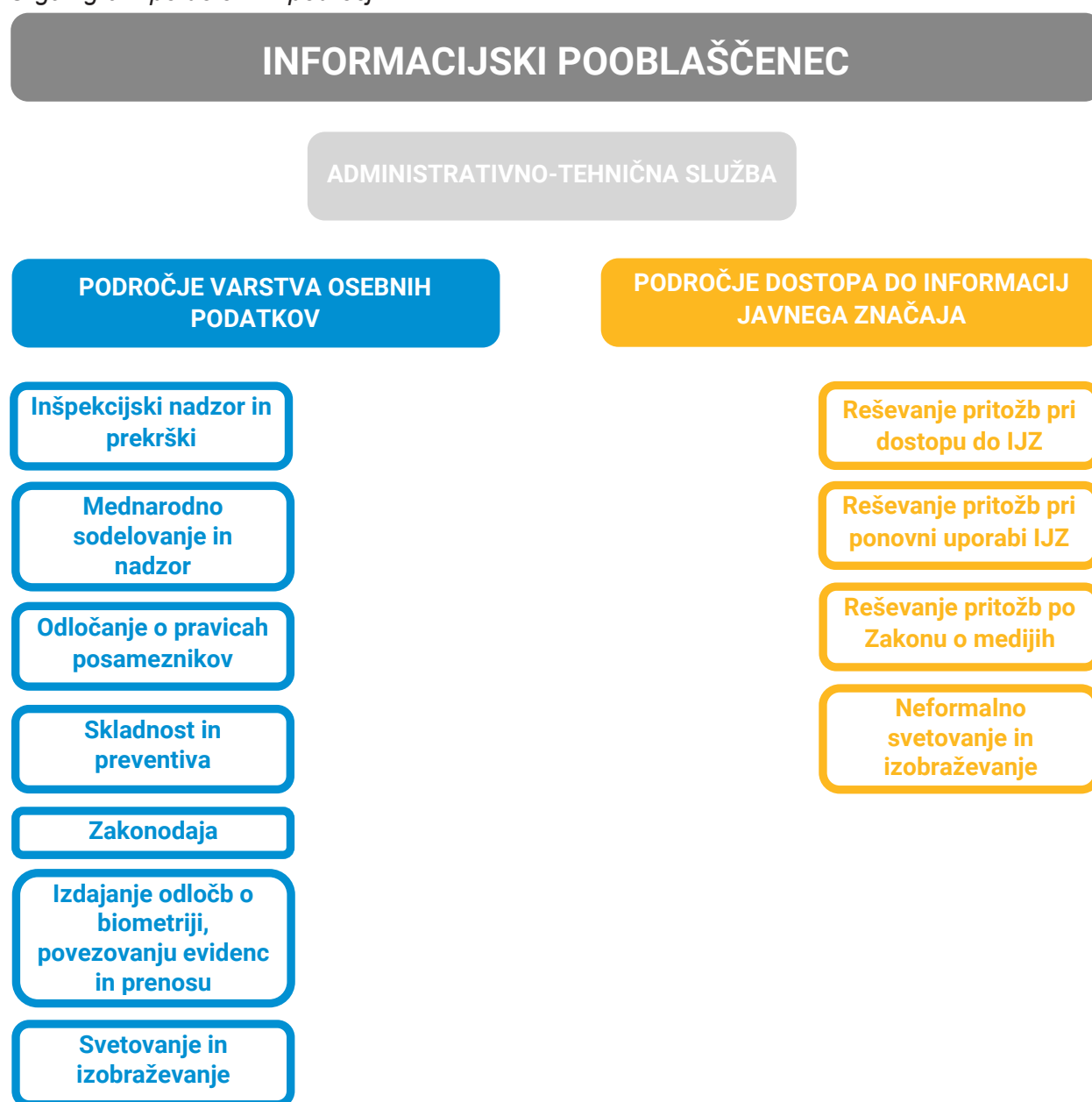
1.1.1 ORGANIZIRANOST

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. 2023 je bil pri Informacijskem pooblaščenju zaposlen 1 funkcionar in 47 javnih uslužbencev. Izobrazbena struktura zaposlenih je razvidna iz preglednice.

Izobrazbena struktura zaposlenih pri Informacijskem pooblaščenju 31. 12. 2023.

	Srednja strokovna šola	Višja strokovna šola	Visoka strokovna šola, univerzitetni program	Univerzitetna izobrazba	Magisterij	Doktorat	Skupaj
Informacijska pooblaščenka				1			1
Namestnik informacijske pooblaščenke				2	2		4
Vodja mednarodnega sodelovanja in nadzora						1	1
Vodja nadzornikov					1		1
Generalni sekretar					1		1
Državni nadzornik za varstvo osebnih podatkov				11	4	1	16
Samostojni svetovalec pooblaščenca				1		1	2
Svetovalec pooblaščenca				5	2		7
Svetovalec pooblaščenca za varstvo osebnih podatkov				2	1		3
Svetovalec pooblaščenca za mednarodne odnose						1	1
Svetovalec pooblaščenca za preventivo				1			1
Asistent svetovalca				1			1
Raziskovalec pooblaščenca			2				2
Strokovni sodelavec za finančne in kadrovske zadeve		1					1
Sistemiški administrator			1				1
Poslovni sekretar			2				2
Dokumentalist		1					1
Projektni sodelavec	2						2
Skupaj	2	2	5	24	11	4	48

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 pooblaščenec 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.

Ključni 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.

Splošna uredba določa naloge Informacijskega pooblaščenca kot nadzornega organa v 57. členu. 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 z 80. členom telo, organizacija ali združenje, v ustreznem obsegu prouči 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 pogodbeno določila iz osmega odstavka 28. člena in točke (d) drugega odstavka 46. člena;
- (k) vzpostavi in vzdržuje seznam v zvezi z zahtevo po oceni učinka v zvezi z varstvom osebnih podatkov v skladu s četrnim odstavkom 35. člena;
- (l) svetuje glede dejanj obdelave iz drugega odstavka 36. člena;
- (m) spodbuja pripravo kodeksov ravnanja v skladu s prvim odstavkom 40. člena ter poda mnenje in v skladu s petim odstavkom 40. člena 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 prvim odstavkom 42. člena in odobri merila potrjevanja v skladu s petim odstavkom 42. člena;
- (o) kadar je ustrezno, izvaja redne preglede potrdil, izdanih v skladu s sedmim odstavkom 42. člena;
- (p) oblikuje in objavi merila za pooblastitev telesa za spremljanje kodeksov ravnanja v skladu z 41. členom in organa za potrjevanje v skladu s 43. členom;
- (q) opravi pooblastitev telesa za spremljanje kodeksov ravnanja v skladu z 41. členom in organa za potrjevanje v skladu s 43. členom;
- (r) odobri pogodbeno določila in določbe iz tretjega odstavka 46. člena;
- (s) odobri zavezujoča poslovna pravila v skladu s 47. členom;
- (t) prispeva k dejavnostim Evropskega odbora za varstvo podatkov;
- (u) hrani notranjo evidenco kršitev te uredbe in sprejetih ukrepov v skladu z drugim odstavkom 58. člena ter
- (v) opravlja vse druge naloge, povezane z varstvom osebnih podatkov.

Skladno s tretjim odstavkom 55. člena 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).

Začetek uporabe Splošne uredbe je terjal sprejetje novega **Zakona o varstvu osebnih podatkov (ZVOP-2)**, da bi se zagotovilo izvajanje Splošne uredbe. ZVOP-2 je bil sprejet 15. 12. 2022 in se je začel uporabljati 26. 1. 2023. Pristojnosti Informacijskega pooblaščenca so določene zlasti v 29., 55. in 56. členu ZVOP-2, in sicer Informacijski pooblaščenec:

1. izvaja nadzore nad izvajanjem določb Splošne uredbe, ZVOP-2 in drugih predpisov s področja varstva osebnih podatkov;
2. odloča v pritožbenem postopku, odloča v postopkih prijav prijaviteljev s posebnim položajem in izvaja inšpekcijski nadzor po ZVOP-2;
3. odreja nadzorne ukrepe iz 29. člena ZVOP-2, in sicer odredi: odpravo nepravilnosti ali pomanjkljivosti, omejitve obdelave (kot so anonimiziranje, blokiranje in arhiviranje), prepoved prenosa v tretjo državo ali posredovanje tujim uporabnikom, brisanje ali uničenje osebnih podatkov ali druge ukrepe, ki pomenijo prepoved obdelave osebnih podatkov;
4. odreja druge nadzorne ukrepe skladno z zakonom, ki ureja splošni upravni postopek, in z Zakonom o varstvu osebnih podatkov na področju obravnavanja kaznivih dejanj (ZVOPOKD) ter izvaja preventivne ukrepe in izreka opozorila skladno z zakonom, ki ureja inšpekcijski nadzor,
5. lahko poda kazensko ovadbo oz. izvaja postopke v skladu z zakonom, ki ureja prekrške, če pri inšpekcijskem nadzoru ugotovi, da obstaja sum storitve kaznivega dejanja ali prekrška;

6. daje in objavlja predhodna mnenja ministrstvom, državnemu zboru, organom samoupravnih lokalnih skupnosti, drugim državnim organom in nosilcem javnih pooblastil o usklajenosti določb predlogov zakonov ter drugih predpisov z zakoni in drugimi predpisi, ki urejajo osebne podatke;
7. izvaja predhodno posvetovanje v skladu s Splošno uredbo in ZVOP-2;
8. vodi postopke o prekrških s področja varstva osebnih podatkov (hitri postopek);
9. vodi upravne postopke za izdajo ugotovitvenih odločb o tem, ali je nameravana uvedba izvajanja biometrijskih ukrepov v skladu z določbami ZVOP-2;
10. pristojnim organom in posameznikom daje in objavlja neobvezna mnenja, pojasnila in stališča o vprašanih glede varstva osebnih podatkov v zvezi z zakoni in z njimi povezanimi predpisi s področja varstva osebnih podatkov;
11. spodbuja ozaveščenost in razumevanje javnosti o tveganjih, pravilih, zaščitnih ukrepih in pravicah v zvezi z obdelavo ter v ta namen izvaja brezplačna izobraževanja in usposabljanja;
12. spodbuja ozaveščenost upravljavcev in obdelovalcev o njihovih obveznostih na podlagi tega zakona;
13. sodeluje z nadzornimi organi drugih držav ali mednarodnih organizacij (npr. v nadzornih organih, ki se ukvarjajo z nadzorom obdelave osebnih podatkov v schengenskem informacijskem sistemu, v informacijskem sistemu za carino, v vizumskem informacijskem sistemu, v okviru Europola ter v sistemu Eurodac);
14. sodeluje z nadzornimi organi drugih držav članic Evropske unije pri izvajanju čezmejnih nadzornih postopkov, pri postopkih izrekanja sankcij in v drugih zadevah čezmejne obdelave osebnih podatkov v skladu s VII. poglavjem Splošne uredbe;
15. deluje kot vodilni nadzorni organ pri izvajanju čezmejnih nadzornih postopkov v skladu s Splošno uredbo;
16. sodeluje pri delovanju EOVP;
17. obvesti pristojno sodišče o kršitvah zakona, lahko pa sodišču v sodnem postopku tudi posreduje mnenje o ugotovljenih kršitvah;
18. sodeluje z upravljavci in obdelovalci pri izvajanju nadzorov v skladu z ZVOP-2;
19. olajša postopek vložitve pritožb in zahtev posameznikov s pripravo obrazcev, ki se lahko vložijo tudi v elektronski obliki (npr. glede uveljavljanja pravic posameznikov ali v zvezi z vlogami inšpekcijskega nadzora);
20. izdaja notranje glasilo in strokovno literaturo ter na spletni strani in na druge ustrezne načine objavlja: odločbe ali mnenja IP, odločbe in sklepe Ustavnega sodišča RS o zahtevah za oceno ustavnosti, ki jih je vložil IP, in odločitve Ustavnega sodišča RS o njih, psevdonimizirane odločbe in sklepe sodišč, ki se nanašajo na varstvo osebnih podatkov, psevdonimizirane pomembnejše odločitve v nadzornih in pritožbenih postopkih IP, podatke o uvedbi in zaključku nadzornih postopkov, uvedenih po uradni dolžnosti, ter druga pomembna obvestila;
21. daje mnenja o skladnosti splošnih pogojev poslovanja oz. njihovih predlogov s predpisi s področja varstva osebnih podatkov;
22. pripravlja in daje neobvezne smernice in priporočila glede varstva osebnih podatkov na posameznem področju;
23. daje izjave za javnost o nadzoru v posamičnih zadevah v skladu s tem zakonom in izvaja konference za medije v zvezi s svojim delom ter
24. izvaja druge naloge, določene v 57. členu Splošne uredbe in v ZVOP-2.

Cilj novega ZVOP-2 je bil med drugim zagotoviti učinkovit nadzor glede varstva osebnih podatkov ter zagotoviti učinkovito prekrškovno kaznovanje kršitev varstva osebnih podatkov. Informacijski pooblaščenec je po ZVOP-2 nadzorni organ za varstvo osebnih podatkov, in sicer je pristojen za nadzor varstva osebnih podatkov za vse obdelave osebnih podatkov v Republiki Sloveniji, razen npr. kadar gre za nadzor in izrekanje sankcij glede obdelav osebnih podatkov, izvršenih pri izvajanju sodne oblasti sodišč in Ustavnega sodišča Republike Slovenije. Informacijski pooblaščenec prav tako ni pristojen za obdelave osebnih podatkov s strani stečajnih upraviteljev, izvršiteljev, sodnih tolmačev, sodnih izvedencev in sodnih cenilcev v zadevah, pri katerih delujejo po postopkih v okviru izvajanja zadeve sodišča. Določene pa so tudi nekatere omejitve pri izvajanju nadzorov, npr. na

področju obveščevalno-varnostne dejavnosti in pri izvajanju nadzora pri Varuhu človekovih pravic. S sprejemom ZVOP-2 je Informacijskemu pooblaščencau omogočeno tudi izrekanje glob za kršitve Splošne uredbe. 95. člen ZVOP-2 določa, da se sankcije za kršitve, ki jih predpisuje Splošna uredba, izrekajo pravnim osebam, samostojnim podjetnikom posameznikom in posameznikom, ki samostojno opravljajo dejavnost, kot globe za prekrške v višini in razponih, ki jih določa Splošna uredba. Dodatno ZVOP-2 opredeljuje tudi globe za odgovorne osebe in posameznike.

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 ministrstvu, 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 z njimi 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-2)**, **Zakonu o centralnem kreditnem registru (ZCKR)**, **Zakonu o potrošniških kreditih (ZPotK-2)** in **Zakonu o kupcih in serviserjih nedonosnih kreditov bank (ZKSNKB)**.

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-2.

Pristojnosti Informacijskega pooblaščenca po **ZPLD-1** in **ZOIzk-1** so omejene na določbe, ki določajo, v kakšnih primerih in na kakšen način lahko upravljavci osebnih podatkov kopirajo potne listine oz. osebne izkaznice ter način hrambe kopij (4. člen ZOIzk-1 in 4.a člen ZPLD-1). Informacijski pooblaščenec v zvezi z navedenimi določbami opravlja naloge inšpekcijskega in prekrškovnega organa, pri čemer o prekršku odloča v skladu s 27. členom ZOIzk-1 in 34.b členom ZPLD-1.

ZEKom-2 določa pristojnosti Informacijskega pooblaščenca v 229. členu, in sicer Informacijski pooblaščenec:

- izvaja inšpekcijski nadzor nad izvajanjem določb 216. člena ZEKom-2, ki ureja notranje postopke o odzivanju na zahteve pristojnih organov za dostop do osebnih podatkov uporabnikov na podlagi področnih zakonov;

- najmanj enkrat letno opravlja inšpekcijski nadzor nad obdelavo podatkov iz 220. člena ZEKom-2, ki določa pogoje in postopke za posredovanje prometnih in lokacijskih podatkov v primerih varovanja življenja in telesa posameznika;
- izvaja inšpekcijski nadzor nad izvajanjem določb 223. člena ZEKom-2, 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 225. člena ZEKom-2, ki ureja shranjevanje podatkov ali pridobivanje dostopa do podatkov, shranjenih v terminalski opremi naročnika ali uporabnika s pomočjo piškotkov in podobnih tehnologij.

Na področju, ki ga nadzoruje, Informacijski pooblaščenec odloča o prekrških za kršitve ZEKom-2 in na njegovi podlagi izdanih predpisov, in sicer kot prekrškovni organ v skladu z zakonom, ki ureja prekrške (298. do 303. člen ZEKom-2).

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 (drugi odstavek 3. člena ZCKR). 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-2. 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.

ZKSNKB je začel veljati 24. 2. 2024 in v petem odstavku 42. člena določa, da je Informacijski pooblaščenec pristojen za nadzor nad izpolnjevanjem obveznosti 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 se pojavi vprašanje ustavnosti ali zakonitosti v zvezi s postopkom, ki ga vodi.

Pristojnosti Informacijskega pooblaščenca opredeljujejo tudi pravila **schengenskega informacijskega sistema (in druga generacija sistema, t. i. SIS II)**, ki nacionalnim organom kazenskega pregona ter pravosodnim in upravnim organom omogočajo izmenjavo in dostop do podatkov o prestopu zunanjih meja in vizumski politiki, v sistem pa so poleg tega vključeni tudi podatki o evropskem zapornem nalogu, izročitvi, biometrični podatki in podatki o iskanju zaradi terorističnih aktivnosti. Pravni okvir SIS II vključuje: **Uredbo (ES) št. 1987/2006 Evropskega parlamenta in Sveta z dne 20. decembra 2006 o vzpostavitvi, delovanju in uporabi druge**

generacije schengenskega informacijskega sistema (SIS II); Sklep Sveta 2007/533/PNZ z dne 12. junija 2007 o vzpostavitvi, delovanju in uporabi druge generacije schengenskega informacijskega sistema (SIS II) in Uredbo (ES) št. 1986/2006 Evropskega parlamenta in Sveta z dne 20. decembra 2006 o dostopu služb držav članic, pristojnih za izdajo potrdil o registraciji vozil, do druge generacije schengenskega informacijskega sistema (SIS II). Informacijski pooblaščenec na podlagi 60. člena Sklepa Sveta 2007/533/PNZ ter 44. člena Uredbe (ES) št. 1987/2006 nadzira zakonitost obdelave osebnih podatkov v SIS II na svojem ozemlju in pri prenosu s svojega ozemlja, vključno z izmenjavo in nadaljnjo obdelavo dopolnilnih podatkov.

Pristojnosti Informacijskega pooblaščenca.

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

Zakon o dostopu do informacij javnega značaja

Zakon o medijih

1.3 FINANČNO POSLOVANJE V LETU 2023

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 2023 **veljavni proračun na integralnih postavkah 2.674.238,00 EUR**, od tega na postavki plače 2.289.417,00 EUR, na postavki materialni stroški 376.322,00 EUR in na postavki investicije 8.499,00 EUR. Evidentiranih odredb na integralnih postavkah je bilo na dan 31. 12. 2023 2.661.477,82 EUR, od tega na postavki plače 2.280.885,53 EUR, na postavki materialni stroški 372.093,62 EUR in na postavki investicije 8.498,67 EUR.

Proračun Informacijskega pooblaščenca 2018–2023.

Proračunsko leto	Veljavni proračun
2018	1.833.399,66 EUR
2019	2.232.236,00 EUR
2020	2.321.085,00 EUR
2021	2.330.548,50 EUR
2022	2.501.202,00 EUR
2023	2.681.559,05 EUR

Informacijski pooblaščenec je v letu 2023 razpolagal z namenskimi sredstvi v višini 7.317,92 EUR. Porabe namenskih sredstev v letu 2023 ni bilo.

V proračun leta 2024 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 proračunsko postavko 7640 – Rezerva Republike Slovenije v letu 2023 ni bilo prenesenih sredstev z integralnih proračunskih postavk zaradi namena zagotavljanja pravic porabe za oblikovanje in uporabo sredstev proračunske rezerve.

Na postavko plače je bilo s postavk materialni stroški in investicije prerazporejenih 67.701,00 EUR ter 5.840,00 EUR iz splošne tekoče proračunske rezervacije na podlagi 41. člena Zakona o javnih financah (ZJF) v decembru 2023.

Podrobnejša razdelitev finančnih sredstev glede na ukrep in projekte, ki se vodijo pri Informacijskem pooblaščenca, je razvidna iz tabele na naslednji strani.

Proračun Informacijskega pooblaščenca 2023.

	Veljavni proračun v EUR	Prevzete obveznosti v EUR	Razpoložljiv proračun v EUR konec leta
Informacijski pooblaščenec	2.681.559,05	2.661.477,82	20.081,23
OPRAVLJANJE DEJAVNOSTI	2.674.238,00	2.661.477,82	12.760,18
PP 1267 Plače	2.289.417,00	2.280.885,53	8.531,41
PP 1271 Materialni stroški	376.322,00	372.093,62	4.228,38
PP 1273 Investicije	8.499,00	8.498,67	0,33
NAMENSKA SREDSTVA	7.317,92	0,00	7.317,92
7459 Namenska sr. kupnine	7.317,92	0,00	7.317,92
7460 Stvarno premoženje – sr. odškodnine	0,00	0,00	0,00
Donacije – EU projekti	3,13	0,00	3,13
PP 9958 Mednarodna spl. str.	0,14	0,00	0,14
PP130134 projekt Taix	2,99	0,00	2,99
PP200001 iDecide	0,00	0,00	0,00

V letu 2023 je bilo finančno poslovanje razdeljeno na ukrep in projekte:

UKREP

Ukrep 1215-18-0001 vsebuje integralne proračunske postavke materialni stroški 1271 in plače 1267. Znesek veljavnega proračuna ob koncu leta 2023 je bil 2.665.739,00 EUR, prevzete obveznosti ob koncu leta so znašale 2.652.979,15 EUR.

UKREP 1215-18-0001 Opravljanje dejavnosti IP

	Veljavni proračun	Prevzete obveznosti	Razpoložljiv proračun v EUR konec leta
Sredstva skupaj po ukrepu	2.665.739,00	2.652.979,15	12.759,85

PP 1267 Plače	2.289.417,00	2.280.885,53	8.531,47
PP 1271 Materialni stroški	376.322,00	372.093,62	4.228,38

Za plače zaposlenih je bilo porabljenih 2.280.885,53 EUR oz. 99,63 % sredstev glede na veljavni proračun za leto 2023. Glede na predhodna leta se je poraba sredstev povečala zaradi napredovanj, realizacije dogovora o ukrepih na področju plač in drugih stroškov dela v javnem sektorju za leti 2022 in 2023 ter aneksov h kolektivnim pogodbam dejavnosti in poklicev, uskladitve vrednosti plačnih razredov plačne lestvice, višje uvrstitve delovnega mesta oz. naziva v plačni razred, višjega regresa za letni dopust in višjega regresa za prehrano, izplačila 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 zadolžitvev, ki so zahtevale dodatne zaposlitve. Porabljena sredstva v višini 2.280.885,53 EUR so bila namenjena za osnovne plače in dodatke v znesku 1.745.389,26 EUR, za regres za letni dopust je bilo namenjenih 58.935,42 EUR, za povračila in nadomestila 96.111,33 EUR, sredstva za delovno uspešnost z naslova povečanega obsega dela zaradi povečanega pripada zadev in redne delovne uspešnosti so znašala 51.571,79 EUR, za druge izdatke zaposlenim je bilo porabljenih

20.462,58 EUR, za prispevke delodajalcev za pokojninsko in invalidsko zavarovanje 156.401,28 EUR, za prispevke za zdravstveno zavarovanje 127.922,33 EUR, za prispevke za zaposlovanje 1.112,31 EUR, za prispevek za starševsko varstvo 1.804,38 EUR, premije kolektivnega dodatnega pokojninskega zavarovanja na podlagi Zakona o kolektivnem dodatnem pokojninskem zavarovanju za javne uslužbenke pa so znašale 21.174,85 EUR. Informacijski pooblaščenec je leta 2023 od Zavoda za zdravstveno zavarovanje Slovenije z naslova refundacij bolezni in invalidnin prejel sredstva na postavko za plače v višini 76.383,30 EUR.

V januarju 2024 je Informacijski pooblaščenec pripravil negativne odredbe za refundacije bolezni iz leta 2023 v višini 7.896,71 EUR (bolezni v juniju, oktobru in novembru 2023), ki jih je prejel konec leta in jih ni bilo mogoče uporabiti za namen poravnave stroškov za izplačilo plač v decembru.

Za izplačilo manjka na postavki plače za december 2023 je Informacijski pooblaščenec finančna sredstva v višini 67.701,00 EUR zagotovil s prerazporeditvijo privarčevanih sredstev s postavke materialni stroški v višini 44.200,00 EUR (30.000,00 EUR v januarju in 14.200,00 EUR v decembru 2023) in investicij v višini 23.501,00 EUR ter s prerazporeditvijo 5.840,00 EUR iz splošne tekoče proračunske rezervacije na podlagi 41. člena ZJF v decembru 2023.

S postavke plače Informacijski pooblaščenec konec leta 2023 ni prerazporedil prostih pravic porabe na proračunsko postavko 7640 – Rezerva Republike Slovenije.

Za materialne stroške je bilo leta 2023 porabljenih 372.093,62 EUR, in sicer za pisarniški in splošni material in storitve 68.027,02 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 3.300,60 EUR (nakup drobnega inventarja, zdravniški pregledi zaposlenih, strokovne naloge s področja varstva pri delu, testi in maske za zaščito pred covidom-19, paketno zavarovanje odgovornosti ter drugi posebni material in storitve); za energijo, vodo, komunalne storitve, pošto in komunikacijo 47.015,79 EUR (električna energija, ogrevanje, voda in komunalne storitve, odvoz smeti, stroški telefonov ter poštna storitve); za prevozne stroške in storitve 5.772,41 EUR (vzdrževanje, popravila, zavarovanje in registracija dveh službenih vozil, gorivo za službeni vozili, taksi storitve ter drugi prevozni in transportni stroški); za izdatke za službena potovanja 29.354,18 EUR (stroški, povezani s službenimi potovanji zaposlenih, dnevnice, nočnine, letalske karte, hotelske storitve in drugi stroški prevozov); za tekoče vzdrževanje 8.938,94 EUR (tekoče vzdrževanje, povezano z najemom poslovnih prostorov, zavarovalne premije, vzdrževanje druge nelicenčne programske opreme – evidence prisotnosti, tekoče vzdrževanje operativnega informacijskega okolja – vzdrževanje spletnega mesta); za poslovne najemnine in zakupnine 160.747,08 EUR (najemnina in zakupnine za poslovne objekte in parkirne prostore, najem programske računalniške opreme – IUS-INFO in prekrškovni portal ter druge najemnine, zakupnine in licenčnine – najem dveh fotokopirnih strojev in licenc); za druge operativne odhodke pa je bilo porabljenih 48.937,60 EUR (stroški konferenc in seminarjev, plačilo dela študentov, izdatki za strokovno izobraževanje zaposlenih, sodni stroški, letne članarine, 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 prejel 15.052,04 EUR in z naslova poročna zavarovalne premije 128,15 EUR s strani zavarovalnice Generali.

Za izplačilo manjka na postavki plače za december 2023 je Informacijski pooblaščenec finančna sredstva v višini 44.200 EUR zagotovil s prerazporeditvijo privarčevanih sredstev s postavke materialni stroški (30.000,00 EUR v januarju in 14.200,00 EUR v decembru 2023).

Prerazporeditev s proračunske postavke 1271 – materialni stroški na proračunske postavke 1273 – investicije, 7640 – Rezerva Republike Slovenije ter druge postavke v letu 2023 ni bilo.

PROJEKTI

PROJEKTI		Veljavni proračun	Prezete obveznosti	Razpoložljiv proračun v EUR konec leta
Sredstva skupaj po projektih		7.321,05	0	7.321,38
1215-21-0001	PP 1273 Investicije	8.499,00	8.498,67	0,33
1215-21-0001	7459 Namenska sr. kupnine	7.317,92	0	7.317,92
1215-16-0001	PP 9958 Mednarodna spl. str.	0,14	0	0,14
1215-16-0001	PP130134 Taiex projekt	2,99	0	2,99

Za investicije je bilo do konca leta 2023 porabljenih 8.498,67 EUR. Sredstva so bila porabljena za nakup pisarniškega pohištva v znesku 283,99 EUR (pisarniška miza), pisarniške opreme v znesku 413,06 EUR (aparatus za vezavo), strojne računalniške opreme v znesku 1.510,00 EUR (en prenosni računalnik), strežnikov in diskovnih sistemov v znesku 337,40 EUR (dva trda diska), opreme za varovanje v znesku 606,36 EUR (železni sef), telekomunikacijske opreme v znesku 100,00 EUR (en mobilni aparat), druge opreme v znesku 2.512,98 EUR (dve spletni kameri, kontrola pristopa ter registrator delovnega časa, poštni nabiralnik in stojalo za kolesa) ter nematerialnega premoženja v znesku 2.734,39 EUR (kontrola pristopa in nadgradnja delovnega časa licence ter licenca za avtomatsko lektorico Amebis Besana za šest uporabnikov, licenca HCL za 50 uporabnikov – nadgradnja poštnega domino strežnika in Microsoft programska oprema za deset uporabnikov). Konec leta 2023 je bilo stanje razpoložljivega proračuna na postavki investicije 0,33 EUR.

Za izplačilo manjka na postavki plače za december 2023 je Informacijski pooblaščenec zagotovil finančna sredstva v višini 23.501 EUR s prerazporeditvijo privarčevanih sredstev s postavke investicij.

Namenska sredstva kupnine – v leto 2023 je bilo prenesenih 7.317,92 EUR finančnih sredstev kupnin. Leta 2023 na postavki ni bilo niti prilivov niti odливov. Finančna sredstva v višini 7.317,92 EUR se prenese v leto 2024.

Mednarodna spletna stran info-commissioners.org – iz leta 2023 je bilo prenesenih 0,14 EUR finančnih sredstev. Leta 2023 na tej postavki ni bilo porabe. Projekt se leta 2024 konča, preostanek sredstev bo nakazan na podračun izvrševanja proračuna.

Projekt Taiex – iz leta 2022 je bilo v leto 2023 prenesenih 2,99 EUR. Za projekt Taiex leta 2023 ni bilo niti prilivov niti odливov. Projekt se v letu 2024 zaključi, preostanek sredstev bo nakazan na podračun izvrševanja proračuna.

DOSTOP DO INFORMACIJ JAVNEGA ZNAČAJA

V IMENU LJUDI IN ZA LJUDI

2.1 PРАВNA 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 zaščiten 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 (EU) 2019/1024 z dne 20. junija 2019 o odprtih podatkih in ponovni uporabi informacij javnega sektorja, ki je začela veljati 16. 7. 2019 in je bila implementirana v zakon z novelo ZDIJZ-G.

Leta 2005 je bil z novelo ZDIJZ-A narejen še korak naprej. Novela je namreč zožila možnost neupravičenega zapiranja dostopa do informacij in uvedla številne novosti, kot so ponovna uporaba informacij javnega značaja in pristojnosti upravne inšpekcije na področju izvajanja tega zakona. Najpomembnejša novost je bil zagotovo test javnega interesa. Z novelo je bila tudi poudarjena odprtost pri podatkih o porabi javnih sredstev in podatkih, povezanih z delovnim razmerjem ali opravljanjem javne funkcije. S tem se je Slovenija pridružila tistim demokratičnim državam, ki, kadar gre za javni interes, tudi izjeme obravnavajo s pridržkom.

Leta 2014 sta bili sprejeti noveli ZDIJZ-C in ZDIJZ-D. Najpomembnejša sprememba, ki sta jo prinesli, je, da se je obveznost posredovanja informacij javnega značaja z organov javnega sektorja razširila tudi na gospodarske družbe in druge pravne osebe pod prevladujočim vplivom (oz. v večinski lasti) države, občin ali drugih oseb javnega prava ter da je AJPES v šestih mesecih po uveljavitvi ZDIJZ-C vzpostavil spletni Register zavezancev za informacije javnega značaja, ki je javen, podatki v njem pa so dostopni brezplačno. Namen sprememb ZDIJZ je bil, da se poleg zagotavljanja javnosti in odprtosti delovanja javnega sektorja krepita 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 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.

Leta 2022 je bila sprejeta novela ZDIJZ-G, ki je v slovenski pravni red z zamudo prenesla Direktivo (EU) 2019/1024. Novela določa, da morajo organi v čim večji meri omogočiti ponovno uporabo raziskovalnih podatkov iz javno financiranih raziskav, omogočiti ponovno uporabo nabora podatkov velike vrednosti (npr. podatkov o okolju, prometu, satelitskih podatkov, meteoroloških podatkov), dinamične podatke (podatke, ki se velikokrat posodablajo) pa dati na voljo takoj, ko jih zberejo. Dostop do podatkov velike vrednosti in dinamičnih podatkov morajo organi zagotoviti z uporabo t. i. API-vmesnikov. Podatki za ponovno uporabo morajo biti na voljo brez zaračunavanja stroškov (oz. se lahko zaračunava povračilo mejnih stroškov, npr. zaradi reprodukcije, zagotavljanja in razširjanja dokumentov).

Časovnica razvoja Zakona o dostopu do informacij javnega značaja.

1991
USTAVA

39. člen Ustave Republike Slovenije določi, da ima vsakdo pravico dobiti informacijo javnega značaja, za katero ima v zakonu utemeljen pravni interes.

Veljati prične Zakon o dostopu do informacij javnega značaja, ki celostno uredi področje dostopa do informacij javnega značaja.

2003
ZDIJZ

2005
ZDIJZ-A

Novela ZDIJZ-A prinese pomembne novosti, kot sta test javnega interesa in ponovna uporaba informacij javnega značaja.

Noveli ZDIJZ-C in ZDIJZ-D razširita krog zavezancev tudi na gospodarske družbe in druge pravne osebe pod prevladujočim vplivom (oz. v večinski lasti) države.

2014
ZDIJZ-C | ZDIJZ-D

2016
ZDIJZ-E

Novela ZDIJZ-E prinese novosti na področju ponovne uporabe informacij javnega značaja ter določi, da organi na nacionalnem portalu odprtih podatkov javnega sektorja OPSI objavijo seznam vseh zbirk podatkov iz svoje pristojnosti z metapodatki ter zbirke odprtih podatkov ali povezave na spletne strani, kjer so zbirke odprtih podatkov objavljene.

Novela ZDIJZ- F uredi institut stranske udeležbe posebej glede na splošno ureditev v zakonodaji, ki ureja splošen upravni postopek.

2018
ZDIJZ-F

2022
ZDIJZ-G

Novela ZDIJZ-G od organov zahteva, da v čim večji meri omogočijo ponovno uporabo raziskovalnih podatkov, podatkov velike vrednosti in dinamičnih podatkov.

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

Kdo so zavezanci za posredovanje informacij javnega značaja?

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

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

Zavezanci so informacije javnega značaja dolžni zagotavljati na dva načina: z objavo na spletu in z omogočanjem dostopa na podlagi individualnih zahtev. Za vsako od skupin zavezancev je pojem »informacija javnega značaja« (torej informacija, ki jo morajo posredovati prosilcu) definiran drugače; pri zavezancih iz druge skupine je ožji. Medtem ko **za organe na splošno velja, da so vsi dokumenti, zadeve, dosjeji, registri, evidence in dokumentarno gradivo, s katerim razpolagajo** (ne glede na to, ali jih je organ izdelal sam, v sodelovanju z drugim organom ali jih je pridobil od drugih oseb), **informacije javnega značaja, razen izjem, za poslovne subjekte pod prevladujočim vplivom oseb javnega prava pa velja ravno obraten miselni proces: informacije javnega značaja so le tisti dokumenti, zadeve, dosjeji, registri, evidence in dokumentarno gradivo, ki jih kot take določa ZDIJZ** (npr. informacije, povezane s sklenjenimi pravnimi posli, ter informacije o članih 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). Drugi 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 pravico na zahtevo 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.

Kaj 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 (torej pojasnila, razlage, analize, komentarji). Če medij zahteva odgovor na vprašanje, se njegova vloga obravnavava 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 2023 je Informacijski pooblaščenec vodil 704 pritožbene postopke, od tega 386 postopkov zoper zavrnilne odločbe organov in 302 postopka zaradi t. i. molka organa oz. neodzivnosti. Zoper poslovne subjekte pod prevladujočim vplivom je Informacijski pooblaščenec vodil 16 pritožbenih postopkov, od tega štiri zaradi molka in 12 zoper zavrnilne odločbe poslovnih subjektov pod prevladujočim vplivom.

Leta 2023 je Informacijski pooblaščenec odgovoril na 317 pisnih prošenj za neformalno pomoč ali mnenje, ki jih je prejel od zavezancev prve stopnje in prosilcev, odgovoril pa je tudi na 837 zaprosil v okviru telefonskih dežurstev. 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 2023 vsebinsko obravnaval 399 pritožb. Izdal je 389 odločb, šest pritožb prosilcev je s sklepom zavrgel (pritožbe so bile nedovoljene oz. prepozne), 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 2023, in 36 odločb, ki so se nanašale na postopke, začete pred letom 2023. Med reševanjem pritožb je na terenu opravil 35 ogledov in camera (tj. ogledov brez prisotnosti stranke, ki zahteva dostop do informacije javnega značaja), na katerih je ugotavljal dejansko stanje pri organu.

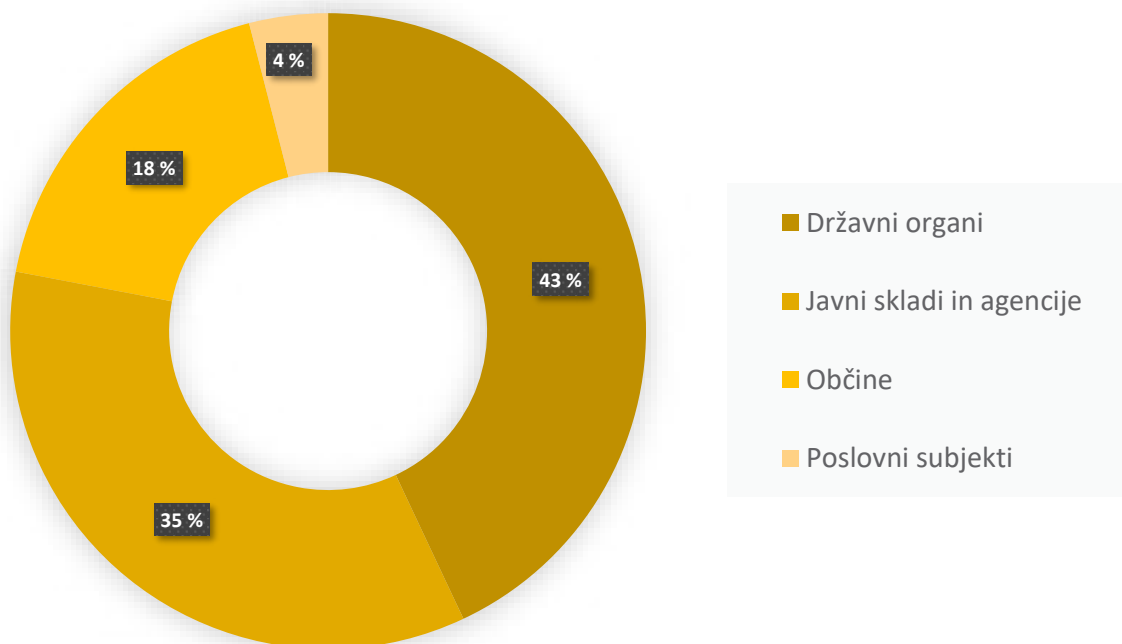
Informacijski pooblaščenec je v izdanih odločbah (389):

- pritožbo zavrnil – 210,
- pritožbi delno ali v celoti ugodil oz. rešil zadevo v korist prosilca – 126,
- pritožbi ugodil in zadevo vrnil prvostopenjskemu organu v ponovno odločanje – 49,
- odločbo prvostopenjskega organa razglasil za nično – 4.

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

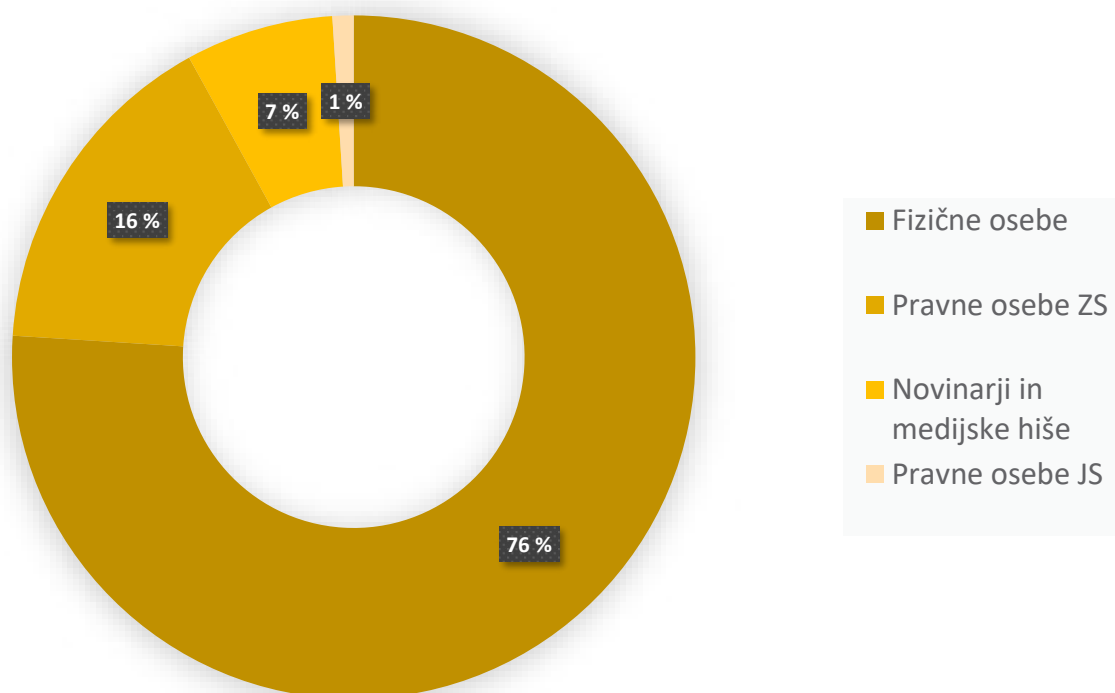
- državni organi – 168, od tega ministrstva in organi v sestavi ter upravne enote 154, sodišča, vrhovno državno tožilstvo in državno odvetništvo pa 14,
- javni skladi, zavodi, agencije, izvajalci javnih služb, nosilci javnih pooblastil in druge pravne osebe javnega prava – 136,
- občine – 69,
- poslovni subjekti pod prevladujočim vplivom države, občin ali drugih oseb javnega prava – 16.

Zoper katere zavezance so bile vložene pritožbe?



V 296 primerih so bili prosilci fizične osebe, v 61 primerih so se pritožile pravne osebe zasebnega sektorja, v 27 primerih novinarji in medijske hiše, petkrat pa so se pritožile pravne osebe javnega sektorja.

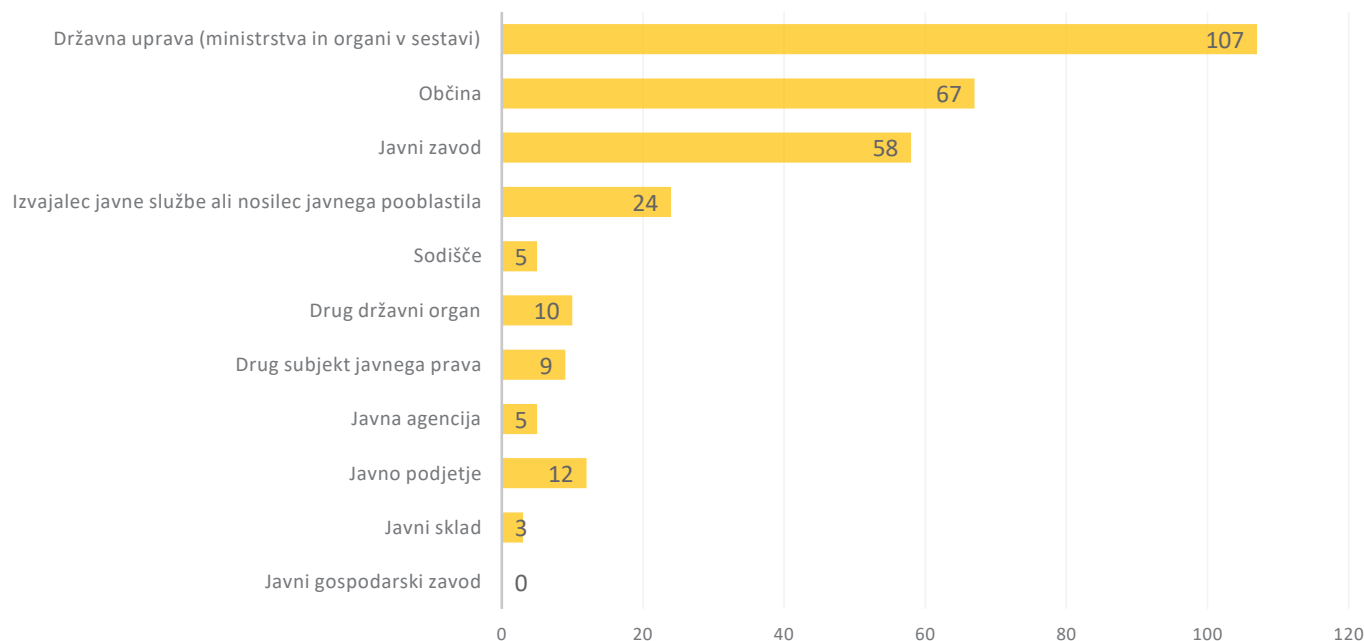
Pritožbe zoper zavrnitve dostopa do informacij.



2.2.2 PRITOŽBE ZOPER MOLK

Informacijski pooblaščenec je v letu 2023 prejel 302 pritožbi zaradi molka organa in štiri pritožbe zaradi neodziva poslovnih subjektov pod prevladujočim vplivom. Največ primerov molka je bilo med organi državne uprave (ministrstva, organi v sestavi itd.), in sicer 107 (število se je v primerjavi z letom 2022, ko je bilo zabeleženih 89 primerov molka organov državne uprave, povečalo), sledile so občine (67 primerov v letu 2023 v primerjavi z letom poprej, ko je bilo takih primerov 45) ter javni zavodi (58 primerov v letu 2023, 51 primerov leta 2022).

Zoper katere zavezance so bile vložene pritožbe.



Največ pritožb zoper molk organa so vložile fizične osebe, in sicer kar 73,9 % (226). V 15 % primerov (46) so pritožbo zaradi molka organa vložili novinarji oz. mediji. V 8,8 % primerov (27) so pritožbo vložile pravne osebe zasebnega prava in v 2,3 % primerov (7) pravne osebe javnega prava.

Po preizkusu formalnih predpostavk Informacijski pooblaščenec v 69 primerih postopka zaradi molka ni uvedel, in sicer je v 29 primerih pritožbo s sklepom zavrgel, od tega v 21 primerih zaradi preuranjenosti, v štirih primerih je bila pritožba pomanjkljiva in je prosilec ni dopolnil, v enem primeru je pritožbo vložila neupravičena oseba, v treh primerih pa pritožba ni bila dovoljena. V 19 primerih je prosilec tekom postopka pritožbo umaknil, saj je od zavezanca že prejel zahtevano informacijo. Informacijski pooblaščenec v nobenem primeru ni prevzel pritožbe v odločanje in sam meritorno odločil. V nobeni zadevi vloge tudi ni odstopil na Upravno inšpekcijo.

V 21 primerih je Informacijski pooblaščenec postopek z molkom zaključil tako, da je prosilcu pojasnil:

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

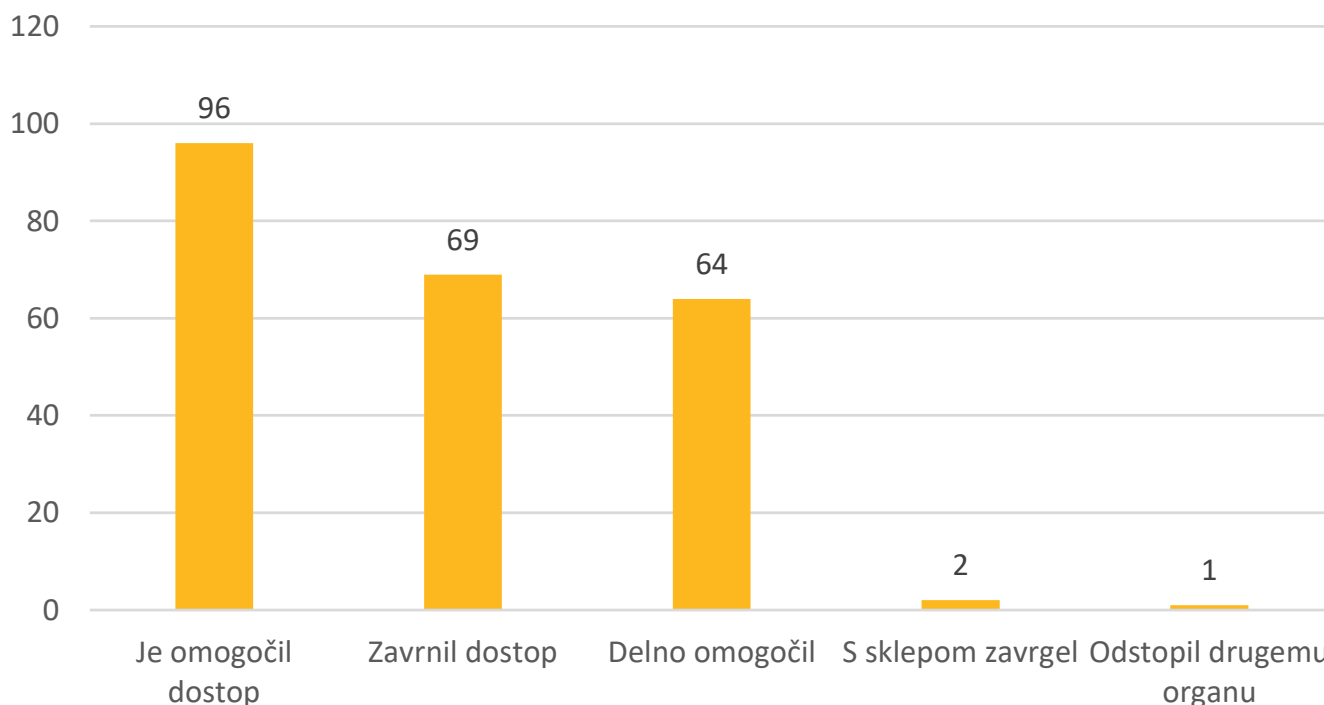
V pritožbenih postopkih je Informacijski pooblaščenec zaradi molka v 232 primerih zavezance pozval, naj o zahtevi prosilca čim prej odločijo. Po pozivu Informacijskega pooblaščenca so zavezanci prosilcu v 96 primerih informacijo posredovali, v 69 primerih so prosilcu dostop zavrnilo ter izdali zavrnilno odločbo, v 64 primerih pa so prosilcu dostop delno omogočili (določene podatke so zakrili oz. so omogočili dostop le do določenih informacij, dostop do preostalih pa so z odločbo zavrnilo). V

dveh primerih je zavezanec zahtevo prosilca s sklepom zavrgel, v enem primeru pa je organ vlogo prosilca za dostop do dokumentov odstopil 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 štiri pritožbene postopke zaradi molka zavezancev, in sicer je po pozivu Informacijskega pooblaščenca zavezanec v enem primeru prosilcu dostop omogočil, v treh primerih pa je zahtevo prosilca zavrnil. Izmed 306 primerov molka je bilo 40 primerov povezanih z Zakonom o medijih, največkrat (v 19 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 2023 je bilo na Upravnem sodišču RS vloženi 38 tožb zoper odločbe Informacijskega pooblaščenca (zoper 9,51 % izdanih odločb). Delež je relativno majhen, kar kaže na uveljavitev transparentnosti in odprtosti javnega sektorja, pa tudi na to, da zavezanci in prosilci sprejemajo odločbe Informacijskega pooblaščenca.

Upravno sodišče je leta 2023 odločilo o 28 tožbah, ki so bile vložene zoper odločbe Informacijskega pooblaščenca, in:

- tožbo zavrnilo – 16,
- tožbi ugodilo, izpodbijano odločbo oz. del odločbe odpravilo in zadevo vrnilo Informacijskemu pooblaščenca v ponovno odločanje – 9,
- tožbi ugodilo, izpodbijano odločbo oz. del odločbe odpravilo in zadevo vrnilo zavezancu v ponovno odločanje – 3.

Leta 2023 so bile na Vrhovno sodišče RS vložene štiri revizije zoper sodbo Upravnega sodišča.

2.4 STORJENI PREKRŠKI PO ZDIJZ, ZInfP IN ZMed

Leta 2023 Informacijski pooblaščenec ni izdal nobene odločbe o prekršku zaradi kršitev določb ZDIJZ, ZInfP ali ZMed.

2.5 IZBRANI PRIMERI NA PODROČJU DOSTOPA DO INFORMACIJ JAVNEGA ZNAČAJA

Računi že pojmovno, kakor tudi po vsebini, ne pomenijo sklenjenega pravnega posla, zato jih ni mogoče opredeliti kot informacije javnega značaja pri poslovnih subjektih pod prevladujočim vplivom oseb javnega prava

Prosilec je od družbe Top energija d.o.o. zahteval prejete račune za dejansko porabo zemeljskega plina in izdane račune za proizvedeno toploto v določenem obdobju. Zavezanec je zahtevo zavrnil, ker zahtevani dokumenti niso informacije javnega značaja. Informacijski pooblaščenec je v pritožbenem postopku ugotovil, da zavezanec ni izvajalec javne službe, zato zahtevani dokumenti niso informacije javnega značaja po 4. členu ZDIJZ. Čeprav je zavezanec poslovni subjekt pod prevladujočim vplivom, zahtevani dokumenti ne spadajo med informacije javnega značaja po prvem odstavku 4.a člena ZDIJZ, na podlagi katerega je informacija javnega značaja »informacija iz sklenjenega pravnega posla, ... ki se nanaša na izdatke subjekta za naročilo ... storitev,« in jo je treba razlagati po njeni jezikovni razlagi in ne širiti pomena besednih zvez. Besedna zveza »informacija iz sklenjenega pravnega posla« pomeni informacijo, ki neposredno izhaja iz nekega pravnega posla. Zahtevani dokumenti že pojmovno, kakor tudi po vsebini, ne pomenijo sklenjenega pravnega posla (pravni posel namreč predstavlja npr. pogodba), zato jih ni mogoče uvrstiti pod definicijo informacije javnega značaja iz prvega odstavka 4.a člena ZDIJZ. Ne ustrezajo pa niti definiciji informacije javnega značaja po drugem odstavku 4.a člena ZDIJZ. Informacijski pooblaščenec ni sledil navedbam prosilca, da gre za porabo javnih sredstev in da je posledično za razkritje teh informacij podan prevladujoč javni interes. Zavezanec ni ne neposredni ne posredni proračunski uporabnik, prav tako ne upravlja javnih sredstev, pridobljenih z izvajanjem javne službe. Prosilec tudi ni izkazal neposredne povezave, kako bi razkritje zahtevanih informacij pripomoglo k seznanitvi javnosti s pomembno družbeno temo (npr. vprašanje javnega zdravja, varnosti,...), ki je v javnem interesu širšega kroga ljudi. Zgolj ugotovitev, da zavezanec kot proizvajalec toplotne energije dobavlja toploto Javnim službam Ptuj d.o.o., ki jo potem vkalkulirajo v prodajno ceno toplote za končne uporabnike, ne zadošča za sklep, da je delovanje zavezanca v tem delu v prevladujočem javnem interesu, kajti sama proizvodnja toplotne energije ni javnopravno regulirana, ampak poteka po tržnih načelih. Pri presoji, ali je izkazan javni interes za dostop do zahtevane informacije na podlagi ZDIJZ, ni mogoče izhajati iz splošnega stališča, da bi bilo za javnost koristno in torej v javnem interesu, da bi bile zahtevane informacije vedno prosto dostopne, temveč mora biti izkazan konkreten javni interes za razkritje konkretnih dokumentov oz. delov dokumenta. Prosilec v obravnavanem primeru ni navedel utemeljenih konkretnih razlogov, zaradi katerih je treba (vse) zahtevane račune šteti med informacije javnega značaja. Tako izhaja tudi iz prakse Upravnega sodišča, ki je že večkrat zavzelo stališče, da se javni interes za razkritje informacij nanaša na konkreten podatek in ne more izhajati iz splošne zahteve po transparentnosti določenih postopkov. Javni interes bi bil močnejši le, če bi bile ogrožene take vrednote, kot je na primer življenje, zdravje ali varnost ljudi, ali če bi grozila neposredna škoda za premoženje večje vrednosti. V obravnavani zadevi takšne vrednote zagotovo niso ogrožene. Posledično pogoji za razkritje zahtevanih informacij na podlagi drugega odstavka 4.a člena v povezavi z drugim odstavkom 6. člena ZDIJZ niso izpolnjeni.

KLJUČNE BESEDE: poslovni subjekt pod prevladujočim vplivom, ali gre za delovno področje organa, številka odločbe 09021-1/2023

Absolutno javni so podatki, ki so bili glede na javno naročilo relevantni za odločitev organa o izbiri ponudbe in jih je moral ponudnik predložiti v okviru dokazovanja izpolnjevanja razpisnih pogojev

Prosilka je na Mestno občino Kranj naslovila zahtevo za dostop do celotne ponudbene dokumentacije, ki jo je na javnem naročilu oddal izbrani ponudnik. Organ je zahtevo delno zavrnil zaradi varstva poslovne skrivnosti (2. točka prvega odstavka 6. člena ZDIJZ). Informacijski pooblaščenec je v pritožbenem postopku ugotovil, da je izbrani ponudnik poslovno skrivnost sicer izkazoval s sklepom o določitvi poslovne skrivnosti, vendar pa Zakon o poslovni skrivnosti (ZPosS) v tretjem odstavku 2. člena določa, da se za poslovno skrivnost ne morejo določiti informacije, ki so po zakonu javne. Gre za t. i. absolutno javne podatke, tj. podatke, na razkritje katerih volja »prizadetega« poslovne subjekta nima vpliva. Zahtevana dokumentacija je bila oddana v postopku javnega naročila, zato je treba upoštevati drugi odstavek 35. člena Zakona o javnem naročanju (ZJN-3), na podlagi katerega 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 so predmet pritožbe podatki izbranega ponudnika in njegovega podizvajalca, zato je 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. Za poslovno skrivnost v postopkih javnega naročanja namreč ni mogoče določiti tistih podatkov iz predložene ponudbe, ki odražajo izpolnjevanje pogojev, saj je na podlagi ocene organa, da je ponudnik izpolnjeval vse pogoje, prišlo do porabe javnih sredstev (tako tudi Upravno sodišče v sodbi št. I U 1647/2017-29 z dne 6. 3. 2019). Ker je Informacijski pooblaščenec ugotovil, da je prosilka zahtevala podatke, ki so bili glede na obravnavano javno naročilo relevantni pri presoji organa, ko je odločal o izbiri ponudbe, hkrati pa so tudi izrecno navedeni kot dokumenti, ki jih je moral ponudnik predložiti v okviru dokazovanja izpolnjevanja razpisnih pogojev, je kot prosto dostopne določil: ESPD-obrazec izbranega ponudnika in njegovega podizvajalca ter seznam referenčnih poslov. Organ je navedene dokumente dolžan posredovati prosilki, pri čemer mora prekriati varovane osebne podatke (3. točka prvega odstavka 6. člena ZDIJZ).

KLJUČNE BESEDE: poslovna skrivnost, javna naročila, številka odločbe 090-355/2022

Podatki, ki vplivajo na imenovanje konzularnega funkcionarja, niso varovani osebni podatki

Prosilka je od Ministrstva za notranje zadeve želela pridobiti predlog za imenovanje častnega konzula in kopijo utemeljitve njegovega imenovanja na to funkcijo. Organ je njeni zahtevi delno ugodil, v posredovanih dokumentih pa je, zaradi varstva osebnih podatkov (3. točka prvega odstavka 6. člena ZDIJZ), prekril vse podatke v življenjepisnem imenovanega. Informacijski pooblaščenec je v pritožbenem postopku ugotovil, da organ ni upošteval, da se zahtevani podatki nanašajo na imenovanje posameznika na mesto častnega konzula Republike Slovenije. Postopek in pogoje za to imenovanje določa Zakon o zunanjih zadevah (ZZZ-1). Ker na imenovanje konzularnega funkcionarja med drugim vplivajo podatki o njegovi izobrazbi ter poklicni in drugi dejavnosti, ki jih organ pred imenovanjem preveri z namenom ugotovitve, ali kandidat uživa ugled ter zaupanje in ali je njegova poklicna in druga dejavnost združljiva s položajem konzularnega funkcionarja, gre pri teh podatkih za podatke v zvezi z opravljanjem javne funkcije, ki v skladu s tretjim odstavkom 6. člena ZDIJZ niso varovani. Posledično je Informacijski pooblaščenec odločil, da mora organ te podatke prosilki posredovati, ob tem pa mora, v skladu s 7. členom ZDIJZ, v presojanih dokumentih prekriati podatke, ki niso v zvezi z opravljanjem javne funkcije (lastnoročni podpis, datum rojstva, datum diplomiranja, datum nadaljevanja študija ter vse datume zaposlitev in članstev v organizacijah, naslov (skupaj s številkami telefonov in e-poštnim naslovom), datume strokovnega razvoja, datume pridobljenih strokovnih izkušenj, vse podatke pri »ostale delovne izkušnje«, vse datume zaposlitev in članstev v organizacijah). Nevarovani osebni podatki, ki so v zvezi z delovnim razmerjem javnega

uslužbenca oz. v zvezi z opravljanjem javne funkcije, so tudi osebni podatki pri organu zaposlenih, ki so v dokumentih navedeni v zvezi z opravljanjem njihovega dela.

KLJUČNE BESEDE: javni funkcionarji, osebni podatek, številka odločbe 090-368/2022

Pri presoji dostopa do dokumenta, ki pravno pripada Evropski komisiji, je treba neposredno uporabiti evropsko pravo in upoštevati pridobljeno stališče Evropske komisije

Prosilec je od Urada RS za okrevanje in odpornost zahteval posredovanje dokumentacije glede projekta tehnične pomoči Evropske komisije Sloveniji. Organ je s sklicevanjem na Uredbo (ES) št. 1049/2001 Evropskega parlamenta in Sveta o dostopu javnosti do dokumentov Evropskega parlamenta, Sveta in Komisije (Uredba) in na notranje delovanje organa (11. točka prvega odstavka 6. člena ZDIJZ) zavrnil dostop do začetnega poročila o navedenem projektu. Informacijski pooblaščenec je v pritožbenem postopku ugotovil, da ta dokument pravno pripada Evropski komisiji, zato je upošteval, da mora Republika Slovenija kot država članica spoštovati načelo lojalnega sodelovanja z evropskimi institucijami in torej ne sme ovirati primarne uporabe Uredbe in pravila glede varnosti evropskih institucij (točka 15 preambule Uredbe). Načelo oz. doktrina lojalne razlage evropskega prava pomeni, da morajo države članice svoje nacionalno pravo interpretirati v luči in v duhu prava EU oz. tako, da s svojimi notranjimi predpisi ne bodo preprečevale uresničevanja evropskih predpisov. Iz njenega mnenja, ki ga je na podlagi 5. člena Uredbe podala Evropska komisija, izhaja, da bi posredovanje zahtevanega poročila javnosti ogrozilo: javni interes, kar zadeva finančno, denarno ali gospodarsko politiko Skupnosti ali države članice (točka (a) prvega odstavka 4. člena Uredbe); postopek odločanja Evropske komisije (tretji odstavek 4. člena Uredbe) in varstvo namena inšpekcij, preiskav in revizij (drugi odstavek 4. člena Uredbe). V konkretnem primeru gre za absolutno izjemo. Po določilu prvega odstavka 4. člena Uredbe dokumenti, varovani z absolutnimi izjemami, javnosti niso dostopni, če bi njihovo razkritje ogrozilo enega izmed izrecno predpisanih javnih ali zasebnih interesov. Kljub »absolutnosti« pa so te izjeme samo »relativno prisilne narave«, saj učinkujejo le, kadar bi razkritje dokumenta dejansko ogrozilo varovano pravno dobrino, in ne zgolj takrat, kadar bi do njene ogrožitve (teoretično) lahko prišlo. Po določilu točke (a) prvega odstavka 4. člena Uredbe pa se v nobenem primeru ne sme razkriti dokumentov, kadar bi to ogrozilo javni interes, ki zadeva javno varnost, obrambne in vojaške zadeve, mednarodne odnose ali finančno, monetarno ali ekonomsko politiko EU ali države članice. Evropska komisija je predlagala, da se dostop do obravnavanega dokumenta zavrne v celoti, na podlagi četrte alineje točke (a) prvega odstavka 4. člena Uredbe, tj. varstvo javnega interesa, kar zadeva finančno, denarno ali gospodarsko politiko Skupnosti ali države članice. Svoje mnenje je utemeljila z dejstvom, da gre za postopek tehnične podpore, ki je v teku, razkritje dokumenta v tej fazi pa bi škodovalo doseganju ciljev Slovenije na varovanem področju ter izvajanju svetovanja in priporočil Evropske komisije v zvezi s podano zahtevo Slovenije za tehnično podporo pri implementaciji slovenskega načrta za okrevanje in odpornost. Informacijski pooblaščenec je ob neposredni uporabi evropskega prava in upoštevanju pridobljenega stališča Evropske komisije ugotovil, da obravnavani dokument v celoti predstavlja izjemo od prostega dostopa na podlagi četrte alineje točke (a) prvega odstavka 4. člena Uredbe (varstvo javnega interesa, kar zadeva finančno, denarno ali gospodarsko politiko Skupnosti ali države članice). Zato tudi ni mogoče izvesti delnega dostopa, kot ga določa šesti odstavek 4. člena Uredbe. Ker zahtevani dokument ne predstavlja izjeme po ZDIJZ, ampak absolutno izjemo po ZDIJZ nadrejeni Uredbi, testa javnega interesa, katerega izvedbo je predlagal prosilec, v konkretnem primeru ni dopustno uporabiti.

KLJUČNE BESEDE: pravo EU, številka odločbe 090-7/2023

Podatki o masi in vrsti embalaže za posameznega proizvajalca se neposredno tičejo odpadkov, zato predstavljajo okoljske podatke, ki so absolutno javni

Agencija Republike Slovenije za okolje je zavrnila zahtevo novinarja za dostop do določenih podatkov o embalaži, za vsakega od proizvajalcev, ki so dolžni te podatke sporočiti organu. Pri tem se je sklicevala na obstoj poslovne skrivnosti (2. točka prvega odstavka 6. člena ZDIJZ) v povezavi z določbami, ki v Zakonu o varstvu okolja (ZVO-2) urejajo dostop do podatkov v informacijskem sistemu o proizvajalčevi razširjeni odgovornosti, in z določbami Uredbe o embalaži in odpadni embalaži, ki urejajo evidenco proizvajalcev. V pritožbenem postopku je Informacijski pooblaščenec ugotovil, da organ ni izpolnil dokaznega bremena glede obstoja pogojev, ki jih za opredelitev poslovne skrivnosti določa Zakon o poslovni skrivnosti (ZPosS), prav tako pa tudi ni vzpostavljena domneva poslovne skrivnosti, ki jo je organ zatrjeval v povezavi s prej navedenimi predpisi. Zatrjevana izjema zato ni podana, sicer pa obravnavanih informacij sploh ni mogoče določiti za poslovno skrivnost, ker gre za okoljske podatke, ki so javni že na podlagi zakona. Informacijski pooblaščenec je poudaril, da se pojem odpadek ne sme razlagati ozko. Embalažo, dano na trg, je opredelil kot odpadek v smislu tretjega odstavka 6. člena ZDIJZ v povezavi s 7. točko 3. člena ZVO-2, iz česar izhaja, da se v konkretnem primeru zahtevani podatki o masi in vrsti embalaže za posameznega proizvajalca neposredno tičejo odpadkov, zato predstavljajo podatke o odpadkih in posledično okoljske podatke. Temeljni podatek za določitev obsega finančne ali finančne in organizacijske odgovornosti za ravnanje s tovrstnimi odpadki predstavljajo prav podatki o masi in vrsti embalaže, dani na trg, za posameznega proizvajalca. Prav na podlagi teh podatkov se izračunajo stroški ravnanja z odpadno embalažo za posameznega proizvajalca, kar pomeni, da so vsi omenjeni podatki, ki so relevantni za ravnanje z odpadki, tesno medsebojno povezani in soodvisni, zato je razkritje podatkov o masi in vrsti embalaže za posameznega proizvajalca nujno, da se javnosti omogoči celovit dostop do vseh relevantnih okoljskih podatkov. Šele na podlagi podatkov o masi in vrsti embalaže, dani na trg, za posameznega proizvajalca, je namreč možno celovito spremljati tudi raznovrstne podatke, ki kažejo na uspešnost doseganja cilja preprečevanja oz. zmanjševanja vplivov embalaže na okolje. Takšna široka opredelitev okoljskih podatkov je skladna tudi z določbami Aarhuške konvencije, evropsko zakonodajo in prakso Sodišča Evropske unije. Nujnost široke razlage ne nazadnje izhaja tudi iz dejstva, da ZVO-2 temelji na načelu javnosti, ki poleg splošne določbe, da so okoljski podatki javni, javnosti daje tudi vrsto drugih pravic, ki jih je nemogoče izvrševati, če javnost nima dostopa do relevantnih okoljskih podatkov. Ozka razlaga osnovnih pojmov s tega področja in posledično omejevanje obsega absolutno prosto dostopnih informacij javnega značaja bi de facto pomenilo tudi negacijo vseh teh pravic. Informacijski pooblaščenec je ugotovil še, da je podan prevladujoč javni interes, da se javnost seznanja z zahtevanimi informacijami, pri čemer je kot bistveno okoliščino upošteval dejstvo, da je za informacijo zaprosil medij, ki ima dolžnost posredovati informacije v vseh zadevah, ki zadevajo javnost. Medij namreč te naloge ne bi mogel opravljati, če javnost ne bi imela pravice teh informacij prejeti. Nedvomno gre za informacije, ki so za javnost pomembne, saj podatki o tem, koliko embalaže je dane na trg in kakšna je ta embalaža, nedvomno omogočajo celovito javno razpravo in posledično javni nadzor nad dejanskimi vplivi te embalaže na okolje, stanje v okolju pa pomembno vpliva na zdravje ljudi. Če sistem proizvajalčeve razširjene odgovornosti ne deluje optimalno, to prav gotovo ogroža zdravje ljudi. Javno izraženi dvomi o ustreznosti ureditve in izvajanja obveznosti proizvajalcev v zvezi z embalažo, dano na trg, pa se pojavljajo v različnih medijih in v različnih obdobjih. Razkritje zahtevanih podatkov bi dejansko pripomoglo k širši razpravi in razumevanju nečesa, kar je pomembno za širšo javnost, kot to omogočajo že javno objavljeni podatki (npr. v javno dostopnem delu Evidenice proizvajalcev). Informacijski pooblaščenec je zaključil, da zatrjevana izjema ni podana, zato je organ prosilcu dolžan posredovati zahtevane podatke.

KLJUČNE BESEDE: poslovna skrivnost, okoljski podatki, test interesa javnosti, številka odločbe 090-1/2023

Kadar iz načina vlaganja zahtev izhaja, da je namen prosilca preko dostopa do informacij javnega značaja zasipavanje organa oz. je namen doseči, da se organ opredeli do njegovih prijav in analiz ter začne inšpekcijski postopek, gre za zlorabo pravice, ker takšen namen ni skladen z ZDIJZ

S sklicevanjem na zlorabo pravice (peti odstavek 5. člena ZDIJZ) je Tržni inšpektorat Republike Slovenije prosilcu zavrnil dostop do zahtevanih podatkov. Informacijski pooblaščenec je v pritožbenem postopku sledil odločitvi organa, pri čemer se ugotovitve obeh nanašajo na celoten sklop zahtev, saj je le tako mogoče presoditi način izvrševanja pravice dostopa v obravnavanem primeru. Upošteva je okoliščine konkretnega primera in kriterije za opredelitev zlorabe pravice iz ZDIJZ ter iz pravne teorije in prakse je Informacijski pooblaščenec ugotovil, da iz načina vlaganja obravnavanih zahtev prosilca izhaja njegov namen, da dokaže nesposobnost oz. nestrokovnost organa, ter da preko postopkov po ZDIJZ doseže, da se organ opredeli do njegovih prijav in analiz oz. da uvede inšpekcijske postopke. Na to kažeta pogostost in način vlaganja zahtev. Vloge prosilca predstavljajo preplet opozoril na nepravilnosti na določenih področjih in prijav za uvedbo inšpekcijskega postopka ter na drugi strani zahtev za dostop do informacij javnega značaja, kot so npr. izpis dokumentov iz posameznih konkretnih inšpekcijskih zadev ali izpis dokumentov, ki naj bi oz. so nastali na podlagi prijave prosilca. Prosilec v vlogah podaja tudi negativno vrednostno sodbo dela organa, tako na podlagi svojih konkretnih prijav kot tudi na splošno organu očita neučinkovito delo. Informacijski pooblaščenec je ugotovil, da prosilec zahteva dostop do informacij javnega značaja, torej do dokumentov iz konkretnih zadev, zgolj in samo z namenom, da bi dokazal neučinkovito delo organa oz. da bi dosegel, da bi organ upošteval njegove prijave in uvedel inšpekcijski postopek glede izdelkov, na katere prosilec opozarja. Namen ZDIJZ je, da se zagotovi javnost in odprtost delovanja organov ter se omogoči uresničevanje pravice fizičnih in pravnih oseb, da pridobijo informacije javnega značaja, nikakor pa ZDIJZ ni orodje za kontrolo dela organa oz. »prisilo« le-tega, da začne inšpekcijski postopek v posameznih zadevah. Poleg tega število in obsežnost obravnavanih vlog prekomerno obremenjujeta organ. Večina vlog je obsežnih, s priloženimi analizami, dopolnjene so z novimi proizvodi ali dodatnimi nepravilnostmi, vsebujejo vprašanja in zahteve za dostop do informacij javnega značaja. V posameznih vlogah se torej prepletajo različni zahtevki. Razumsko ni mogoče pričakovati, da bo organ v zakonskem roku uspel odločiti o tolikšnem številu obsežnih vlog z različno vsebino. Takšnega pričakovanja zato tudi ni mogel imeti prosilec in ga po presoji Informacijskega pooblaščenca tudi ni imel. Kljub temu to ne pomeni, da organ ne dela oz. da je njegovo delo neučinkovito in nestrokovno, prav to pa hoče prosilec preko zahtev za dostop do informacij javnega značaja po ZDIJZ dokazati. V obravnavanem primeru torej ne gre za pošteno uporabo pravice prosilca po ZDIJZ. Poleg vsega tudi ni dvoma, da takšen način vlaganja zahtev s strani prosilca organu otežuje oz. onemogoča tudi ravnanje v skladu z načelom ekonomičnosti postopka. Informacijski pooblaščenec je zato sledil ugotovitvam organa v izpodbijani odločbi, da je prosilec s svojim ravnanjem očitno prestopil meje pravice dostopa do informacije javnega značaja, s čimer je podana zloraba pravice.

KLJUČNE BESEDE: ali gre za zlorabo pravice, številka odločbe 090-127/2023

Izjeme, s katero se varujejo sodni postopki, ni mogoče aplicirati tudi na postopke, ki nimajo narave sodnih postopkov

Novinar je od Splošne bolnišnice Celje zahteval odgovor na vprašanje glede višine odškodninskega zahtevka, ki ga je organ prejel v primeru zamenjave identitet pacientov. Organ je zahtevo zavrnil s sklicevanjem na izjemo po 8. točki prvega odstavka 6. člena ZDIJZ, pri čemer je trdil, da se stranki nahajata v intenzivni fazi obravnave odškodninskega zahtevka, ter da organ ne izključuje možnosti alternativnih rešitev spora, ki temeljijo na zaupnosti podatkov, zato bi razkritje podatka lahko povzročilo škodo za nadaljevanje postopka. Za obstoj zatrjevane izjeme morata biti kumulativno izpolnjena dva pogoja, in sicer (1) zahtevana informacija predstavlja podatek, ki je bil pridobljen ali sestavljen zaradi konkretnega pravnega, nepravdnega ali drugega sodnega postopka, in (2) razkritje zahtevanega

podatka bi škodovalo izvedbi konkretnega postopka. Informacijski pooblaščenec je v pritožbenem postopku ugotovil, da v obravnavani zadevi pravdni, nepravdni ali drug sodni postopek ni v teku. Organ je glede tega zavzel napačno stališče, da je zatrjevano izjemo mogoče razlagati širše in jo aplicirati tudi na druge postopke, ki nimajo narave sodnih postopkov. Iz sodne prakse namreč izhaja, da je treba vse izjeme od prostega dostopa razlagati restriktivno oz. ozko in jih ni dovoljeno širiti na primere, ki so taksativno naštetim izjemam v prvem odstavku 6. člena ZDIJZ bistveno podobni. Organu tudi ni uspelo izkazati obstoja drugega pogoja, po drugi strani pa so utemeljene pritožbene navedbe prosilca, da samo iz višine zahtevane odškodnine ni mogoče sklepati ne na konkretne oškodovance, ne na njihovo število, ne na naravo zahtevane odškodnine (materialna/nematerialna škoda), ne na višino posameznih delov zahtevane odškodnine niti ne na relevantne okoliščine, zaradi katerih je odškodnina zahtevana in bodo vplivale na njeno višino. Prav tako iz višine zahtevane odškodnine ni mogoče sklepati, kako bo z zahtevkom postopala zavarovalnica, ali ga bo štela kot utemeljenega, na kakšnem pravnem temelju in v kakšni višini, predvsem pa ni mogoče sklepati, ali in na kakšen način se bosta stranki poravnali (torej, ali in kakšna bo dejanska dogovorjena odškodnina). Informacijski pooblaščenec je zaključil, da ni izpolnjen niti drugi pogoj za obstoj zatrjevane izjeme, ki zato ni podana, kar pomeni, da je organ prosilcu dolžan posredovati skupen znesek zahtevane odškodnine.

KLJUČNE BESEDE: varstvo sodnega postopka, številka odločbe 090-96/2023

Zaradi širše javne razprave je javni interes za razkritje podatkov o prestajanju zaporne kazni za določene posameznike prevladal nad interesi varstva osebnih podatkov

Uprava za izvrševanje kazenskih sankcij je zaradi varstva osebnih podatkov (3. točka prvega odstavka 3. člena ZDIJZ) zavrnila zahtevo novinarka za dostop do podatkov o prestajanju zaporne kazni za določene posameznike. Informacijski pooblaščenec je pritožbi prosilke ugodil, ker je ugotovil, da javni interes za razkritje zahtevanih podatkov prevlada nad pravico posameznikov, na katere se ti nanašajo, do varstva zasebnosti. Pri izvedbi testa interesa javnosti je veliko težo pripisal naslednjim ugotovitvam: da so vsi obravnavani posamezniki absolutno javne osebe; da ne gre za razkrivanje podatkov iz njihovega intimnega življenja; da zahtevani podatki izkazujejo, kako so pristojni državni organi odločali o nekaterih vprašanjih v zvezi z izvrševanjem zaporne kazni; da je obravnavana tema že večkrat sprožala javno razpravo in da je prosilka novinarka, ki ima dolžnost posredovati informacije v vseh zadevah, ki zadevajo javnost; da bi razkritje podatkov dejansko pripomoglo k širši razpravi in razumevanju nečesa pomembnega za širšo javnost, kot to omogočajo že javno objavljeni podatki; da je razkritje pomembno tudi z vidika pozitivne generalne prevencije, ker bi se javnost seznanila s podatki o tem, na kakšen način in v kakšnem obsegu so obravnavani posamezniki dejansko prestali zaporno kazen. Pri izvedbi testa interesa javnosti v obravnavani zadevi je bilo ključno vprašanje, ali bi se z razkritjem zahtevane dokumentacije dejansko pripomoglo k širši razpravi in razumevanju nečesa pomembnega za širšo javnost, kot to omogočajo že javno dostopni podatki v zvezi s politiko izvrševanja zaporne kazni točno določenih posameznikov. Informacijski pooblaščenec je ugotovil, da so delno objavljeni nekateri podatki, ki so predmet zahteve, vendar teh podatkov ni objavil neposredno organ, temveč različni mediji, posledično pa ti podatki niso točni in zanesljivi, kar pomeni, da ne omogočajo celovite in informirane javne razprave ter razumevanja obravnavane teme. Le celostne informacije so pregledne in povečujejo razumevanje aktualnih vsebin v javni razpravi ter prispevajo k verodostojni in odgovorni razpravi. Na ta način se izognemo temu, da bi se izpostavljale le tiste informacije, ki bi bile v korist zasebnih interesov, in prikrije informacije, ki so v škodo javnega interesa. Informacijski pooblaščenec je zaključil, da bi razkritje zahtevanih podatkov dejansko pripomoglo k širši razpravi in razumevanju nečesa pomembnega za širšo javnost, kot to omogočajo že javno objavljeni podatki. Ker je glede na vse navedeno škoda, ki bi nastala z razkritjem obravnavanih osebnih podatkov manjša, kot je javni interes po seznanitvi z njimi, je Informacijski pooblaščenec organu naložil, da jih posreduje prosilki.

KLJUČNE BESEDE: osebni podatek, test interesa javnosti, številka odločbe 090-78/2023/21

Predlog Vlade RS, ki ga je pristojna ministrica podpisala in je bil poslan na Vlado RS, ni dokument v izdelavi

Prosilec je pri Ministrstvu za javno upravo vložil zahtevo za dostop do analize in alternativne rešitve za odpravo prekršnosti v državni upravi, ki jo je pripravil organ. Organ je zahtevo zavrnil z utemeljitvijo, da gre za dokument v izdelavi, vladno gradivo medresorsko še ni usklajeno in sklepa (vlade) pristojna oseba še ni podpisala. V pritožbenem postopku je Informacijski pooblaščenec ugotavljal, ali so kumulativno izpolnjeni vsi pogoji, ki jih za obstoj zatrjevana izjema določa 9. točka prvega odstavka 6. člena ZDIJZ: (1) dokument mora biti še v postopku izdelave, (2) dokument mora biti še predmet posvetovanja in (3) razkritje dokumenta bi povzročilo napačno razumevanje njegove vsebine. Zahtevani dokument je priloga predloga Vlade RS, ki ga je pristojna ministrica podpisala in je bil poslan na Vlado RS (čeprav kasneje umaknjen), iz česar izhaja, da prva dva pogoja nista izpolnjena. Organ je zgolj pavšalno zatrjeval, da bi razkritje zahtevanega dokumenta povzročilo napačno razumevanje njegove vsebine, Informacijski pooblaščenec pa je ugotovil, da glede na vsebino zahtevanega dokumenta že po naravi stvari njegovo razkritje ne bi moglo povzročiti napačnega razumevanja njegove vsebine. Ne vsebuje namreč odločitve za eno od alternativnih rešitev in tako javnosti ne ponuja priložnosti, da bi lahko preuranjeno sklepala in napačno razumela vsebino dokumenta. Zahtevani dokument analizira dosedanje stanje, predstavlja različne alternativne rešitve, opisuje pričakovane posledice in vplive teh rešitev, vse pa temelji na ekonomski analizi in študiji ter tako ne more vplivati na napačne predstave, ki bi si jih javnost ustvarila o bodočih odločitvah pristojnih odločevalcev. Nasprotno, z dostopom do navedenega dokumenta bi javnost lahko preverila, kako se je z aktualno problematiko prekršnega dela soočil organ, potem ko je bila tema odprave prekršnosti že večkrat predmet javne razprave. Ker zatrjevana izjema ni podana, je organ prosilcu dolžan posredovati zahtevani dokument.

KLJUČNE BESEDE: dokument v izdelavi, številka odločbe 090-167/2023

Podatki iz pogodbe o opravljanju koncesionirane gospodarske javne službe so podatki, ki so javni že po zakonu, zato ne predstavljajo poslovne skrivnosti

Mestna občina Murska Sobota je prosilcu zavrnila dostop do koncesijske pogodbe o opravljanju javne gospodarske službe čiščenja odpadnih komunalnih in padavinskih voda iz razloga poslovne skrivnosti (2. točka prvega odstavka 6. člena ZDIJZ). Informacijski pooblaščenec je v pritožbenem postopku ugotovil, da zahtevana pogodba, ki je nastala pred uveljavitvijo Zakona o poslovni skrivnosti (ZPosS), ne predstavlja poslovne skrivnosti, ker v zvezi z njo niso izpolnjeni kriteriji iz 39. člena Zakona o gospodarskih družbah (ZGD-1). Niti iz zahtevane pogodbe niti iz odgovora stranskih udeležencev ne izhaja, da bi bila ta pogodba označena kot poslovna skrivnost, zgolj sklicevanje na to, da organ oz. stranski udeleženci varujejo podatke iz te pogodbe pred nepooblaščenimi vpogledi in kot poslovno skrivnost, pa ne zadostuje za utemeljitev subjektivnega kriterija. Za obstoj objektivnega kriterija mora biti potreba po varstvu očitna in izkazana škoda občutna, pri čemer je dokazno breme na zainteresiranem subjektu. Stranska udeleženca sta zgolj pavšalno navajala, da gre pri zahtevani pogodbi za poslovno skrivnost in nista posebej izkazovala škode, ki bi jima nastala z razkritjem podatkov, zato nastanek škode ni bil izkazan, kar pomeni, da tudi objektivni kriterij za določitev poslovne skrivnosti ni izpolnjen. Poleg tega se zahtevana pogodba nanaša na izvajanje javne funkcije in na porabo javnih sredstev, zato gre za absolutno javne podatke po prvi alineji tretjega odstavka 6. člena ZDIJZ. Predmet zahtevane pogodbe je namreč opravljanje gospodarske javne službe čiščenja komunalnih odpadnih in padavinskih voda na območju organa. Vsebinska takšne pogodbe je zakonsko regulirana in ni prepuščena svobodi volj sodelujočih. Izvajanje javne službe je v javnem interesu, zato je v teh segmentih izrednega pomena nadzor javnosti nad koncesionirano dejavnostjo. Če bi dopustili možnost, da koncesionar in koncedent podatke iz koncesijskih pogodb označita za poslovno skrivnost, bi povsem onemogočili nadzor javnosti nad zakonitostjo postopka sklepanja in izvajanja koncesijske pogodbe. Podatki iz koncesijske pogodbe so zato javni že na podlagi zakona, saj so povezani z opravljanjem javne funkcije. Pojem »javne funkcije« namreč ni

vezan zgolj na funkcionarje v državnih organih in organih lokalnih skupnosti, ampak ga je treba s sistematično in teleološko razlago povezati s pojmom »javne službe« v javnopravnem pomenu te pojmovne zveze. Nadalje se vsebina koncesijske pogodbe nanaša tudi na porabo javnih sredstev. Pri tem je Informacijski pooblaščenec poudaril, da pojem »poraba javnih sredstev« ne vključuje samo proračunskih sredstev, temveč tudi sredstva, ki jih izvajalec za izvajanje javne službe pridobi iz drugih virov, npr. od končnih uporabnikov. Poraba javnih sredstev namreč ni zgolj »trošenje«, pač pa vse oblike razpolaganja z javnimi sredstvi. Vsak, ki sklene pravni posel z osebo javnega prava, se mora zavedati, da sklepa posel z javnim sektorjem, v katerem veljajo posebna pravila glede transparentnosti, javnosti in odgovornosti. Vsakdo ima pravico vedeti, kako se razpolaga z javnimi sredstvi ne glede na to, ali je drugi partner v nekem poslu, kjer javnopravni subjekt razpolaga z javnimi sredstvi, oseba javnega prava ali zasebnopravni subjekt. Podatki o porabi javnih sredstev so vedno javni. Informacijski pooblaščenec je zaključil, da je vsebina zahtevane pogodbe prosto dostopna.

KLJUČNE BESEDE: poslovna skrivnost, številka odločbe 090-184/2023/9

Organ je kot pravna oseba javnega prava zavezan k preglednemu poslovanju v svojem celotnem delovanju, tudi glede revidiranih notranjih procesov delovanja organa

Prosilka je od Slovenskega državnega holdinga d.d. zahtevala dokumente, povezane z notranjo revizijo. Organ se je pri zavrnitvi skliceval na izjemo poslovne skrivnosti (2. točka prvega odstavka 6. člena ZDIJZ) in notranjega delovanja (11. točka prvega odstavka 6. člena ZDIJZ). Informacijski pooblaščenec je v pritožbenem postopku ugotovil, da so navedbe organa, ki nosi dokazno breme glede obstoja poslovne skrivnosti, pavšalne in nekonkretizirane, pa tudi neutemeljene, saj glede obravnavane dokumentacije niso kumulativno izpolnjeni pogoji, ki jih za opredelitev poslovne skrivnosti določa Zakon o poslovni skrivnosti (ZPosS). Informacijski pooblaščenec je nato ugotavljal še obstoj izjeme notranjega delovanja, za katero morata biti kumulativno izpolnjena dva kriterija: (1) podatek mora izhajati iz dokumenta, ki je bil sestavljen v zvezi z notranjim delovanjem oz. dejavnostjo organa, in (2) razkritje takšnega podatka bi povzročilo motnje pri delovanju oz. dejavnosti organa. Informacijski pooblaščenec je ugotovil, da zahtevani dokumenti izpolnjujejo prvi kriterij zatrjevanje izjeme. Pri zatrjevanju drugega kriterija je organ navajal, da bi razkritje onemogočilo njegovo delovanje in nemoteno ter stabilno poslovanje v vseh okoliščinah. Informacijski pooblaščenec takšni utemeljitvi ni sledil, saj organ z njo ni izkazal, niti s stopnjo verjetnosti, motnje pri delovanju organa, temveč gre zgolj za nepojasnjena in nedokazana predvidevanja organa. Razkritje temeljne listine o delovanju notranje revizije, s katero organ opredeli namen, pomen in naloge revizije, po stališču Informacijskega pooblaščenca ne more povzročiti motnje pri delovanju organa, saj gre za splošen akt, ki opredeljuje poslanstvo in položaj izvajalcev notranje revizijske dejavnosti, področje dela, pooblastila ter odgovornost notranjih revizorjev in ne posega v temeljno dejavnost organa, ki naj bi bila motena, tj. v upravljanje z naložbami organa in države. Gre za krovni ustanovitveni akt službe notranje revizije, katerega vsebina je načeloma splošna in praviloma predvidljiva. Posledično razkritje navedenega dokumenta ne more povzročiti relevantnih motenj pri njegovem delovanju. Enako velja tudi za načrt dela notranje revizije za konkretno leto (oz. rebalans navedenega načrta), saj dejstvo, da bi bila javnost seznanjena s področji notranjega delovanja, ki jih želi organ v konkretnem letu revidirati, samo po sebi ne more predstavljati resne in konkretne nevarnosti povzročitve motenj v delovanju organa. Obravnavana poročila redne notranje revizije so bila pripravljena z namenom pregleda ustreznosti, učinkovitosti, skladnosti in zakonitosti notranjih procesov delovanja organa. Iz samih poročil notranje revizije ni mogoče prepoznati, kaj naj bi po mnenju organa predstavljalo informacije, zaradi katerih bi bilo organu ob razkritju onemogočeno poslovanje, saj se področja revizije niso nanašala na temeljno poslovno dejavnost organa, temveč na tehnične in organizacijske procese delovanja organa, ki morajo biti učinkoviti in skladni s predpisi, vendar ne predstavljajo temeljnega delovanja organa, njihovo razkritje pa posledično ne more onemogočiti delovanja in stabilnega poslovanja organa, prav tako tega v izpodbijani odločbi ni pojasnil ali izkazal niti organ. Organ motenj ni konkretiziral na dejansko stanje in ni presojal, zakaj bi razkritje konkretnega poročila

ali podatkov iz konkretnega poročila redne notranje revizije ogrozilo njegovo poslovanje, pavšalne in nekonkretizirane navedbe organa pa za obstoj navedene izjeme ne morejo biti pravno upoštevne. Ključno je tudi to, da če notranja revizija ni zaznala nepravilnosti, razkritje poročila ne more škodovati ali povzročiti motnje pri delovanju organa. Če pa je bilo ugotovljeno delovanje morebiti v nasprotju s pravili in zakonodajo, pa je prav, da se take nepravilnosti razkrijejo, kar pa je možno le, če je revizijsko poročilo dostopno javnosti. Pri tem pa je treba izhajati iz načelnega stališča, da je organ kot pravna oseba javnega prava zavezan k preglednemu poslovanju v svojem celotnem delovanju, torej tudi glede revidiranih notranjih procesov delovanja organa. Iz vsega navedenega izhaja, da organ s pavšalnimi in abstraktnimi navedbami svojega dokaznega bremena ni izpolnil, zato ne obstaja resna in konkretna nevarnost povzročitve motenj v delovanju organa, ki bi nastale zaradi seznanitve prosilke oz. javnosti z zahtevanimi dokumenti. Ker v obravnavani zadevi ni izpolnjen drugi kumulativni pogoj, ki ga za obstoj izjeme po 11. točki prvega odstavka 6. člena določa ZDIJZ, ni podana izjema notranjega delovanja organa. Informacijski pooblaščenec je zato organu naložil, da prosilki posreduje zahtevane dokumente s prekritimi varovanimi osebnimi podatki.

KLJUČNE BESEDE: notranje delovanje, številka odločbe 090-251/2023

Pri odločanju o dostopu do sodbe je treba upoštevati, v kakšnem obsegu je bila javnost izključena, sicer bi lahko prišlo do izvotlitve namena izključitve javnosti na narokih in pri razglasitvi sodbe

Okrožno sodišče v Ljubljani ni ugodilo zahtevi, s katero je prosilec zahteval dostop do sodbe v kazenski zadevi iz razloga varstva osebnih podatkov (3. točka prvega odstavka 6. člena ZDIJZ). Informacijski pooblaščenec je po proučitvi pritožbe ugotovil, da zahtevana sodba vsebuje varovane osebne podatke, in sicer se skozi celotno vsebino prepletajo različni osebni podatki ter veliko naveznih okoliščin, iz katerih je mogoče določiti posamezne osebe, pri čemer ni znana pravna podlaga, ki bi določala, da se vsi ti podatki lahko posredujejo javnosti kot prosto dostopne informacije javnega značaja. Pri izvedbi delnega dostopa do obravnavane sodbe je Informacijski pooblaščenec smiselno sledil namenu tistih določb Zakona o kazenskem postopku (ZKP) o izključitvi javnosti, katerih namen je, da se zavaruje osebno življenje oškodovancev in obtožencev ter udeležba mladoletnih oseb v postopku (360. člen ZKP v povezavi z 295. členom ZKP). V konkretnem primeru je bila javnost izključena iz glavnih obravnav in v delu razglasitve sodbe zoper mladoletnega storilca ter v celoti glede razglasitve razlogov in kratke obrazložitve sodbe. Navedeno je Informacijski pooblaščenec upošteval pri odločanju o dostopu do sodbe, saj bi sicer lahko prišlo do tega, da bi bil izvotljen namen izključitve javnosti na narokih in pri razglasitvi sodbe. Organu je tako naložil, da prekrije posamične osebne podatke v uvodu, izreku in zaključku sodbe, obrazložitev pa v celoti. Slednja ima namreč tolikšno vsebnost in koncentracijo varovanih osebnih podatkov, da delnega dostopa ni mogoče izvesti na način, da se izločijo zaupni (varovani) podatki, saj bi bilo mogoče izločene podatke razbrati iz drugih informacij, vsebovanih v dokumentu. Pri tem je Informacijski pooblaščenec upošteval tudi rezultat testa interesa javnosti, v okviru katerega je ugotovil, da v obravnavani zadevi ne gre za podatke, ki bi bili pomembni za širšo javnost (npr. širša tema, ki je v splošnem javnem interesu, poraba javnega denarja, vprašanje javnega zdravja, javne varnosti ...). Glede na to, da se obravnavana zadeva nanaša na sojenje, iz katerega je bila javnost izključena, pa obstaja močan interes, da se obravnavana sodba ne razkrije javnosti v celoti. V zadevi zato ni podanih dovolj argumentov, ki bi tehtanje obrnili v smer javnega razkritja, zato prevladujoč interes javnosti za razkritje sodbe v celoti ni podan. Takšno stališče izhaja tudi iz ustaljene prakse Upravnega sodišča RS, ki šteje, da je razkritje informacij na podlagi testa interesa javnosti dovoljeno le v izjemnih primerih (javna varnost, javno zdravje, življenje ljudi in podobno); zgolj medijska odmevnost zadeve ne zadostuje.

KLJUČNE BESEDE: osebni podatek, test interesa javnosti, številka odločbe 090-307/2023

ZDIJZ med zavezanca uvršča organe vseh treh vej oblasti, torej tudi sodno, in to ne le v zvezi z upravnimi funkcijami, temveč tudi glede izvajanja funkcije sojenja v celoti

Okrožno sodišče v Kranju je delno zavrnilo zahtevo prosilca za dostop do vseh dokumentov in prilog sodnega spisa. Prosilcu je omogočilo dostop do sodb, v preostalem delu pa je zahtevo zavrnilo in se pri tem sklicevalo na odločitev Vrhovnega sodišča v zadevi št. X Ips 4/2020 z dne 27. 5. 2020. Po mnenju organa je uporaba ZDIJZ izključena za vse dokumente iz sodnih spisov, razen sodb, prosilec pa lahko dostop do teh dokumentov zahteva na podlagi 150. člena Zakona o pravdnem postopku (ZPP). Informacijski pooblaščenec je v pritožbenem postopku ugotovil, da organ pri odločitvi ni upošteval, da je bila v zadevi št. X Ips 4/2020 prosilka tudi stranka kazenske zadeve, iz katere je zahtevala dokumente, v obravnavani zadevi pa prosilec po ZDIJZ ne zahteva dostopa do dokumentov iz zadeve, v kateri sam nastopa kot stranka. Prav tako je odločitev v zadevi št. X Ips 4/2020 temeljila na določbi ZKP, ki je bila kasneje spremenjena na način, da je ne glede na določbe ZKP mogoča zahteva za dostop do informacij javnega značaja po ZDIJZ. Poleg tega je organ spregledal, da je Republika Slovenija ratificirala Konvencijo Sveta Evrope o dostopu do uradnih dokumentov, v skladu s katero pravosodnih organov ni zavezala le k posredovanju dokumentov, ki se nanašajo na upravne funkcije, ampak tudi tistih, ki so povezani z izvajanjem funkcije sojenja. Upoštevajoč vse navedeno je Informacijski pooblaščenec zaključil, da je predmet presoje po ZDIJZ celoten zahtevani sodni spis s prilogami, pri čemer je ugotovil, da sicer vsebuje podatke, ki so izjema po 2. in 3. točki prvega odstavka 6. člena ZDIJZ, vendar je z izvedbo delnega dostopa možno zahtevi delno ugoditi. V zvezi z opredelitvijo izjem od prostega dostopa v obravnavani zadevi je Informacijski pooblaščenec poudaril tudi dejstvo, da se je sodni postopek nanašal na kupoprodajno pogodbo za zemljišča v lasti tožene stranke, ki je občina, kar pomeni, da se je s to kupoprodajno pogodbo razpolagalo z javnimi sredstvi. Gre torej za podatke o porabi javnih sredstev, ki so absolutno javni na podlagi tretjega odstavka 6. člena ZDIJZ.

KLJUČNE BESEDE: kršitev materialnega prava, številka odločbe 090-272/2023

Dogovor več nasprotnih strani, ki sanira neustavno ureditev in posledično omogoča izvajanje človekove pravice do neodvisnega sodišča, ni izjema notranjega delovanja in je hkrati tudi materija, ki zadeva širši javni interes

Generalni sekretariat Vlade RS je, sklicujoč se na izjemo notranjega delovanja (11. točka prvega odstavka ZDIJZ), zavrnil zahtevo prosilca za dostop do dogovorov o ureditvi plač funkcionarjev Ustavnega sodišča Republike Slovenije, funkcionarjev sodne oblasti in državno tožilskih funkcionarjev. Za obstoj te izjeme morata biti kumulativno izpolnjena dva pogoja: (1) podatek mora izhajati iz dokumenta, ki je bil sestavljen v zvezi z notranjim delovanjem oz. dejavnostjo organa, in (2) razkritje takšnega podatka bi povzročilo motnje pri delovanju oz. dejavnosti organa. Informacijski pooblaščenec je v pritožbenem postopku ugotovil, da že prvi pogoj ni podan, saj ne gre za akt, ki bi nastal v okviru Vlade RS ali posameznega ministrstva niti ne gre za dokument, ki je (še) v medresorskem usklajevanju, ampak za dokument, ki odraža dogovor, do katerega je prišlo s pogajanjem več »nasprotnih« strani. Ne gre torej za notranje delovanje oz. dejavnost organa in za njegovo interno politiko, saj od tedaj, ko je vsebina nove plačne ureditve za funkcionarje (sodnike, funkcionarje Ustavnega sodišča in državne tožilce) postala del dogovora, pri katerem so sodelovale in ga sooblikovale različne, zunanje, strani, ki so na koncu dosegle dogovor, ni mogoče govoriti o politiki organa in o notranjem delovanju, temveč o dogovorjeni ureditvi. Nadalje je Informacijski pooblaščenec ugotovil, da tudi drugi pogoj za obravnavano izjemo ni podan. Organ je motnje, ki naj bi z razkritjem dokumentov nastale, utemeljil predvsem s svojimi pogajanjem, ki jih vodi s sindikati javnega sektorja, pri čemer ni prepričljivo utemeljil, kako je položaj zadevnih funkcionarjev (sodnikov, funkcionarjev Ustavnega sodišča in državnih tožilcev) in javnih uslužbencev podoben oz. v zahtevanih dokumentih povezan. Argumenti organa nasprotujejo stališču predstavnikov države, ki so bili izraženi ob sklenitvi zahtevanih dogovorov, ter odločitvi Ustavnega sodišča (št. U-I-772/21-37 z dne 1. 6. 2023). Da položaj zadevnih funkcionarjev in javnih uslužbencev ni povezan do te

mere, da bi se ju uredilo hkrati, je za javnost navedla tudi nekdanja ministrica za javno upravo ob sklenitvi zahtevanih dogovorov, ki je tudi javno razkrila že vse bistvene elemente dokumenta. Upošteva vse navedeno je Informacijski pooblaščenec ugotovil, da zatrjevana izjema ni podana, in še poudaril, da gre za podatke, ki so javni na podlagi tretjega odstavka 6. člena ZDIJZ, saj zahtevana dogovora vsebujeta informacije, ki so povezane s porabo javnih sredstev, saj so vsi obravnavani funkcionarji plačani iz javnih sredstev. Prav tako dogovora urejata pravice (do plačila) funkcionarjev in gre tako nedvomno tudi za podatke, povezane z opravljanjem javne funkcije. Hkrati transparentnost te vrste podatkov določa tudi ZSPJS v 38. členu. Informacijski pooblaščenec je izvedel še test interesa javnosti, pri katerem je bilo ključno vprašanje, ali bi razkritje zahtevanih dokumentov dejansko pripomoglo k širši informiranosti javnosti in razumevanju nečesa za širšo javnost pomembnega, kot to omogočajo že javno objavljeni podatki. Dogovor, ki sanira neustavno ureditev in posledično omogoča izvajanje človekove pravice do neodvisnega sodišča, zadeva širši javni interes. Ne gre zgolj za vprašanje, ali sta zahtevana dogovora sklenjena na način in v duhu Ustavne odločbe, ki ureditev položaja in plač sodnikov povezuje z njihovo neodvisnostjo. Gre za vprašanje, ali ta dogovora ustavno skladno zagotavljata varstvo pravice do neodvisnosti sojenja vsem udeležencem sodnih postopkov. Glede na jasno odločitev Ustavnega sodišča, da je stanje ureditve plač sodnikov neustavno, brez poznavanja vsebine obeh sklenjenih dogovorov širša javna razprava o tem, ali dogovora neustavnost sanirata, ni mogoča. Dostop do sklenjenih dogovorov namreč odgovori na vprašanja, ali navedeni funkcionarji ostajajo v enotnem sistemu, na kakšen način se vzpostavlja njihov položaj in v kakšnem odnosu oz. razmerju so do drugih, ki jih ureja plačni sistem javnega sektorja. Informacijski pooblaščenec je zaključil, da javni interes prevlada nad interesom, ki ga zatrjuje organ, in organu naložil, da prosilcu omogoči dostop do zahtevanih dokumentov tudi na tej podlagi.

KLJUČNE BESEDE: notranje delovanje, test interesa javnosti, številka odločbe 090-304/2023

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 sta bistvenega pomena za njihovo boljše delovanje, kar hkrati prinaša koristi vsem članom družbe. Zato Informacijski pooblaščenec pozornost namenja tudi ozaveščanju strokovne in splošne javnosti, s čimer 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 Advocates Network (FOIANet), leta 2015 ga je za svetovni dan dostopa do informacij izglasovala Generalna konferenca UNESCA, na 74. Generalni skupščini Združenih narodov leta 2019 pa je bil ta dan razglašen za mednarodni dan univerzalne pravice dostopa do informacij.

V okviru dogodkov ob svetovnem dnevu pravice vedeti je Informacijski pooblaščenec 27. 9. 2023 v prostorih Akademije za glasbo v Ljubljani priredil svečano akademijo z naslovom **Informacije javnega značaja so in bodo krojile odprtost družbe.**

Dogodek je kot častna gostja otvorila dr. Nataša Pirc Musar, predsednica republike, nato pa sta udeležence pozdravili informacijska pooblaščenka Mojca Prelesnik in ministrica za javno upravo Sanja Ajanović Hovnik. Informacijska pooblaščenka je poudarila, da Zakon o dostopu do informacij javnega značaja že 20 let nudi dobro podlago za uresničevanje pravice vedeti v Sloveniji, na njegovi podlagi vodeni pritožbeni postopki pa vselej stremijo k odpiranju informacij, s čimer Informacijski pooblaščenec pomembno prispeva k uspešnemu razvoju transparentnosti javnega sektorja. Posebej je poudarila pomen seznanitve javnosti z informacijami na področjih sprejemanja predpisov, delovanja pravosodnih organov, porabe javnih sredstev ter okoljskih in tajnih podatkov. Zaključila je, da mora biti še naprej naš skupen cilj, da na dobri zakonski podlagi gradimo trdno kulturo transparentnosti, ki je nujen pogoj za uresničevanje drugih pravic v demokratični družbi.

V nadaljevanju dogodka je Informacijski pooblaščenec podelil tudi nagrado ambasador transparentnosti. Prejel jo je zavod Danes je nov dan, Inštitut za druga vprašanja, ki s številnimi projekti krepi zavedanje javnosti o pomenu transparentnega delovanja in vključevanju civilne družbe v procese demokratičnega odločanja tako na državni kot na lokalni ravni. Udeležence je z video izjavo nagovoril tudi dr. Gregor Virant, nekdanji minister za javno upravo. Sledila je okrogla miza, na kateri so udeleženci zaključili, da se zakon v praksi dobro uresničuje in dosega svoj namen, kljub temu pa so še možne izboljšave, zlasti na področju poenostavitve postopkov in skrajšanja časa reševanja zadev. V luči hitrega razvoja modernih tehnologij in umetne inteligence so opozorili tudi na izzive, ki jih prinaša prihodnost, in se strinjali, da je treba v javnem sektorju še naprej spodbujati vrednostni sistem, ki stremi k odprtosti.

Da bi bili postopki dostopa do informacij javnega značaja še hitrejši in še učinkovitejši, je Informacijski pooblaščenec ob tej priložnosti izdal priročnik za zavezance in prosilce, v katerem so zbrani odgovori na najpogostejše dileme iz prakse.

Dogodek ob dnevu pravice vedeti, Ljubljana, 27. 9. 2023.



2.6.2 Mednarodno sodelovanje

Od 11. do 13. oktobra 2023 je v Dubrovniku potekalo 4. srečanje Iniciative 2020, združenja, ki je bilo oktobra 2020 ustanovljeno na pobudo slovenskega Informacijskega pooblaščenca in v katerega so se povezali pritožbeni organi s področja dostopa do informacij javnega značaja iz Slovenije, Hrvaške, Bosne in Hercegovine, Črne gore, Srbije, Kosova in Severne Makedonije. Namen združenja je krepitev sodelovanja in izmenjava dobrih praks pri promociji in varstvu pravice dostopa do informacij javnega značaja.

Udeleženci so razpravljali o doseženih standardih pri dostopu do informacij javnega značaja v posameznih državah, odprtih vprašanjih pri dostopu do informacij v konkretnih primerih ter o proaktivnem posredovanju informacij. Posebna pozornost je bila namenjena problematiki molka organov in zlorabi pravice dostopa. Glede molka so poudarili, da molk organov derogira pravico dostopa do informacij javnega značaja in je zato treba v okviru veljavnega pravnega reda poiskati učinkovita sredstva za sankcioniranje odgovornih oseb organov, ki v praksi najpogosteje ignorirajo zahteve za dostop do informacij. V zvezi z zlorabo pravice dostopa do informacij so izpostavili, da prekomerno otežuje delo zavezancev in škoduje uresničevanju te pravice v praksi. Cilj teh prosilcev ni zagotavljanje transparentnosti, odprtosti in nadzora nad javnimi oblastmi, ampak oteževanje dela zavezancev, nekatere zahteve pa so celo finančno motivirane. Takšno izvrševanje pravice je nedopustno in ni v skladu z njenim namenom. V nacionalnih zakonih je zato nujno treba vzpostaviti pravne varovalke za takšne primere, urediti institut zlorabe pravice oz. nepoštene uporabe prava.

4. srečanje združenja Iniciative 2020 v Dubrovniku.



2.7 SPLOŠNA OCENA IN PRIPOROČILA

V letu 2023 je Informacijski pooblaščenec na tem področju obravnaval 1.021 zadev, kar je 50 več kot v letu 2022 in največ od svoje ustanovitve. Od tega je obravnaval 704 pritožb (386 zoper zavrnilne odločbe, 302 zaradi molka organa in 16 zoper odločitve poslovnih subjektov pod prevladujočim vplivom) ter pripravil 317 odgovorov na zaprosila zavezancev in prosilcev. Povprečen čas reševanja pritožbene zadeve je bil 28 dni.

Informacijski pooblaščenec ugotavlja, da je glede na leto 2022 skupno število prejetih pritožb naraslo za 10 %, pri čemer je skrb vzbujajoč podatek, da je bistveno naraslo število prejetih pritožb zaradi molka organa (302 v letu 2023 v primerjavi z 241 v letu 2022). To pomeni, da so se zavezanci glede na predhodno leto slabše odzivali na prejete zahteve za posredovanje informacij javnega značaja, stopnja transparentnosti pa se je posledično znižala. Največ prejetih pritožb je bilo vloženih zoper državne organe (državna uprava in drugi državni organi), pri čemer je pri teh zavezancih v primerjavi z letom poprej naraslo tako število pritožb zoper zavrnilne odločbe kot zoper molk organa. Tudi v zvezi z občinami je Informacijski pooblaščenec zaznal povečanje števila prejetih pritožb, pri čemer se je po nekaj letih upadanja žal ponovno naraslo število pritožb zaradi molka (v letu 2022 je bilo teh 44, v letu 2023 pa 67).

Po oceni Informacijskega pooblaščenca je omenjeno posledica več okoliščin. S spremembo pravil upravnega poslovanja (večina zahtev je vložena po navadni elektronski pošti, v elektronske predale zavezancev) se je za prosilce način uveljavljanja pravice dostopa do informacij javnega značaja še poenostavil, zavezanci pa na tako povečano število zahtev in hitrejši način komunikacije niso ustrezno pripravljeni in se posledično ne odzivajo dovolj hitro. Obenem je zaradi organizacijskih razlogov (reorganizacija državne uprave) pri zavezancih prihajalo do kadrovske spremembe in do menjav uradnih oseb, ki so pristojne za to področje. Ker je dostop do informacij javnega značaja v demokratični družbi za državljane pomembno orodje za spremljanje dela javne uprave, Informacijski pooblaščenec zavezance poziva, naj temu področju namenijo še več pozornosti. Postopki dostopa do informacij javnega značaja so v praksi vsebinsko vse kompleksnejši in procesno vse bolj zahtevni, zato naj za uradne osebe za posredovanje informacij javnega značaja imenujejo osebe z ustreznim strokovnim (pred)znanjem in dobrim poznavanjem vodenja upravnega postopka na prvi stopnji, vse zaposlene pa naj seznanijo z osnovnimi obveznostmi, ki jih zakon prinaša. V praksi Informacijski pooblaščenec namreč opaža, da zavezanci s tem področjem še vedno niso dovolj seznanjeni, čeprav je od uveljavitve zakona minilo že več kot 20 let.

Ker je Informacijski pooblaščenec na področju dostopa do informacij javnega značaja pritožbeni organ, lahko zavezancem in javnosti svetuje le neformalno, v okviru dosedanje prakse. V letu 2023 je tako odgovoril na 317 zaprosil zavezancev in prosilcev glede uporabe zakona v praksi, kar je bistveno več kot v letu 2022, ko je bilo teh zaprosil 275. Ker je za svetovanje javnosti in zavezancem glede uporabe zakona v praksi pristojno Ministrstvo za javno upravo, ga Informacijski pooblaščenec ponovno poziva (kot že leta 2022), naj temu nameni več pozornosti, npr. v obliki dodatnih brezplačnih usposabljanj izdaje mnenj in smernic, objave predhodnih mnenj na svojih spletnih straneh ...

Po drugi strani pa so prosilci s pravicami, ki jih prinaša ta zakon, dobro seznanjeni in porast pritožbenih zadev gre nedvomno pripisati tudi dejstvu, da se pravnega varstva v pritožbenih postopkih pred Informacijskim pooblaščenecem poslužujejo pogosteje in hitreje. Pritožbeni postopek pred Informacijskim pooblaščenecem je namreč enostaven, hiter in brez posebnih stroškov (ni upravne takse), prosilci pa se običajno zastopajo sami, kar kaže na to, da pritožbeni postopek ni pretirano formaliziran in ga tudi laični prosilci dobro razumejo. V preteklem letu je Informacijski pooblaščenec v praksi žal zaznal tudi več primerov, v katerih način uveljavljanja te pravice ni bil skladen z zakonom. Očitno prekomerno naslavljanje obsežnih in nerazumnih zahtev na zavezance namreč ne uživa pravnega varstva. Pravica dostopa do informacij javnega značaja kot temeljna ustavna pravica je sicer res zasnovana široko, kljub temu pa ne sme biti orodje v rokah tistih prosilcev, ki z namenom

šikaniranja in zasipavanja zavezancev onemogočajo njihovo delo in ogrožajo njihovo javnopravno poslanstvo. V tovrstnih primerih lahko govorimo tudi o zlorabi pravice, ki jo zakon o dostopu do informacij javnega značaja ureja v petem odstavku 5. člena. Kriterije, kdaj gre za zlorabo pravice, je v praksi treba razlagati ozko in v vsakem primeru posebej, utemeljitev obstoja zlorabe pravice pa mora vselej ostati skrajno sredstvo in se sme uporabiti le v primeru, ko od organa objektivno ni mogoče pričakovati, da bi zahteve prosilca obravnaval v skladu z določbami ZDIJZ. Ob tem je treba upoštevati tudi to, da so se za opredelitev zlorabe pravice v praksi Informacijskega pooblaščenca in sodni praksi že razviti kriteriji, ki naj jim zavezanci, v izogib stroškom in zavlačevanju postopkov, v čim večji meri sledijo.

V zvezi s pritožbenimi postopki zoper poslovne subjekte pod prevladujočim vplivom, je Informacijski pooblaščenec v letu 2023 sicer zaznal porast primerov (12), vendar število teh pritožb v skupnem številu vseh že vsa leta ostaja nizko (1,7 %).

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, po katerem 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. Z zakonom določen 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.

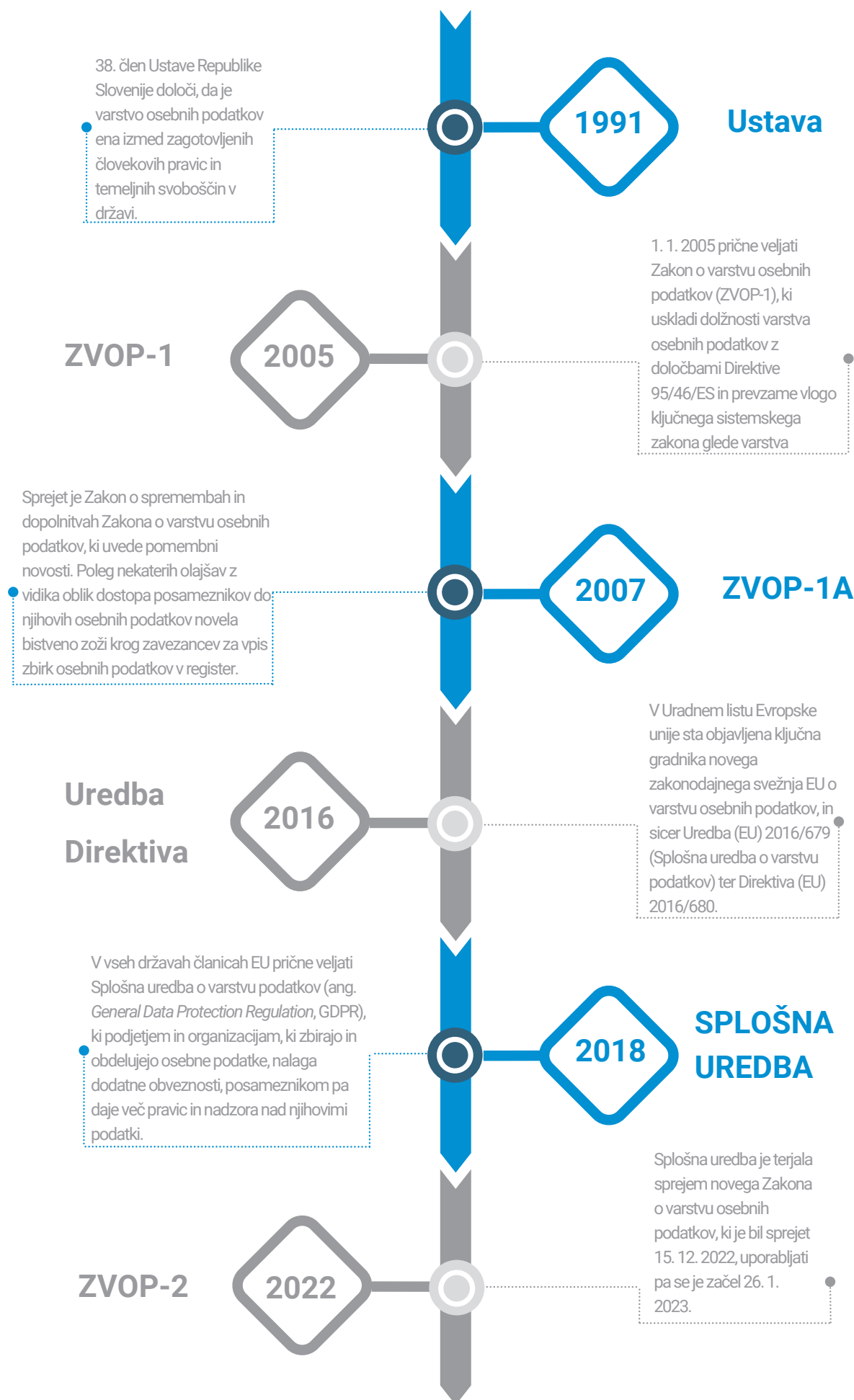
S Splošno uredbo so se okrepile pravice posameznika, poleg obstoječe pravice dostopa do osebnih podatkov ter pravice do popravka še pravica do pozabe, izbrisa, omejitve obdelave, ugovora in prenosljivosti podatkov. Precej večji poudarek je zdaj na transparentnosti obdelave, tj. glede zagotavljanja preglednih 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 dolžni 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 se zagotavlja doslednost pri izvajanju zakonodaje o varstvu podatkov v vsej EU. Bistveno je, da je v primerih, ko obdelava osebnih podatkov poteka 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 v postopkih nadzora sodelujejo 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*).

Splošna uredba je terjala sprejem novega Zakona o varstvu osebnih podatkov (ZVOP-2), s katerim se v Republiki Sloveniji zagotavlja izvajanje navedene uredbe. Novi Zakon o varstvu osebnih podatkov (ZVOP-2) je bil sprejet šele 15. 12. 2022 in se je začel uporabljati 26. 1. 2023.

Časovni razvoj Zakona o varstvu osebnih podatkov.



3.2 NADZOR V LETU 2023

3.2.1 INŠPEKCIJSKI NADZOR

Postopek inšpekcijskega nadzora, ki ga izvaja Informacijski pooblaščenec oz. državni nadzorniki za varstvo osebnih podatkov, poleg Zakona o varstvu osebnih podatkov (ZVOP-2), 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-2 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 58. členu 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 upravljavcu ali obdelovalcu izda 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 ter 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 z 42. in

43. členom, 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 83. členom;
- da odredi prekinitev prenosov podatkov uporabniku v tretji državi ali mednarodni organizaciji.

Informacijski pooblaščenec je leta 2023 zaradi suma kršitev določb Splošne uredbe in/ali ZVOP-2 vodil 702 inšpekcijski zadevi, od tega 198 v javnem in 504 v zasebnem sektorju. V javnem sektorju je 187 inšpekcijskih postopkov začel na podlagi prejetih prijav, 11 pa na lastno pobudo, v zasebnem pa je 499 postopkov vodil na podlagi prejetih prijav, pet pa jih je uvedel na lastno pobudo.

Inšpekcijske prijave, ki jih je prejel Informacijski pooblaščenec, so se nanašale na naslednje sume kršitev določb Splošne uredbe in ZVOP-2:

Sum kršitve	Število prijav
Nezakonito izvajanje videonadzora	203
Nezakonito razkrivanje, posredovanje osebnih podatkov nepooblaščenim uporabnikom in nezakonita objava osebnih podatkov	112
Nezakonito zbiranje oz. zahtevanje osebnih podatkov	91
Neustrezno zavarovanje osebnih podatkov	44
Nezakonit vpogled v osebne podatke	44
Nezakonita obdelava osebnih podatkov pri izvajanju neposrednega trženja	38
Kršitev pravice do informacij po 13. členu	18
Piškotki	11
Obdelava osebnih podatkov v nasprotju z namenom zbiranja	9
Hekerski napadi in vdori v informacijske sisteme	3
Razno – obdelava osebnih podatkov po poteku roka hrambe, uporaba netočnih podatkov, kršitev pravice do seznanitve z osebnimi podatki in pravice do ugovora, sumi kršitev, ki ne sodijo v pristojnost Informacijskega pooblaščenca	113
Skupaj prijav	686

3.2.2 INŠPEKCIJSKI NADZOR V JAVNEM SEKTORJU

Zaradi suma kršitev določb Splošne uredbe in/ali ZVOP-2 je Informacijski pooblaščenec zoper zavezanca v javnem sektorju leta 2023 vodil 198 zadev, 187 jih je začel na podlagi prejetih prijav, 11 pa na lastno pobudo.

Informacijski pooblaščenec je 37 prijaviteljem pisno pojasnil, zakaj v prijavi opisano ravnanje ne pomeni kršitve zakonodaje s področja varstva osebnih podatkov, v 36 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 31 kršiteljev uvedel postopke o prekršku oz. je kršiteljem izrekel ukrepe v skladu z Zakonom o prekrških (ZP-1), v štirih 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 pa postopka ni uvedel zaradi zastaranja pregona. V 35 zadevah Informacijski pooblaščenec postopka ni uvedel, saj so bile zatrjevane nepravilnosti že odpravljene. 16 prijaviteljev je Informacijski pooblaščenec napotil na pravice posameznika po Splošni uredbi (predvsem na pravice do seznanitve z lastnimi osebnimi podatki). V 27 zadevah prijavitelji pri utemeljevanju kršitve niso navedli ustreznih dokazov, v 28 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 2023 zavezancem v javnem sektorju izdal 10 t. i. predodločb¹ ter dve ureditveni odločbi, vse ostale kršitve so zavezanci sami prostovoljno odpravili takoj po pozivu državnega nadzornika za varstvo osebnih podatkov.

Leta 2023 je bilo v javnem sektorju 74 inšpekcijskih postopkov zaključenih z izdajo sklepa o ustavitvi postopka. Informacijski pooblaščenec je 38 postopkov ustavil, ker so zavezanci ugotovljene nepravilnosti odpravili, v 15 postopkih ni zaznal kršitev določb Splošne uredbe ali ZVOP-2, v sedmih primerih ni bilo predloženih dovolj dokazov za nadaljevanje postopka, 14 postopkov pa je ustavil zato, ker je šlo za kršitve, ki so predstavljale enkratna dejanja v preteklosti, ki jih z inšpekcijskimi ukrepi za nazaj ni bilo več mogoče odpraviti.

Informacijski pooblaščenec je prejel dve sodbi Upravnega sodišča RS, in sicer je sodišče tožbi, ki je bila vložena leta 2020, ugodilo in zadevo v zvezi z obdelavo osebnih podatkov prisilceve za mednarodno zaščito vrnilo Informacijskemu pooblaščenec v ponovno odločanje. Prav tako je sodišče ugodilo tožbi, vloženi leta 2020 zoper odločbo glede posredovanja poročil izmene Operativno-komunikacijskega centra Uprave za policijske specialnosti Generalne policijske uprave in izpodbijano odločbo Informacijskega pooblaščenca odpravilo.

3.2.3 INŠPEKCIJSKI NADZOR V ZASEBNEM SEKTORJU

Informacijski pooblaščenec je zoper zavezance v zasebnem sektorju vodil 504 zadeve, od tega jih je 499 vodil na podlagi prejetih prijav, pet postopkov pa je uvedel na lastno pobudo. 270 postopkov je bilo uvedenih po iniciativi drugih nadzornih organov v EU v okviru čezmejnega sodelovanja – v teh je Informacijski pooblaščenec sodeloval kot zadevni organ (več v poglavju 3.2.8).

Po proučitvi prijav je Informacijski pooblaščenec 70 prijaviteljev obvestil, da postopka inšpekcijskega nadzora ne bo uvedel, ker iz prijave ne izhaja sum kršitev določb Splošne uredbe in ZVOP-2, 60 prijaviteljev pa je napotil na pravice, ki jih morajo pri upravljavcih osebnih podatkov uveljavljati sami, največkrat na pravico do seznanitve z lastnimi osebnimi podatki in na pravico do ugovora. V 25 primerih Informacijski pooblaščenec 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 13 kršiteljem izrekel ukrep po ZP-1, v 12 primerih je ocenil, da ukrepa po ZP-1 ne bo izrekel, ker gre za prekršek neznatnega pomena. V 122 primerih Informacijski pooblaščenec postopka ni uvedel, ker niso bili predloženi ustrezni dokazi, ki bi zatrjevano kršitev utemeljevali, v 59 primerih pa za ukrepanje ni bil pristojen. V 45 primerih inšpekcijski postopek ni bil uveden, ker je kršitelj nepravilnosti že odpravil. V 15 zadevah je Informacijski pooblaščenec vlogo odstopil pristojnemu organu.

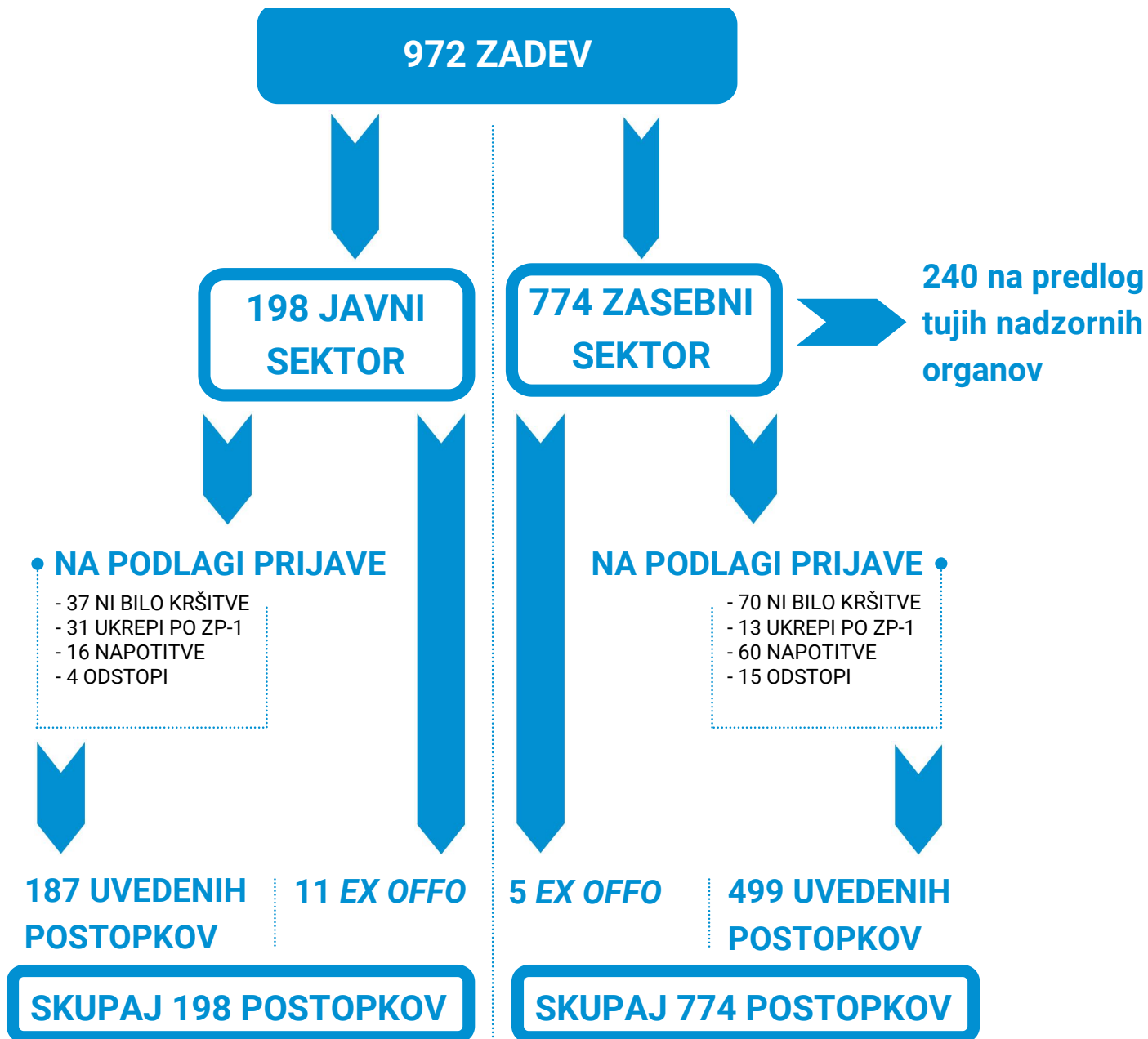
Informacijski pooblaščenec je leta 2023 zavezancem v zasebnem sektorju izdal 39 t. i. predodločb ter 11 ureditvenih odločb, preostale kršitve so zavezanci sami prostovoljno odpravili takoj po pozivu državnega nadzornika za varstvo osebnih podatkov.

¹ Informacijski pooblaščenec mora v primeru, ko ugotovi nezakonito obdelavo osebnih podatkov, pred izdajo odločbe, s katero odredi prenehanje takšne obdelave, zavezanca skladno z načelom zaslišanja stranke (9. člen ZUP) predhodno seznaniti s tem, zakaj po njegovem mnenju za predmetno obdelavo osebnih podatkov nima pravne podlage, ter ga seznaniti z argumenti, ki njegovo mnenje potrjujejo. Zavezancu je namreč glede na sodno 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.

Leta 2023 je Informacijski pooblaščenec pri zavezancih v zasebnem sektorju s sklepom ustavil 156 postopkov: 35 postopkov je ustavil, ker ni zaznal kršitev določb ZVOP-2, 81 postopkov je ustavil po tem, ko so zavezanci odpravili ugotovljene nepravilnosti, 28 postopkov je zaključil, ker v zvezi z ugotovljenimi prekrški ni bilo mogoče izreči inšpekcijskih ukrepov, saj je šlo za enkratna dejanja v preteklosti, v 12 primerih pa ni bilo predloženih dovolj dokazov za nadaljevanje postopka.

Informacijski pooblaščenec je prejel eno sodbo Upravnega sodišča RS v zvezi s tožbo, vloženo leta 2020 zoper odločbo glede izvajanja videonadzora; sodišče je tožbo zavrnilo.

Pregled inšpekcijskih zadev v javnem in zasebnem sektorju leta 2023.



3.2.4 PRIJAVE KRŠITEV VARNOSTI OSEBNIH PODATKOV

Skladno s 33. členom 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 2023 prejel 183 uradnih obvestil o kršitvi varnosti osebnih podatkov, t. i. samoprijav, ki so jih poslali zavezanci. 87 obvestil so poslali zavezanci iz zasebnega sektorja (npr. banke, trgovska podjetja, zavarovalnice), 96 pa zavezanci iz javnega sektorja (predvsem zdravstvene in izobraževalne ustanove).

Kršitve varnosti osebnih podatkov (183) so se nanašale na:

- posredovanje dokumentov z osebnimi podatki (npr. zdravniških izvidov, računov, dokumentov v upravnih postopkih, debetne kartice) napačnim osebam kot posledica nenamerne človeške napake ali netočnih podatkov v zbirkah osebnih podatkov (npr. e-naslovov strank) – 50,
- hekerski vdor oz. kibernetiski napad – 38,
- nezakonito razkritje osebnih podatkov nepooblaščenim osebam – 37,
- nepooblaščen dostop do osebnih podatkov oz. njihova obdelava s strani zaposlenih – 23,
- 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) – 10,
- nezakonito objavo osebnih podatkov – 10,
- izgubo ali krajo prenosnega računalnika ali drugih nosilcev osebnih podatkov (USB-ključek, zdravstveni karton, zvezek z osebnimi podatki strank) – 7.
- razkritje osebnih podatkov zaradi napake v aplikaciji oz. tehnične napake – 4,
- neustrezno zagotavljanje varnosti osebnih podatkov – 3,
- nezakonita uporaba e-naslovov za druge namene – 1.

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

3.2.5 PRITOŽBENI POSTOPKI PO 77. ČLENU SPLOŠNE UREDBE

Poleg inšpekcijskih postopkov vodi Informacijski pooblaščenec tudi postopke prijave po 30. členu ZVOP-2, ki se vodijo na zahtevo prijavitelja s posebnim položajem, s čimer se zagotavlja pravica do pritožbe po 77. členu Splošne uredbe (pritožba zaradi kršitve varstva osebnih podatkov).

Postopek s prijavo zaradi kršitve varstva osebnih podatkov se vodi na zahtevo posameznika, na katerega se nanašajo osebni podatki. V tem primeru gre za nadzorni postopek posebne vrste, v katerem ima tudi prijavitelj položaj stranke nadzornega postopka, zaradi česar mora taka vloga oz. prijava vsebovati vse sestavine, ki jih za vlogo določa Zakon o splošnem upravnem postopku (ZUP). V tem postopku lahko Informacijski pooblaščenec uporabi tudi vsa nadzorna pooblastila (npr. vsa prej naštetá preiskovalna in popravljalna pooblastila iz 58. člena Splošne uredbe) in izreka vse

nadzorne ukrepe, ki mu jih dajejo predpisi (ZVOP-2, Splošna uredba, ZUP in področni zakoni). V tem postopku vsaka stranka krije svoje stroške postopka. V primeru ugotovljenih kršitev pa lahko Informacijski pooblaščenec uvede tudi postopek izreka sankcije po Splošni uredbi, ZVOP-2 in ZP-1.

Posameznik, na katerega se nanašajo osebni podatki, lahko v postopku prijave zahteva:

1. ugotovitev, ali se njegovi osebni podatki v trenutku vložitve prijave obdelujejo nezakonito oz. v nasprotju s Splošno uredbi in ZVOP-2 (in predlaga ukrep za odpravo nepravilnosti) ali
2. informacije, dostop, izbris, popravek ipd. v okviru pravic, ki jih ima po Splošni uredbi (15.–22. člen) – pravica do seznanitve z lastnimi osebnimi podatki, pravica do izbrisa oz. pozabe, pravica do omejitve obdelave, pravica do popravka, pravica do ugovora itd.; v tem primeru mora posameznik pravice uveljavljati pri upravljavcu njegovih osebnih podatkov, preden vloži pritožbo pri Informacijskem pooblaščenecu. Upravljavec je dolžan odgovoriti v enem mesecu od prejema zahteve. Če upravljavec v predpisanem roku ne odgovori ali če posameznikovo zahtevo zavrne, lahko posameznik vloži pritožbo pri Informacijskem pooblaščenecu. Rok za vložitev prijave je 15 dni od prejema zavrnilnega odgovora. Postopki v zvezi z uveljavljanjem pravic so opisani v naslednjem poglavju.

Če državni nadzornik za varstvo osebnih podatkov v takšnem nadzornem postopku zazna sum takšne kršitve varstva osebnih podatkov, ki bi lahko vplivala tudi na pravice drugih posameznikov, mora po uradni dolžnosti uvesti tudi postopek inšpekcijskega nadzora.

Pri obravnavi prijav prijaviteljev s posebnim položajem se pogosto dogaja, da so prijave oz. vloge nepopolne, največji problem pa se kaže v tem, da prijavitelji v njih najpogosteje zatrjujejo enkratno preteklo kršitev (npr. nezakonit vpogled v njihove osebne podatke ali posredovanje osebnih podatkov nepooblaščenemu uporabniku), ki v času vložitve prijave ne obstaja več. Taka prijava praviloma ne more biti predmet nadzornega postopka, v okviru katerega Informacijski pooblaščenec obravnava prijavo prijavitelja s posebnim položajem, saj se skladno s 30. in 34. členom ZVOP-2 v tem postopku obravnavajo le tiste zatrjevane kršitve obdelave osebnih podatkov prijavitelja s posebnim položajem, ki v trenutku vložitve prijave še obstajajo. Ugotavljanje preteklih kršitev varstva osebnih podatkov lahko posameznik skladno z določbami 11. člena ZVOP-2 s tožbo zahteva od sodišča, Informacijski pooblaščenec pa lahko v takih primerih kršitev obravnava v okviru postopka o prekršku, nadzorni postopek pa lahko praviloma uvede le v primeru, ko iz prijave izhaja, da je treba upravljavcu naložiti sprejem ukrepov (npr. organizacijskih in tehničnih ukrepov za zagotavljanje varnosti osebnih podatkov), s katerimi se bodo preprečevale podobne možne kršitve v prihodnosti.

Informacijski pooblaščenec večkrat prejme tudi sicer popolne prijave prijavitelja s posebnim položajem, iz katerih izhaja, da se opisana kršitev varstva osebnih podatkov ne nanaša zgolj na prijavitelja, temveč na več posameznikov. Informacijski pooblaščenec mora na podlagi take prijave prijavitelja s posebnim položajem zaradi identične kršitve (npr. nezakonite obdelave osebnih podatkov) zoper istega upravljavca voditi dva nadzorna postopka, in sicer nadzorni postopek, v okviru katerega preverja in odloča zgolj o zakonitosti obdelave osebnih podatkov prijavitelja s posebnim položajem, ter inšpekcijski postopek, v okviru katerega preverja in odloča o zakonitosti obdelave osebnih podatkov vseh ostalih posameznikov.

Posamezniki so v letu 2023 skupno vložili 130 prijav (v 51 primerih zoper upravljavce javnega sektorja in v 79 primerih zoper upravljavce zasebnega sektorja), s katerimi so zahtevali ugotovitev, da se njihovi osebni podatki obdelujejo nezakonito oz. v nasprotju s Splošno uredbi oz. ZVOP-2.

V okviru postopkov, ki so se vodili zoper upravljavce javnega sektorja, je Informacijski pooblaščenec izdal skupno osem odločb, s katerimi je v dveh primerih ugotovil kršitev Splošne uredbe oz. ZVOP-2, v šestih primerih pa je ugotovil, da kršitev ni. V 22 primerih je vlogo iz postopkovnih oz.

formalnih razlogov s sklepom zavrgel oz. postopka ni uvedel, po podanem pojasnilu v eni zadevi, da kršitev ne obstaja, ter po treh obvestilih, da pri utemeljevanju kršitve niso podani ustrezni dokazi, saj prijavitelji svojih vlog niso ustrezno dopolnili.

Upravljavcem zasebnega sektorja je Informacijski pooblaščenec v letu 2023 izdal pet odločb, s katerimi je v enem primeru ugotovil kršitev Splošne uredbe oz. ZVOP-2, v štirih primerih pa je ugotovil, da kršitev ni. V 28 primerih je vlogo prijavitelja zavrgel, v šestih pa je postopke s sklepom ustavil. V desetih primerih Informacijski pooblaščenec po prejemu nepopolne vloge postopka ni uvedel.

3.2.6 PRAVICE POSAMEZNIKOV

Pravica do seznanitve z lastnimi osebnimi podatki je zagotovljena vsakemu posamezniku v tretjem odstavku 38. člena Ustave RS in v 15. členu Splošne uredbe. Postopkovna pravila so urejena v 11. in 12. členu Splošne uredbe ter v 12. do 21. členu ZVOP-2.

Po 15. členu 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 opredeljuje 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 12. člena 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 pooblaščenču.

Informacijski pooblaščenec je v letu 2023 prejel 75 pritožb posameznikov v zvezi s kršitvami pravice do seznanitve z lastnimi osebnimi podatki po Splošni uredbi. Posamezniki se vedno bolj zavedajo ustavne pravice do seznanitve z lastnimi osebnimi podatki, številni upravljavci pa še vedno ne izpolnjujejo svojih obveznosti in posameznikom ne omogočajo izvrševanja pravic, ki jim jih zagotavljajo različni predpisi.

Vložene pritožbe so v 44 primerih zadevale upravljavce iz javnega sektorja (zlasti ministrstva in organe v njihovi sestavi, šole in javne zdravstvene zavode), 31 pritožb pa se je nanašalo na upravljavce iz zasebnega sektorja (npr. banke, zavarovalnice, operaterje elektronskih komunikacij, trgovska podjetja in druge gospodarske družbe).

V 37 primerih (torej v 49,33 %) so se posamezniki pritožili, ker jim upravljavci na njihove zahteve sploh niso odgovorili oz. so bili v molku, drugi (38) 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 39 primerih, ki so se vodili zaradi molka upravljavca (vključno s postopki, ki so se začeli pred letom 2023), so upravljavci po prejemu poziva Informacijskega pooblaščenca o zahtevah posameznikov odločili na način, da so jim posredovali zahtevane podatke in dokumente ali pa so zahteve zavrnil s formalnim obvestilom z obrazložitvijo (zoper katerega je možna vsebinska pritožba), zaradi česar je Informacijski pooblaščenec postopke ustavil. Pet posameznikov je Informacijskega pooblaščenca po vložitvi pritožbe obvestilo, da pritožbe umikajo, ker so s strani upravljavca prejeli ustrezna pojasnila in podatke, Informacijski pooblaščenec pa je nato postopke s sklepom ustavil.

Leta 2023 je Informacijski pooblaščenec, vključno s postopki, začetimi v letih 2021 in 2022, izdal 22 upravnih odločb v zvezi s seznanitvijo z lastnimi osebnimi podatki in 12 predodločb. V 17 odločbah je ugotovil, da je v trenutku vložitve prijave obstajala kršitev Splošne uredbe oz. ZVOP-2, ter upravljavcem naložil posredovanje določenih osebnih podatkov, s petimi odločbami pa je ugotovil, da kršitev ni bilo. Upravljavec je zoper dve odločitvi Informacijskega pooblaščenca sprožil upravni spor pred Upravnim sodiščem RS, in sicer zoper delni odločbi, izdani v letu 2022 v zadevi zoper istega upravljavca. Informacijski pooblaščenec je s sklepom zavrgel šest 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), ter s sklepom ustavil 19 postopkov. Štirim posameznikom je Informacijski pooblaščenec posredoval predlog za ravnanje, šest pritožb pa je odstopil v reševanje pristojnim organom.

Leta 2023 je Informacijski pooblaščenec obravnaval tudi štiri pritožbe zaradi kršitve pravice do popravka po 16. členu Splošne uredbe, eno pritožbo zaradi kršitve pravice do ugovora po 21. členu Splošne uredbe in 41 pritožb zaradi kršitve pravice do izbrisa po 17. členu Splošne uredbe. Vključno s postopki, začetimi v preteklih letih, je Informacijski pooblaščenec zaradi kršitve pravice do izbrisa izdal šest odločb, in sicer je v treh zadevah ugotovil obstoj kršitve, v dveh je ugotovil, da ni kršitve, v eni zadevi, ki se je vodila skladno z 32. členom ZVOP-1 pa je zahtevo posameznika zavrnil. Zoper dva sklepa o zavrženju in zoper eno zavrnilno odločbo so upravljavci oz. posameznik vložili tožbo pred Upravnim sodiščem RS. V 15 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 devetih pa je bil postopek ustavljen (zaradi umika pritožbe).

Za zahteve posameznikov, ki se nanašajo na področje preprečevanja, odkrivanja, preiskovanja in pregona kaznivih dejanj ter izvrševanja kazenskih sankcij, se uporablja ZVOPOKD. Ta 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 predhodno veljalo po ZVOP-1. Pravice posameznikov v primeru uveljavljanja pravic pri pristojnih organih po ZVOPOKD urejajo 23. do 27. člen ZVOPOKD, postopkovna pravila pa 18. do 22. člen ZVOPOKD.

Informacijski pooblaščenec je v letu 2023 prejel sedem pritožb posameznikov v zvezi s kršitvami pravice do seznanitve z lastnimi osebnimi podatki po ZVOPOKD ter dve pritožbi glede kršitev drugih pravic. V zvezi s pritožbami po ZVOPOKD je Informacijski pooblaščenec izdal šest odločb. V zvezi s pravico dostopa posameznika je Informacijski pooblaščenec izdal štiri odločbe, in sicer tri ugodilne in eno zavrnilno. Pritožbi glede popravka in izbrisa po ZVOPOKD pa je Informacijski pooblaščenec v enem primeru z odločbo ugodil, v enem primeru pa jo je zavrnil.

3.2.7 OSTALI PRITOŽBENI POSTOPKI

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.

Na pravico do seznanitve z zdravstveno dokumentacijo po ZPacP se je nanašalo 26 pritožb (od tega 14 na pravico do seznanitve z lastno zdravstveno dokumentacijo in 12 na pravico do seznanitve z zdravstveno dokumentacijo po pacientovi smrti).

Glede pritožb, ki jih je Informacijski pooblaščenec vodil po ZPacP, je bilo izdanih osem odločb, od tega so bile izdane tri zavrnilne odločbe glede pravice do seznanitve z zdravstveno dokumentacijo po 41. členu ZPacP ter pet odločb glede seznanitve z zdravstveno dokumentacijo po pacientovi smrti (dve odločbi je Informacijski pooblaščenec kot neutemeljeni zavrnil, trem pa je ugodil). Informacijski pooblaščenec je s sklepom ustavil tri postopke zaradi umika. Tri vloge je s sklepom zavrgel, v šestih primerih pa so upravljavci posredovali zahtevane podatke oz. pritožbe posameznikov zavrnil, zaradi česar je Informacijski pooblaščenec postopke ustavil.

Informacijski pooblaščenec po novem na podlagi četrtega odstavka 41. člena ZVOP-2 odloča tudi o pritožbah zoper odločitve upravljavcev v zvezi z zahtevami za posredovanje osebnih podatkov iz uradnih evidenc ali javnih knjig. V letu 2023 je Informacijski pooblaščenec prejel štiri tovrstne pritožbe, pri čemer je v vseh štirih primerih pritožbe zavrgel. V treh primerih ni šlo za zahteve za posredovanje osebnih podatkov iz uradnih evidenc ali javnih knjig, v enem primeru pa za odločanje o pritožbi ni bil pristojen na podlagi tretjega odstavka 55. člena Splošne uredbe, v skladu s katerim nadzorni organi po Splošni uredbi niso pristojni za nadzor dejanj obdelave sodišč, kadar ta delujejo kot sodni organ. Glede vseh zahtev za posredovanje osebnih podatkov tako iz uradnih evidenc ali javnih knjig kot tudi iz drugih zbirk ima posameznik na voljo sodno varstvo.

3.2.8 SODELOVANJE PRI ČEZMEJNIH INŠPEKCIJSKIH NADZORIH

Splošna uredba v 7. poglavju 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 (60. člen Splošne uredbe);
- **vzajemna pomoč** med organi za varstvo osebnih podatkov v državah članicah EU in EGS (61. člen Splošne uredbe);
- **skupno ukrepanje** organov za varstvo osebnih podatkov v državah članicah EU in EGS (62. člen Splošne uredbe).

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

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

V letu 2023 je bil Informacijski pooblaščenec udeležen v skupno 524 postopkih sodelovanja po 60. in 61. členu Splošne uredbe v zvezi z upravljavci, ki izvajajo čezmejno obdelavo osebnih podatkov. V 274 novo pričetih postopkih sodelovanja pri čezmejnem nadzoru po 60. členu Splošne uredbe je Informacijski pooblaščenec nastopal kot zadevni organ (po 56. členu Splošne uredbe), v treh primerih pa je bil v vlogi vodilnega organa. Informacijski pooblaščenec je leta 2023 sodeloval tudi v 247 postopkih zagotavljanja medsebojne pomoči med nadzornimi organi po 61. členu Splošne uredbe.

Sodelovanje Informacijskega pooblaščenca v čezmejnih postopkih nadzora v letu 2023.

2023	524 POSTOPKOV
2022	368 POSTOPKOV
2021	216 POSTOPKOV
2020	200 POSTOPKOV

Temelj za izvedbo čezmejnega sodelovanja po 60. členu Splošne uredbe je opredelitev vodilnega in zadevnih nadzornih organov po 56. členu Splošne uredbe. Informacijski pooblaščenec se opredeli 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 Meta, Google, Amazon, Apple, Twitter, Microsoft, TikTok itd.

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

Na temelju postopkov določitve vodilnega in zadevnih nadzornih organov je Informacijski pooblaščenec v letu 2023 **obravnaval 277 novih zadev** čezmejnega sodelovanja pri nadzoru nad podjetji, ki poslujejo čezmejno, poleg postopkov, začelih pred letom 2023, ki so še v teku. V teh postopkih je pričakovan sprejem odločitve nadzornih organov po 60. členu Splošne uredbe, po načelu »vse na enem mestu«. Vodilni nadzorni organ zelo pogosto predstavlja irski nadzorni organ, pa tudi nadzorni organi Luksemburga, Francije, Nizozemske, Nemčije, Francije in Avstrije.

V 274 čezmejnih postopkih je Informacijski pooblaščenec nastopal v vlogi zadevnega organa. Primeri niso zadevali le storitev priljubljenih spletnih velikanov (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 kršitve glede ustreznega zavarovanja podatkov, med prizadetimi pa so bili tudi uporabniki iz Slovenije, kršitve glede izvajanja pravic posameznikov do dostopa do podatkov in izbrisa podatkov, pretirane zahteve po podatkih za identifikacijo strank, posredovanje podatkov tretjim osebam, obdelavo osebnih podatkov brez ustrezne pravne podlage, neustrezno informiranje o obdelavi osebnih podatkov itd. Informacijski pooblaščenec je prejel 18 prijav oz. pritožb zoper subjekte izven Slovenije (EU in tretje države). Kadar gre v takem primeru za subjekt s sedežem v državi članici EU, Informacijski pooblaščenec pri nadzoru sodeluje z vodilnim organom.

V treh novih čezmejnih primerih po 60. členu Splošne uredbe je šlo za upravljavca s sedežem iz Slovenije, zato je vlogo vodilnega organa prevzel Informacijski pooblaščenec. Primeri, v katerih je bil Informacijski pooblaščenec vodilni nadzorni organ, so v letu 2023 vključevali predvsem primere izvajanja pravic posameznikov s strani upravljavcev spletnih strani, pa tudi obdelavo osebnih podatkov za namen genetskih testiranj.

V letu 2023 je bil v čezmejnih postopkih, v katerih je sodeloval Informacijski pooblaščenec, izdanih 221 osnutkov odločb po 60. členu Splošne uredbe, dva osnutka odločb je izdal Informacijski pooblaščenec kot vodilni nadzorni organ. 291 postopkov je bilo končanih s končno odločbo po 60. členu Splošne uredbe. Na spletni strani Evropskega odbora za varstvo podatkov je dostopen javni register končnih odločb v postopkih čezmejnega sodelovanja po 60. členu: https://edpb.europa.eu/our-work-tools/consistency-findings/register-for-article-60-final-decisions_en.

Postopki »vse na enem mestu« v letu 2023.

277 postopkov čezmejnega sodelovanja pri inšpekcijskem nadzoru nad podjetji, ki poslujejo čezmejno (po načelu »vse na enem mestu«):

- 3 na podlagi prijav, ki jih je glede čezmejnih zavezancev prejel Informacijski pooblaščenec,
- 274 na iniciativo drugih nadzornih organov.

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

Informacijski pooblaščenec je leta 2023 **sodeloval tudi v 247 postopkih** zagotavljanja medsebojne pomoči med nadzornimi organi po 61. členu Splošne uredbe. Prejel je 219 zahtev drugih organov, v 44 primerih je podal mnenje glede izvajanja določb Splošne uredbe. 28 zahtev za sodelovanje je Informacijski pooblaščenec poslal drugim organom v EU. Postopki po 61. členu se razlikujejo glede na njihovo prostovoljno naravo v smislu formalno določenih rokov. Podrobnejši prikaz postopkov sledi v spodnji tabeli.

240 postopkov prostovoljne medsebojne pomoči med nadzornimi organi po 61. členu:

- 22 zahtev Informacijskega pooblaščenca,
- 218 zahtev drugih organov,
- 44 podanih mnenj Informacijskega pooblaščenca.

7 postopkov medsebojne pomoči med nadzornimi organi po 61. členu:

- 6 zahtev Informacijskega pooblaščenca za druge organe,
- 1 zahteva 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 krajevno pristojen nadzorni organ v drugi državi članici. Postopki medsebojne pomoči pa običajno pomenijo zahtevo za izvedbo ukrepov zoper zavezanca, ki izvajajo čezmejno obdelavo osebnih podatkov.

Postopki spora po 65. členu

V letu 2023 sta bili sprejeti dve končni odločitvi, ki sta sledili postopku spora po 65. členu pred EOVP:

- Postopek spora v primeru TikTok Technology Limited z glavno ustanovitvijo na Irskem je zadeval vprašanja obdelave osebnih podatkov registriranih mladoletnih uporabnikov TikToka (starih 13–17 let), in sicer kršitve načela poštenosti zaradi zavajajočih vzorcev, ki jih omrežje uporablja v procesu registracije uporabnikov ter kršitve načela privzetega varstva osebnih podatkov zaradi pomanjkljivega preverjanja starosti uporabnikov. EOVP je analiziral prakse TikToka pri dveh

pojavnih oknih, kijih je omrežje uporabljalo pri registraciji uporabnikov in pri deljenju videoposnetkov. V obeh primerih je oblikovanje pojavnega okna mladoletne uporabnike spodbujalo, da so izbrali zasebnosti manj prijazne nastavitve. Poleg tega bi morale biti posledice različnih izbir v pojavnih oknih posameznikom bolj jasno predstavljane, posebej ker gre za mladoletne uporabnike. Irski nadzorni organ je preverjal tudi skladnost ukrepov za preverjanje starosti uporabnikov z načelom vgrajenega varstva osebnih podatkov iz prvega odstavka 25. člena Splošne uredbe (privacy by design). Mehanizem za preverjanje starosti z vpisovanjem datuma rojstva (t. i. age gate) so tudi uporabniki, mlajši od 13 let, zlahka zaobšli, ukrepi za odstranjevanje uporabnikov pod dopustno starostno mejo pa niso bili uporabljeni dovolj sistematično. Vendar pa je EOVP v svoji odločitvi ugotovil, da zaradi pomanjkanja informacij zlasti glede stopnje tehnološkega razvoja v obdobju, na katerega se nanaša končna odločitev, ne more dokončno odločiti o tem, ali je TikTok obdeloval osebne podatke v skladu s prvim odstavkom 25. člena Splošne uredbe. V končni odločitvi je irski nadzorni organ omrežju TikTok zaradi kršitev naložil globo 345 milijonov evrov.

- Postopek spora v primeru Meta Platforms Ireland Limited z glavno ustanovitvijo na Irskem je zadeval vprašanje zakonitosti prenosa osebnih podatkov uporabnikov omrežja Facebook v Združene države Amerike, v času, ko je bil s strani Sodišča EU razveljavljen t. i. zasebnostni ščit, dogovor, ki je zagotavljal podlago za prenos osebnih podatkov v ZDA. Postopek pred EOVP je zadeval vprašanje, ali mora biti zaradi ugotovljenih kršitev družbi Meta izrečena globa in ukrep za vzpostavitev zakonitega stanja. V končni odločitvi je irski nadzorni organ zavezancu zaradi ugotovljenih kršitev, tj. zaradi prenosa podatkov uporabnikov v ZDA brez pravne podlage, naložil globo 1,2 milijarde evrov, najvišjo izrečeno globo po Splošni uredbi.

Nujna zavezujoča odločitev po 66. členu

EOVP je v letu 2023 sprejel nujno zavezujočo odločitev, s katero je irskemu organu za varstvo podatkov kot vodilnemu nadzornemu organu naložil, naj v dveh tednih sprejme končne ukrepe v zvezi z družbo Meta Ireland Limited (Meta IE) in prepove obdelavo osebnih podatkov za vedenjsko oglaševanje na podlagi pogodbe in zakonitega interesa. Nujna zavezujoča odločitev je bila sprejeta na podlagi zahteve norveškega organa za varstvo podatkov, da se sprejmejo končni ukrepi v tej zadevi, ki bi veljali v celotnem Evropskem gospodarskem prostoru (EGP).

Ključne sodbe Sodišča EU

V letu 2023 je pomembno sodbo v zvezi s sodelovanjem pristojnih organov (v tem primeru organa za varstvo konkurence in organa za varstvo osebnih podatkov) sprejelo tudi Sodišče EU. V sodbi št. C-252/21 je pojasnilo, da lahko organ države članice, pristojen za konkurenco, v okviru preizkusa zlorabe prevladujočega položaja s strani podjetja v smislu 102. člena Pogodbe o delovanju Evropske unije (PDEU) ugotovi, da splošni pogoji uporabe tega podjetja v zvezi z obdelavo osebnih podatkov in njihovo izvajanje niso v skladu s Splošno uredbo, če je ta ugotovitev potrebna za ugotovitev obstoja take zlorabe. Nacionalni organ, pristojen za konkurenco, pa ne sme odstopati od odločitve pristojnega nacionalnega nadzornega organa ali pristojnega vodilnega nadzornega organa oz. se mora v primeru dvoma posvetovati z organi za varstvo osebnih podatkov in zaprositi za njihovo sodelovanje.

3.2.9 PREKRŠKOVNI POSTOPKI

Informacijski pooblaščenec je zaradi suma kršitev določb ZVOP-1 oz. ZVOP-2 v letu 2023 uvedel 111 postopkov o prekršku, od tega 55 zoper pravne osebe javnega sektorja in njihove odgovorne osebe, 29 zoper pravne osebe zasebnega sektorja in njihove odgovorne osebe, 27 pa zoper posameznike. Med slednje 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.

Za ugotovljeni prekršek lahko prekrškovni organ v skladu s 53. členom izreče opozorilo, če je storjeni prekršek neznaten in če pooblaščen uradna oseba oceni, da je glede na pomen dejanja opozorilo zadosten ukrep. 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 je v prekrškovnih postopkih v letu 2023 izdal:

- **77 odločb o prekršku (38 glob in 39 opominov),**
- **60 opozoril.**

Poleg opozoril, ki so bila izrečena v prekrškovnih postopkih, je Informacijski pooblaščenec v okviru postopkov inšpekcijskega nadzora v skladu z načelom ekonomičnosti izrekel tudi 30 opozoril po 53. členu ZP-1. Šest postopkov o prekršku je Informacijski pooblaščenec ustavil.

V zvezi s 77 odločbami, ki so po ZP-1 najprej izdane brez obrazložitve, je bilo na podlagi napovedi zahtev za sodno varstvo izdanih 10 odločb z obrazložitvijo, pri čemer so po prejemu odločbe z obrazložitvijo vsi kršitelji vložili zahtevo za sodno varstvo. Kršitelji so torej zoper izdane odločbe o prekršku vložili deset zahtev za sodno varstvo (zoper 12,98 % odločb). Sedem zahtev za sodno varstvo je bilo vloženih zoper odločbe, s katerimi je Informacijski pooblaščenec kršiteljem izrekel globe, tri zahteve pa za sodno varstvo zoper odločbo, s katero je bil izrečen opomin. Relativno majhen delež vloženih zahtev za sodno varstvo kaže na to, da storilci storjene prekrške priznavajo in se zavedajo svoje odgovornosti.

Spodnja preglednica prikazuje, na katere kršitve so se nanašali uvedeni prekrškovni postopki v letu 2023.

Kršitve varstva osebnih podatkov v letu 2023.

Vrsta kršitve	Število kršitev (v okviru enega postopka je lahko več kršitev)
Nezakonita obdelava osebnih podatkov in kršitev temeljnih načel za obdelavo (8. člen ZVOP-1 ter 5., 6., 7. in 9. člen Splošne uredbe)	42
Neustrezno zavarovanje osebnih podatkov (24. in 25. člen ZVOP-1)	14
Kršitve določb v zvezi z izvajanjem videonadzora (74., 75., 76. in 77. člen ZVOP-1 in 76., 78. in 80. člena ZVOP-2)	16
Neizpolnjevanje ukrepov, izrečenih v postopkih inšpekcijskega nadzora, kršitev drugega odstavka 29. člena ZIN	5
Nezakonit vpogled oz. prepis osebnih podatkov iz osebne izkaznice po četrtem odstavku 4. člena ZOIZk-1)	1

S sprejetjem novega ZVOP-2 je Informacijski pooblaščenec postal pristojen tudi za izrekanje sankcij za kršitve, ki jih predpisuje Splošna uredba o varstvu podatkov. Te kršitve se skladno z določbami ZVOP-2 pravnim osebam, samostojnim podjetnikom posameznikom in posameznikom, ki samostojno opravljajo dejavnost, izrekajo kot globe za prekrške.

Splošna uredba o varstvu podatkov za kršitve te uredbe, ki so jih storile odgovorne osebe, sankcij ne predpisuje, ZVOP-2 pa je predpisal tudi sankcije, ki se za kršitve Splošne uredbe o varstvu podatkov izrekajo odgovornim osebam pravih oseb, samostojnim podjetnikom posameznikom ali posameznikom, ki samostojno opravljajo dejavnost, ter odgovornim osebam v državnih organih ali organih samoupravnih lokalnih skupnosti. Poleg tega je ZVOP-2 za nekatere kršitve Splošne uredbe o varstvu osebnih podatkov predpisal tudi sankcije za posameznike.

Informacijski pooblaščenec poudarja, da je na vodenje prekrškovnih postopkov in izrekanje sankcij za ugotovljene kršitve vplivala zamuda pri sprejetju ZVOP-2. Informacijski pooblaščenec je lahko v letu 2023 vodil postopke o prekršku zaradi kršitev določb Splošne uredbe o varstvu podatkov le za tiste kršitve, ki so bile storjene po 26. 1. 2023, ko je začel veljati ZVOP-2, v primeru prekrškov, ki so bili storjeni pred tem datumom, pa je postopek o prekršku lahko uvedel le v primeru, če je šlo za kršitev tistih členov ZVOP-1, ki so po uveljavitvi Splošne uredbe o varstvu podatkov še veljali, pri čemer je bilo v nekaterih primerih težko presoditi, kateri predpis je za storilca milejši. Postopkov o prekršku, ki jih je v letu 2023 vodil Informacijski pooblaščenec, je bilo zato manj, kot če bi ZVOP-2 veljal že v letu 2022.

Leta 2023 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 2019, 2020 in 2021:

- zahtevi za sodno varstvo je bilo v celoti ugodeno tako, da se je odločba v celoti spremenila tako, da se postopek ustavi – 3,
- zahtevi za sodno varstvo je bilo delno ugodeno tako, da se storilcu izreče nižja globa oz. se izreče enotna sankcija – 2,
- zahteva za sodno varstvo je bila zavrnjena kot neutemeljena – 1.

Informacijski pooblaščenec je prejel tudi tri sodbe, s katerimi je višje sodišče odločalo o pritožbi zoper sodbo o zavrnitvi zahteve za sodno varstvo, in sicer:

- sodba Okrajnega sodišča se je glede sankcije razveljavila po uradni dolžnosti in se je v tem obsegu vrnila sodišču v ponovno odločanje – 2,
- zahteva za sodno varstvo je bila zavrnjena kot neutemeljena, potrdila se je sodba sodišča prve stopnje – 1.

3.2.10 IZBRANI PRIMERI OBDELAVE OSEBNIH PODATKOV

V nadaljevanju so predstavljeni nekateri primeri, v zvezi s katerimi je Informacijski pooblaščenec prejel večje število prijav, pritožb, uradnih obvestil in vprašanj.

Ukrep označevanja torb dostavljavcev ni nujno potreben za nadzor dostavljavcev z vidika spoštovanja cestnoprometnih predpisov

Informacijski pooblaščenec je obravnaval kršitvi s strani dveh upravljavcev, ki se ukvarjata z dostavo hrane in sta sprejela ukrep označevanja torb dostavljavcev z vidnimi identifikacijskimi številkami. Ukrep naj bi bil preventiven; njegov namen naj bi bilo bolj dosledno upoštevanje cestnoprometnih predpisov, omogočal pa naj bi tudi izvajanje nadzora v primeru kršitev posameznih dostavljavcev s strani policije in redarstva. Kot pravno podlago sta upravljavca uveljavljala izvajanje pogodbe o

izvajanju kurirskih storitev (točka (b) prvega odstavka 6. člena Splošne uredbe) ter zakonite interese (točka (f) prvega odstavka 6. člena Splošne uredbe). Upravljavca sta zatrjevala, da je njun zakoniti interes zakonito, pravilno in skrbno izvajanje dostave. Prav tako naj bi bilo v zakonitem interesu upravljavca, da skrbi za lastna sredstva (dostavne torbe) in ima vzpostavljeno njihovo evidenco.

Upravljavca sta trdila, da milejši ukrepi za doseg te ciljev ne obstajajo oz. da so ukrepi, kot so npr. zapore središča mesta, sistemsko spremljanje s pomočjo GPS, obveščanje dostavljavcev, poostren nadzor s strani policije in mestnega redarstva, neučinkoviti oz. neustrezni.

Informacijski pooblaščenec je poudaril, da gre pri tem za dve različni dejanji obdelave, ki sta ju v zvezi z identifikacijskimi številkami dostavljavcev izvajala upravljavca, in sicer beleženje identifikacijskih številk dostavljavcev v zbirkah upravljavca in posredovanje osebnih podatkov policiji ter mestnemu redarstvu. Pravno podlago bi tako morala upravljavca zagotoviti za obe dejanji obdelave.

Upravljavca nista dokazala, da bi bila obdelava objektivno potrebna za izvajanje pogodbe. Ni sporno, da so dostavljavci odgovorni tudi za spoštovanje Zakona o varnosti v cestnem prometu, vendar se pogodba o izvajanju kurirskih storitev sklepa zaradi dostave prehrabnih in drugih izdelkov in ne z namenom spoštovanja cestnoprometnih predpisov – ta obveznost namreč izhaja neposredno iz zakonodaje. Informacijski pooblaščenec je odločil, da upravljavca nista dokazala, da bi bila obdelava osebnih podatkov na način označevanja torb dostavljavcev z identifikacijskimi številkami nujno in neobhodno potrebna za nadzor dostavljavcev z vidika spoštovanja cestnoprometnih predpisov. Upravljavca namreč nista navedla razlogov za neustreznost oz. neučinkovitost nadzora s strani policije, ki ima vsa pooblastila za ustavitev dostavljavca in identifikacijo morebitnih kršitev ali pa povečanje števila redarjev v mestnem središču.

Kar zadeva zakoniti interes, je Informacijski pooblaščenec poudaril, da ta sicer obstaja, vendar upravljavca nista izkazala pogoja potrebnosti za uresničitev zakonitega interesa, ki se presoja v povezavi s predvidenim namenom obdelave, prav tako nista preverila oz. uporabila drugih ukrepov (kot je pojasnjeno zgoraj). Informacijski pooblaščenec je tako zaključil, da upravljavca ne zagotavljata pravne podlage za obdelavo identifikacijskih številk, ki so za namen identifikacije dostavljavcev nameščene na zunanji, vidni strani torb za dostavo, ter je odredil ukrep prenehanja obdelave identifikacijskih številk dostavljavcev, nameščenih na torbah za dostavo, in sicer tako, da upravljavca identifikacijske številke odstranita z zunanjih, vidnih strani vseh torb dostavljavcev.

Z videonadzorom je načeloma prepovedano snemati delovna mesta, kjer delavec po navadi dela

Informacijski pooblaščenec je presojal zakonitost videonadzora nad delovnimi prostori v lokalu. Upravljavec je videonadzor izvajal s sedmimi kamerami. Ena kamera je snemala pripravo hrane, posnetki pa so se predvajali v živo preko spletne strani lokala. Prenašanje žive slike in objavljanje le-te na spletu je upravljavec prekinil že tekom postopka. Ostale delujoče kamere so snemale območje vstopa, blagajne in mize za goste.

Upravljavec je izkazal pravno podlago za območje vstopa (na podlagi 77. člena ZVOP-2, ki ureja videonadzor dostopa v uradne službene oz. poslovne prostore) ter blagajne. Ni pa izkazal pravne podlage za snemanje gostov lokala na podlagi zakonitih interesov in delovnih prostorov na podlagi 78. člena ZVOP-2, saj snemanje ni nujno potrebno za varnost ljudi in premoženja ali varovanja poslovne skrivnosti, namen varovanja pa se doseže že s snemanjem vstopa, alarmnim sistemom in neposrednim nadzorom s strani upravljavca. 78. člen ZVOP-2 namreč določa, da je prepovedano z videonadzorom snemati delovna mesta, kjer delavec po navadi dela, razen če je to nujno v skladu s prvim odstavkom 78. člena ZVOP-2. Neposredno spremljanje dogajanja pred kamerami je lahko dopustno le, če ga izvaja izrecno pooblaščen osebje upravljavca. Informacijski pooblaščenec je ugotovil, da neposredno spremljanje dogajanja pred kamerami ni bilo izvedeno

s strani pooblaščenega osebjja upravljavca, dostop do posnetkov sta namreč imela prokuristka in del vodstva. Prokuristka tudi ni mogla izkazati sledljivosti vpogledov v posnetke, prav tako je kot nadrejena z vpogledom v živo sliko na nedopusten način spremljala delo zaposlenih.

Upravljavec je navajal, da gre za poslovni model upravljavca, ki gostom omogoča, da spremljajo pripravo hrane, ter poudaril, da so bili zaposleni s tem seznanjeni. Upravljavec za takšno obdelavo osebnih podatkov zaposlenih ni izkazal pravne podlage skladno s 6. členom Splošne uredbe. Pisna izjava oz. morebitno soglasje zaposlenih kot šibkejše stranke pogodbenega razmerja ne more predstavljati zakonite pravne podlage za tovrstno obdelavo osebnih podatkov. Prav tako upravljavec ni izkazal zakonitega interesa, saj pravice zaposlenih prevladajo nad opisanim tržnim modelom upravljavca, ki je namenjen zgolj ekonomskim interesom zavezanca in ne prestane t. i. testa sorazmernosti. Cilj varne in zdrave priprave hrane bi lahko upravljavec zagotovil z drugim, manj invazivnim ukrepom v pričakovano zasebnost zaposlenih na delovnem mestu. Informacijski pooblaščenec je zavezanca med drugim pozval k prenehanju prenosa žive slike na telefonu zaposlene, k prenehanju snemanja delovnih prostorov priprave hrane in miz za goste ter k ustreznemu zavarovanju dostopa do snemalnika. Ker je upravljavec izpolnil vse inšpekcijske ukrepe, je Informacijski pooblaščenec inšpekcijski postopek ustavil, ugotovljeno preteklo kršitev pa obravnaval v prekrškovnem postopku.

V registru dejanskih lastnikov se lahko objavi le država stalnega in začasnega prebivališča posameznikov, ne pa tudi naslov stalnega in začasnega prebivališča

Informacijski pooblaščenec je obravnaval prijavo glede javne objave podatkov o naslovu stalnega in začasnega prebivališča zastopnice zavoda, ki se vodi v registru dejanskih lastnikov. Odločal je tudi o pritožbi posameznika o izbrisu njegovih podatkov.

V zadevi je bilo sporno, ali ima upravljavec pravno podlago za objavo naslova stalnega in začasnega prebivališča prijavitelja in ali je posledično utemeljeno zavrnil njegovo zahtevo po izbrisu. Upravljavec je trdil, da je dolžan podatke objaviti na podlagi Zakona o preprečevanju pranja denarja in financiranja terorizma (ZPPDFT-2), zaradi česar jih na podlagi tretjega odstavka 17. člena Splošne uredbe ne more izbrisati. Informacijski pooblaščenec je ugotovil, da upravljavec objavo utemeljuje na določbi Pravilnika o vzpostavitvi, vzdrževanju in upravljanju Registra dejanskih lastnikov, neposredno iz zakona pa ne izhaja obveznost objave stalnega in začasnega prebivališča, temveč le države stalnega in začasnega prebivališča. Poudaril je tudi, da ZPPDFT-2 izpolnjuje zahteve, določene v ZVOP-2 v zvezi z zakonitostjo obdelave osebnih podatkov, torej da je v zakonu določena obdelava osebnih podatkov, vrste osebnih podatkov, kategorije posameznikov, namen obdelave osebnih podatkov in rok hrambe. Uporaba pravilnika pa ne more priti v poštev v delu, ki izrecno nasprotuje zakonski ureditvi. V preteklosti je sicer obstajala pravna podlaga za objavo naslova začasnega in stalnega prebivališča z ZPPDFT-1, ki pa je z dnem 11. 7. 2020 odpadla, ko je stopil v veljavo Zakon o spremembah in dopolnitvah Zakona o preprečevanju pranja denarja in financiranja terorizma (ZPPDFT-1B). Upravljavec ima tako pravno podlago le za objavo države stalnega in začasnega prebivališča. S tem je upravljavec kršil 6. člen Splošne uredbe in posledično v nasprotju s 17. členom Splošne uredbe odločil o zahtevi o izbrisu osebnih podatkov posameznika, saj bi moral v odsotnosti pravne podlage podatek umakniti s spletne strani. Informacijski pooblaščenec je upravljavcu odredil, da na svoji spletni strani onemogoči dostop do podatka o naslovu stalnega in začasnega prebivališča prijavitelja.

Upravljavec mora na zahtevo posameznika o izbrisu njegovih osebnih podatkov obvestiti tudi druge upravljivce, da izbrišejo povezave do njegovih osebnih podatkov oz. njihove kopije

Prijaviteljica je od upravljavca (policije) zahtevala izbris svojih osebnih podatkov o pogrešani osebi iz spletnih medijev. Upravljavec njeni zahtevi ni ugodil z utemeljitvijo, da ni pristojen za vsebino in izbris vsebine s spletnih portalov. Prijaviteljica se je zoper odgovor upravljavca pritožila in zatrjevala,

da bi moral upravljavec, ki je z dovoljenjem njenega moža objavil njeno fotografijo, poskrbeti tudi za njeno odstranitev s spletnih mest.

Drugi odstavek 17. člena Splošne uredbe določa, da mora upravljavec, kadar objavi osebne podatke in je v skladu s prvim odstavkom 17. člena Splošne uredbe osebne podatke obvezan izbrisati, ob upoštevanju razpoložljive tehnologije in stroškov izvajanja sprejeti razumne ukrepe, vključno s tehničnimi, da upravljavce, ki obdelujejo osebne podatke, obvesti, da posameznik, na katerega se osebni podatki nanašajo, od njih zahteva, naj izbrišejo morebitne povezave do teh osebnih podatkov ali njihove kopije. O dejstvu, da je bila pogrešana oseba najdena, je upravljavec sicer obvestil tudi druge upravljavce, vendar s tem navedene obveznosti ni izpolnil, saj bi moral po prejemu zahteve za izbris sprejeti razumne ukrepe, da tudi upravljavce, ki jim je osebne podatke posredoval, obvesti, da prijaviteljica od njih zahteva izbris svojih osebnih podatkov.

Informacijski pooblaščenec je v svoji odločitvi poudaril, da je smisel določbe drugega odstavka 17. člena Splošne uredbe zamejiti razširjanje objavljenih osebnih podatkov z vložitvijo zahteve pri viru, če so izpolnjeni pogoji za izbris, in sicer z namenom, da bi posameznik lažje in bolj učinkovito zaščitil svojo zasebnost. Dodatno je poudaril, da lahko informacije o pogrešani osebi in okoliščine, povezane z njenim izginotjem znatno zaznamujejo njeno javno podobo in posegajo v njeno dostojanstvo v prihodnosti. Zato je razumljivo, da oseba, ki je bila pogrešana, upravičeno pričakuje zasebnost glede dejstva svojega izginotja. Namen obveščanja policije o izginotju je hitrejše in čim širše iskanje, kar pa ni več relevantno, ko je oseba najdena. Policija tako osebne podatke izbriše s svoje spletne strani, novice o tem pa lahko ostanejo na spletnih portalih še dolgo po tem, ko so osebe najdene. Ob tem je Informacijski pooblaščenec še poudaril, da obvestilo policije o pogrešanih osebah nima narave obvestila za javnost s ciljem zagotavljanja transparentnega delovanja policije v smislu ZDIJZ.

Upravljavec je tekom postopka kršitev odpravil, zato Informacijski pooblaščenec ni odredil ukrepov za odpravo posledic.

Spremljanje gibanja posameznikov po prostorih in na zunanjih površinah ni dopusten namen za izvajanje videonadzora

Informacijski pooblaščenec je obravnaval kršitve v zvezi z videonadzorom nad kopališči in drugimi poslovnimi prostori. Upravljavec (terme) je izvajal videonadzor s skupno 165 kamerami tako, da je poleg vhodov in izhodov iz prostorov nadziral celotne prostore in zunanje površine, kar mu je omogočalo spremljanje gibanja gostov in zaposlenih.

Upravljavec je navajal, da je videonadzor uvedel izključno z namenom zagotavljanja varovanja premoženja in varnosti ljudi, varovanja premičnin in opreme, varovanja službenih prostorov ter nadzora vstopov v objekt, in sicer skladno z določbami 75. člena ZVOP-1 (ki ureja videonadzor dostopa v uradne službene oz. poslovne prostore) in 77. člena ZVOP-1 (ki ureja videonadzor delovnih prostorov).

Prav tako je izvajal videonadzor na določenih delih, ki so enkrat tedensko v omejenem času opredeljeni kot nudistični, in sicer skladno z navedenimi nameni, sprejetim pravilnikom in kopališkim redom. Kamere so bile na tem delu nameščene zaradi zahtev varstva pred utopitvami na kopališčih, saj naj bi šlo za specifično arhitekturo, ki ima precej okroglin in mrtvih kotov in naj bi bilo zato iz razglednih stolpov reševalcev brez videonadzora nemogoče izvajati kvaliteten nadzor. Snemal se je tudi del ob vodnem telesu (ležalniki, vstop v vodno telo) za potrebe nadzora in hitrejšega ukrepanja, če bi prišlo do zdrsov, slabosti, vročinskega šoka (npr. po koncu savnanja), kar naj bi zagotovilo hitrejše ukrepanje reševalcev. Upravljavec je na več mestih zagotavljal tudi vpogled v posnetke oz. v živo sliko.

Upravljavec je tako vzpostavljeni videonadzor utemeljeval tudi z obstojem zakonitih interesov (točka (f) prvega odstavka 6. člena Splošne uredbe), in sicer zagotavljanje varnosti pred utopitvami, hitrega reagiranja v primeru nezgod, odpravljanje nevarnosti, zagotavljanje varnosti obiskovalcev in njihovega premoženja. Navajal je, da mu pravilnik o ukrepih za varstvo pred utopitvami na kopališčih nalaga ne samo varstvo pred utopitvami, temveč tudi preprečevanje širokega nabora drugih nevarnosti (npr. neprekinjeno opazovanje kopalnih površin in bazenske ploščadi, vzdrževanje reda in odpravljanje razlogov, ki bi lahko privedli do nevarnosti). Glede na to, da zadošča potrebam pravilnika glede števila mest opazovanja in števila reševalcev, je menil, da s tem upošteva vse milejše ukrepe za doseganje varnosti, kar utemeljuje dejstvo, da z izvajanjem videonadzora zasleduje zakoniti interes.

Informacijski pooblaščenec je ugotovil, da upravljavec s 110 kamerami nadzira celotne prostore in zunanje površine, kar mu omogoča spremljanje gibanja gostov in zaposlenih. Navedene kamere prikazujejo celotne prostore ali dele prostorov, kjer se ne nahaja premoženje, ki bi ga lahko upravljavec kakorkoli varoval (glede na določbe 78. člena ZVOP-2 oz. v zvezi z zakonitimi interesi), ter jih uporabljajo gostje in zaposleni. Spremljanje gibanja posameznikov po prostorih pa ni dopusten namen, zaradi katerega bi se lahko vršil videonadzor nad poslovnimi prostori ter zunanjimi površinami. Zgolj navedbe o tem, da se pokrivajo tudi prostori za počitek, hodniki itd., kjer bi se posameznik lahko onesvestil, ne vzdrži pravne podlage za izvajanje videonadzora. Varnost ljudi in premoženja bi upravljavec lahko zagotovil tudi tako, da bi kamere pokrivale zgolj področja konkretnega premoženja (npr. blagajno, delovno opremo itd.), ki ga ni mogoče varovati z milejšimi sredstvi, ali dele kopališč in bazenskih ploščadi, skladno z določbami pravilnika.

V zvezi z zakonitim interesom je Informacijski pooblaščenec poudaril, da ni izkazan prvi pogoj (obstoj samega zakonitega interesa), kakor tudi ne kriterij nujnosti in tehtanja interesov, saj vzpostavitev videonadzora ni najustreznejši, najprimernejši in najbolj potreben ukrep za doseganje namena, saj bi se lahko ta na nekaterih delih dosegel z milejšimi ukrepi. Dodatno je poudaril, da je razumno pričakovanje posameznika, da nad njim ni videonadzora, kadar se nahaja v javnih prostorih, še posebej če se ti uporabljajo za regeneracijo oz. prostočasne aktivnosti v prostorih, kjer se posamezniki zbirajo in komunicirajo, npr. v lokalih, parkih itd. Na teh javnih površinah bodo tako legitimni interesi posameznikov prevladali nad zakonitimi interesi upravljavca.

Glede spremljanja žive slike je Informacijski pooblaščenec poudaril, da bi moralo biti slednje namenjeno zgolj varovanju premoženja in varnosti ljudi, ki ga je po naravi stvari mogoče doseči le z neprekinjenim snemanjem žive slike s strani za to pooblaščen osebe (npr. varnostnika, reševalca, ne pa npr. vodje, receptorja itd.), ki bo lahko ustrezno ukrepal in preprečil nastanek večje škode oz. poškodbe gosta. Informacijski pooblaščenec je ugotovil, da je videonadzor nezakonit v delu, kjer za njegovo izvajanje ni podana pravna podlaga, in z odločbo odredil prenehanje izvajanja videonadzora s skupno 110 kamerami.

Upravljavec mora izkazati, da je izvajanje GPS sledenja za varstvo zakonitega interesa primeren in potreben ukrep

Upravljavec je izvajal GPS sledenje petih službenih vozil, ki si jih njegovi zaposleni uporabljali za opravljanje svojih delovnih nalog. Gre za osebna vozila, kombije in tovorna vozila, ki se uporabljajo za dostavo izdelkov, izvajanje montaž in servisov, naloge komercialistov in druge delovne naloge. Službena vozila so uporabljali komercialisti, monterji, serviserji, dostavljavci in tudi člani uprave. Zaposlenim službenih vozil ni bilo dovoljeno uporabiti za zasebno uporabo. GPS sledenje se je izvajalo s pomočjo oddajnika v vozilu in posebne aplikacije, v kateri je sistem kontinuirano beležil opravljeno pot vozila in te podatke tudi shranjeval. GPS sledenje je upravljavec izvajal na način, da je v celoti sledil vsem vožnjam službenih vozil, ne glede na to, kdo od zaposlenih je službeno vozilo uporabljal; uporabnik GPS sledenja ni mogel izklopiti. Upravljavec je zaposlene o izvajanju GPS sledenja obvestil, sledenje službenih vozil pa uredil s pravilnikoma.

Informacijski pooblaščenec je poudaril, da gre pri izvajanju GPS sledenja vozil nedvomno za obdelavo osebnih podatkov posameznikov, ki ta vozila uporabljajo, saj je posameznik, ki je vozilo upravljal, vedno določen ali vsaj določljiv. Upravljavec lahko namreč v vsakem primeru, na podlagi podatkov, s katerimi razpolaga, ugotovi, kdo od zaposlenih v določenem času uporablja ali je uporabljal službeno vozilo, kar pomeni, da je posameznik, na katerega se lokacijski podatki nanašajo, nedvomno določljiv. Z izvajanjem GPS sledenja je pri upravljavcu nastajala posebna zbirka osebnih podatkov, ki je vsebovala veliko količino lokacijskih podatkov zaposlenih posameznikov o njihovi mikrolokaciji v določenem trenutku.

Upravljavec je zatrjeval, da pravno podlago za obdelavo osebnih podatkov zaposlenih predstavljajo zakoniti interesi po točki (f) prvega odstavka 6. člena Splošne uredbe, in sicer varstvo njegovega premoženja, varnost delavcev, organizacija in racionalizacija delovnih procesov prevozov.

Glede varstva svojega premoženja je navedel, da bi naj z izvajanjem GPS sledenjem varoval službena vozila ter tudi opremo in dokumente, ki se v vozilih nahajajo. Informacijski pooblaščenec je sicer pritrdil, da varstvo premoženja vsekakor predstavlja zakoniti interes, vendar upravljavec v konkretnem primeru ni izkazal, da je izvajanje GPS sledenja za varstvo tega interesa primeren in potreben ukrep. Namreč, upravljavec GPS sledenje izvaja tedaj, ko zaposleni upravlja vozilo ter sta tako oprema in premoženje v vozilu pod neposrednim in stalnim nadzorom zaposlenega, zato sta v tem času tako vozilo kot oprema najmanj ogrožena pred morebitno odtujitvijo. Takšno izvajanje GPS sledenja upravljavcu tudi ne bi koristilo pri morebitnem vplomu v vozilo in odtujitvi opreme in dokumentov. GPS oddajnik bi lahko bil primeren ukrep, ki pomaga izslediti vozilo v primeru njegove odtujitve, če bi npr. lahko zaposleni GPS napravo vklopil, ko vozilo parkira, na lokaciji, ko bi lahko bilo ogroženo, ter bi ga ob vrnitvi v vozilo znova izklopil.

Kot zakoniti interes je upravljavec navedel tudi varnost delavcev, saj bi se lahko v primeru prometne nesreče ugotovilo, kje se vozilo nahaja. Informacijski pooblaščenec je poudaril, da bi bilo malo verjetno, da bi bilo ob nesreči treba vozilo locirati s pomočjo sistema GPS, saj je kraj nesreče običajno znan. Če bi se nesreča zgodila na odročnejšem kraju, bi lahko obvestilo o nesreči in lokaciji posredoval tudi voznik vozila preko mobilnega telefona. Upravljavec je obstoj zakonitega interesa sicer dokazal, vendar bi to lahko pripomoglo k varovanju zaposlenih zgolj v izjemnih, hipotetičnih primerih, verjetnost nastanka katerih pa je minimalna, poleg tega bi lahko za doseg tega namena uporabil tudi druga, v informacijsko zasebnost manj posegajoča sredstva. Lahko bi sicer ob upoštevanju najmanjšega obsega podatkov izvajal GPS sledenje v ta namen tudi na način, da bi zaposleni ob nesreči vklopil GPS sledenje in zavezancu poslal podatek o svoji lokaciji.

Glede zakonitega interesa organizacije in racionalizacije delovnih procesov prevozov se je upravljavec pri utemeljevanju osredotočil na opravljanje določenih delovnih nalog s službenimi vozili (npr. namen prevoza blaga in izdelkov ter potrebe montaže in servisov), za opravljanje drugih delovnih nalog pa uporabe GPS sistema ni utemeljeval (npr. vožnje članov uprave). Informacijski pooblaščenec je potrdil, da organizacija in racionalizacija oz. optimizacija delovnih procesov predstavlja zakoniti interes zavezanca, vendar ta v postopku ni izkazal, da bi bilo glede na okoliščine za doseganje tega zakonitega interesa res potrebno sistematično in kontinuirano sledenje vseh poti službenih vozil in da te racionalizacije ni mogoče doseči z drugimi sredstvi, ki bi v manjši meri posegale v informacijsko zasebnost zaposlenih. Namreč, zaposleni svoje delovne naloge opravljajo z relativno majhnim številom službenih vozil, pri čemer so službene poti vnaprej načrtovane, kar pomeni, da je upravljavec seznanjen s tem, katere poti njegovi zaposleni na določen dan opravljajo. Upravljavec tudi ni izkazal, da bi nepredvidene in v času izvajanja prevoza nastale delovne naloge predstavljale takšen delež, da jih zavezanec ne bi mogel usklajevati na druge načine (npr. s komunikacijo z voznikom, poslanim SMS-sporočilom itd.). Obveščeni strank bi lahko upravljavec zagotovil z drugimi ukrepi, ki manj posegajo v informacijsko zasebnost zaposlenih, npr. z obveščanjem ob začetku poti in v primeru zamude, saj lahko zaposleni na terenu, za razliko od direktorja, stranki nudi bolj točno in ažurno informacijo o času prihoda k njej, ki se je iz GPS sistema ne da razbrati.

Informacijski pooblaščenec je zaključil, da upravljavec za obdelavo osebnih podatkov ni zagotovil ustrezne pravne podlage ter da obdelava lokacijskih podatkov ni v skladu z načelom najmanjšega obsega podatkov. Obstoj zakonitega interesa je namreč zgolj prvi predpogoj za obdelavo osebnih podatkov na podlagi te točke, poleg tega pa mora biti obdelava osebnih podatkov primerna in potrebna za doseganje tega zakonitega interesa, dodatno pa nad zakonitim interesom ne smejo prevladati interesi in temeljne pravice in svoboščine posameznika. Določenih namenov tako z izvajanjem GPS sledenja sploh ni mogoče doseči, medtem ko bi glede nekaterih namenov lahko upravljavec te naprave uporabljal, če bi zavezanec lokacijske podatke zbiral in obdeloval skladno z načelom najmanjšega obsega podatkov, zgolj v omejem obsegu in selektivno (npr. lahko bi zbiral podatke o lokaciji vozil, ki so parkirana na način, da zaposleni, ki vozilo uporablja, ob parkiranju GPS vklopi in ga ob vrnitvi v vozilo izklopi).

Privolitev posameznika za obdelavo posebnih vrst osebnih podatkov mora biti prostovoljna, konkretna, informirana, nedvoumna in izrecna

Upravljavec je s storitvijo platforme Gospodar zdravja uporabnikom zagotovil infrastrukturo, ki omogoča varno shranjevanje, urejanje in upravljanje z njihovimi zdravstvenimi podatki ter varno elektronsko komunikacijo in izmenjavo zdravstvenih podatkov med posameznikom in njegovim izbranim zdravstvenim izvajalcem. V okviru spletne platforme se posamezniki registrirajo, nato pa v t. i. osebni zdravstveni zapisu nalagajo, hranijo, urejajo in shranjujejo različne podatke o svojem zdravstvenem stanju (npr. dnevnik jemanja zdravil, višino krvnega sladkorja in krvnega tlaka, podatek o telesni teži, podatke o alergijah, diagnozah ter različno zdravstveno dokumentacijo, npr. izvide).

Upravljavec je navedel, da je pravna podlaga za obdelavo osebnih podatkov (shranjevanje, urejanje in upravljanje) osebna privolitev. Posameznik je na spletni strani podal privolitev na način, da je po vnosu zahtevanih registracijskih podatkov s kljukico označil okence, ob katerem se nahaja besedilo »Strinjam se s splošnimi pogoji uporabe«. Poleg tega besedila se je nahajal še dokument o splošnih pogojih in povezava na informacije o varstvu osebnih podatkov.

Zdravstvena dokumentacija posameznika ter vsi podatki, povezani z njegovim zdravjem, sodijo med t. i. posebne vrste osebnih podatkov. Njihova obdelava je načeloma prepovedana, razen če velja ena od izjem, ki so navedene v drugem odstavku 9. člena Splošne uredbe, npr. če je posameznik, na katerega se osebni podatki nanašajo, dal izrecno privolitev v obdelavo navedenih osebnih podatkov za enega ali več določenih namenov, razen kadar pravo Unije ali pravo države članice določa, da posameznik, na katerega se osebni podatki nanašajo, ne sme odstopiti od prepovedi obdelave iz prvega odstavka.

Privolitev posameznika, na katerega se osebni podatki nanašajo, pomeni vsako prostovoljno, konkretno, informirano in nedvoumno ravnanje v obliki izjave volje ali jasnega pritrdilnega ravnanja, iz katerega je mogoče sklepati na želje posameznika. Pogoji za zakonito privolitev so navedeni v 7. členu Splošne uredbe. Tako ne zadostuje zgolj, da privolitev kot pravna podlaga obstaja, temveč mora biti tudi ustrezna – prostovoljna, konkretna, informirana in nedvoumna ter v primeru zdravstvenih osebnih podatkov tudi izrecna.

Informacijski pooblaščenec je v konkretnem primeru ugotovil, da konkretna privolitev za obdelavo zdravstvenih podatkov na način, kot jo je opredelil zavezanec (torej z označitvijo okenca na spletni strani zavezanca, ob katerem se nahaja besedilo »Strinjam se s splošnimi pogoji uporabe«) ni v skladu s Splošno uredbo, saj ne izpolnjuje pogojev prostovoljnosti, konkretnosti, nedoumnosti in izrecnosti. Izjava je namreč neprostovoljna, saj je privolitev dana v povezavi s strinjanjem s splošnimi pogoji uporabe, o katerih se posameznik ne more pogajati. Obdelava zdravstvenih osebnih podatkov ni nujna za golo nudenje storitev zavezanca (nudenje in zagotavljanje opisane spletne rešitve). Privolitev bi morala biti tudi konkretna, nanašati bi se morala na enega ali več

namenov in bi morala biti jasno in nedvoumno ločena od morebitne privolitve za katerikoli drug namen obdelave zdravstvenih podatkov posameznika. Privolitev bi morala biti tudi nedvoumna, kar pomeni, da privolitve ni mogoče pridobiti z istim dejanjem, kot je potrebno za sprejetje pogodbe ali strinjanje s splošnimi pogoji storitve. Podana privolitev bi morala biti tudi izrecna, kar se nanaša na način, na katerega posameznika poda privolitev. Posameznik mora torej dati izrecno izjavo o privolitvi (npr. v pisni izjavi).

Prav tako je Informacijski pooblaščenec ugotovil nekatere neskladnosti glede podanih informacij o obdelavi osebnih podatkov po 13. členu Splošne uredbe. Posameznik mora biti namreč jasno in pravočasno informiran o tem, kateri njegovi osebni podatki se bodo obdelovali, za katere namene, kdo jih bo obdeloval, komu in pod kakšnimi pogoji bodo posredovani in kakšni so roki hrambe. Tako je npr. ugotovil, da iz besedila Splošnih pogojev za paciente ni jasno in nedvoumno, katere funkcionalnosti vsebuje t. i. Osnovni uporabniški paket (samo varno e-komunikacijo ali tudi varno hrambo podatkov o zdravstvenem stanju).

Informacijski pooblaščenec je tako upravljavcu z odločbo naložil, da odpravi nepravilnosti v zvezi z izvajanjem določb Splošne uredbe, in sicer da mora biti privolitev skladna z zahtevami iz Splošne uredbe. Upravljavcu je naložil tudi, da vsebino dokumentov splošnih pogojev za uporabo programske opreme Gospodar zdravja za uporabnike ter Informacije o obdelavi osebnih podatkov popravi oz. dopolni na način, da bodo informacije o obdelavi osebnih podatkov navedene v jedrnatih, preglednih in razumljivi obliki in da bodo iz njih v takšni obliki razvidne vse informacije o obdelavi osebnih podatkov iz prvega in drugega odstavka 13. člena Splošne uredbe.

Upravljavec mora posamezniku podati informacijo o zaposlenih, ki obdelujejo njegove osebne podatke, če je to potrebno za varstvo njegovih pravic

Prosilec je na podlagi 15. člena Splošne uredbe od upravljavca zahteval, da mu posreduje informacijo o tem, kdo je obdeloval njegove osebne podatke v določenih dokumentih, in sicer iz lastnosti Wordovih dokumentov. Upravljavec je zahtevo zavrnil, saj je presodil, da pravica do imen konkretnih zaposlenih pri upravljavcu, ki so pripravljali dokumente, ne sodi pod domet pravice iz točke (c) prvega odstavka 15. člena Splošne pravice, ki opredeljuje pravico do informacije o uporabnikih osebnih podatkov. Prosilec je v pritožbi vztrajal pri tem, da ima pravico do informacij iz zavihka Wordovega dokumenta lastnosti »zgodovina različica«.

Informacijski pooblaščenec je ugotovil kršitev 15. člena Splošne uredbe, saj je bila odločitev upravljavca neobrazložena, upravljavcu pa je kot ukrep za odpravo nepravilnosti naložil ponovno odločanje o zahtevi prosilca na podlagi 12. in 15. člena Splošne uredbe. Informacijski pooblaščenec je v odločitvi poudaril, da iz sodbe Sodišča EU št. C 579/21 z dne 22. 6. 2023 izhaja, da posameznik načeloma res ni upravičen do informacij o notranjih uporabnikih, če so ti izvedli dejanja obdelave pod vodstvom upravljavca in v skladu z njegovimi navodili. Vendar iz omenjene sodbe izhaja tudi, da je pri tem pomembno ugotoviti, ali so zaposleni pri upravljavcu dejansko delovali v njegovem imenu in za njegov račun ali pa so morda presegli navodila svojega delodajalca glede obdelave osebnih podatkov. V konkretnem primeru je bilo to toliko bolj pomembno, ker je prosilec zatrjeval morebitno nezakonnost pri obdelavi njegovih osebnih podatkov. Informacijski pooblaščenec je poudaril, da kategorična in pavšalna zavrnitev pravice do informacije o uporabnikih osebnih podatkov ne zadosti standardu obrazloženosti. Neobrazložena odločitev posamezniku onemogoča učinkovito pravno sredstvo. Prosilec je zahteval tudi informacijo o času obdelave njegovih osebnih podatkov, zavrnitev tega dela prosilčeve zahteve pa upravljavec sploh ni obrazložil, zato je Informacijski pooblaščenec upravljavcu naložil, naj to stori v novem postopku.

Upravljalavec ne sme zavrniti dostopa do osebnih podatkov posameznika zaradi povezanosti podatkov s sodnim postopkom v teku

Prosilka je od upravljavca zahtevala dostop do svojih osebnih podatkov in podatkov svojega mladoletnega otroka ter določene informacije o obdelavi njenih osebnih podatkov. Dokumentacija je izhajala iz postopka psihoterapevtske obravnave pri izvajalcu takšne dejavnosti in bila povezana s sodnim postopkom v teku. Upravljalavec o zahtevi prosilke ni odločil v roku iz 12. člena Splošne uredbe, zaradi njegovega neustreznega sodelovanja v postopku pri Informacijskem pooblaščenca in posledične dolgotrajnosti postopka pa je Informacijski pooblaščenec odločil, da o zahtevi prosilke odloči v postopku s polno jurisdikcijo (tj. da sam odloči o zahtevi prosilke).

Informacijski pooblaščenec je v postopku ugotovil, da določeni dokumenti, s katerimi razpolaga upravljalavec, pri njem obstajajo, nekatere osebne podatke pa je uničil, ker je namen njihove hrambe potekel (v primeru posnetkov terapevtskih srečanj), ali jih ni hranil, ker jih ni bil dolžan hraniti (na primer po pravilih o hrambi zdravstvene dokumentacije) oz. je menil, da jih ne sme hraniti. V postopku je Informacijski pooblaščenec zavrnil argumentacijo upravljavca, da gre za sodni postopek v teku in je le sodišče tisto, ki lahko odloča o vpogledu v dokumentacijo. Informacijski pooblaščenec je namreč ugotovil, da upravljalavec ni deloval kot podaljšana roka sodišča, kot sodniški pomočnik ali v kakršnikoli drugi kapaciteti, ki bi bila sorodna varovanemu položaju sodnih izvedencev (prvi in tretji odstavek 57. člena ZVOP-2). Upravljalavec je v postopku zatrjeval tudi, da bi bilo zaradi varstva koristi mladoletne osebe treba postaviti izvedenca ustrezne stroke, vendar je Informacijski pooblaščenec ugotovil, da to v konkretnem primeru ni potrebno. Prav tako pa niso bili podani pogoji iz 20. člena ZVOP-2, po katerem se lahko zahteva zavrne, če obstajajo konkretne in objektivne okoliščine, zaradi katerih bi bilo utemeljeno sklepati, da bi nastala škoda mladoletnemu otroku z razkritjem njenih osebnih podatkov enemu od staršev. Informacijski pooblaščenec je utemeljitev med drugim argumentiral z uporabo določb Družinskega zakonika ter vsemi dokazi, izvedenimi v okviru postopka.

Informacijski pooblaščenec je nato odločil o zahtevi prosilke, in sicer je upravljavcu naložil posredovanje tistih dokumentov, s katerimi je ta razpolagal, pri tem pa je upravljavcu naložil prekritje podatkov, ki ne sodijo pod definicijo osebnega podatka prosilke ali njene mladoletne hčere.

Posameznik lahko v okviru dostopa prejme dele pisnih izjav, ki neposredno govorijo o njegovih ravnanjih, lastnostih in stanjih

Posameznik je prejel izredno odpoved delovnega razmerja. Pri nekdanjem delodajalcu (javni zdravstveni zavod) je vložil zahtevo za pridobitev kopije pisnih izjav (v obliki e-pošte ali kot papirnih dokumentov), ki so jih njegovi nekdanji sodelavci in nadrejeni podali o njem oz. v zvezi z njegovim delom in obnašanjem ter odnosi s sodelavci pri delu. Upravljalavec je zahtevo zavrnil z utemeljitvijo, da gre za zasebno komunikacijo, ki je bila namenjena le osebni razjasnitvi okoliščin v postopku odločanja o izredni odpovedi delovnega razmerja. V nadzornem postopku je Informacijski pooblaščenec odločil, da je posameznik upravičen do vseh izjav, vendar le do tistih delov, ki neposredno govorijo o njegovih ravnanjih, lastnostih in stanjih (npr. o neprimernem obnašanju in o kršitvi varnostnih pravil ter pravil stroke); med odobrenimi zapisi so bili tudi taki, ki so izražali subjektivna mnenja o posamezniku (npr. o tem, da je žaljiv, nemogoč, z domnevno temno preteklostjo). Ni pa posameznik upravičen do tistih delov izjav, ki se nanašajo zgolj na ravnanja, lastnosti in stanja njegovih sodelavcev in nadrejenih (npr. o posledicah, ki so jih občutili zaradi posameznikovega ravnanja, o njihovih reakcijah na posameznikova ravnanja, o njihovih ravnanjih v zvezi s posameznikom). Vse izjave so sicer bile uporabljene v podporo odločanja o izredni odpovedi in so se nahajale v spisu. Ker je posameznik že v zahtevi vedel, kdo je podal katero izjavo, je bil upravičen tudi do osebnih imen oseb, ki so podale izjavo.

Posameznik je upravičen prejeti fotografijo, ki prikazuje njegovo delovno mesto

Posameznik je prejel odpoved delovnega razmerja. Pri nekdanjem delodajalcu (javni zdravstveni zavod) je vložil zahtevo za pridobitev fotografije njegovega delovnega mesta, ki je bila uporabljena v podporo postopka odpovedi delovnega razmerja. Upravljavec je zahtevo zavrnil, češ da ne gre osebne podatke in da posameznik na fotografiji ni identificiran. Informacijski pooblaščenec je v nadzornem postopku odločil, da je posameznik upravičen do fotografije, ki prikazuje njegovo delovno mesto (npr. delovne pripomočke, omare ter stvari na omarah), ker fotografija prikazuje specifičen prostor, kjer posameznik opravlja delo, zlasti pa prikazuje posameznikova ravnanja (uporabljene pripomočke, snovi, razporeditev stvari) in posledično domnevno kršitev pravil stroke. Poleg tega je bila fotografija uporabljena kot dokaz o kršitvah, posameznik pa je posredno določljiv s pomočjo podatkov, ki se nahajajo v spisu, ki se je vodil v zvezi z odpovedjo delovnega razmerja.

Upravljavec mora posamezniku zagotoviti informacijo o konkretnih namenih obdelave osebnih podatkov

Posameznik je zahteval izpis dnevnika obdelave pri policiji za vse zbirke osebnih podatkov, v katerih se posameznik pojavlja, in sicer za določeno obdobje. Dnevnik obdelave je, poleg drugih podatkov, vseboval tudi osebna imena in ID notranjih uporabnikov, ni pa vseboval konkretnih namenov. Upravljavec je zahtevo v celoti zavrnil. Informacijski pooblaščenec je v nadzornem postopku odločil, da mora policija posamezniku razkriti vrstice (obdelave) z naslednjimi podatki o obdelavah: čas obdelave in konkretni namen, pri čemer mora policija konkretne namene za vsako od vrstic še ugotoviti (jih ustvariti) na podlagi notranjega poizvedovanja ter primerjave z drugimi zbirkami podatkov. Ni pa posameznik upravičen do identitete zaposlenih (ker ni šlo za kršitve varstva osebnih podatkov in ti podatki tudi sicer niso bili pomembni za širše varstvo posameznikovih pravic).

3.3 DRUGI UPRAVNI POSTOPKI

3.3.1 DOPUSTNOST IZVAJANJA BIOMETRIJSKIH UKREPOV

Biometrijske ukrepe urejajo 81., 82., 83. in 84. člen ZVOP-2. Obdelava biometričnih osebnih podatkov v nasprotju z določbami navedenih členov ZVOP-2 je prepovedana.

Če drug zakon določa obdelavo biometričnih osebnih podatkov, mora poleg pogojev za zakonitost obdelave osebnih podatkov iz drugega ali tretjega odstavka 6. člena ZVOP-2 določiti tudi pogoje za njeno uporabo, lahko pa uporabo biometričnih osebnih podatkov tudi omeji. Prepovedano je povezovati zbirke biometričnih osebnih podatkov z drugimi zbirkami in omogočati prenosljivost teh podatkov, razen če to določa drug zakon ali v to privoli posameznik, na katerega se biometrični osebni podatki nanašajo.

a) Biometrija v zasebnem sektorju

Obdelava biometričnih osebnih podatkov v zasebnem sektorju se lahko skladno s 83. členom ZVOP-2 izvaja le, **če je to nujno potrebno za opravljanje dejavnosti, za varnost ljudi, varnost premoženja, varovanje tajnih podatkov ali varovanje poslovnih skrivnosti**, pri tem morajo biti dejanja obdelave biometričnih osebnih podatkov potrjena v skladu z 52. členom ZVOP-2 (gre za vzpostavitev mehanizmov certificiranja za varstvo podatkov ter pečatov in označb za varstvo podatkov za izkazovanje, da so dejanja obdelave s strani upravljavcev in obdelovalcev v skladu s Splošno uredbo).

Oseba zasebnega sektorja lahko obdeluje biometrične osebne podatke tudi **zaradi varstva točnosti identitete svojih strank** (če to za zgoraj navedene namene varovanja interesov določa drug zakon, če to posebej določa pogodba ali so stranke dale izrecno privolitev).

Oseba zasebnega sektorja lahko biometrične osebne podatke obdeluje tudi pod pogojem, **če so dejanja obdelave teh podatkov stranke pod njenim izključnim nadzorom ali njeno izključno oblastjo ter potrjena** v skladu s pristojnostmi nadzornega organa za potrjevanje iz 52. člena ZVOP-2 in če omogoča stranki, da izrecno dovoli obdelavo teh podatkov drugim obdelovalcem in upravljavcem za namen dokazovanja točnosti svoje identitete. V tem primeru stranki izjemoma ni treba pridobiti odločbe Informacijskega pooblaščenca.

Pred začetkom obdelave biometričnih osebnih podatkov morajo biti posamezniki o tem pisno obveščeni, kadar gre za zaposlene, pa mora upravljavec z njimi izvesti predhodno posvetovanje o sorazmernosti obdelave.

ZVOP-2 prepoveduje tudi **pridobivanje biometričnih osebnih podatkov v zvezi s trženjem**, in sicer določa, da se v okviru trženja ali podobne druge poslovne dejavnosti ne sme zahtevati, pridobiti ali nadalje obdelovati biometričnih osebnih podatkov v zamenjavo za določene storitve, četudi so te storitve za posameznika, na katerega se osebni podatki nanašajo, brezplačne.

Oseba zasebnega sektorja, ki namerava obdelovati biometrične osebne podatke, mora **pred začetkom obdelave Informacijskem pooblaščenцу posredovati opis nameravanih obdelav in razloge za njihovo uvedbo** ([Obrazec za prijavo biometrijskih ukrepov Informacijskemu pooblaščenцу](#)). Informacijski pooblaščenec po prejemu potrebnih informacij v dveh mesecih odloči, ali je biometrija dovoljena v skladu z določbami ZVOP-2. Rok se ob upoštevanju zapletenosti predvidene obdelave lahko podaljša za največ dva meseca. Upravljavec osebnih podatkov sme izvajati biometrijske ukrepe šele po prejemu odločbe Informacijskega pooblaščenca, s katero je izvajanje biometrijskih ukrepov dovoljeno. Zoper odločbo Informacijskega pooblaščenca ni pritožbe, dovoljen pa je upravni spor.

Ob tem velja izpostaviti, da 121. člen ZVOP-2 v prehodnih določbah glede potrjevanja določa, da Slovenska akreditacija začne izvajati postopke akreditacije 1. 1. 2024, do začetka izvajanja postopkov akreditacije po tem zakonu pa se šteje, da so dejanja obdelave upravljavcev in obdelovalcev, ki morajo po določbah tega zakona za dejanja obdelave pridobiti certifikat, skladna z merili iz mehanizma potrjevanja. Upravljalci vloge za potrjevanje in vloge po drugem stavku prvega odstavka 83. člena tega zakona vložijo v roku šestih mesecev po poteku roka iz prvega odstavka tega člena. Obdelave, za katere je bila v roku iz prejšnjega stavka dana vloga za potrjevanje², se štejejo za skladne z merili iz mehanizma potrjevanja do 31. 12. 2024.

b) Biometrija v javnem sektorju

Obdelava biometričnih osebnih podatkov v javnem sektorju se lahko skladno z 82. členom ZVOP-2 **določi le z zakonom, če je to nujno potrebno za varnost ljudi, varnost premoženja ali za varovanje tajnih podatkov, za identifikacijo pogošenih ali umrlih posameznikov ali za varovanje poslovnih skrivnosti**, teh namenov pa ni mogoče doseči z milejšimi sredstvi.

Obdelavo biometričnih osebnih podatkov v javnem sektorju je izjemoma dopustno izvajati tudi **pod pogojem, da so dejanja obdelave teh podatkov potrjena** v skladu s pristojnostmi nadzornega organa za potrjevanje iz 52. člena ZVOP-2 na način, ki zagotavlja obdelavo in uporabo teh podatkov posameznika pod njegovim izključnim nadzorom ali izključno oblastjo ter mu omogoča, da izrecno dovoli obdelavo teh podatkov drugim obdelovalcem in upravljavcem za namen dokazovanja točnosti svoje identitete.

Obdelavo biometričnih osebnih podatkov pa se lahko določi tudi z zakonom, če gre za **izpolnjevanje obveznosti iz obvezujoče mednarodne pogodbe ali za identifikacijo posameznikov pri prehajanju državnih meja**.

Obdelava biometričnih osebnih podatkov v javnem sektorju se lahko **določi z zakonom tudi za namen identifikacije posameznikov pri izdaji sredstev elektronske identifikacije** v skladu z zakonom, ki ureja sredstva elektronske identifikacije, in če je tako identifikacijo zahteval posameznik.

V javnem sektorju se lahko z drugim zakonom izjemoma uvede obdelava biometričnih osebnih podatkov **v zvezi z vstopom v stavbo ali dele stavbe**, ki se izvedejo ob smiselni uporabi četrtega, petega in šestega odstavka 83. člena tega zakona, če je to nujno potrebno za varnost ljudi, varnost premoženja, varovanje tajnih podatkov ali varovanje poslovnih skrivnosti. Slednje pomeni, da je za te namene treba pridobiti odločbo Informacijskega pooblaščenca, posamezniki morajo biti o tem pisno obveščeni, kadar gre za zaposlene, pa mora upravljavec z njimi izvesti predhodno posvetovanje o sorazmernosti obdelave.

Informacijski pooblaščenec je leta 2023 prejel dve vlogi za izdajo dovoljenja za uvedbo biometrijskih ukrepov v zasebnem sektorju. Uvedbo biometrijskih ukrepov je zaradi varstva točnosti identitete strank vlagatelja v obeh primerih odobril.

3.3.2 POVEZOVANJE ZBIRK OSEBNIH PODATKOV

Informacijski pooblaščenec je bil po ZVOP-1 pristojen za izdajo predhodnega dovoljenja za povezovanje zbirk osebnih podatkov, zato je te postopke vodil do uveljavitve ZVOP-2 (torej do 26. 1. 2023).

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

² Opozarjamo, da je na tem mestu v ZVOP-2 uporabljen napačen izraz »akreditacija«.

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 ta zagotavlja ustrezno zavarovanje osebnih podatkov. Postopki in ukrepi za zavarovanje morajo biti ustrezni glede na tveganje, ki ga predstavljata obdelava in narava osebnih podatkov, ki se obdelujejo. Poleg ugotavljanja ustreznosti zavarovanja osebnih podatkov mora Informacijski pooblaščenec pri odločanju o izdaji dovoljenja za povezovanje zbirk osebnih podatkov opraviti tudi vsebinski preizkus, ali za povezovanje zbirk osebnih podatkov obstaja ustrezna zakonska podlaga. V okviru povezave zbirk osebnih podatkov se lahko posredujejo oz. obdelujejo le tisti osebni podatki, ki jih določa veljavna zakonodaja. Povezovanje zbirk predstavlja avtomatsko in elektronsko povezovanje zbirk osebnih podatkov, ki jih vodijo upravljavci za različne namene, in sicer tako, da se določeni podatki samodejno ali na zahtevo prenesejo ali vključijo v drugo povezano zbirko ali v več povezanih zbirk. Zbirki osebnih podatkov sta povezani, če se določeni podatki iz ene zbirke neposredno vključijo v drugo zbirko, s čimer se druga zbirka spremeni (poveča, ažurira ipd.); pri tem gre lahko zgolj za enosmeren tok prenosa podatkov.

Informacijski pooblaščenec leta 2023 ni prejel nobene vloge za pridobitev dovoljenja za povezovanje zbirk osebnih podatkov. V zvezi z vlogami, prejetimi v letu 2022, pa je izdal tri odločbe in sicer dve ugodilni in eno zavrnilno. Vlogo je zavrnil, saj za nameravano povezovanje zbirk osebnih podatkov ni obstajala ustrezna zakonska podlaga. Poleg tega je Informacijski pooblaščenec izdal dva sklepa o zavrženju, v eni zadevi zato, ker stranka ni uveljavljala kakšne svoje pravice ali pravne koristi oz. ni mogla biti stranka v postopku, v drugi zadevi pa je vlogo zavrnil, ker mu ZVOP-2 ne daje več pristojnosti za izdajo predhodnega dovoljenja za povezovanje zbirk osebnih podatkov.

Povezovanje zbirk osebnih podatkov je po novem določeno v 87. členu ZVOP-2, ki opredeljuje povezovanje zbirk zgolj določenih podatkov iz uradnih evidenc in knjig. 87. člen ZVOP-2 določa, da kadar se posebne vrste osebnih podatkov, osebni podatki v zvezi s kazenskimi obsodbami in prekrški, podatki o dohodkih v skladu z zakonom, ki ureja dohodnino, podatki o premoženju posameznika v skladu z zakonom, ki ureja uveljavljanje pravic iz javnih sredstev, podatki o nepremičninah v lasti posameznika v skladu z drugimi zakoni, podatki oziroma informacije o kreditni sposobnosti v skladu z zakonom, ki ureja centralni kreditni register, ter uradne evidence v skladu z zakonom, ki ureja naloge in pooblastila policije, in zakonom, ki ureja preprečevanje pranja denarja in financiranja terorizma, obdelujejo v uradnih evidencah ali javnih knjigah, se jih lahko povezuje med seboj ali z drugimi zbirkami samo, če taka povezovanja izrecno določa zakon. Upravljavec oz. obdelovalec mora pred začetkom povezovanja zbirk izdelati oceno učinka (35. člen Splošne uredbe) in se predhodno posvetovati z Informacijskim pooblaščencom (36. člen Splošne uredbe). Informacijski pooblaščenec z uveljavitvijo ZVOP-2 torej ne izdaja več odločb glede povezovanja zbirk.

ZVOP-2 povezave uradnih evidenc in javnih knjig, ki ne vsebujejo zgoraj navedenih vrst osebnih podatkov, posebej ne ureja, kar pomeni, da so povezave drugih uradnih evidenc in javnih knjig dopustne pod pogojem, če za takšno obdelavo obstaja katera od pravnih podlag iz prvega odstavka 6. člena Splošne uredbe in če je zagotovljena ustrezna varnost osebnih podatkov, vključno z zagotavljanjem dnevnika obdelave iz 22. člena ZVOP-2.

3.3.3 PRENOS OSEBNIH PODATKOV V TRETJE DRŽAVE

Splošna uredba opredeljuje 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 (45. člen);
2. izvoznik podatkov zagotovi ustrezne zaščitne ukrepe na podlagi 46. in 47. člena;
3. gre za posebne primere, ki so določeni v 49. členu, 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 46. člena, 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) tretjega odstavka 46. člena);
- ko gre za prenos podatkov med javnimi organi na podlagi določb, ki se vstavijo v upravne dogovore (točka (b) tretjega odstavka 46. člena);
- če se podatki prenašajo na podlagi zavezujočih poslovnih pravil, mora le-te predhodno odobriti pristojni nadzorni organ (prvi odstavek 47. člena).

Prenosi osebnih podatkov so urejeni tudi v ZVOP-2, ki pa se nanašajo le na zelo ozek krog obdelav osebnih podatkov, in sicer zgolj na tiste obdelave, ki se vršijo na področjih zunaj uporabe prava EU, torej na področjih, ki so popolnoma ali delno v samostojni pristojnosti Republike Slovenije. Gre na primer za področja državne varnosti in obrambe države, med taka področja pa sodi tudi obdelava podatkov o umrlih. Določbe ZVOP-2 v zvezi s prenosi se torej nanašajo zgolj na upravljavce, kot sta npr. SOVA, OVS in Ministrstvo za obrambo, v delu mednarodnih civilnih misij tudi na Ministrstvo za zunanje zadeve, na upravljavce, ki želijo v tretjo državo prenesti podatke o umrlih itd. Za vse ostale upravljavce in obdelovalce, ki so zavezanci po Splošni uredbi, se v celoti uporabljajo zgolj določbe V. poglavja Splošne uredbe, torej od 44. do 49. člena Splošne uredbe.

Informacijski pooblaščenec v letu 2023 ni prejel nobene vloge v zvezi s prenosom podatkov v tretje države.

Na spletni strani Informacijskega pooblaščenca so objavljene smernice, v katerih je podrobno predstavljena ureditev prenosov osebnih podatkov v tretje države in mednarodne organizacije po Splošni uredbi in po ZVOP-2. Smernice so dostopne na [tej povezavi](#).

Evropska komisija je 10. 7. 2023 sprejela sklep o ustreznosti varstva osebnih podatkov na podlagi okvira za varstvo zasebnosti podatkov med EU in ZDA (angl. *EU-US Data Privacy Framework – DPF*). Iz sklepa izhaja, da ZDA zagotavljajo ustrezno raven varstva (primerljivo z EU) za tiste osebne podatke, ki se iz EU v ameriška podjetja prenašajo v skladu z novim okvirom za varstvo zasebnosti podatkov med EU in ZDA. Na podlagi sklepa o ustreznosti se lahko osebni podatki iz EU varno prenašajo tistim podjetjem v ZDA, ki sodelujejo v okviru za varstvo zasebnosti podatkov med EU in ZDA, ob tem pa ni treba uvesti dodatnih zaščitnih ukrepov za varstvo podatkov v skladu s 46. členom Splošne uredbe. Ameriška podjetja se lahko okvira za varstvo zasebnosti podatkov pridružijo na podlagi zaveze, da bodo izpolnjevala podrobno določen sklop obveznosti glede varstva zasebnosti, na primer zahtevo po izbrisu osebnih podatkov, ko ti niso več potrebni za namen, za katerega so bili zbrani, in po zagotavljanju neprekinjenega varstva, kadar se osebni podatki posredujejo tretjim

osebam. Seznam podjetij, ki sodelujejo v okviru, je javno dostopen na strani ameriškega ministrstva za trgovino (<https://www.dataprivacyframework.gov/s/participant-search>). Posamezniki iz EU imajo v primeru, da ameriška podjetja z njihovimi osebnimi podatki ne ravnajo pravilno, na voljo več pravnih sredstev, vključno z brezplačnimi neodvisnimi mehanizmi za reševanje sporov. V zvezi z zbiranjem in uporabo njihovih podatkov s strani ameriških obveščevalnih agencij imajo dostop do neodvisnega in nepristranskega mehanizma pravnega varstva, ki vključuje novoustanovljeno sodišče za presojo varstva podatkov (angl. *Data Protection Review Court – DPRC*). Slednje je namenjeno neodvisnim preiskavam in reševanju pritožb, med drugim tudi s sprejemanjem zavezujočih popravnih ukrepov.

Sklep o ustreznosti je na voljo na spletni strani Evropske komisije: https://commission.europa.eu/system/files/2023-07/Adequacy%20decision%20EU-US%20Data%20Privacy%20Framework_en.pdf.

3.4 PRIPRAVA MNENJ IN POJASNIL

3.4.1 SPLOŠNA POJASNILA

Na podlagi 57. člena Splošne uredbe, 76. člena ZVOPOKD in 56. člena ZVOP-2 Informacijski pooblaščenec izdaja neobvezna mnenja, pojasnila in stališča o vprašanih s področja varstva osebnih podatkov, s katerimi prispeva k ozaveščenosti upravljavcev in obdelovalcev ter širše javnosti.

Leta 2023 je Informacijski pooblaščenec svetoval 2.580 posameznikom in pravnim osebam, ki so se nanj obrnili z vprašanji s področja varstva osebnih podatkov.

Informacijski pooblaščenec je izdal **1011 pisnih mnenj in napotitev na mnenja (od tega je izdal 925 pisnih mnenj, v 86 primerih je prosilcem svetoval po telefonu oz. posredoval kratka napotila)**. Na spletni strani <https://www.ip-rs.si/mnenja-zvop-2/> so objavljena mnenja, ki so bila izdana po začetku veljavnosti ZVOP-2. Uporabniki lahko z ločenim iskalnikom brskajo po mnenjih, ki so bila izdana po ZVOP-1, preden je v veljavo stopila Splošna uredba, in do mnenj, ki so bila izdana po uveljavitvi Splošne uredbe (in pred začetkom uporabe ZVOP-2). Mnenja so razvrščena v kar 73 vsebinskih področij, **objavljenih je več kot 8.000 mnenj**.

Informacijski pooblaščenec spodbuja svetovanje oz. posredovanje ustnih odgovorov na vprašanja, zato je bil tudi v letu 2023 v uradu vsak delovnik na voljo dežurni državni nadzornik za varstvo osebnih podatkov, ki je na vprašanja odgovarjal po telefonu. **Leta 2023 so državni nadzorniki po telefonu svetovali 1.569 posameznikom in organizacijam.**

3.4.2 MNENJA NA PREDPISE

Informacijski pooblaščenec podaja mnenja na predpise skladno s točko (c) prvega odstavka 57. člena Splošne uredbe, 56. členom ZVOP-2 in 76. členom ZVOPOKD, ki določajo, da nadzorni organ svetuje državnemu zboru, vladi oz. ministrstvom 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 vprašanih glede varstva osebnih podatkov.

Leta 2023 je **Informacijski pooblaščenec pripravil 93 mnenj na predloge sprememb zakonov ter na predloge novih zakonov in drugih predpisov**. Informacijski pooblaščenec je pri predlagateljih predpisov, s katerimi se uvajajo nove kompleksne oblike obdelav osebnih podatkov ali obsežne obdelave osebnih podatkov z uporabo modernih tehnologij, še vedno pogrešal zavedanje o nujnosti temeljite predhodne analize in naslovitve tveganj, ki jih takšne obdelave prinašajo. Skladno z novimi določbami ZVOP-2 morajo upravljavci glede določenih obdelav osebnih podatkov pripraviti tudi oceno učinka po 35. členu Splošne uredbe ali pa opraviti predhodno posvetovanje z Informacijskim pooblaščenecem po 36. členu Splošne uredbe (več o tem v poglavju 3.5.3).

Informacijski pooblaščenec je leta 2023 med drugim podal mnenje, pripombe oz. je sodeloval pri pripravi naslednjih predpisov (v zvezi z nekaterimi je podal več mnenj):

- Predlog Zakona o digitalizaciji zdravstva,
- Predlog ureditve razvida medijev v novem Zakonu o medijih,
- Predlog novega Energetskega zakona (EZ-2),
- Predlog Zakona o spremembah in dopolnitvah Zakona o izvrševanju kazenskih sankcij,
- Zakonodajni predlogi s področja uvedbe digitalnega evra in odprtih financ, ki jih je Evropska komisija objavila 28. 6. 2023,
- Predlog Zakona o postopku sodnega varstva nekdanjih imetnikov kvalificiranih obveznosti bank,

- Predlog Zakona o spremembah in dopolnitvah Zakona o sodnih izvedencih, sodnih cenilcih in sodnih tolmačih,
- Predlog Zakona o spremembah in dopolnitvah Zakona o obveznih zavarovanjih v prometu,
- Predlog Zakona o sodniški službi,
- Predlog Zakona o detektivski dejavnosti,
- Predlog Zakona o spremembah in dopolnitvah Zakona o urejanju trga dela,
- Predlog Zakona o nujnih ukrepih na področju zdravstvenega varstva,
- Predlog Zakona o obnovi, razvoju in zagotavljanju finančnih sredstev,
- Predlog Zakona o sodiščih,
- Predlog Zakona o spremembah in dopolnitvah Zakona o sodnem svetu,
- Predlog Zakona o spremembah in dopolnitvah Zakona o gospodarskih družbah,
- Predlog sprememb 135.a, 135.b in 135.č člena Zakona o organizaciji in financiranju vzgoje in izobraževanja,
- Predlog Zakona o cestninjenju,
- Predlog Zakona o spremembah in dopolnitvah Zakona o lokalnih volitvah,
- Predlog Zakona o osebni asistenci,
- Predlog ureditve obdelave podatkov iz evidenc podatkov o gibalnih sposobnostih in morfoloških značilnostih v Zakonu o organizaciji in financiranju vzgoje in izobraževanja,
- Ustavnorevizijski Predlog,
- Predlog Zakona o spremembah in dopolnitvah Zakona o osnovni šoli,
- Predlog Zakona o gospodarskih javnih službah varstva okolja,
- Predlog Zakona o izvajanju Uredbe (EU) o enotnem trgu digitalnih storitev,
- Predlog Zakona o spremembah in dopolnitvah Zakona o trgu finančnih instrumentov,
- Predlog Zakona o javnih uslužbencih,
- Predlog Zakona o spremembah in dopolnitvah Zakona o davku na dodano vrednost,
- Predlog Zakona o spremembah Zakona o reševanju in prisilnem prenehanju bank (ZRPPB-1A),
- Predlog Zakona o kupcih in serviserjih nedonosnih kreditov bank,
- Predlog Zakona o skupnih temeljnih sistema plač v javnem sektorju,
- Predlog Zakona o centralnem kreditnem registru,
- Predlog Zakona o spremembah in dopolnitvah Zakona o železniškem prometu,
- Predlog Zakona o dolgotrajni oskrbi,
- Predlog Pravilnika o enotnem informacijskem sistemu na področju javnega naročanja,
- Predlog Zakona o spremembah in dopolnitvah Zakona o zunanjih zadevah,
- Predlog Pravilnika o spremembah in dopolnitvah Pravilnika o tehničnih pregledih motornih in priklopnih vozil,
- Predlog Pravilnika o pooblastilih za obdelavo podatkov v Centralnem registru podatkov o pacientih,
- Predlog Zakona o Zdravstvenem informacijskem sistemu,
- Predlog Zakona o Zavodu za zdravstveno zavarovanje Slovenije,
- Predlog za ratifikacijo Protokola o spremembi Konvencije o varstvu posameznikov glede na avtomatsko obdelavo osebnih podatkov,
- Predlog Zakona o letalstvu,
- Predlog Pravilnika o stroških seznanitve z lastnimi osebnimi podatki,
- Predlog Zakona o spremembah in dopolnitvah Zakona o divjadi in lovstvu,
- Predlog pravilnika o tehničnih pogojih, ki jih morajo izpolnjevati videoelektronska identifikacijska sredstva,
- Predlog Zakona o spremembah in dopolnitvah Zakona o maturi,
- Predlog Zakona o spremembah in dopolnitvah Zakona o višjem strokovnem izobraževanju,
- Predlog Uredbe o prostem letenju,
- Predlog Uredbe o izvedbi intervencij kmetijske politike za leto 2023,
- Predlog Zakona o ureditvi nekaterih vprašanj v zvezi s prekrški, izvršenimi v času veljavnosti ukrepov zaradi nalezljive bolezni COVID-19,
- Pravna podlaga za obdelavo podatkov članov čebelarskih društev v okviru Uredbe o izvajanju

intervencij v sektorju čebelarških proizvodov iz strateškega načrta skupne kmetijske politike 2023–2027, ki določa izvajanje intervencij v sektorju čebelarških proizvodov,

- Predlog Uredbe o izvajanju znanstvenoraziskovalnega dela v skladu z načeli odprte znanosti,
- Predlog Pravilnika o načinu izvajanja 220. člena Zakona o elektronskih komunikacijah,
- Predlog Zakona o spremembah in dopolnitvah Zakona o nalogah in pooblastilih policije.

3.4.3 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 2023 vodil pritožbeni postopek zaradi kršitve pravice do seznanitve z zdravstveno dokumentacijo po 41. členu ZPacP. Pri obravnavanju pritožbe se je Informacijski pooblaščenec srečal s problematiko obstoječe zakonske ureditve pravice zdravnika do zamolčanja podatkov (t. i. terapevtski privilegij oziroma obzirni molk zdravnika).

41. člen ZPacP med drugim določa, da ima pacient ob prisotnosti zdravnika ali drugega zdravstvenega delavca oziroma zdravstvenega sodelavca pravico do neoviranega vpogleda in prepisa zdravstvene dokumentacije, ki se nanaša nanj, pri čemer mora upoštevati tudi določbe prvega odstavka 22. člena. Prvi odstavek 22. člena ZPacP pa določa, da 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 najboljšo zdravstveno korist, izrecno zahteva, da je o svojem zdravstvenem stanju popolnoma obveščen. Razloge za zamolčanje podatkov se ločeno dokumentira v zdravstveni dokumentaciji.

Pacient je v konkretnem primeru pri izvajalcu zdravstvene dejavnosti vložil zahtevo za seznanitev z zdravstveno dokumentacijo po 41. členu ZPacP, izvajalec pa je presodil, da bi seznanitev s to dokumentacijo pacientu povzročila resno zdravstveno škodo, zaradi česar je njegovo zahtevo zavrnil. Pacient je nato vložil še izrecno zahtevo za seznanitev z zdravstveno dokumentacijo (upoštevajoč prvi odstavek 22. člena v povezavi z 41. členom ZPacP). Izvajalec je tudi to zahtevo zavrnil z utemeljitvijo, da pacient ni sposoben odločanja v svojo korist. Informacijski pooblaščenec je v pritožbenem postopku presodil, da ta odločitev ni bila ustrezno obrazložena, zato je odločbo odpravil in jo vrnil izvajalcu zdravstvene dejavnosti v ponovno odločanje. Ta je pacientovo zahtevo ponovno zavrnil brez podrobnejše utemeljitve, pacient pa je pri Informacijskem pooblaščenecu vložil pritožbo.

Po zakonski ureditvi bi lahko torej pacient, ki bi mu seznanitev z zdravstveno dokumentacijo povzročila resno zdravstveno škodo, dostopal do te dokumentacije v primeru, da poda izrecno zahtevo, pri čemer pa mora biti sposoben odločanja v svojo najboljšo zdravstveno korist.

Informacijski pooblaščenec meni, da je omejitev pravice do seznanitve z zdravstveno dokumentacijo, kot izhaja iz prvega odstavka 22. člena v zvezi z osmim odstavkom 41. člena ZPacP, v neskladju s tretjim odstavkom 38. člena Ustave v povezavi z 2., 15., 34., 35. členom in tretjim odstavkom 51. člena Ustave, saj je pojem »sposobnost odločanja v svojo najboljšo zdravstveno korist« preveč nejasen in nedoločen, takšna omejitev ustavne pravice do seznanitve z lastnimi osebnimi podatki pa je nesorazmerna in v nasprotju s 23. členom Splošne uredbe v zvezi z 18. členom ZVOP-2.

Pravica do seznanitve z osebnimi podatki in zdravstveno dokumentacijo

Pravica posameznika do seznanitve z osebnimi podatki, ki se nanašajo nanj, katere izpeljava je tudi pravica do seznanitve z zdravstveno dokumentacijo, je ustavna pravica. Ustava RS v tretjem odstavku 38. člena določa, da se ima vsakdo pravico seznaniti z zbranimi osebnimi podatki, ki se nanašajo nanj, in pravico do sodnega varstva ob njihovi zlorabi. Splošna uredba v 15. členu še

konkretnije določa pravico dostopa posameznika, na katerega se nanašajo osebni podatki; cilj te pravice je posamezniku omogočiti nadzor nad njegovimi osebnimi podatki. Posameznik ima tako dostop tudi do podatkov v zvezi s svojim zdravjem, npr. podatkov v njegovi zdravstveni kartoteki, ki vključuje informacije, kot so diagnoze, izvidi preiskav, posegi, itd. Pravica posameznika do seznanitve z zdravstveno dokumentacijo pa izhaja tudi iz pravice posameznika do dostojanstva, samoodločbe in avtonomije (35. člen Ustave v zvezi z 34. členom Ustave) ter iz pravice do prostovoljnega zdravljenja oz. prepovedi prisilnega zdravljenja (tretji odstavek 51. člena Ustave). Človekove pravice in svoboščine so lahko omejene samo s pravicami drugih in v primerih, ki jih določa Ustava. Po ustaljeni ustavnosodni praksi so posegi v varstvo osebnih podatkov dopustni, če so skladni z načelom sorazmernosti.

Omejitev pravice do lastnih osebnih podatkov so po določbah ZVOP-2 in Splošne uredbe dopustne zgolj izjemoma. Skladno s 23. členom Splošne uredbe mora vsak zakonodajni ukrep, ki omejuje pravico dostopa, spoštovati bistvo temeljnih pravic in svoboščin ter mora biti potreben in sorazmeren ukrep v demokratični družbi za zagotavljanje, med drugim varstva posameznika, na katerega se nanašajo osebni podatki. Prav tako je določeno, kaj mora vsak tak zakonodajni ukrep vsebovati, npr. posebne določbe glede namenov obdelave ali vrst obdelave; vrst osebnih podatkov; obsega uvedenih omejitev; zaščitnih ukrepov za preprečitev zlorab ali nezakonitega dostopa ali prenosa itd. Informacijski pooblaščenec meni, da izpodbijana ureditev navedenih pogojev ne izpolnjuje.

Določbe Ustave, ki so kršene

a) Načelo jasnosti in določnosti predpisov

Načelo pravne države med drugim zahteva, da so predpisi jasni in določni tako, da je mogoče nedvomno ugotoviti vsebino in pomen norme. Norme morajo biti takšne, da jih je mogoče izvajati, da ne omogočajo arbitrarnega ravnanja ter da nedvoumno in dovolj določno opredeljujejo pravni položaj subjektov, na katere se nanašajo. Po mnenju Informacijskega pooblaščenca izpodbijanih določb ZPacP niti z razlago ni mogoče vsebinsko jasno opredeliti, predvsem zaradi pojma »sposobnost odločanja v svojo najboljšo zdravstveno korist« iz prvega odstavka 22. člena ZPacP. Ne ZPacP ne noben drug zakon ne določa, kdaj je pacient sposoben odločanja v svojo najboljšo zdravstveno korist. V 19. točki 2. člena ZPacP je določeno le, da je sposobnost odločanja o sebi sposobnost pacienta, da samostojno uveljavlja pravice iz tega zakona, še zlasti da odloča o izvedbi medicinskega posega oziroma zdravstvene obravnave. Pacient je sposoben odločanja o sebi, če je glede na starost, zrelost, zdravstveno stanje ali druge osebne okoliščine sposoben razumeti pomen in posledice uveljavljanja pravic iz tega zakona, še zlasti privolitve, zavrnitve ali preklica zavrnitve medicinskega posega oz. zdravstvene obravnave.

Sposobnost odločanja o sebi se torej povezuje s t. i. privolitveno oz. zavrnitveno sposobnostjo, ki pomeni sposobnost privoliti v medicinski poseg oz. ga zavrniti, in je odvisna od razsodnosti pri odločanju (sposobnosti razumeti pomen in posledice svojih dejanj). Presoja se neodvisno od civilnopravne poslovne sposobnosti posameznika, saj so zahteve za priznanje razsodnosti, ki je potrebna za priznanje poslovne sposobnosti, višje kot tiste, ki so potrebne za priznanje privolitvene sposobnosti (celo pacient, ki mu je odvzeta poslovna sposobnost, lahko poda izjavo o privolitvi za zdravljenje v psihiatrični bolnišnici pod posebnim nadzorom).

Omejitev pravice do seznanitve z zdravstveno dokumentacijo v ZPacP pa ni vezana na »sposobnost odločanja o sebi« ali na »sposobnost skrbeti za svoje pravice in koristi brez škode zase«, temveč na nedoločen, nejasen in odprt pojem »sposobnost odločanja v svojo najboljšo zdravstveno korist«. Zakonodajalec je torej vpeljal nedoločen pravni pojem, ki ni opredeljen niti v ZPacP niti ni običajno uporabljen v predpisih s področja zdravstva. Presoja je tako prepuščena vsakokratni prosti presoji, razlagi in oceni izvajalca zdravstvene dejavnosti oz. zdravnika. Ker je standard nedoločen do te mere, da omogoča prekomerno različno razlago, lahko vodi v zmanjšano predvidljivost pravnega položaja pacientov in neutemeljen poseg v pravice posameznikov. Prav tako se v praksi pojem

enači s konceptom povzročitve resne zdravstvene škode na način, da sta pogoja glede navadne in izrecne zahteve izenačena.

b) Načelo sorazmernosti

Izpodbijana ureditev pomeni poseg v pravico do seznanitve z lastno zdravstveno dokumentacijo, zato mora poseg ustrezati načelu sorazmernosti. Informiranost pacienta o njegovem zdravstvenem stanju je nujni pogoj za uveljavitev pravice do dejavnega sodelovanja pri izbiri načina zdravljenja. Zamolčanost resnice posega v avtonomnost in dostojanstvo pacienta, onemogoča izvrševanje pravice do samoodločbe ter nasprotuje informirani privolitvi. Pacient, ki ni informiran ali ni dovolj informiran, ne more dejavno sodelovati pri svojem zdravljenju oz. lahko celo sprejema odločitve v zmoti glede svojega zdravstvenega stanja. Informacijski pooblaščenec meni, da bi bilo zato treba izjemo od pravice do obveščeniosti v povezavi s pravico do seznanitve z zdravstveno dokumentacijo razlagati skrajno restriktivno, saj lahko sicer preširoko tolmačenje te izjeme pripelje do hudega posega v pravico do samoodločanja, osebnega dostojanstva in varstva osebnih podatkov. V primeru izrecne zahteve po popolni obveščeniosti o svojem zdravstvenem stanju in zahteve za seznanitev z lastno zdravstveno dokumentacijo je izvajalec zdravstvene dejavnosti pacientu praviloma dolžan omogočiti seznanitev s celotno zdravstveno dokumentacijo. Če pacient izrecno zahteva, da je o svojem zdravstvenem stanju obveščen, mora izvajalec zdravstvene dejavnosti njegovi zahtevi ugoditi, pa čeprav meni, da bo pacientu zaradi seznanitve nastala zdravstvena škoda ne glede na morebitne posledice. S tem pacient prevzame odgovornost za morebitno nastalo zdravstveno škodo.

Vežanost sposobnosti za veljavno podajo takšne izrecne zahteve na sposobnost odločanja v najboljšo zdravstveno korist je že na prvi pogled nesorazmerna, saj pri tem ne gre za omejitev na poslovno nesposobnega pacienta niti na pacienta, ki ni sposoben odločanja o sebi, temveč na drugačno, zakonsko neopredeljeno ter strožjo presojo sposobnosti pacienta, ki se želi seznaniti s svojo zdravstveno dokumentacijo.

Tudi z vidika pacientove pravice do avtonomije pri odločanju glede zdravljenja ter prepovedi prisilnega zdravljenja je nesorazmerno, da se posamezniku, ki je sposoben odločanja o sebi, omejuje pravica do seznanitve z zdravstveno dokumentacijo. Če posameznik prevzame tveganje za nastanek resne zdravstvene škode, potem bi mu bilo treba dopustiti dostop do njegovih zdravstvenih podatkov, čeprav zdravnik meni, da to ni v njegovo najboljšo korist in lahko vodi do poslabšanja zdravja. Pacient ima pravico vedeti, v kakšnem zdravstvenem stanju je, da lahko na tej podlagi sprejema odločitve. Zaradi neustrezne pravice do obveščeniosti in seznanitve z zdravstveno dokumentacijo so lahko ogrožene ali celo izvotljene tudi druge pravice pacientov, npr. pravica do sodelovanja, pravica do samostojnega odločanja o zdravljenju in pravica do upoštevanja vnaprej izražene volje.

Na podlagi navedenega Informacijski pooblaščenec meni, da je obstoječa zakonska ureditev pravice do seznanitve z zdravstveno dokumentacijo neustavna, saj krši načelo sorazmernosti ter načelo jasnosti in določnosti pravnih norm in pomeni hud poseg v ustavno zaščitene pravice do seznanitve z osebnimi podatki in zdravstveno dokumentacijo ter do dostojanstva, samoodločbe in avtonomije.

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-presajo-ustavnosti-oz-zakonitosti-predpisov>.

3.5 SKLADNOST IN PREVENTIVA

Z uveljavitvijo ZVOP-2 konec januarja 2023 je bil pred zavezance dan nov predpis, ki ga morajo razumeti in spoštovati, zato je bilo leto 2023 z vidika preventivnih aktivnosti Informacijskega pooblaščenca v pomembnem delu posvečeno ozaveščanju zavezancev glede ZVOP-2. Sprejem novega zakona smo naslovili z različnimi preventivnimi dejavnostmi, kot so telefonsko in pisno svetovanje, ažuriranje vsebin na spletnih straneh, posodobitev smernic, priprava infografik, izvajanje brezplačnih izobraževanj in komunikacija prek družabnih omrežij. Informacijski pooblaščenec je o novem ZVOP-2 pripravil več brezplačnih izobraževanj, ki se jih je udeležilo več kot 1000 udeležencev, pospešeno pa smo izdajali tudi pisna mnenja za posameznike in zavezance ter izvajali svetovanje po telefonu.

V letu 2023 smo pristopili k izvajanju usklajene aktivnosti za skladnost v sodelovanju z drugimi nadzornimi organi za varstvo osebnih podatkov na temo položaja in delovanja pooblaščenih oseb za varstvo osebnih podatkov, okrepili sodelovanje s pooblaščenimi osebami za varstvo podatkov ter pripravili dodatne zahteve za akreditacijo, ki je predpogoj za začetek izdaje certifikatov na področju varstva osebnih podatkov.

Poleg preventivnih aktivnosti Sektor za skladnost in preventivo Informacijskega pooblaščenca nudi tudi podporne dejavnosti drugim sektorjem, tako glede informacijske tehnologije kot glede pomoči sektorju za inšpekcijski nadzor; med drugim razvija določene interne aplikacije, vzdržuje in nadgrajuje intranet Informacijskega pooblaščenca ter izvaja številne druge preventivne dejavnosti, ki so opisane v nadaljevanju.

3.5.1 NOVE OBVEZNOSTI UPRAVLJAVCEV PO ZVOP-2

ZVOP-2 kot nacionalni predpis glede na določbe Splošne uredbe ureja določena vsebinska področja, kot so uporaba zdravstvenih, biometrijskih in genskih podatkov, nekatere postopkovne vidike (npr. postopek izrekanja sankcij in pravna sredstva) ter relacijo do drugih področij in pravic (npr. dostop do informacij javnega značaja, uporaba osebnih podatkov v raziskovalne, arhivske in statistične namene). Poleg tega ZVOP-2 ureja dodatne pogoje za pooblaščenice osebe za varstvo podatkov, spreminja ureditev videonadzora (na novo ureja videonadzor na javnih površinah, prepoveduje uporabo sistemov za prepoznavo obrazov in prepoznavo registrskih tablic na javnih površinah itd.), podrobneje določa zahteve glede zagotavljanja sledljivosti (dnevnik obdelave) in nekatera druga področja. ZVOP-2 ne sme spreminjati določb Splošne uredbe, saj je treba uredbo neposredno uporabljati, zavezanci pa morajo upoštevati, da veljata tako Splošna uredba kot ZVOP-2 in je treba določbe ZVOP-2 interpretirati v skladu z določbami Splošne uredbe. Za lažje razumevanje novosti ZVOP-2 smo pripravili tudi pregled sprememb glede na predhodni zakon (ZVOP-1).

Sprememba	Kratka razlaga
Biometrija	<p>Nova ureditev biometrije (členi 80 do 84). Obdelava biometričnih osebnih podatkov v nasprotju z ZVOP-2 je prepovedana. Drug zakon lahko določa obdelavo biometričnih osebnih podatkov in pogoje za njeno uporabo, lahko pa uporabo biometričnih osebnih podatkov tudi omeji. Prepovedano je povezovati zbirke biometričnih osebnih podatkov z drugimi zbirkami in omogočati prenosljivost teh podatkov, razen če to določa drug zakon.</p> <p>V zasebnem sektorju ostaja omejenost dopustnih namenov, ne samo nad zaposlenimi, temveč pod določenimi pogoji tudi nad strankami. V javnem sektorju mora biometrijo urejati zakon, ostaja zahteva po odločbi Informacijskega pooblaščenca v zasebnem (in deloma v javnem) sektorju (razen če je biometrija pod nadzorom posameznika), dodana je prepoved pridobivanja biometričnih osebnih podatkov v zvezi s trženjem.</p>
Definicije	<p>Veljajo definicije iz Splošne uredbe (4. člen), poleg teh pa nove (npr. povezovanje) ali spremenjene (npr. javni sektor) definicije iz ZVOP-2:</p> <ul style="list-style-type: none"> · nadzorni organ, · nadzorne osebe, · javni sektor, · zasebni sektor, · povezovalni znak, · zadeva sodišča, · zakon, · varnost države, · kazenske evidence, · prekrškovne evidence, · storitev informacijske družbe, · povezovanje zbirk podatkov.
Evidentiranje vstopov v službene prostore in izstopov iz njih	<p>Ureditev je podobna kot v ZVOP-1. 85. člen ZVOP-2 določa, da je dopusten vpogled v osebni dokument, določa tudi, kaj se sme zabeležiti: osebno ime, številko in vrsto uradnega identifikacijskega dokumenta, naslov prebivališča, zaposlitev, vrsto in registrsko številko vozila ter datum, uro in razlog vstopa v prostore ali izstopa iz njih. Dodana je registrska številka vozila, skrajšan je rok hrambe, in sicer s 3 let na 2 leti od konca koledarskega leta.</p>
Genski podatki	<p>Nova ureditev v 81. členu ZVOP-2 določa, da je genske podatke posameznika (npr. DNK-material) dopustno obdelovati, kadar to določa drug zakon, za namene zagotavljanja zdravstvenega varstva ali kadar je obdelava potrebna za izvajanje pogodbe, sklenjene izključno zaradi obdelave genskih podatkov v korist pogodbene stranke, ki je posameznik.</p>
Izjema družinske rabe in zasebne rabe	<p>Izjema družinske rabe in zasebne rabe (1. odstavek 7. člena ZVOP-1) vsebinsko gledano ostaja, urejena je v drugem odstavku 3. člena ZVOP-2.</p>
Izjeme glede članov določenih organizacij	<p>Izjeme glede podatkov o članih politične stranke, sindikata, društva ali verske skupnosti ter za upravljavce osebnih podatkov z manj kot 50 zaposlenimi ne veljajo več.</p>
Katalogi in register zbirk	<p>Dolžnosti glede sprejema katalogov in prijave zbirk v register zbirk pri Informacijskem pooblaščenca prenehajo veljati; ostaja dolžnost sprejema evidenc dejavnosti po 30. členu Splošne uredbe.</p>
Neposredno trženje (72. in 73. člen ZVOP-1) – člena prenehata veljati	<p>Za neposredno trženje posameznikom po elektronskih poteh (npr. e-pošta, SMS ipd.), vključno s trženjem po telefonu in s pomočjo telefonskih imenikov, veljajo določbe Zakona o elektronskih komunikacijah (ZEKom-2); za trženje po navadni pošti velja Splošna uredba. ZVOP-2 tega ne ureja več posebej ali drugače.</p>
Obdelava kontaktnih podatkov	<p>Nove so določbe glede obdelave kontaktnih podatkov (93. člen ZVOP-2). Za namene organiziranja uradnih srečanj, izobraževanj ipd., dajanja izjav za javnost, razen izvajanja neposrednega trženja, je dovoljena uporaba kontaktnih podatkov posameznikov iz javno dostopnih virov ali v okviru izvrševanja svojih javnih nalog, če so jih posamezniki prostovoljno razkrili ali dali privolitev.</p>

	Določen je nabor podatkov: osebno ime, telefonska številka, e-poštni naslov ali druga komunikacijska številka/oznaka, podatki o delodajalcu/organizaciji ter podatki o področju dela, položaju, funkciji, članstvu v klubu ali hobiju posameznika. Za namene obveščanja javnosti sme oseba javnega ali zasebnega sektorja obdelovati, vključno z objavo: osebna imena, nazive, fotografije in videoposnetke posameznikov, pridobljene na dogodkih, ki jih v okviru svojih nalog, pristojnosti ali dejavnosti organizira ta oseba, če posameznik te obdelave ni prepovedal.
Obdelava osebnih podatkov in dostop do informacij javnega značaja	Zavezanci po Zakonu o dostopu do informacij javnega značaja (ZDIJZ) javnosti posredujejo osebne podatke, če so ti po zakonu javni ali če je za njihovo razkritje dan prevladujoč javni interes v skladu z ZDIJZ. Kadar zakon določa javnost podatkov ali kadar gre za podatke, ki so informacije javnega značaja, jih upravljavec, ki z njimi razpolaga, lahko javno objavi (74. člen ZVOP-2).
Obdelava osebnih podatkov in mediji	Nova ureditev po 83. členu ZVOP-2. Obdelava za namene obveščanja javnosti s strani medijev, književnega, umetniškega ali raziskovalnega ustvarjanja, resne kritike, obrambe kakšne pravice ali varstva upravičene koristi in izobraževanja je dopustna, če: je posameznik za obdelavo, objavo ali razkritje dal privolitev; je posameznik osebne podatke že javno objavil ali dal na razpolago javnosti; so na zakonit način že bili dostopni javnosti; so bili pridobljeni na podlagi prisotnosti posameznika na javno dostopnih krajih ali dogodkih, kjer posameznik glede na vse okoliščine ne more razumno pričakovati varstva zasebnosti, gre za zakonito objavo mnenja ali vrednostne ocene, je objava nujna za utemeljitev tega mnenja ali vrednostne ocene; so bili osebni podatki pridobljeni na drug zakonit način; pretehta javni interes po obveščanju javnosti, pravica do obveščenosti ter svoboda izražanja ali tako določa drug zakon. Uveljavljanje pravic posameznikov poteka pred sodišči, za namene izvajanja svobode izražanja ni dopustno nezakonito razkrivanje osebnih podatkov.
Obdelava za arhivske namene	Je dovoljena, če to določa zakon. Posameznik nima pravice do dostopa do lastnih podatkov v arhivskem gradivu po 15. členu Splošne uredbe, če bi dajanje informacij ali kopij njegovih osebnih podatkov zahtevalo očitno nesorazmeren napor. Pravice posameznika do popravka osebnih podatkov zaradi netočnosti ali neposodobljenosti, izbrisa, omejitve obdelave, prenosljivosti osebnih podatkov in izvršitve pravice do ugovora (kot jih opredeljuje Splošna uredba) so omejene. Posameznik, ki navaja netočnost ali neposodobljenost svojih osebnih podatkov, ima možnost dati dopolnilno izjavo z navedbo nasprotnih dejstev, ki se priloži arhivskemu gradivu ali pa se na gradivu ustrezno označi, kje je ta izjava. 71. člen ZVOP-2 se ne uporablja, če zakon, ki ureja varstvo dokumentarnega in arhivskega gradiva ter arhive, določa drugače.
Obdelava za raziskovalne namene	Obdelava osebnih podatkov za raziskovanje (znotraj zavezanca) ostaja dopustna. Raziskovalne organizacije pridobijo osebne podatke, vključno s posebnimi vrstami osebnih podatkov, če tako obdelavo dovoljuje drug zakon ali če posameznik ni prepovedal obdelave. Raziskovalci morajo predložiti opis raziskave (»elaborat«), 69. člen ZVOP-2 pa določa, kaj mora vsebovati ter priložiti oceno učinka, če je obvezna po Splošni uredbi. Upravljavec zavrne posredovanje pod določenimi pogoji. Posameznikov se o obdelavah za te namene ne obvešča, razen če zakon določa drugače. Podatki, ki so bili predmet raziskave, se ob zaključku raziskave uničijo ali nepovratno anonimizirajo, razen izjemoma. Rezultati raziskave se objavijo v anonimizirani obliki, izjemoma tudi v psevdonimizirani obliki, če objava podatkov v anonimizirani obliki iz tehničnih razlogov ali zaradi zasledovanja ciljev raziskave ni mogoča. Določena je tudi možnost kontaktiranja posameznikov za pridobivanje privolitev za sodelovanje v raziskavi (70. člen).
Obdelava za statistične namene	Podobno ureditvi obdelave za arhivske namene (omejitve pravic posameznika, podlaga v področnem zakonu) – ureja 72. člen ZVOP-2.
Objava kontaktnih podatkov	106. člen ZVOP-1 nadomešča 92. člen ZVOP-2, ki določa, kateri podatki zaposlenih so lahko objavljeni javno (npr. na spletni strani) ali posredovani javnosti. Osebe javnega ali zasebnega sektorja lahko javnosti posredujejo in javno objavijo: osebno ime, naziv ali funkcijo, službeno telefonsko številko in naslov službene e-pošte vodilnih oseb in tistih zaposlenih, katerih delo je potrebno zaradi poslovanja s strankami.
Pogodbena obdelava	ZVOP-2 bistveno ne spreminja določb Splošne uredbe, ki so nadomestile zahteve ZVOP-1 glede pogodbene obdelave. ZVOP-2 določb glede pogodbene obdelave v smislu ureditve medsebojnega razmerja ter pravic in obveznosti upravljavcev in

	obdelovalcev posebej ali drugače ne ureja – velja Splošna uredba, obdelovalci pa se morajo zavedati, da tudi zanje veljajo tako določbe Splošne uredbe kot številne določbe ZVOP-2 (npr. glede zavarovanja osebnih podatkov, ki so predmet postopka, glede dnevnikov obdelave in varnosti osebnih podatkov na področju posebnih obdelav itd.).
Pooblaščenice osebe za varstvo podatkov (DPO)	Poleg zavezancev po Splošni uredbi morajo pooblaščenice osebo določiti zavezanci po 22. členu ZVOP-2 ter nekateri drugi subjekti zaradi širše definicije javnega sektorja (npr. zasebni vrtci in šole z javnimi programi). Določen je rok za vpis, objavo in sporočanje podatkov Informacijskemu pooblaščenicu (8 dni), že imenovanih ni treba vnovič sporočati. ZVOP-2 določa le osnovne zahteve: poslovna sposobnost, znanje/izkušnje, neobsojenost; DPO državnega organa mora biti iz javnega sektorja, v drugih državnih organih in v zasebnem sektorju pa je lahko DPO zunanji (iz javnega ali zasebnega, s pogodbo). Ne sme biti konflikta interesov, ki je natančneje opredeljen (npr. skrbnik informacijskih sistemov, vodja informacijske varnosti, predstojnik itd.), za določene organe (npr. za sodišča, upravne enote, ministrstva, sindikate) veljajo specifična določila.
Posredovanje osebnih podatkov	V javnem sektorju se posredujejo podatki, če obstaja podlaga v skladu s Splošno uredbi, ter na podlagi zahteve po prvem odstavku 41. člena ZVOP-2, razen če drug zakon določa drugače. Prejemnik sme osebne podatke obdelovati samo za namen, za uresničevanje katerega se mu posredujejo, posredujejo pa se brezplačno, če zakon ne določa drugače. V zasebnem sektorju, če je podana podlaga in ustrezna zahteva. 41. člen opredeljuje zahtevo, ki mora vsebovati naslednje podatke: vlagatelj, pravna podlaga, namen, katere podatke se posreduje, številka zadeve, navedba organa, oblika in način pridobitve; za posredovanje je določen rok 15 dni od popolne zahteve, ob zavrnitvi/molku lahko zahteva vlagatelj zahteve odločitev nadzornega organa oz. ima na voljo ima sodno varstvo. Ureditev ne posega v pravico do pregleda in prepisa spisa, zahteva se sledljivost posredovanja (dve leti).
Povezovanje zbirk osebnih podatkov – drugačna ureditev	Dodana je definicija povezovanja (5. člen), ni več zahteve po obveščanju in pridobivanju odločbe Informacijskega pooblaščenca, izrecna zakonska podlaga je zahtevana le za taksativno naštetih zbirke osebnih podatkov. Pred povezovanjem je treba izdelati oceno učinka in se posvetovati z nadzornim organom (87. člen ZVOP-2).
Prehodne določbe	<ul style="list-style-type: none"> · ZVOP-2 dopušča različna časovna obdobja za prilagoditev (od dneva uveljavitve, tj. 26. 1. 2023), in sicer: · Posebni ukrepi za zagotavljanje varnosti osebnih podatkov na področju posebnih obdelav (23. člen) se vzpostavijo v treh letih. · Minister, pristojen za pravosodje, v soglasju z ministrom, pristojnim za zdravje, po predhodnem mnenju nadzornega organa sprejme pravilnik o zaračunavanju stroškov v treh mesecih (peti odstavek 17. člena). · Pooblaščenice osebe, ki so jih do uveljavitve ZVOP-2 določili predstojniki organov v sestavi ministrstev, nadaljujejo opravljanje dela pooblaščenice osebe po ZVOP-2. · Prekrškovni postopki, ki so se začeli pri Informacijskem pooblaščenicu ali na sodiščih pred uveljavitvijo ZVOP-2, se končajo v skladu z ZVOP-1, razen če je ZVOP-2 za storilca milejši. Postopki inšpekcijskega nadzora, začeti na podlagi ZVOP-1 se nadaljujejo v skladu z ZVOP-2. · Seznam tretjih držav iz 66. člena ZVOP-1 (prenos podatkov v tretje države) se razveljavi. · Z dnem uveljavitve tega zakona preneha delovati Register zbirk osebnih podatkov pri Informacijskem pooblaščenicu. · Vodenje dnevnikov obdelav se uskladi z 22. členom ZVOP-2 v dveh letih. · Slovenska akreditacija začne izvajati postopke akreditacije 1. 1. 2024; upravljavci vloge vložijo v roku šestih mesecev po poteku roka iz prvega odstavka 121. člena. · Videonadzor v prevoznih sredstvih, namenjenih javnemu potniškemu prometu, se uskladi z določbami 79. člena ZVOP-2 v roku šest mesecev. · Ni treba vnovič posredovati informacij, če se podatki o pooblaščenih osebah niso spremenili. · Veljati prenehajo:

	<ul style="list-style-type: none"> - Pravilnik o metodologiji vodenja registra zbirk osebnih podatkov (Uradni list RS, št. 28/05 in 30/11); - Pravilnik o pridobivanju potrebnih informacij za odločanje o iznosu osebnih podatkov v tretje države (Uradni list RS, št. 79/05); - Pravilnik o zaračunavanju stroškov pri izvrševanju pravice posameznika do seznanitve z lastnimi osebnimi podatki (Uradni list RS, št. 85/07 in 5/12). <p>Do sprememb določb o višinah in razponih glob, ki jih določa zakon, ki ureja prekrške, se globe za kršitve po 83. členu Splošne uredbe izrekajo v skladu s 83. členom Splošne uredbe.</p>
Prenosi osebnih podatkov v tretje države	Razveljavi se seznam tretjih držav po ZVOP-1 in ustrezni pravilnik, ostaja ureditev za zavezance, za katere se Splošna uredba ne uporablja, sicer za prenose veljajo določbe Splošne uredbe.
Prijavitelj s posebnim položajem	Če oseba prijavi kršitve <i>svojih</i> pravic, lahko dobi status prijavitelja s posebnim položajem. Vlogo mora oddati po ZUP, nadzorni organ ima tri mesece za odločitev, sproti ga obvešča o ukrepih in stanju zadeve (glej 30. do 34. člen ZVOP-2).
Rok hrambe osebnih podatkov	21. člen ZVOP-1 se vsebinsko bistveno ne spreminja. V 43. členu ZVOP-2 so podobne določbe, bistvena je nova zahteva, da mora upravljavec ob upoštevanju narave obdelovanih podatkov in tveganj občasno in na dokumentiran način preverjati, ali se upoštevajo določbe omejevanja roka hrambe.
Sankcije	Kazenske določbe ZVOP-1 prenehajo veljati, s sprejemom ZVOP-2 bo možno izrekanje sankcij po Splošni uredbi, v višini, kot jo določa uredba. Določene so kazni za kršitve določb ZVOP-1, kazni se lahko izrekajo tudi odgovornim osebam (poleg pravnih oseb).
Sledljivost obdelav osebnih podatkov	ZVOP-2 sledljivost obdelav poimenuje »dnevnik obdelav«, izrecno se zahtevajo za določene zbirke (22. člen ZVOP-2), določeno je, kaj je treba voditi v njih, za katera dejanja obdelave, za kaj se lahko uporabljajo ter krajši rok hrambe (22. člen ZVOP-2). Sledljivost se zahteva tudi za dostop in uporabo videonadzornih posnetkov (76. člen ZVOP-2).
Splošno sodno varstvo pravic posameznika	<p>Na novo urejeno v 11. členu ZVOP-2. Posameznik lahko zahteva sodno varstvo svojih pravic ves čas trajanja kršitve, brez predhodnega uveljavljanja pravic po drugih določbah tega zakona ali uporabe drugih pravnih sredstev.</p> <p>Posameznik lahko s sodnim varstvom poleg prenehanja kršitve in vzpostavitve zakonitega stanja zahteva tudi povrnitev škode. Če je kršitev prenehala, lahko posameznik s tožbo zahteva ugotovitev, da je kršitev obstajala.</p> <p>Odloča upravno sodišče po Zakonu o upravnem sporu, posameznik lahko v tožbo vključi tudi odškodninski zahtev.</p> <p>V postopku pred upravnim sodiščem je javnost izključena, če sodišče na predlog posameznika iz utemeljenih razlogov ne odloči drugače. Se ne uporablja za postopke proti upravljavcem ali obdelovalcem glede obdelav osebnih podatkov s področja varnosti države.</p>
Strokovni nadzor	Strokovni nadzor je podrobneje opredeljen (89., 90. in 91. člen ZVOP-2). Izvajalec strokovnega nadzora obdeluje vse osebne podatke, ki jih obdelujejo upravljavci osebnih podatkov, nad katerimi izvaja strokovni nadzor; ima pravico do vpogleda, izpisa, prepisovanja ali kopiranja, dolžan je varovati njihovo tajnost. V poročilu ali oceni ob zaključku zapiše le tiste osebne podatke, ki so nujni za doseg namena strokovnega nadzora. Stroške vpogleda, izpisa, prepisovanja ali kopiranja krije upravljavec. Določena je ureditev obveščanja in možnost kontaktiranja drugih oseb. Če se obdelujejo posebne vrste osebnih podatkov, se naredi uradni zaznamek ali drug uradni zapis v zadevo organa.
Uveljavljanje pravic posameznika	Glede pravic ali zahtev posameznika velja Splošna uredba in 2. poglavje I. dela ZVOP-2 (12. do 20. člen). Smiselno se uporablja ZUP, veljajo roki iz Splošne uredbe. ZVOP-2 določa: postopek obravnavanja zahtevkov (13. in 14. člen), sestavine odločbe (15. člen). Kadar upravljavec zahtevi ugodni, ne izda posebne odločbe, temveč o tem napravi uradni

	<p>zaznamek in posameznika seznaniti z odločitvijo. Kadar upravljavec zahtevi ne ugotovi, izda odločbo, ki poleg sestavin po ZUP vsebuje tudi sestavine, ki jih določa ZVOP-2. Če posameznik to zahteva, ga lahko upravljavec z osebnimi podatki seznaniti tudi ustno. Seznanitev z osebnimi podatki je brezplačna (razen če gre za očitno neutemeljene ali pretirane stroške, v tem primeru lahko upravljavec zahtevi ugotovi in zaračuna razumne stroške, tj. samo materialne stroške posredovanja informacij, sporočil, odgovorov oz. izvajanja zahtevanega ukrepanja; pravilnik bo urejal višino stroškov, način zaračunavanja, obveščanja o stroških). Posameznika bo o možnih stroških treba obvestiti vnaprej.</p>
<p>Varstvo osebnih podatkov umrlih oseb</p>	<p>Določbe so podobne tistim iz ZVOP-1, a deloma spremenjene. Podatki o umrlih se posredujejo uporabnikom, ki so za obdelavo pooblaščenici z zakonom, in tistim uporabnikom, ki izkažejo pravni interes za uveljavljanje pravic pred subjekti javnega sektorja. Na njihovo zahtevo tudi zakoncu, zunajzakonskemu partnerju, otrokom, staršem ali dedičem, če umrli posameznik upravljavcu posredovanja ni pisno prepovedal ali če drug zakon ne določa drugače. Ureja se tudi uporaba za namene znanstvenega raziskovanja, zgodovinskega raziskovanja, za izobraževalne, statistične ali arhivske namene ter za objavo ali drugo obdelavo v zgodovinskih in drugih izobraževalnih publikacijah.</p> <p>Določbe ZVOP-2 se uporabljajo za osebne podatke umrlih 20 let po njihovi smrti, če drug zakon ne določa drugače.</p>
<p>Videonadzor</p>	<p>Nameni uvedbe videonadzora ostajajo podobni, prav tako zahteva, da se objavi (bolj podrobno) obvestilo, seznaniti zaposlene, sprejme pisni sklep o uvedbi. Ni več posebne ureditve videonadzora večstanovanjskih stavb (blokovi), obvestilo mora imeti več informacij (nekateri lahko na spletu), prepovedan je v hotelskih sobah in podobnih prostorih, kjer upravičeno pričakujemo večjo stopnjo zasebnosti. Na novo se ureja videonadzor potniškega prometa in videonadzor na javnih površinah. Videonadzor lahko uporablja samo pooblaščenico osebje, voditi je treba sledljivost uporabe in dostopov. Pri nadzoru znotraj delovnih prostorov se zahteva posvetovanje s predstavniki sindikatov, pri nadzoru cest pa sta zahtevana ocena učinka in mnenje Informacijskega pooblaščenca. Na javnih površinah je prepovedana uporaba sistemov za avtomatsko prepoznavo registrskih tablic in biometrije, če drug zakon ne določa drugače.</p>
<p>Zavarovanje občutljivih osebnih podatkov pri prenosu po nezavarovanih elektronskih poteh</p>	<p>Ni več zahteve, da morajo biti občutljivi osebni podatki (npr. zdravstveni podatki, članstvo v sindikatu) šifrirani pri pošiljanju po nezavarovanih elektronskih poteh (npr. prek navadne e-pošte).</p>
<p>Zavarovanje osebnih podatkov, ki so predmet postopka</p>	<p>ZVOP-2 vsebuje tudi določbe, ki se nanašajo na zavarovanje osebnih podatkov, ki so predmet postopka (21. člen ZVOP-2) – gre za to, kdaj in kako morajo upravljavci osebnih podatkov v primeru, da so določeni osebni podatki zahtevani v določenem postopku (npr. inšpekcijskem, v postopku zahteve posameznika za dostop do lastnih podatkov ipd.), zaščititi zahtevane podatke. Bistveno je, da zavezanec potrebnih podatkov ne sme izbrisati ali spremeniti, dokler traja postopek (do pravnomočnosti odločitve).</p>

3.5.2 OZAVEŠČANJE OB SPREJEMU ZVOP-2

Informacijski pooblaščenec je v letu 2023 nadaljeval s številnimi preventivnimi aktivnostmi, katerih cilj je zagotavljanje skladnosti s predpisi brez potreb po uvajanju inšpekcijskih postopkov. Pomemben del aktivnosti se je nanašal na ozaveščanje splošne in strokovne javnosti glede sprememb, ki jih je prinesel ZVOP-2, saj to pomeni, da morajo zavezanci spoštovati tako Splošno uredbo kot ZVOP-2.

Informacijski pooblaščenec je najprej pripravil obsežno vsebinsko prenovo spletne strani, s katero je želel na razumljiv način pojasniti, kaj ureja ZVOP-2, kdaj stopijo obveznosti po ZVOP-2 v veljavo in kakšne so prehodne določbe, ter podati primerjavo določb ZVOP-1 in ZVOP-2. Spletno stran je bila posodobljena, objavljene so bile obrazložitve posameznih ključnih delov ZVOP-2, povezave do smernic in drugih uporabnih gradiv. Posodobljene so bile informacije o ključnih vidikih novega zakona, in sicer³:

- [Privolitev](#),
- [Pogodbena obdelava](#),
- [Videonadzor](#),
- [Biometrija](#),
- [Varnost podatkov](#),
- [Prijava kršitev varnosti](#),
- [Pooblaščenec osebe za varstvo osebnih podatkov \(DPO\)](#),
- [Ocene učinka na varstvo osebnih podatkov](#),
- [Obveščanje posameznikov o obdelavi](#),
- [Povezovanje zbirk osebnih podatkov](#),
- [Prenos osebnih podatkov v tretje države in mednarodne organizacije](#),
- [Evidenca dejavnosti obdelave](#),
- [Pravice posameznika](#),
- [Pristojnosti Informacijskega pooblaščenca](#),
- [Inšpekcijski nadzor oz. nadzorni postopki](#),
- [Kodeksi ravnanja](#).

Posebno pozornost je bila v letu 2023 zaradi sprejema ZVOP-2 namenjena tudi prenovi in posodobitvi smernic Informacijskega pooblaščenca. Objavljene so bile naslednje prenovljene smernice⁴:

- Smernice za upravnike večstanovanjskih stavb,
- Smernice o uporabi piškotkov in podobnih sledilnih tehnologij,
- Smernice glede izvajanja videonadzora,
- Smernice za organizatorje dogodkov,
- Smernice glede biometrije po ZVOP-2,
- Smernice glede prenosa osebnih podatkov v tretje države in mednarodne organizacije.

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, povezanih z varstvom osebnih podatkov. Ocene učinkov se zlasti pomembne, kadar gre za nove projekte, ki predvidevajo množično obdelavo osebnih podatkov, še posebej kadar gre za uporabo modernih tehnologij, za ranljive skupine posameznikov ali za obdelavo posebnih vrst osebnih podatkov. V postopku predhodnega posvetovanja, kot ga opredeljuje 36. člen Splošne uredbe, lahko zavezanci svoje ocene učinka na varstvo osebnih podatkov pošljejo v predhodno mnenje Informacijskemu pooblaščenca ter tako pridobijo stališča in priporočila glede izdelanih ocen učinka. Slednje so namreč zlasti pri velikih

³ Posamezne alineje na seznamu vsebujejo hiperpovezave na ustrezno mesto na spletni strani Informacijskega pooblaščenca.

⁴ Smernice so dostopne na povezavi: <https://www.ip-rs.si/publikacije/prilo%C4%8Dniki-in-smernice/>.

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 lahko opozori na neidentificirana tveganja ter pomanjkljive ukrepe za obvladovanje teh tveganj, s pravočasnim obvladovanjem tveganj pa se lahko zavezanci izognejo občutnim stroškom popravljalnih ukrepov, visokim sankcijam zaradi kršitev ter okrnitvi ali celo izgubi ugleda pri strankah in v javnosti.

Pomembno novost na področju ocen učinka je prinesla predvsem določba tretjega odstavka 24. člena ZVOP-2, ki uvaja t. i. zakonodajne ocene učinka. Omenjena določba od predlagateljev predpisov zahteva, da kadar se z zakonom določa obdelava osebnih podatkov, za katero je treba izdelati oceno učinka, predlagatelj predpisa izvede zakonodajno oceno učinka in jo posreduje v predhodno posvetovanje Informacijskemu pooblaščenca. Posledično se je občutno povečalo število prejetih ocen učinka glede varstva osebnih podatkov. Če je bilo v letu 2022 izdanih 14 mnenj na ocene učinka (za primerjavo, v letu 2021 je bilo izdanih zgolj šest mnenj), se je v letu 2023 število izdanih mnenj na ocene učinka več kot podvojilo – Informacijski pooblaščenec je v postopku predhodnega posvetovanja izdal 29 mnenj.

ZVOP-2 poleg zakonodajnih ocen učinka določa dodatne obveznosti glede ocene učinka, in sicer glede naslednjih področij:

- vodenje dnevnikov obdelav in ocena učinka (22. in 24. člen ZVOP-2),
- obdelava osebnih podatkov za raziskovalne namene (69. člen ZVOP-2),
- videonadzor cestnega prometa (80. člen ZVOP-2),
- ocena učinka pri povezovanju zbirk osebnih podatkov (87. člen ZVOP-2).

Posebej je urejeno tudi področje varnosti države, in sicer za obdelavo osebnih podatkov na področju varnosti države pristojni organ s področja varnosti države pripravi oceno učinka s smiselno uporabo določb tega člena.

V letu 2023 je Informacijski pooblaščenec v postopku predhodnega posvetovanja izdal mnenja glede naslednjih tem na t. i. projektne ocene učinka:

- Mnenje glede ocene učinkov na varstvo osebnih podatkov v zvezi z razvojem platforme na področju preprečevanja pranja denarja,
- Mnenje glede ocene učinka v zvezi z uvedbo sistema inteligentne analitike za štetje objektov pred informacijskimi zasloni,
- Mnenje glede ocene učinkov na varstvo osebnih podatkov v zvezi z informacijskim sistemom državnega odvetništva,
- Povezovanje zbirk v javnem sektorju,
- Mnenje glede ocene učinkov v zvezi z videonadzorom javnih površin,
- Mnenje glede ocene učinkov na varstvo osebnih podatkov v zvezi s postavitvijo sistema za parkiranje z uporabo sistema prepoznave registrskih tablic (ANPR),
- Mnenje glede ocene učinkov v zvezi z varstvom osebnih podatkov pri vzpostavitvi sistema poslovne analitike v državni upravi,
- Mnenje glede ocene učinka na varstvo podatkov pri elektronskem pridobivanju podatkov Zemljiške knjige v postopkih varstva kulturne dediščine na podlagi Zakona o varstvu kulturne dediščine (ZVKD-1),
- Mnenje glede ocene učinkov v zvezi z varstvom osebnih podatkov, obdelovanih v okviru digitalne platforme pametnega mesta,
- Mnenje glede ocen učinkov v zvezi z videonadzorom javnih površin (mestnih tržnic),
- Mnenje glede ocene učinka na varstvo podatkov v zvezi z aplikacijo prekrškovnega organa,
- Mnenje glede ocene učinkov na varstvo osebnih podatkov v zvezi s postavitvijo avtomatske zapornice pri vstopu v krajinski park,

- Mnenje glede ocene učinkov na varstvo osebnih podatkov v zvezi z vzpostavitvijo multimedijskega kontaktne centra za informiranje strank.

V letu 2023 smo izdali mnenja glede naslednjih zakonodajnih ocen učinka:

- Mnenje glede ocene učinka na varstvo podatkov v zvezi z 12. členom Predloga zakona o spremembah in dopolnitvah Zakona o gospodarskih družbah (ZGD-1L; EVA 2023-2180-0001),
- Mnenje glede ocene učinka na varstvo podatkov v zvezi s Predlogom Zakona o spremembah in dopolnitvah Zakona o nadzoru državne meje (dve mnenji),
- Mnenje glede ocene učinka na varstvo podatkov v zvezi s predlogom Zakona o začasni zaščiti razseljenih oseb (dve mnenji),
- Mnenje glede ocene učinka na varstvo podatkov v zvezi z avtomatiziranim pridobivanjem podatkov o obdelavi podatkov oseb (dve mnenji),
- Mnenje glede ocene učinka na varstvo podatkov v zvezi s predlogom Zakona o spremembah in dopolnitvah Zakona o finančnem poslovanju, postopkih zaradi insolventnosti in prisilnem prenehanju,
- Mnenje glede ocene učinka na varstvo podatkov v zvezi s Predlogom Zakona o spremembah in dopolnitvah Zakona o sodnem registru (EVA 2022 2030 0007),
- Mnenje glede ocene učinka na varstvo podatkov v zvezi z osnutkom predloga sprememb ZOFVI – ureditev obdelave osebnih podatkov iz zbirk o gibalnih sposobnostih in morfoloških značilnostih, ki jih vodijo šole po področnih zakonih, in pripadajoča ocena učinkov v zvezi z varstvom osebnih podatkov,
- Mnenje glede ocene učinka na varstvo podatkov v zvezi s predlogom Zakona o letalstvu,
- Mnenje glede ocene učinka na varstvo osebnih podatkov v zvezi s predlogom Zakona o nujnih ukrepih na področju zdravstvenega varstva,
- Mnenje glede ocene učinka na varstvo osebnih podatkov v zvezi s Predlogom Zakona o Zdravstvenem informacijskem sistemu.

Ocenjujemo, da je vključitev zahteve po zakonodajnih ocenah učinka na varstvo osebnih podatkov v ZVOP-2 (24. člen) bistveno vplivala na višjo kakovost predpisov z vidika upoštevanja pravice do varstva osebnih podatkov, težave pa se kažejo v pravočasnosti priprave zakonodajnih ocen učinka.

PRIMERI

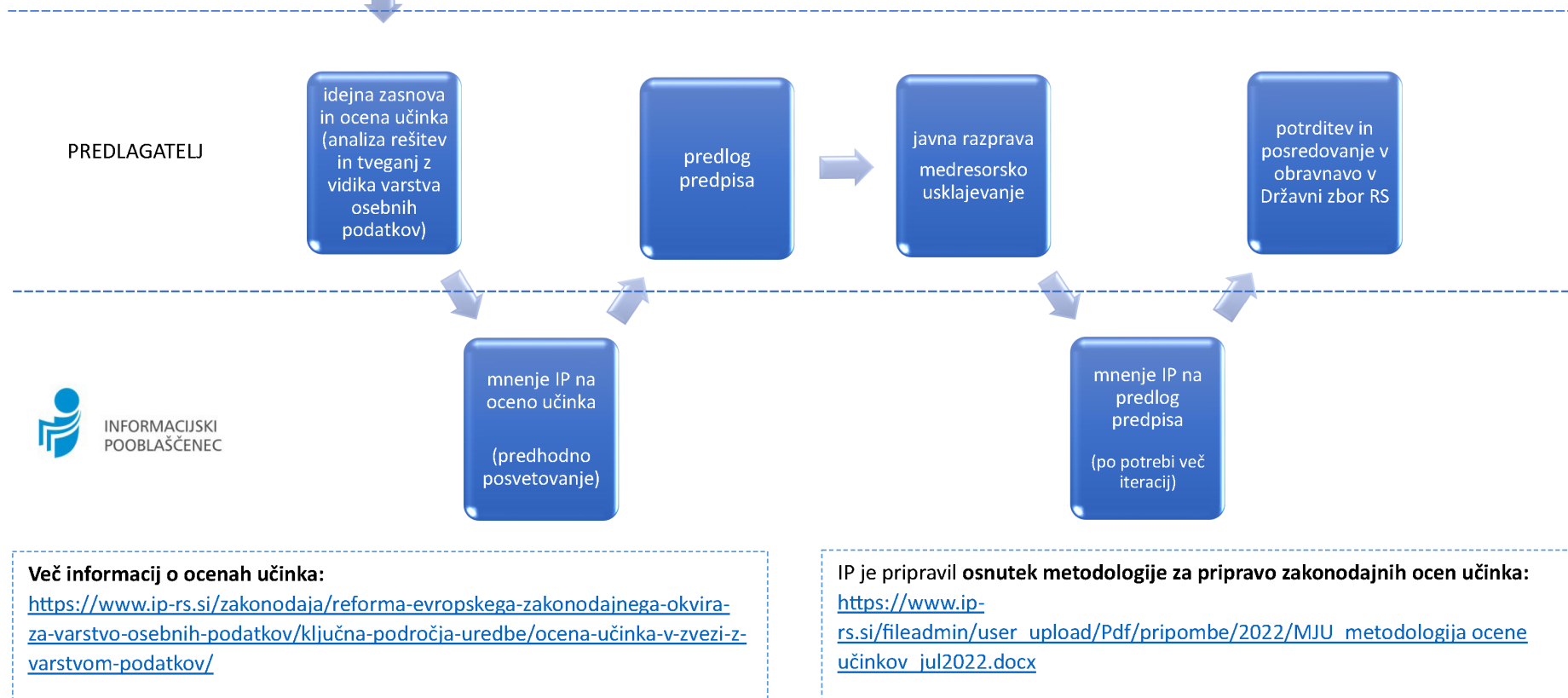
- digitalizacija zdravstva
- povezovanje zbirk
- uvajanje novih informacijskih sistemov
- avtomatizirano odločanje
- obdelava posebnih vrst osebnih podatkov

problematika, ki terja zakonsko urejanje

Ocene učinkov na varstvo osebnih podatkov pri pripravi predpisov (zakonodajne ocene učinka)

Ocena učinkov je orodje za pravočasno **identifikacijo, analizo in zmanjševanje tveganj glede nezakonitih ravnanj z osebnimi podatki**. 24. člen **ZVOP-2** določa zahtevo po ocenah učinka pri pripravi zakonov: kadar se z zakonom določa obdelava osebnih podatkov, za katero je treba izdelati oceno učinka, predlagatelj predlogu zakona priloži oceno učinka v skladu s 35. členom Splošne uredbe (»zakonodajne ocene učinka«). Prav tako ZVOPOKD v 49. členu za določene primere zahteva izvedbo takšne zakonodajne ocene učinka.

Namen **zakonodajnih ocen učinka** je, da se še pred oblikovanjem dokončnega besedila členov opravi **pravočasne razmisleke** o tem, kako **ustrezno upoštevati temeljna načela varstva osebnih podatkov pri določanju besedila zakona**. Te razmisleke (npr. ali je za doseg ciljev zakona resnično treba obdelovati osebne podatke, kakšne namene zasledujemo, kateri nabor osebnih podatkov je potreben, katere ukrepe je treba vključiti za zagotovitev zakonite in poštene obdelave, kakšne varovalke moramo vključiti v zakon, ali bo šlo za povezovanje zbirk podatkov, določitev rokov hrambe ipd.) se **opiše v oceni učinkov**, jo pošlje IP v mnenje (v t.i. **predhodno posvetovanje**) in na podlagi mnenja IP oblikuje (bolj) dokončno besedilo členov, ki gre lahko nato v medresorsko usklajevanje.



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 osebja naj bi izvajala svetovalne in nadzorne naloge na področju varstva osebnih podatkov ter delovala kot notranji revizor za varstvo osebnih podatkov, ki poleg nadzora upravljavce in obdelovalce opozarja na njihove obveznosti ter izobražuje in ozavešča zaposlene.

Do konca leta 2023 je bilo Informacijskemu pooblaščenju sporočenih 3340 pooblaščenih oseb za varstvo podatkov. Podatke o pooblaščenih osebja za varstvo osebnih podatkov je možno enostavno sporočiti in popraviti s pomočjo spletnega obrazca <https://www.ip-rs.si/pooblastcene-osebe>. Ocenjujemo, da je večina zavezancev izpolnila dolžnosti glede posredovanja podatkov o pooblaščenih osebja v register pooblaščenih oseb, zato gre z vidika registra zdaj v pretežni meri za vzdrževalne aktivnosti ob spremembah podatkov (npr. ob razrešitvi ali imenovanju novih pooblaščenih oseb).

3.5.5 AKTIVNOSTI IZOBRAŽEVANJA IN OZAVEŠČANJA

Tudi v letu 2023 je Informacijski pooblaščenec uporabnikom na prijazen način podajal najpomembnejše informacije o ključnih področjih zakonodaje na podstrani Ključna področja⁵, kjer so posamezne teme (npr. pogodbeno obdelava osebnih podatkov) obdelane na razumljiv način, uporabnik pa ima na enem mestu podane ključne informacije o tem področju, napotitve na relevantne člene Splošne uredbe in ZVOP-2 ter povezavo do uporabnih gradiv, kot so smernice (Informacijskega pooblaščenca in EOVP), infografike, vzorci in obrazci.

Informacijski pooblaščenec je pripravil tudi tri nove infografike (ocene učinkov na varstvo osebnih podatkov pri pripravi predpisov (zakonodajne ocene učinka), o potrjevanju in akreditaciji po Splošni uredbi in ZVOP-2 ter o konceptu osebnih podatkov). Infografike lahko zavezanci prosto uporabijo tudi v okviru svojih izobraževalnih aktivnosti.

Informacijski pooblaščenec je tudi v letu 2023 redno izdajal mnenja za splošno in strokovno javnost – izdal je 1011 pisnih mnenj na zaprosila posameznikov in organizacij⁶ ter 93 pripomb na predpise⁷. Če je bilo izdano mnenje na oceno učinka ob mnenju na predlog predpisa, je objavil tudi mnenje na oceno učinka. Prenovili smo tudi iskalnik po pisnih mnenjih, tako da je sedaj mogoče ločeno iskanje po mnenjih iz časa pred Splošno uredbo, po sprejemu Splošne uredbe in pred sprejemom ZVOP-2 ter po mnenjih, ki so bila izdana po sprejemu ZVOP-2. Poleg pisnih mnenj je bilo opravljenih tudi 1569 svetovanj po telefonu.

Evropski dan varstva osebnih podatkov, ki ga vsako leto obeležujemo 28. januarja, je Informacijski pooblaščenec leta 2023 obeležil z organizacijo dogodka, katerega rdeča nit je bila uveljavitev novega Zakona o varstvu osebnih podatkov (ZVOP-2). Informacijska pooblaščenka je predstavila bistvene izzive v času uporabe Splošne uredbe o varstvu podatkov brez ZVOP-2 in z ZVOP-2, sledila pa je okrogla miza s strokovnjaki s področja varstva osebnih podatkov. Udeleženci so med drugim predstavili svoje poglede na sam postopek sprejema ZVOP-2, posamezne določbe zakona, izrekanje sankcij pred in po sprejemu ZVOP-2 ter bistvene novosti za zavezance, posameznike in nadzorni organ.

Tudi v letu 2023 je Informacijski pooblaščenec podelil priznanja organizacijam, ki so v preteklem letu pridobile certifikat po standardu ISO/IEC 27001:2013 s področja informacijske varnosti. Slednjega

⁵ <https://www.ip-rs.si/zakonodaja/reforma-evropskega-zakonodajnega-okvira-za-varstvo-osebni-podatkov/klju%C4%8Dna-podro%C4%8Dja-uredbe/>

⁶ Mnenja so dostopna na povezavi: <https://www.ip-rs.si/mnenja-zvop-2/>.

⁷ Mnenja so objavljena na povezavi: <https://www.ip-rs.si/zakonodaja/pripombe-informacijskega-poobla%C5%A1%C4%8Denca-na-predloge-predpisov/>.

je v letu 2022 pridobilo rekordno število organizacij – 30. S pridobitvijo certifikata dobitniki izkazujejo veliko stopnjo zavedanja o pomenu varovanja informacij in s tem tudi osebnih podatkov ter sistematično vlagajo v ustrezne ukrepe za zagotovitev varnosti podatkov, Informacijski pooblaščenec pa s podelitvijo posebnih priznanj promovira najbolj uveljavljen standard na področju varovanja informacij ter s tem tudi osebnih podatkov.

Tradicionalno je bilo podeljeno tudi priznanje ambasador zasebnosti, ki ga je za leto 2022 prejel izr. prof. dr. Blaž Markelj, predstojnik Katedre za informacijsko varnost na Fakulteti za varnostne vede Univerze v Mariboru, in sicer za uspešno povezovanje deležnikov, organizacijo aktualnih konferenc in delo z mladimi na področju informacijske varnosti.

Kot vsako leto je bilo izvedeno tudi veliko število pro bono predavanj na področju varstva osebnih podatkov, in sicer je bilo takih predavanj v letu 2023 kar 73. Informacijski pooblaščenec je veliko pozornosti namenil ozaveščanju zavezancev glede dolžnosti, ki jih je prinesel ZVOP-2: med drugim je bilo organiziranih več ponovitev predavanj za javni sektor, ki se jih je udeležilo več kot 1000 udeležencev, poseben seminar pa je bil organiziran tudi na temo uveljavljanja pravic posameznikov po Splošni uredbi in ZVOP-2. Predstavniki informacijskega pooblaščenca so aktivno sodelovali na konferencah, seminarjih in drugih dogodkih.

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, vsak mesec pa naročnikom ne e-novice pošlje novičnik s povezavami do aktualnih vsebin, mnenj in drugih objav s področja svojega delovanja. Na omrežju LinkedIn, ki je namenjeno strokovni javnosti, objave Informacijskega pooblaščenca spremlja 1871 sledilcev, na omrežju Facebook, ki je namenjeno predvsem splošni javnosti, pa 2232 sledilcev. V letu 2023 je Informacijski pooblaščenec:

- objavil 52 sporočil na omrežju LinkedIn,
- objavil 36 objav na omrežju Facebook ter
- poslal 12 novičnikov.

3.5.6 PREVENTIVNE AKTIVNOSTI ZA SKLADNOST

Tudi v letu 2023 je Informacijski pooblaščenec izvajal preventivne aktivnosti za skladnost (angl. *privacy sweep*), in sicer je sodeloval v prvi usklajeni akciji sodelovanja (*Coordinated Enforcement Framework – CEF*) Evropskega odbora za varstvo podatkov (EOVP) na temo pooblaščenih oseb za varstvo osebnih podatkov. Vabilo k izpolnitvi usklajenega vprašalnika smo posredovali celotnemu registru pooblaščenih oseb in prejeli skoraj 1000 odgovorov. Nadzorni organi za varstvo osebnih podatkov smo nato vsak v svoji državi analizirali stanje in pripravili ukrepe za izboljšanje stanja, kot izhajajo iz enotnega poročila⁸. Na seznamu priporočil in ukrepov so predlogi za dvig sredstev, ki jih organizacije namenjajo delu pooblaščenih oseb, več izobraževanj ter ukrepi za izogibanje konfliktu interesov.

Informacijski pooblaščenec je izvedel tudi preventivno aktivnost za zagotavljanje skladnosti na področju uvajanja GPS-sistemov pri podjetjih s področja komunalnega gospodarstva; ukrep je preko Zbornice komunalnega gospodarstva naslovil več kot 100 zavezancev, aktivnost pa je bila potrebna predvsem zato, ker se na tem področju zadevni sistemi čedalje bolj uporabljajo, težave pa se ob odsotnosti izrecne zakonske ureditve področja kažejo predvsem glede spoštovanja načela sorazmernosti in transparentnosti.

⁸ Poročilo je dostopno na povezavi: https://www.edpb.europa.eu/system/files/2024-01/edpb_report_20240116_cef_dpo_en.pdf.

Konec leta 2023 je bila izvedena tudi preventivna aktivnost za zagotavljanje skladnosti na področju obveščanja posameznikov (13. člen Splošne uredbe) glede obdelav osebnih podatkov pri merjenju hitrosti, v okviru katere smo naslovili 45 zavezancev na področju občinskih ter medobčinskih redarstev, inšpektoratov in služb. Obveščanje posameznikov glede obdelave osebnih podatkov, kot to zahteva 13. oz. 14. člen Splošne uredbe, ostaja eno od področij, kjer v praksi zaznavamo precej pomanjkljivosti, saj informacije za posameznike pogosto niso celovite, obenem pa se kaže, da je treba več pozornosti nameniti tudi samemu načinu obveščanja, saj 12. člen Splošne uredbe zahteva, da so informacije za posameznike podane v jasnem in razumljivem jeziku ter na enostaven in dostopen način.

3.6. MEDNARODNO SODELOVANJE

3.6.1 SODELOVANJE V EVROPSKEM ODBORU ZA VARSTVO PODATKOV

Evropski odbor za varstvo podatkov (EOVP) je neodvisen evropski organ, ustanovljen s Splošno uredbo o varstvu podatkov; njegov glavni cilj je zagotoviti dosledno, usklajeno in učinkovito izvajanje pravil o varstvu osebnih podatkov po celotni Evropski uniji. EOVP sestavljajo predstavniki nacionalnih nadzornih organov iz vseh držav članic EU, vključno s Slovenijo, ter Islandije, Lihtenštajna in Norveške, ki so del Evropskega gospodarskega prostora (EGP). Glavni namen EOVP je varovati temeljne pravice posameznikov skozi varstvo osebnih podatkov v digitalni dobi, omogočiti prost pretok osebnih podatkov v EU in hkrati zagotoviti njihovo varstvo. Sodelovanje Slovenije v odboru predstavlja pomemben del njenih prizadevanj za spodbujanje mednarodnega sodelovanja na področju varstva osebnih podatkov. V letu 2023 je predsedovanje EOVP prevzela Anu Talus, predstojnica nadzornega organa za varstvo podatkov iz Finske.

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 EOVP za zagotavljanje dosledne uporabe evropske zakonodaje o varstvu podatkov (po 64. členu 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 65. členu 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 66. členu Splošne uredbe) s sprejemom začasnih ukrepov v izjemnih primerih, ko je ukrepanje potrebno zaradi varstva pravic in svoboščin posameznikov.

EOVP je razdeljen na dva glavna dela, in sicer na plenarno zasedanje in ekspertne podskupine. Plenarno zasedanje je organ odločanja EOVP, ki je odgovoren za sprejemanje smernic, mnenj, priporočil in drugih dokumentov, povezanih z varstvom osebnih podatkov. Predstavniki Informacijskega pooblaščenca so v letu 2023 aktivno sodelovali na 15 plenarnih zasedanjih. Ekspertne podskupine pa so bile ustanovljene posebej za obravnavo pomembnih tem, povezanih z varstvom osebnih podatkov. Njihovi člani delujejo tudi v okviru različnih delovnih skupin, ustanovljenih glede na potrebe po usklajevanju glede specifičnih tem. V letu 2023 so predstavniki Informacijskega pooblaščenca delovali v 11 rednih ekspertnih podskupinah ter v 12 posebnih delovnih ter koordinacijskih skupinah oz. odborih glede specifičnih tem. Udeležili so se 147 sestankov.

Plenarno zasedanje poteka mesečno, prav tako se mesečno sestajajo ekspertne podskupine, da razpravljajo o aktualnih vprašanjih, povezanih z varstvom osebnih podatkov, ter glede na področje svojega dela pripravljajo smernice in mnenja odbora, poleg tega 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. Predstavniki vseh nadzornih organov, vključno s predstavniki Informacijskega pooblaščenca, se teh srečanj udeležujejo fizično v Bruslju ali virtualno.

Srečanja in s tem sodelovanje vseh nadzornih organov v okviru EOVP so bistveni za zagotavljanje doslednega izvajanja Splošne uredbe po vsej EU in za usklajevanje prizadevanj nacionalnih organov za učinkovito varstvo osebnih podatkov. S sodelovanjem na teh srečanjih Slovenija prispeva k oblikovanju pomembnih smernic in priporočil v zvezi z varstvom osebnih podatkov ter je na tekočem z najnovejšimi dognanji na tem hitro razvijajočem se področju.

Ekspertna podskupina za meje, potovanja in kazenski pregon ima ključno vlogo pri obravnavi zapletenih pravnih in tehničnih vprašanj, povezanih s čezmejnimi kazenskimi pregoni in varnostnim sodelovanjem na področju varstva osebnih podatkov. Osredotoča se na zagotavljanje smernic o temah, kot so: direktiva o kazenskem pregonu (t. i. LED direktiva), čezmejne zahteve za e-dokaze, odločitve na podlagi sklepov o ustreznosti glede prenosov osebnih podatkov v tretjo državo ali mednarodno organizacijo, dostop organov kazenskega pregona in nacionalnih obveščevalnih organov v tretjih državah do podatkov, evidence podatkov o potnikih in mejne kontrole. Njeno delo je pomembno za zagotavljanje učinkovitega čezmejnega sodelovanja organov kazenskega pregona in usklajevanje njihovih prizadevanj, hkrati pa varujejo temeljne pravice in svoboščine posameznikov.

Ekspertna podskupina za skladnost, e-upravo in zdravje je odgovorna za pripravo smernic in priporočil v zvezi s kodeksi ravnanja, certificiranjem in akreditacijo. Poleg tega se podskupina osredotoča na zagotavljanje skladnosti z javnim pravom in politikami e-uprave ter obravnavanje pomislekov v zvezi z obdelavo osebnih podatkov za znanstvenoraziskovalne in zdravstvene namene. Podskupina tesno sodeluje z ekspertno podskupino za tehnologijo in s tem zagotavlja, da so v njeno delo vključene prakse v zvezi z oceno učinka na varstvo osebnih podatkov; s to skupino sodeluje tudi glede vprašanj vgrajene in privzete zasebnosti.

Ekspertna podskupina za sodelovanje se osredotoča predvsem na zagotavljanje učinkovitih mehanizmov sodelovanja med nadzornimi organi, vzpostavljenih s Splošno uredbo. Njene glavne naloge vključujejo zagotavljanje smernic o postopkovnih vprašanjih, povezanih z mehanizmom sodelovanja, ter proučevanje mednarodne medsebojne pomoči in drugih orodij sodelovanja za uveljavljanje Splošne uredbe zunaj EU.

Ekspertna podskupina za izvrševanje je odgovorna za zagotavljanje učinkovitega izvrševanja Splošne uredbe. Pri tem analizira praktične izkušnje s VI., VII. in VIII. poglavjem Splošne uredbe ter ugotavlja, ali so potrebne dodatne smernice in pojasnila. Poleg tega podskupina spremlja nadzorne dejavnosti in zagotavlja smernice o praktičnih vprašanjih v zvezi z nadzori, vključno z izmenjavo mnenj o konkretnih primerih. Podskupina tesno sodeluje s podskupino za sodelovanje pri posodabljanju obstoječih postopkov sodelovanja in zagotavljanju učinkovitega izvajanja nadzorov. Podskupina je zadolžena za usmerjanje pri praktični uporabi VII. in VIII. poglavja Splošne uredbe, tesno pa sodeluje tudi z delovno skupino za upravne globe. Podskupina je odgovorna tudi za postopke po 65. in 66. členu Splošne uredbe v zvezi s čezmejnimi primeri.

Ekspertna podskupina za finančne zadeve se osredotoča na področje uveljavljanja načel varstva osebnih podatkov v finančnem sektorju. Sem spada vrsta vprašanj, kot so samodejna izmenjava osebnih podatkov za davčne namene, vpliv t. i. FATCA (Zakona o spoštovanju davčnih predpisov v zvezi z računi v tujini) na varstvo osebnih podatkov ter medsebojno vplivanje evropske direktive o plačilnih storitvah (PSD2 direktiva) in Splošne uredbe. Podskupina se ukvarja tudi z uravnoteženjem varstva osebnih podatkov z obveznostmi, ki jih določajo predpisi o preprečevanju pranja denarja (AML) in preprečevanju terorizma (CTP).

Ekspertna podskupina za mednarodne prenose se ukvarja z zagotavljanjem varnega čezmejnega prenosa osebnih podatkov. Podskupina pregleduje odločitve Evropske komisije o tem, katere države ponujajo ustrezne ukrepe za varstvo osebnih podatkov, zadolžena je tudi za pripravo smernic za javne organe in druge organizacije glede skladnega prenosa osebnih podatkov zunaj EU. Podskupina obravnava tudi uporabo certificiranja in kodeksov ravnanja kot ustreznih orodij za prenos ter zagotavlja informacije o tem, kako se določbe Splošne uredbe ujemajo z drugimi predpisi, ko se podatki prenašajo na mednarodni ravni. Dodatno si člani podskupine izmenjujejo informacije o pregledu zavezujočih poslovnih pravil (BCR) in ad hoc pogodbenih klavzul v skladu s 64. členom Splošne uredbe.

Ekspertna podskupina za uporabnike informacijske tehnologije se osredotoča na razvoj in preizkušanje praktičnih orodij informacijske tehnologije, ki jih uporablja EOVP. Zbira povratne informacije uporabnikov o sistemih informacijske tehnologije in slednje glede na to ustrezno prilagaja. Podskupina razpravlja tudi o drugih poslovnih potrebah, kot so sistemi za tele- in videokonference, sistem IMI (Informacijski sistem za notranji trg) ter druga orodja za podporo delu odbora.

Ekspertna podskupina za ključne določbe se osredotoča na zagotavljanje smernic o temeljnih konceptih in načelih Splošne uredbe. Podskupina ponuja smernice o ključnih določbah v I. in II. poglavju Splošne uredbe, ki zajemajo področje uporabe uredbe in njena temeljna načela, smernice za III. in IV. poglavje, ki obravnavata pravice posameznikov in vlogo pooblaščenca osebe za varstvo podatkov (DPO) ter tudi smernice za IX. poglavje Splošne uredbe, ki obravnava posebne primere obdelave, kot je obdelava za namene arhiviranja ali obdelava v javnem interesu.

Ekspertna podskupina za družbene medije se osredotoča na analizo platform družbenih medijev in funkcij, ki jih te ponujajo, kot so ciljanje uporabnikov, personalizacija, preverjanje istovetnosti uporabnikov, analitika in objavljanje vsebin. Pri tem ocenjujejo dejavnosti obdelav osebnih podatkov, ki so povezane s tovrstnimi funkcionalnostmi in morebitna tveganja, ki jih takšne obdelave predstavljajo za pravice in svoboščine posameznikov. Podskupina razvija tudi smernice in zbira primere dobre prakse za uporabo in ponujanje funkcij družbenih medijev, zlasti iz gospodarskih ali političnih namenov. Člani podskupine pomagajo tudi drugim podskupinam, in sicer tako, da jim predlagajo pomembne teme za izvajanje nadzora ter v sodelovanju z njimi razvijajo vrsto drugih smernic EOVP ali posodablajo že obstoječe smernice.

Ekspertna podskupina za strateško svetovanje zagotavlja smernice o pomembnih vprašanjih, ki zadevajo celoten EOVP. To vključuje razprave o strategiji odbora in o njegovih delovnih programih za različne ekspertne podskupine. Člani podskupine tudi pomagajo razjasniti vprašanja, ki jih druge ekspertne podskupine morda ne uspejo. Ekspertna podskupina za strateško svetovanje deluje kot podporni sistem za celoten EOVP, ki zagotavlja strateške usmeritve glede ključnih vprašanj za zagotovitev učinkovitega izvajanja in uveljavljanja Splošne uredbe.

Ekspertna podskupina za tehnologijo se osredotoča na vprašanja, povezana z vprašanji varstva osebnih podatkov pri uporabi sodobnih tehnologij v digitalni dobi. Podskupina tako pripravlja smernice o temah, kot so e-zasebnost, šifriranje osebnih podatkov, ocene učinkov na varstvo podatkov (DPIA) in obvestila o kršitvah varstva podatkov (DBN obvestila). Podskupina spremlja tudi nastajajoče tehnologije in inovacije v družbi ter ocenjuje morebitna tveganja za zasebnost, ki jih te prinašajo. Podskupina zagotavlja tudi mnenja o tehnoloških zadevah, ki so pomembne za druge ekspertne podskupine.

EOVP je v letu 2023 objavil številne splošne smernice, npr.:

- Smernice 02/2023 o tehničnem obsegu 5. člena direktive o eZasebnosti, ki pojasnjujejo, kateri tehnični procesi in operacije, zlasti z vidika novih tehnologij, sodijo v okvir direktive.
- Smernice 01/2023 o 37. členu 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. Smernice pojasnjujejo pravila glede prenosov podatkov v tretje države s strani pristojnih organov.

- Posodobitve Smernic 05/2021 glede prepletanja uporabe 3. člena Splošne uredbe in določb glede prenosov v tretje države, ki pojasnjujejo odnos med teritorialno uporabo 3. člena in med pravili o prenosu podatkov. Smernice vsebujejo konkretne primere za upravljavce podatkov.
- Posodobitve Smernic 07/2022 o certifikaciji kot orodju za prenose podatkov, podajajo pojasnila glede praktične uporabe tega orodja, kadar gre za prenose podatkov v tretje države. Smernice dopolnjujejo smernice št. 1/2018 glede certificiranja, ki na splošno pokrivajo področje potrjevanja po Splošni uredbi.
- Posodobitve Smernic 03/2022 o zavajajočih vzorcih in socialnih omrežjih, ki pojasnjujejo, kakšni so zavajajoči vzorci na teh platformah in na kakšen način kršijo določbe Splošne uredbe, ter podajajo priporočila.
- Po javni konzultaciji je bila sprejeta končna verzija Smernic 01/2022 glede pravice dostopa do lastnih podatkov.

Na področju svetovanja Evropski komisiji v zvezi z vprašanji varstva podatkov in pripravo evropskih predpisov s področja varstva podatkov je EOVP v letu 2023 med drugim deloval na naslednjih področjih:

- EOVP je pripravil mnenje 5/2023 glede osnutka sklepa o ustreznosti okvira o zasebnosti podatkov EU-ZDA, ki poudarja bistvene dopolnitve sistema varstva podatkov v ZDA in nov mehanizem za obrambo pravic, ki je dostopen posameznikom. Hkrati pa mnenje izraža skrb glede izvajanja pravic posameznikov, nadaljnjih prenosov, glede obsega izjem in začasnega množičnega zbiranja podatkov ter glede delovanja mehanizma obrambe v praksi.
- EOVP je skupaj z Evropskim nadzornikom za varstvo podatkov izdal mnenje o predlogu uredbe o digitalnem evru kot digitalni valuti centralne banke. Digitalni evro naj bi posamezniku nudil izvajanje plačil elektronsko, na spletu in izven spleta, bil bi dodatno plačilno sredstvo poleg denarja. V mnenju so poudarjeni vidiki varstva osebnih podatkov pri uporabi digitalnega evra, podana so tudi različna priporočila. Posamezniki naj bi vedno imeli možnost izbire pri plačevanju z digitalnim evrom ali denarjem.
- EOVP je pripravil pismo glede deljenja podatkov v okviru zakonodaje za preprečevanje pranja denarja in financiranja terorizma (AML/CTF).
- EOVP je sprejel poročilo glede izvajanja Splošne uredbe, izdano v okviru evalvacije, ki jo redno izvaja Evropska komisija. Iz poročila izhaja, da je izvajanje Splošne uredbe v zadnjih petih letih in pol uspešno in da je preuranjeno razmišljati o spremembah uredbe. Hkrati EOVP poudarja, da je nujen čim hitrejši sprejem t. i. procesne uredbe, ki bo bolj podrobno predpisala postopke sodelovanja pri čezmejnem nadzoru. EOVP poudarja, da nadzorni organi potrebujejo zadostna sredstva za izvajanje svojih pristojnosti.
- EOVP je skupaj z Evropskim nadzornikom za varstvo podatkov izdal mnenje 01/2023 o predlogu uredbe o določitvi dodatnih postopkovnih pravil v zvezi z izvrševanjem Uredbe (EU) 2016/679. Uredba naj bi podrobneje predpisala procesne korake in zagotovila pri čezmejnih postopkih nadzora, ki jih bodo morali upoštevati vodilni in zadevni organi.

V okviru promocije sodelovanja in izmenjave izkušenj med nacionalnimi nadzornimi organi za varstvo podatkov je EOVP izvajal postopke reševanja sporov s strani odbora po 65. členu Splošne uredbe ter sprejel dve zavezujoči odločitvi, kot sta bili predstavljeni v 3.2.8 poglavju (v primeru Meta in TikTok).

EOVP je v letu 2023 sprejel tudi nujno zavezujočo odločitev po 66. členu Splošne uredbe, ki se nanaša na obdelavo osebnih podatkov s strani Meta Ireland Limited, glede pravnih podlag, na katerih družba obdeluje osebne podatke uporabnikov za namen vedenjskega oglaševanja. Iz zavezujoče odločitve izhaja, da v tem primeru obdelava ne more temeljiti na pravni podlagi pogodbe

z uporabnikom oziroma na zakonitem interesu družbe. Na podlagi te odločitve je irski nadzorni organ sprejel končno določitev, ki je dostopna v registru končnih odločitev po 60. členu Splošne uredbe⁹.

Poleg naštetih nalog pa EOVP na podlagi 64. člena Splošne uredbe izdaja tudi mnenja o skladnosti (t. i. *consistency opinions*) v zvezi z vsemi vprašanji splošne uporabe določb Splošne uredbe in vprašanji, ki imajo učinke v več kot eni državi članici. Nacionalni nadzorni organi lahko v zvezi s temi zadevami zaprosijo EOVP za mnenje, kadar gre za:

- dejanja obdelave, za katera je potrebna ocena učinka v zvezi z varstvom podatkov (DPIA),
- kodekse ravnanja v zvezi z dejavnostmi obdelave,
- merila za akreditacijo certifikacijskega organa in merila certificiranja,
- standardne klavzule o varstvu osebnih podatkov in
- zavezujoča poslovna pravila.

Mnenja o skladnosti so za zadevne nadzorne organe zavezujoča in jih morajo upoštevati pri sprejemanju končnih odločitev o zadevi, pri tem pa pomagajo zagotoviti, da je izvajanje Splošne uredbe dosledno po vsej EU. EOVP je v letu 2023 izdal 37 takšnih mnenj, in sicer na temo zavezujočih poslovnih pravil (27), meril certificiranja (1), meril za akreditacijo certifikacijskega organa (6) in kodeksov ravnanja (3). Med izdanimi mnenji je tudi Mnenje 38/2023 glede kriterijev za akreditacijo certifikacijskih teles, ki jih je pripravil Informacijski pooblaščenec skladno s tretjim odstavkom 43. člena Splošne uredbe. Po sprejemu ZVOP-2 so namreč tudi v Sloveniji stekle priprave za procese akreditacije in certificiranja po Splošni uredbi.

EOVP je v okviru svoje strategije za okrepljeno sodelovanje med nadzornimi organi med letoma 2021 in 2023 ustanovil **podporno skupino strokovnjakov**, katere cilj je zagotoviti vsebinsko podporo članicam EOVP pri njihovih nadzorih v zvezi z vprašanji, pri katerih bi ti potrebovali dodatno pomoč. Strokovnjaki prihajajo z različnih področij varstva osebnih podatkov, in sicer pokrivajo ekspertna znanja, npr. na področju storitev v oblaku, tehnik anonimizacije, vedenjskega oglaševanja, umetne inteligence, digitalnega prava itd.¹⁰ Namen ustanovitve te skupine je okrepiti sodelovanje in solidarnost med članicami z izmenjavo in krepitvijo ekspertnega znanja po celotni EU ter skupno naslavljanje operativnih potreb posameznih nadzornih organov.

Poleg naštetega je EOVP skladno s svojo strategijo okrepljenega sodelovanja začel delovati tudi v okviru **usklajene skupne akcije nadzora**, ki zagotavlja strukturo ponavljajočih se letnih usklajevanj ukrepov nadzornih organov glede posamezne teme. Cilj je spodbujati skladnost, opolnomočiti posameznike, na katere se osebni podatki nanašajo, ter povečati ozaveščenost vseh deležnikov s skupnimi ukrepi in delovanjem na področju, ki ga EOVP za tisto leto izbere kot prednostno. Tema usklajenega skupnega nadzora za leto 2023 je bil **položaj pooblaščenih oseb za varstvo podatkov** (t. i. DPO). V usklajeni nadzorni akciji je sodelovalo 25 nadzornih organov iz EU, med njimi tudi Informacijski pooblaščenec. Poročilo usklajene akcije je na voljo na spletni strani EOVP¹¹ in izpostavlja nekatere skrbi in izzive. Rezultati akcije so načeloma vzpodbudni, saj večina pooblaščenih oseb zatrjuje, da imajo potrebna znanja in veščine za opravljanje svojih nalog in da se redno izobražujejo. Imajo jasno definirane naloge glede na Splošno uredbo in navajajo, da se z njimi izvajajo potrebna posvetovanja in da so njihova mnenja precej dobro upoštevana. Vendar pa je pri nekaterih pooblaščenih osebah njihovo delo tudi izziv, zato poročilo naniza priporočila za organizacije, kako okrepiti vlogo pooblaščenih oseb in kako ravnati v skladu s Splošno uredbo.

V letu 2023 so predstavniki Informacijskega pooblaščenca sodelovali tudi v številnih delovnih

⁹ https://www.edpb.europa.eu/our-work-tools/consistency-findings/register-decisions/2023/enforcement-notice-matter-meta_en

¹⁰ Za več informacij o pozivu s strani EOVP in temah glej: https://edpb.europa.eu/system/files/2022-02/call_for_expressions_of_interest_support_pool_of_experts.pdf.

¹¹ https://www.edpb.europa.eu/our-work-tools/our-documents/other/coordinated-enforcement-action-designation-and-position-data_en

in koordinacijskih skupinah, ki pokrivajo posamezna ključna področja. Nekaj skupin je na kratko predstavljenih v nadaljevanju.

Delovna skupina za upravne globe pripravlja smernice za zagotovitev usklajenosti izračunov upravnih glob v konkretnih postopkih skladno s Splošno uredbo. Namen teh smernic je zagotoviti jasnost in doslednost pri izračunavanju upravnih glob po vsej EU, da bi zagotovili pravično in enotno odgovornost vseh upravljavcev in obdelovalcev za kršitve Splošne uredbe ne glede na to, kje v EU se obdelava osebnih podatkov izvaja. Delovna skupina pri pripravi smernic upošteva tudi sorazmernost upravnih glob in druge dejavnike, ki lahko vplivajo na njihov izračun, kot so narava in resnost kršitve ter finančna sredstva organizacije. Delovna skupina je v letu 2023 v skladu z javno konzultacijo revidirala Smernice št. 04/2022 o izračunu upravnih glob v skladu s Splošno uredbo,¹² ki služijo usklajevanju metodologije, ki naj bi jo nadzorni organi uporabljali pri izračunu zneska upravnih glob za morebitne kršitve varstva osebnih podatkov.

Delovna skupina za piškotke se je osredotočala na analizo številnih pravnih vprašanj in morebitnih kršitev, povezanih z implementacijo piškotkov na spletnih straneh. Cilj delovne skupine je bil z oblikovanjem skupnega poročila zagotoviti podporo nacionalnim dejavnostim pri izvajanju tovrstnih nadzorov. Namen delovne skupine je bil uskladiti postopek nadzora spletnih strani v povezavi s piškotki in doseči čim bolj enotno interpretacijo pravil vseh pristojnih nadzornih organov. V začetku leta 2023 je skupina izdala skupno poročilo¹³, v katerem izpostavlja prakse pri uporabi piškotkov, ki ne izpolnjujejo zahtev veljavne zakonodaje (v skladu s tem je Informacijski pooblaščenec posodobil svoje smernice glede piškotkov¹⁴):

1. Mehanizem za pridobivanje privolitve ne vsebuje gumba za zavrnitev piškotkov v prvem koraku.
2. Predobkljukana polja v mehanizmih za privolitev ne izpolnjujejo zahtev veljavne privolitve.
3. Veljavna privolitev ni mogoča, kadar je možnost za zavrnitev piškotkov predstavljena le v besedilu ali na povezavi, ki ni grafično enako izpostavljena kot gumb za potrditev privolitve ali pa se nahaja izven mesta, kjer je mogoče podati privolitev.
4. Veljavna privolitev ni mogoča, kadar je možnost za zavrnitev podana z gumbom, pri čemer pa je kontrast med barvo gumba in tekstom tako majhen, da je ta možnost težko berljiva.
5. Piškotkov ni mogoče nalagati na pravni podlagi zakonitega interesa iz Splošne uredbe o varstvu podatkov.
6. Piškotki so napačno uvrščeni med nujne.
7. Ni ikone, gumba oz. povezave za naknadni preklic privolitve.

Delovna skupina za 101 prijavo se je osredotočala na poenoteno in usklajeno postopanje nadzornih organov glede 101 identične pritožbe, vložene na številne nadzorne organe glede vprašanj uporabe storitev Google Analytics in Facebook Connect, ki vključujejo prenos osebnih podatkov v tretje države. Naloga delovne skupine je bila predvsem analiza prejetih prijav in zagotavljanje tesnega sodelovanja med člani odbora, da bi bile odločitve posameznih nadzornih organov v podobnih primerih usklajene. Tudi ta delovna skupina je v letu 2023 objavila končno poročilo¹⁵, v katerem pojasnjuje vidike prenosa podatkov v tretje države, ki jih morajo spletne strani, ki uporabljajo omenjeni orodji, upoštevati, ter tudi na kakšen način lahko izkazujejo svoje upoštevanje načela odgovornosti.

EOVP je kot odziv na nadzorne aktivnosti italijanskega nadzornega organa v zvezi s ChatGPT,

¹² https://edpb.europa.eu/our-work-tools/documents/public-consultations/2022/guidelines-042022-calculation-administrative_en

¹³ https://edpb.europa.eu/our-work-tools/our-documents/other/report-work-undertaken-cookie-banner-taskforce_en

¹⁴ <https://www.ip-rs.si/publikacije/priro%C4%8Dniki-in-smernice/smernice-po-splo%C5%A1ni-uredbi-o-varstvu-podatkov-gdpr/smernice-o-uporabi-pi%C5%A1kotkov-in-podobnih-sledilnih-tehnologij>

¹⁵ https://www.edpb.europa.eu/system/files/2023-04/edpb_20230328_report_101task_force_en.pdf

katerega uporabniki so v vseh državah članicah EU, v letu 2023 uvedel novo delovno skupino ChatGPT, katere namen je usklajevanje pri vprašanjih skladnosti generativne umetne inteligence s Splošno uredbo.

Kontaktna skupina za dostop do dokumentov je delovna skupina članov EOVP iz nacionalnih nadzornih organov, ki delujejo kot kontaktne točke za usklajevanje zahtev za dostop do dokumentov v skladu z Uredbo (ES) št. 1049/2001 Evropskega parlamenta in Sveta z dne 30. maja 2001 o dostopu javnosti do dokumentov Evropskega parlamenta, Sveta in Komisije. Naloge skupine obsegajo opredelitev in izmenjavo najboljših nacionalnih praks v zvezi z obravnavo zahtev za dostop do informacij javnega značaja s strani nadzornih organov ter izmenjavo informacij in sodelovanje pri postopkih, povezanih s takšnimi zahtevami.

Mreža DPO ima svetovalno vlogo, svetuje odboru in posebej nadzornim organom, saj zagotavlja neodvisna stališča o zadevah, povezanih z varstvom osebnih podatkov. Kljub temu da mreža pripravi odločitev za odbor, je na nacionalni ravni vsak nadzorni organ sam odgovoren za sprejemanje svojih odločitev.

Mreža za komuniciranje združuje člane nadzornih organov, ki koordinirajo vprašanja, povezana s komuniciranjem z javnostmi, in skrbijo za medsebojno obveščanje nadzornih organov (npr. medsebojno obveščanje o odmevnejših primerih, usklajevanje skupnih odgovorov in sporočil za javnost, koordiniranje prevodov dokumentov v nacionalne jezike, koordiniranje in obveščanje o dogodkih EOVP, sodelovanje pri pripravi letnega poročila EOVP itd.). Mreža za komuniciranje je v letu 2023 sodelovala pri pripravi Vodiča za varstvo osebnih podatkov za mala in srednja podjetja¹⁶.

3.6.2 SODELOVANJE V DRUGIH NADZORNIH TELESIH EVROPSKE UNIJE

Informacijski pooblaščenec je leta 2023 na ravni EU aktivno sodeloval v petih delovnih telesih, ki se ukvarjajo z nadzorom nad izvajanjem varstva osebnih podatkov v okviru velikih informacijskih sistemov EU, in sicer:

- 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.

V letu 2023 je bilo v okviru nadzora nad obdelavo osebnih podatkov v VIS sprejeto poročilo o predčasnem izbrisu podatkov v VIS, ki ga ureja 25. člen Uredbe (ES) št. 767/2008 Evropskega parlamenta in Sveta z dne 9. julija 2008 o vizumskem informacijskem sistemu (VIS) in izmenjavi podatkov med državami članicami o vizumih za kratkoročno prebivanje.

Predstavniki Informacijskega pooblaščenca je oktobra 2023 sodeloval pri evalvaciji izvajanja schengenskega pravnega reda na področju varstva podatkov v Latviji.

¹⁶ https://www.edpb.europa.eu/sme-data-protection-guide/respect-individuals-rights_en

3.6.3 SODELOVANJE V DRUGIH MEDNARODNIH TELESIH

POSVETOVALNI ODBOR T-PD

V okviru Sveta Evrope je predstavnik Informacijskega pooblaščenca tudi leta 2023 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. Na plenarnih zasedanjih v juniju in novembru je Odbor obravnaval stanje pridruževanja držav ter postopek sprejema Protokola o spremembi te konvencije (t. i. Konvencija 108+). Slovenija je 20. 6. 2023 postala 26. država, ki je Konvencijo 108+ ratificirala. 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 aktivno obravnaval aktualne teme, vključno z obdelavo osebnih podatkov v okviru volitev ter izjeme in omejitve osnovnih načel varstva osebnih podatkov po Konvenciji 108+. Sprejel je dva modula vzorčnih pogodbenih določil za mednarodni prenos osebnih podatkov: prvi je namenjen prenosom od enega do drugega upravljavca, drugi pa prenosom od upravljavca do obdelovalca. Izdal je tudi smernice o varstvu osebnih podatkov pri obdelavi za namene preprečevanja pranja denarja in financiranja terorizma ter podelil nagrado Stefano Rodotà.

SVETOVNA SKUPŠČINA ZA ZASEBNOST

Svetovna skupščina za zasebnost (ang. *Global Privacy Assembly – GPA*), ki povezuje prizadevanja več kot 130 nadzornih organov za varstvo zasebnosti in osebnih podatkov z vsega sveta, se je v preteklem letu posvečala zlasti izzivom učinkovitega mednarodnega sodelovanja med nadzornimi organi ter različnim vidikom ukrepanja glede varstva zasebnosti pri uporabi modernih tehnologij. V skladu s strateškimi usmeritvami, ki temeljijo na prizadevanjih za vzpostavitev mednarodnega okvira standardov varstva zasebnosti ter krepitvi različnih oblik sodelovanja pri izvajanju nadzorov je GPA v letu 2023 v okviru različnih delovnih skupin med drugim obravnavala področje varstva zasebnosti v okviru digitalnega gospodarstva, etičnih dilem in tveganj za zasebnost ter pravice posameznikov pri uporabi umetne inteligence ter v okviru varstva pravic potrošnikov. Delo konference vodi izvršni odbor, katerega člani so bili v letu 2023 predstavniki mehiškega, korejskega, nemškega, bolgarskega in maroškega nadzornega organa, nadzornega organa Bermudov ter države Jersey. Med pomembnejšimi resolucijami, sprejetimi na zadnji konferenci leta 2023, ki je potekala na Bermudih in se je Informacijski pooblaščenec ni udeležil, so resolucija, posvečena izzivom na področju uporabe umetne inteligence v zaposlovanju, resolucija na temo uporabe zdravstvenih podatkov v znanstvenem raziskovanju ter resolucija o generativnih sistemih umetne inteligence.

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

Mednarodna delovna skupina za varstvo osebnih podatkov v tehnoloških zadevah (*International Working Group on Data Protection in Technology – IWGDPT*¹⁷; t. i. *Berlin group*) je ena najdlje delujočih mednarodnih skupin na področju varstva osebnih podatkov, saj že od leta 1983 združuje predstavnike informacijskih pooblaščenec in organov za varstvo osebnih podatkov in zasebnosti s celega sveta. Nastala je na pobudo informacijskega pooblaščenca Berlina, sčasoma pa je svoje delovanje razširila z domene telekomunikacij na preostala tehnološka področja. Sprejeta mnenja skupine so pomemben prispevek k mednarodni konferenci informacijskih pooblaščenec, usmerjajo delo nadzornih organov in regulatorjev ter podajajo priporočila razvijalcem, prodajalcem in uporabnikom različnih tehnoloških rešitev.

¹⁷ Spletna stran IWGDPT: <https://www.bfdi.bund.de/EN/Fachthemen/Gremienarbeit/Berlin-Group/Berlin-Group-node.html>

V letu 2023 je bil sprejet dokument na temo pametnih mest (*Working Paper on "Smart Cities"*¹⁸). Pametna mesta predstavljajo trend, ki se pojavlja po celem svetu, gre pa za željo izkoristiti možnosti digitalizacije za boljše upravljanje mest z naprednimi storitvami, kot so inteligentni transportni sistemi, boljše upravljanje s parkirnimi površinami ter odpadki, zagotavljanje varnosti, učinkovitejša izraba energije in druge napredne storitve. Pametna mesta temeljijo na obsežnem zbiranju podatkov in na njihovi analizi, med podatki pa so pogosto tudi osebni podatki, zato je nujno, da se že pri oblikovanju naprednih rešitev upoštevajo vsa temeljna načela varstva osebnih podatkov, kar je ključno za doseganje zaupanja v nove storitve. Mednarodna delovna skupina IWGDPT v svojem dokumentu vse deležnike poziva k upoštevanju načel vgrajenega in privzetega varstva podatkov ter implementacije rešitev skladno s podanimi priporočili.

V letu 2023 je bil sprejet tudi dokument na temo telemetričnih in diagnostičnih podatkov (*Working Paper on Telemetry and Diagnostic Data*¹⁹), gre pa za uporabo diagnostičnih in telemetrijskih podatkov v mobilnih in namiznih operacijskih sistemih in aplikacijah (smiselno tudi za interne vidike znotraj organizacij) za namene, ki niso povezani s primarnimi nameni uporabe naprave oz. aplikacije, kot so reševanje uporabniških težav, nadzor učinkovitosti delovanja, zagotavljanje kakovosti ter izboljšave in razvoj storitev in produktov. Prodajalci in proizvajalci vgrajujejo diagnostične funkcionalnosti z različnimi nameni – od poročanja napak ob sesutjih, do npr. zaznav uporabe nelicenčnih kartuš in skoraj stalnega in obsežnega nadzora nad napravo oz. aplikacijo, obseg zbranih podatkov pa se giblje od osnovnih konfiguracij do celotnih kopij pomnilnika. IWGDPT proizvajalcem in prodajalcem priporoča, da v prvi vrsti sprejmejo dejstvo, da sodijo omenjeni podatki v mnogih primerih med osebne podatke (četudi namen zbiranja podatkov ni neposredna identifikacija posameznika), priporoča jim, naj jasno definirajo in dokumentirajo namene zbiranja podatkov in vrste podatkov, ki jih zbirajo, da bi lahko znali upravičiti obdelavo in utemeljiti sorazmernost obdelave, ter naj omejijo obseg podatkov, zbranih za te namene.

IWGDPT je v letu 2023 nadaljevala delo na delovnih dokumentih na temo digitalnih valut centralnih bank, umetne inteligence, deljenja podatkov in sintetičnih podatkov ter na temo nevrotehnologij. Slednje za zasebnost predstavljajo poseben izziv, saj gre za tehnologije, katerih cilje je dobesedno branje naših možganskih tokov, tako rekoč misli, in možnost vplivanja nanje. Sektorji možnih uporab so številni: zdravstvo, šport, raziskave in razvoj, delovna okolja (npr. zaznavanje koncentracije, utrujenosti, odnosa do strank itd.), igre in zabava, trženje, izobraževanje, nadzor migracij, pregon kaznivih dejanj. Naprave, ki so predmet razvoja, so vgradne ali nosljive, z zavednim ali nezavednim vplivom na posameznika. Posledično se že pojavljajo pozivi k ponovnem premisleku o obsegu pravice do zasebnosti in potencialno definiranju novih *neuropravic*, med njimi pravice do kognitivne zasebnosti (do tega, da svoje misli zadržiš zase).

INITIATIVE 20i7



Nadzorni organi za varstvo osebnih podatkov iz Hrvaške, Severne Makedonije, Črne Gore, Kosova in Slovenije so se v Peji na Kosovu srečali na petem letnem zasedanju pobude Initiative 20i7, ki je nastala na pobudo Informacijskega pooblaščenca z namenom izmenjave izkušenj med nadzornimi organi s področja nekdanje Jugoslavije ter njihovega približevanja EU.

Na zasedanju so nadzorni organi sprejeli skupno izjavo, s katero so poudarili nujnost izmenjave prakse in stališč na področjih varstva osebnih podatkov, kot so videonadzor, kršitve varnosti osebnih podatkov, pooblaščenec oseb za varstvo podatkov, ocene učinkov glede varstva osebnih podatkov ter prenos podatkov v tretje države. Nadzorni organi so poudarili pomen medsebojnega sodelovanja,

¹⁸ https://www.bfdi.bund.de/SharedDocs/Downloads/EN/Berlin-Group/20230608_WP-Smart-Cities.pdf?__blob=publicationFile&v=3

¹⁹ https://www.bfdi.bund.de/SharedDocs/Downloads/EN/Berlin-Group/20230608_WP-Telemetry-Diagnostic-Data.pdf?__blob=publicationFile&v=4

ki je zlasti pomembno v času hitrega tehnološkega razvoja, kot je razvoj umetne inteligence, kjer je pravočasen odziv regulatorjev ključen za zagotovitev ustrezne ravni temeljnih človekovih pravic ter prenosa znanj iz članic EU v države, ki si prizadevajo za vstop v EU. Predstojniki nadzornih organov bodo zato nadaljevali tako z letnimi srečanji kakor tudi z bilateralnimi sodelovanji in skupnim sodelovanjem, ko se pojavi potreba po skupnem ukrepanju glede ozaveščanja javnosti in drugih deležnikov ali potreba po izvajanju nadzornih ukrepov. V letu 2024 bo srečanje pobude gostila Hrvaška.

3.7 SPLOŠNA OCENA STANJA VARSTVA OSEBNIH PODATKOV

Informacijski pooblaščenec je na področju varstva osebnih podatkov opravljal naloge, ki mu jih nalagajo Splošna uredba o varstvu podatkov ter drugi zakoni, ki urejajo obdelavo ali varstvo osebnih podatkov. Splošna uredba, ki se od 25. 5. 2018 neposredno uporablja v vseh državah članicah EU, je terjala sprejem novega Zakona o varstvu osebnih podatkov (ZVOP-2), ki pa je bil sprejet šele 15. 12. 2022 in se je začel uporabljati 26. 1. 2023, torej na začetku obravnavanega obdobja.

S sprejetjem novega ZVOP-2 je Informacijski pooblaščenec postal pristojen tudi za izrekanje sankcij za kršitve, ki jih predpisuje Splošna uredba. Te kršitve se skladno z določbami ZVOP-2 pravnim osebam, samostojnim podjetnikom posameznikom in posameznikom, ki samostojno opravljajo dejavnost, izrekajo kot globe za prekrške.

Bistvena novost, ki jo je glede nadzornih postopkov uvedel ZVOP-2, so nadzorni postopki, v katerih Informacijski pooblaščenec obravnava prijave prijavitelja s posebnim položajem. V teh nadzornih postopkih Informacijski pooblaščenec obravnava izključno kršitve, ki jih v svojih zahtevah zatrjujejo posamezniki, ki menijo, da obdelava osebnih podatkov s strani upravljavca ali obdelovalca krši določbe Splošne uredbe, ZVOP-2 ali drugih zakonov, ki urejajo obdelavo ali varstvo osebnih podatkov.

Informacijski pooblaščenec je v obravnavanem obdobju prejel 1.146 prijav oz. pobud za uvedbo inšpekcijskega postopka, od tega je uvedel 686 inšpekcijskih postopkov, dodatno pa je v 270 inšpekcijskih postopkih sodeloval kot zadevni nadzorni organ po 60. členu Splošne uredbe (postopek čezmejnega sodelovanja).

Prijave, ki jih je v letu 2023 prejel in obravnaval Informacijski pooblaščenec, so bile vložene iz podobnih razlogov kot v preteklih letih. Največ prijav je bilo vloženi zaradi nezakonitega razkrivanja in posredovanja osebnih podatkov neupravičenim osebam, izvajanja videonadzora, uporabe osebnih podatkov za namene neposrednega trženja, nezakonitega ali prekomernega zbiranja osebnih podatkov, nezakonitih vpogledov v zbirke osebnih podatkov ter neustreznega zagotavljanja varnosti osebnih podatkov. Kar zadeva obravnavo prijav v zvezi z izvajanjem videonadzora, velja vnovič opozoriti zlasti na problematiko izvajanja videonadzora v delovnih prostorih, ki se pogosto izvaja z namenom nadzora nad zaposlenimi ter na način, da se dogajanje pred kamerami neposredno prenaša na osebne računalnike ali mobilne telefone vodilnih, kar je v nasprotju z zakonsko dopustnimi nameni za izvajanje videonadzora v delovnih prostorih. Prav tako se je veliko prijav nanašalo na izvajanje videonadzora s strani fizičnih oseb, ki so izvajale videonadzor s kamerami, ki so jih namestile na svoje objekte. V teh primerih se praviloma šteje, da posameznik izvaja videonadzor izključno za svoje lastne, domače namene, zato se Splošna uredba (na katero je vezana pristojnost Informacijskega pooblaščenca) načeloma ne uporablja. Informacijski pooblaščenec je v takih primerih pristojen le, kadar posameznik videonadzor izvaja ob opravljanju poklicne ali komercialne dejavnosti, kadar posnetke posameznikov posreduje nepooblaščen tretji osebi ali pa jih objavi na internetu oziroma če videonadzor pomeni snemanje javnega prostora. Pomembno pa je opozoriti, da morajo biti za uvedbo postopka zoper posameznika, ki izvaja videonadzor s kamerami, ki jih je namestil na svoje objekte, podani konkretni dokazi o nezakonitem izvajanju videonadzora (npr. konkretni videoposnetek ali posnetek zaslonske slike), torej o tem, da posameznik dejansko snema površine, ki niso v njegovi lasti ali da posnetke uporablja za namene, ki presegajo domačo uporabo, ter da so posnetki takšne kakovosti, da omogočajo prepoznavo posameznikov. To je pomembno, ker vstop v stanovanje zaradi ustavne določbe nedotakljivosti stanovanja ni dopusten brez odredbe sodišča, poleg tega pa že zgolj sama uvedba inšpekcijskega postopka zoper posameznika pomeni poseg v njegovo zasebnost.

Informacijski pooblaščenec pri obravnavi prijav, prejetih od posameznikov, ugotavlja, da so te v mnogih primerih vložene zaradi nerazumevanja določb Splošne uredbe ter da so za vlaganje

prijav pogosto krivi tudi upravljavci, ki ob zbiranju ali pridobitvi osebnih podatkov posamezniku ne zagotovijo preglednih, razumljivih in lahko dostopnih informacij, kot jim to nalagajo 12., 13. in 14. člen Splošne uredbe.

Zagotavljanje jedrnatih, preglednih, razumljivih in lahko dostopnih informacij iz 13. in 14. člena Splošne uredbe je bila kljub ozaveščanju upravljavcev in kljub vzorcem takšnih obvestil, ki jih je Informacijski pooblaščenec pripravil in objavil na svojih spletnih straneh, tudi v letu 2023 ena od pogosto ugotovljenih kršitev. Informacije, ki jih je treba zagotoviti posamezniku ob zbiranju njegovih osebnih podatkov, so določene v 13. in 14. členu Splošne uredbe, posameznik pa na podlagi takšnih informacij izve, kdo je upravljavec osebnih podatkov, za kakšne namene in na kakšni pravni podlagi se osebni podatki obdelujejo, kdo so uporabniki osebnih podatkov, koliko časa se podatki hranijo itd.

Informacijski pooblaščenec je v letu 2023 prejel in v okviru inšpekcijskih postopkov obravnaval še sedem primerov nedovoljenega sporočanja ali druge nedovoljene obdelave osebnih podatkov o pacientih, ki so mu jih na podlagi 46. člena Zakona o pacientovih pravicah poslali izvajalci zdravstvene dejavnosti, ter 183 uradnih obvestil o kršitvi varnosti osebnih podatkov, ki so mu jih na podlagi 33. člena Splošne uredbe poslali upravljavci osebnih podatkov.

Upravljavci osebnih podatkov so uradna obvestila o kršitvi varnosti osebnih podatkov Informacijskemu pooblaščenцу najpogosteje pošiljali zaradi nezakonitega razkritja ali posredovanja osebnih podatkov nepooblaščenim ali napačnim osebam, zaradi nepooblaščenega dostopanja do osebnih podatkov zaradi programske napake ali zlorabe pooblastil s strani zaposlenih ter zaradi izgube ali kraje nosilcev osebnih podatkov (npr. osebnih računalnikov in USB-ključkov). V zadnjem času so vse pogostejša tudi obvestila o kršitvi varnosti osebnih podatkov zaradi kibernetkega napada oz. vdora v informacijski sistem z izsiljevalskim virusom, kar upravljavcem osebnih podatkov, ki niso izvajali ustreznih tehničnih in organizacijskih ukrepov za zagotavljanje varnosti obdelave osebnih podatkov, povzroča velike stroške ter probleme pri zagotavljanju zmožnosti pravočasne povrnitve razpoložljivosti in dostopnosti osebnih podatkov.

Poleg obravnave inšpekcijskih prijav, sporočenih nedovoljenih obdelav osebnih podatkov o pacientih ter uradnih obvestil o kršitvi varnosti osebnih podatkov je Informacijski pooblaščenec v letu 2023 prejel in obravnaval še 251 pritožb prijaviteljev s posebnim položajem po 77. členu Splošne uredbe ter 30. členu ZVOP-2. Od tega je bilo 130 pritožb vloženih zaradi suma nezakonite obdelave osebnih podatkov pritožnika, 121 pa zaradi suma kršitve pravic pritožnika, in sicer 75 zaradi suma kršitve pravice dostopa do lastnih osebnih podatkov, 41 zaradi suma kršitve pravice do izbrisa, štiri zaradi suma kršitve pravice do popravka in ena zaradi suma kršitve pravice do ugovora.

Na področju pacientovih pravic je Informacijski pooblaščenec obravnaval še 14 pritožb zaradi kršitve pravice do seznanitve z lastno zdravstveno dokumentacijo (41. člen ZPacP) ter 12 pritožb zaradi kršitve pravice do seznanitve z zdravstveno dokumentacijo po pacientovi smrti (42. člen ZPacP).

Informacijski pooblaščenec je v letu 2023 obravnaval tudi devet pritožb posameznikov, ki so bile vložene po ZVOPOKD, in sicer eno zaradi suma nezakonite obdelave osebnih podatkov pritožnika, sedem zaradi suma kršitve pravice dostopa do lastnih osebnih podatkov ter eno zaradi suma kršitve pravice do izbrisa in popravka.

V četrtem odstavku 41. člena ZVOP-2 je bila Informacijskemu pooblaščenцу podeljena tudi pristojnost za odločanje o pritožbah vlagateljev, ki jim je upravljavec zavrnil posredovanje osebnih podatkov iz uradnih evidenc ali javnih knjig. V letu 2023 je Informacijski pooblaščenec obravnaval štiri takšne pritožbe.

Informacijski pooblaščenec je, podobno kot v preteklih letih, tudi v letu 2023 poleg obravnave prijav in pritožb skladno z letnim delovnim načrtom izvajal redne in sistematične inšpekcijske nadzore, v okviru katerih je pri zavezancih nadzoroval zlasti:

1. zakonitost obdelave osebnih podatkov ter spoštovanje splošnih načel za obdelavo osebnih podatkov;
2. ustreznost postopkov in ukrepov za zagotavljanje varnosti osebnih podatkov iz 25. in 32. člena Splošne uredbe ter s tem povezano ustreznost notranjih aktov, s katerimi upravljavci in obdelovalci predpisujejo te postopke;
3. izvajanje določb Splošne uredbe, ki urejajo zagotavljanje informacij o obdelavi osebnih podatkov (13. in 14. člen), pogodbeno obdelavo osebnih podatkov (28. in 29. člen) ter vodenje evidenc obdelave (30. člen);
4. zakonitost izvajanja videonadzora znotraj delovnih prostorov in s tem povezano zakonitost neposrednega spremljanja dogajanja pred kamerami, ustreznost pisnih odločitev o uvedbi videonadzora ter ustreznost obvestil o njegovem izvajanju.

Podobno kot v preteklosti so bile ugotovljene kršitve tudi tokrat največkrat posledica nepoznavanja oz. nerazumevanja predpisov, ki urejajo obdelavo osebnih podatkov, nekatere ugotovljene kršitve pa so bile posledica malomarnega ali neustreznega zagotavljanja varnosti osebnih podatkov ter njihove namerne nezakonite obdelave s strani vodstva ali zaposlenih pri upravljavcih osebnih podatkov (sem sodijo nezakoniti vpogledi v zbirke osebnih podatkov, sporna obdelava osebnih podatkov za namene neposrednega trženja ter neupravičeno izvajanje videonadzora v delovnih prostorih z namenom nadzora nad zaposlenimi).

Informacijski pooblaščenec mora v letnem poročilu na podlagi drugega odstavka 62. člena ZVOP-2 poročati tudi o sodelovanju z drugimi organi pri izvajanju nadzorov po tem zakonu ter o predlaganih in opravljenih nadzorih iz 38. ter četrtega odstavka 63. člena tega zakona. Informacijski pooblaščenec je pri nadzoru največ sodeloval z Agencijo za komunikacijska omrežja in storitve RS, s katero je sodeloval na področju elektronskih komunikacij, ter z Uradom Vlade RS za informacijsko varnost, s katerim je sodeloval na področju zagotavljanja varstva zasebnosti in informacijske varnosti na področju elektronskih omrežij, sistemov, storitev in informacij ter s tem povezanih obravnav varnostnih groženj in incidentov. Opravljeni nadzori po 38. členu ZVOP-2 se nanašajo na področje posebnih obdelav, ki so opredeljene v 23. členu ZVOP-2. Gre za nadzore nad informacijskimi sistemi, v katerih se obdelujejo osebni podatki, določeni v zakonih, ki urejajo področje notranjih zadev, finančne uprave, državljanstva, Slovenske obveščevalno-varnostne agencije, obrambe, zdravstvenega varstva, obveznega zdravstvenega zavarovanja, uveljavljanje pravic iz javnih sredstev ter kazenskih in prekrškovnih evidenc, pa tudi za informacijske sisteme, v katerih se obdelujejo osebni podatki več kot 100.000 posameznikov na podlagi zakona, kadar upravljavec ali obdelovalec kot svojo temeljno dejavnost izvaja obsežne obdelave posebnih vrst osebnih podatkov ter kadar se obdeluje posebne vrste osebnih podatkov več kot 10.000 posameznikov. Za področje posebnih obdelav velja prehodna določba 116. člena ZVOP-2, skladno s katero so upravljavci in obdelovalci dolžni obdelave osebnih podatkov, ki jih vključuje prvi odstavek 23. člena ZVOP-2, z določbami 23. člena tega zakona uskladiti v roku treh let od uveljavitve zakona, torej najkasneje do 26. 1. 2026. Navedeno pa ni ovira, da ne bi Informacijski pooblaščenec nadzora nad upravljavci teh informacijskih sistemov opravljal že zdaj. Obdelava osebnih podatkov v teh sistemih namreč zaradi narave in količine osebnih podatkov predstavlja še posebej velika tveganja zaradi nevarnosti namernega ali nezakonitega uničenja, izgube, spremembe ter nepooblaščenega razkritja ali dostopa, pri čemer je treba opozoriti, da omenjeni 116. člen ZVOP-2 upravljavcev in obdelovalcev takšnih sistemov ne odvezuje zagotavljanja varnosti osebnih podatkov in javljanja kršitev varnosti osebnih podatkov na način, kot jim ga že zdaj nalagajo 25., 32., 33. in 34. člen Splošne uredbe. Zaradi zaznanih sumov neskladnosti obdelave osebnih podatkov z določbami Splošne uredbe in ob upoštevanju ugotovitev iz že opravljenih nadzorov pri upravljavcih in obdelovalcih na področju posebnih obdelav je Informacijski pooblaščenec v letu 2023 skladno z letnim načrtom inšpekcijskih nadzorov izvedel šest postopkov inšpekcijskega nadzora, ki so se nanašali predvsem na: zagotavljanje dostopnih pravic ter seznanjanje zaposlenih z dolžnostjo zagotavljanja varnosti, sledljivost obdelave osebnih podatkov na tekočih zadevah, splošno zagotavljanje varnosti osebnih podatkov, preverjanje suma neavtoriziranega dostopa do baze podatkov ter morebiten prenos ali izbris teh osebnih podatkov. Skladno s četrtem odstavkom 63. člena ZVOP-2 bi Varuh človekovih pravic lahko nadzornemu organu

predlagal izvedbo inšpekcijskega nadzora pri katerem koli upravljavcu ali obdelovalcu. V letu 2023 Informacijski pooblaščenec takega predloga Varuha človekovih pravic ni prejel.

Na področju nadzora in sodelovanja pri čezmejnih primerih obdelave osebnih podatkov število primerov, s katerimi se vsako leto ukvarja Informacijski pooblaščenec, strmo narašča. V letu 2023 je bil tako Informacijski pooblaščenec udeležen v 524 postopkih sodelovanja po 60. in 61. členu Splošne uredbe v zvezi z upravljavci, ki izvajajo čezmejno obdelavo osebnih podatkov. V 274 novo začelih postopkih sodelovanja pri čezmejnem nadzoru po 60. členu Splošne uredbe je Informacijski pooblaščenec nastopal kot zadevni organ (po 56. členu Splošne uredbe), v treh primerih pa je bil v vlogi vodilnega organa. Splošna uredba je namreč prinesla formalizirane postopke sodelovanja nadzornih organov za varstvo osebnih podatkov v državah članicah EU in EGS, kjer postopek nadzora v čezmejnem primeru obdelave osebnih podatkov vodi t. i. vodilni organ in pri tem sodeluje z drugimi organi za varstvo osebnih podatkov, uvedla pa je tudi mehanizme vzajemne pomoči in skupnega ukrepanja organov za varstvo osebnih podatkov v državah članicah EU. V čezmejnih postopkih, v katerih je sodeloval Informacijski pooblaščenec, je bilo leta 2023 izdanih 221 osnutkov odločb po 60. členu Splošne uredbe, dva osnutka odločb je Informacijski pooblaščenec izdal kot vodilni nadzorni organ. 291 postopkov je bilo končanih s končno odločbo po 60. členu Splošne uredbe.

Informacijski pooblaščenec je leta 2023 sodeloval tudi v 247 postopkih zagotavljanja medsebojne pomoči med nadzornimi organi po 61. členu Splošne uredbe. Prejel je 219 zahtev drugih organov, v 44 primerih je podal mnenje glede izvajanja določb Splošne uredbe. 28 zahtev za sodelovanje je Informacijski pooblaščenec poslal drugim organom v EU.

Sodelovanje v čezmejnih primerih inšpekcijskega nadzora, kot ga je uvedla Splošna uredba, je nedvomno ena ključnih novosti in okrepitev, predvsem v smislu enotnega delovanja nadzornih organov v različnih državah članicah EU in EGS. 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, porast primerov je namreč iz leta v leto večji: v letu 2021 je bilo skupno 216 postopkov sodelovanja po 60. in 61. členu Splošne uredbe, v letu 2022 je bilo takih postopkov 368, v letu 2023 pa že 524 postopkov.

V letu 2023 so bile sprejete tudi tri zavezujoče odločitve po 65. in 66. členu, ki jih obravnava Evropski odbor za varstvo podatkov (EOVP), v katerem sodeluje tudi Informacijski pooblaščenec. Postopek spora v primeru TikTok Technology Limited z glavno ustanovitvijo na Irskem je zadeval vprašanja obdelave osebnih podatkov registriranih mladoletnih uporabnikov TikToka (13–17 let), in sicer kršitve načela poštenosti zaradi zavajajočih vzorcev, ki jih omrežje uporablja v procesu registracije uporabnikov, ter zaradi kršitve načela privzetega varstva osebnih podatkov zaradi pomanjkljivega preverjanja starosti uporabnikov. EOVP je analiziral prakse TikToka pri dveh pojavnih oknih, ki jih je omrežje uporabljalo pri registraciji uporabnikov in pri deljenju videoposnetkov. V obeh primerih je oblikovanje pojavnega okna mladoletne uporabnike spodbujalo, da so izbrali zasebnosti manj prijazne nastavitve. V končni odločitvi je zato irski nadzorni organ omrežju TikTok zaradi kršitev naložil globo 345 milijonov evrov.

Postopek spora v primeru Meta Platforms Ireland Limited z glavno ustanovitvijo na Irskem je zadeval vprašanje zakonitosti prenosa osebnih podatkov uporabnikov omrežja Facebook v Združene države Amerike, v času, ko je bil s strani Sodišča EU razveljavljen t. i. zasebnostni ščit, dogovor, ki je zagotavljal podlago za prenos osebnih podatkov v ZDA. V končni odločitvi je irski nadzorni organ zavezancu zaradi ugotovljenih kršitev, tj. zaradi prenosa podatkov uporabnikov v ZDA brez pravne podlage, naložil globo 1,2 milijardi evrov, najvišjo izrečeno globo po Splošni uredbi.

Evropska komisija je sicer v letu 2023 sprejela nov sklep o ustreznosti varstva osebnih podatkov na podlagi okvira za varstvo zasebnosti podatkov med EU in ZDA. Na podlagi sklepa o ustreznosti se lahko osebni podatki iz EU varno prenašajo tistim podjetjem iz ZDA, ki sodelujejo v okviru za varstvo

zasebnosti podatkov med EU in ZDA (angl. *EU-US Data Privacy Framework – DPF*), ob tem pa ni treba uvesti dodatnih zaščitnih ukrepov za varstvo podatkov v skladu s 46. členom Splošne uredbe.

V letu 2023 je bila sprejeta tudi nujna zavezujoča odločitev, s katero je EOVP irskemu organu za varstvo podatkov kot vodilnemu nadzornemu organu naložil, naj v dveh tednih sprejme končne ukrepe v zvezi z družbo Meta Ireland Limited (Meta IE) in prepove obdelavo osebnih podatkov za vedenjsko oglaševanje na podlagi pogodbe in zakonitega interesa. Nujna zavezujoča odločitev je bila sprejeta na podlagi zahteve norveškega organa za varstvo podatkov.

Na področju skladnosti in preventive je treba izpostaviti nekatere novosti, ki jih je prinesel ZVOP-2 in ki za zavezance predstavljajo pomembne nove dolžnosti, o katerih morajo biti ustrezno ozaveščeni in ki so posledično vplivale tudi na usmeritev preventivnih aktivnosti Informacijskega pooblaščenca v letu 2023.

Informacijski pooblaščenec je že v začetku leta 2023, še pred uveljavitvijo ZVOP-2, pripravil obsežno vsebinsko prenovo spletne strani, s katero je želel na razumljiv način pojasniti, kaj ureja ZVOP-2, kdaj stopijo obveznosti po ZVOP-2 v veljavo in kakšne so prehodne določbe, ter podati primerjavo določb ZVOP-1 in ZVOP-2. Posodobljene so bile informacije o ključnih vidikih novega zakona, in sicer²⁰:

- [Privolitev](#),
- [Pogodbena obdelava](#),
- [Videonadzor](#),
- [Biometrija](#),
- [Varnost podatkov](#),
- [Prijava kršitev varnosti](#),
- [Pooblaščenec osebe za varstvo osebnih podatkov \(DPO\)](#),
- [Ocena učinka na varstvo osebnih podatkov](#),
- [Obveščanje posameznikov o obdelavi](#),
- [Povezovanje zbirk osebnih podatkov](#),
- [Prenos osebnih podatkov v tretje države in mednarodne organizacije](#),
- [Evidenca dejavnosti obdelave](#),
- [Pravice posameznika](#),
- [Pristojnosti Informacijskega pooblaščenca](#),
- [Inšpekcijski nadzor oz. nadzorni postopki](#),
- [Kodeksi ravnanja](#).

Objavljene so bile tudi naslednje prenovljene smernice²¹:

- Smernice za upravnike večstanovanjskih stavb,
- Smernice o uporabi piškotkov in podobnih sledilnih tehnologij,
- Smernice glede izvajanja videonadzora,
- Smernice za organizatorje dogodkov,
- Smernice glede biometrije po ZVOP-2,
- Smernice glede prenosa osebnih podatkov v tretje države in mednarodne organizacije.

Za boljšo ozaveščenost je bil pripravljen tudi strnjen pregled sprememb ZVOP-2 glede na določbe ZVOP-1.²²

Dvig ozaveščenosti bo potreben na področju ocen učinka glede varstva osebnih podatkov, kjer

²⁰ Posamezne alineje na seznamu vsebujejo hiperpovezave na ustrezno mesto na spletni strani Informacijskega pooblaščenca.

²¹ Smernice so dostopne na povezavi: <https://www.ip-rs.si/publikacije/priro%C4%8Dniki-in-smernice/>.

²² Pregled sprememb je dostopen na: <https://www.ip-rs.si/zakonodaja/zakon-o-varstvu-osebni-podatkov/zvop-2>.

je določba tretjega odstavka 24. člena ZVOP-2 uvedla t. i. zakonodajne ocene učinka in od predlagateljev predpisov zahteva, da v primerih, ko se z zakonom določa obdelava osebnih podatkov, za katero je treba izdelati oceno učinka, predlagatelj predpisa izvede zakonodajno oceno učinka ter jo posreduje v t. i. predhodno posvetovanje Informacijskemu pooblaščenču. V letu 2023 je Informacijski pooblaščenec podal 13 mnenj na prejete zakonodajne ocene učinka, ki so večinoma sledile metodologiji, ki jo je pripravil za ta namen.

Namen zakonodajnih ocen učinka je, da se še pred oblikovanjem dokončnega besedila členov pravočasno razmisli o tem, kako ustrezno upoštevati temeljna načela varstva osebnih podatkov pri določanju besedila zakona. Te razmisleke (npr. kakšne namene zasleduje zakon, kateri nabor osebnih podatkov je potreben, kakšne varovalke moramo vključiti v zakon, ali bo šlo za povezovanje zbirk podatkov, določitev rokov hrambe ipd.) se opiše v oceni učinkov in se jih pošlje Informacijskemu pooblaščenču v mnenje (t. i. predhodno posvetovanje), na podlagi slednjega pa se nato oblikuje (bolj) dokončno besedilo členov in zakon gre lahko v medresorsko usklajevanje. Idealno je torej izdelava ocene učinka nekakšna predhodna faza pred dokončnim oblikovanjem konkretnih zakonskih določb, včasih pa, razumljivo, zaradi nujnosti to poteka vzporedno s samim oblikovanjem zakonske ureditve. V pomoč zavezancem je Informacijski pooblaščenec pripravil infografiko, ki pojasnjuje namen in proces priprave zakonodajnih ocen učinka²³. V zvezi z zakonodajnimi ocenami učinka ugotavljamo, da vsi predlagatelji predpisov te obveznosti še niso povsem sprejeli, v določenih primerih pa se ocene učinka pripravijo prepozno, torej po tem, ko je besedilo predpisa v večji meri že določeno. Ocenjujemo, da zakonodajne ocene učinka glede varstva osebnih podatkov pozitivno pripeljejo k pravočasnemu naslavljanju tveganj z vidika varstva osebnih podatkov pri sprejemanju predpisov in s tem k njihovi kakovosti.

Informacijski pooblaščenec posebej opozarja, da morajo biti predlagatelji ob pripravi zakonodajnih ocen učinka pozorni na zahteve drugega odstavka 6. člena ZVOP-2 glede sestavin, ki naj bi jih vsebovali zakoni, ki urejajo obdelave osebnih podatkov zaradi izvajanja zakonske obveznosti, javnega interesa ali izvajanja javne oblasti, in sicer naj bi zakon določal obdelavo osebnih podatkov, vrste osebnih podatkov, ki se bodo obdelovale, kategorije posameznikov, na katere se ti osebni podatki nanašajo, namen njihove obdelave in rok hrambe osebnih podatkov ali rok za redni pregled potrebe po hrambi. Če je mogoče, se v zakonu določijo tudi uporabniki osebnih podatkov, posamezna dejanja obdelave in postopki obdelave ter drugi ukrepi za zagotovitev zakonite, poštene in pregledne obdelave.

ZVOP-2 poleg zakonodajnih ocen učinka določa dodatne obveznosti glede ocene učinka, in sicer za naslednja področja:

- vodenje dnevnikov obdelav in ocena učinka (22 in 24. člen ZVOP-2),
- obdelava osebnih podatkov za raziskovalne namene (69. člen ZVOP-2),
- videonadzor cestnega prometa (80. člen ZVOP-2),
- ocena učinka pri povezovanju zbirk osebnih podatkov (87. člen ZVOP-2).

Posebej je urejeno tudi področje varnosti države, in sicer za obdelavo osebnih podatkov na področju varnosti države pristojni organ s področja varnosti države pripravi oceno učinka s smiselno uporabo določb 24. člena ZVOP-2. Ocenjujemo, da je širitev obveznosti glede izdelave ocen učinka za nekatere zavezance sicer novost, a menimo, da bo s časom ta pomemben instrument načela odgovornosti prinesel dobre rezultate.

S sprejemom ZVOP-2 je pomemben zagon dobilo tudi področje potrjevanja (certifikacije) in s tem povezane akreditacije po Splošni uredbi. Slednja namreč omogoča, da se določni procesi obdelav osebnih podatkov (npr. kadrovska funkcija, klub zvestobe, mobilna aplikacija) certificirajo, zavezanci pa s tem izkazujejo visoko raven spoštovanja zakonodaje. Certifikacija je po Splošni

²³ Infografika je dostopna na: https://www.ip-rs.si/fileadmin/user_upload/Pdf/infografike/infografika%20-%20DPIA.pdf

uredbi prostovoljna, ne posega pa v pooblastila nadzornih organov za varstvo osebnih podatkov. Pred sprejemom ZVOP-2 tovrstna certifikacija ni bila možna, s sprejemom ZVOP-2 pa je bilo odločeno, da bo akreditacijo teles, ki bodo izvajala certifikacijo (t. i. organi za potrjevanje oziroma certifikacijska telesa), izvajala Slovenska akreditacija, dodatne zahteve za akreditacijska merila pa predpiše Informacijski pooblaščenec. Informacijski pooblaščenec je konec leta 2023 pripravil tovrstne zahteve in jih poslal v mnenje EOVP skladno z določbami Splošne uredbe. Ocenjujemo, da bo certifikacija na tem področju možna v drugi polovici leta 2024, za lažje razumevanje zadevnih postopkov pa je Informacijski pooblaščenec pripravil posebno infografiko.²⁴

Poudariti je treba, da je certifikacija, ki je sicer po določbah Splošne uredbe prostovoljna, za zavezanca na področju biometrije glede na določbe ZVOP-2 obvezna. Zavezanci iz zasebnega sektorja, ki bi želeli uporabljati biometrijo, morajo v postopku potrjevanja (certifikacije) pridobiti potrdilo oz. certifikat, ki ga izda akreditirano certifikacijsko telo. Ocenjujemo, da lahko ta določba v praksi povzroči kar nekaj težav, saj je potrjevanje po Splošni uredbi – s tem pa tudi akreditacija teles za potrjevanje, ki bi izdajala potrdila – prostovoljno in ne obvezno. Ob pomanjkanju interesa certifikacijskih teles za pridobitev akreditacije, ki terja nezanemarljive resurse in znanja, ne bo možno potrditi dejanj obdelave biometričnih osebnih podatkov. Prehodna določba v 121. členu ZVOP-2 to problematiko sicer deloma rešuje, saj se obdelave, za katere bo do 1. 7. 2024 dana vloga za certifikacijo, štejejo za skladne z merili iz mehanizma potrjevanja do 31. 12. 2024. Po preteku tega obdobja pa zavezanci, ki bi morali pridobiti certifikat, ne bodo mogli zagotoviti skladnosti, če postopki potrjevanja ne bodo na voljo. Pri tem velja omeniti, da so tudi v drugih državah EU postopki akreditacije in certifikacije večinoma v začetnih fazah. Interes po certifikaciji naj bi bil zlasti prisoten na področju nujenja različnih informacijskih rešitev, kot so vzdrževanje programske opreme in mobilnih aplikacij.

Pomembno vlogo pri zagotavljanju načela odgovornosti in s tem skladnosti imajo tudi pooblaščenec osebe za varstvo osebnih podatkov. Glede tega je v letu 2023 potekala prva usklajena akcija sodelovanja (Coordinated Enforcement Framework – CEF) Evropskega odbora za varstvo podatkov (EOVP), v kateri so praktično vsi nadzorni organi v EU sodelovali pri analizi stanja in izvedbi drugih ukrepov na tem področju. Informacijski pooblaščenec se je odločil, da bo k usklajeni akciji pristopil na način preventivne aktivnosti za skladnost (angl. privacy sweep), v okviru katere smo vabilo k izpolnitvi usklajenega vprašalnika posredovali celotnemu registru pooblaščenih oseb in prejeli skoraj 1000 odgovorov. Nadzorni organi za varstvo osebnih podatkov smo nato analizirali stanje in pripravili ukrepe za izboljšanje stanja.

Usklajena akcija sodelovanja na evropskem nivoju je pokazala, bo v nadaljevanju treba več pozornosti nameniti vprašanju, ali so pooblaščenec osebe ustrezno podprte in izobražene, ali opravljajo predvidene naloge na področju nadzora, svetovanja in ozaveščanja in ali so v morebitnem konfliktu interesov bodisi zaradi izvajanja nalog, ki ne sodijo med naloge pooblaščenec osebe, bodisi kot zunanje pooblaščenec osebe zaradi nujenja drugih storitev.²⁵ Glede na uspeh usklajene akcije bo tovrstna akcija nadelavala tudi v letu 2024, in sicer na temo pravice posameznikov do dostopa do lastnih osebnih podatkov.

Informacijski pooblaščenec je okrepil sodelovanje s pooblaščenimi osebami za varstvo osebnih podatkov in konec leta 2023 organiziral posvet s pooblaščenimi osebami za varstvo osebnih podatkov na ministrstvih, ki so med ključnimi zavezanci glede varstva osebnih podatkov tako zaradi vodenja številnih velikih zbirk osebnih podatkov kot zaradi priprave sprememb zakonodaje. Udeleženci so se strinjali, da je tovrstno sodelovanje koristno, zato bomo s takšnimi srečanji nadaljevali tudi v prihodnje, s poudarkom na določenih posebej izpostavljenih sektorjih, kot sta npr. vzgoja in izobraževanje ter zdravstvo, saj omenjena sektorja (glede na zahteve Splošne uredbe in ZVOP-2 po imenovanju

²⁴ Dostopna je na povezavi: https://www.ip-rs.si/fileadmin/user_upload/Pdf/infografike/Infografika%20potrjevanje_akreditacija.pdf.

²⁵ Poročilo je dostopno na povezavi: https://www.edpb.europa.eu/system/files/2024-01/edpb_report_20240116_cef_dpo_en.pdf.

pooblaščenih oseb) predstavljata največji del registra pooblaščenih oseb.

Prav tako ocenjujemo, da so za doseganje skladnosti na področjih, kjer so opazne sistemske nepravilnosti, pomanjkljivosti ali kršitve, preventivne aktivnosti za skladnost zelo učinkovito orodje. Zlasti so primerno orodje tam, kjer je nabor zavezancev znan oziroma določljiv, kjer obstajajo združenja zavezancev, ki lahko pomagajo pri distribuciji gradiv, in tam, kjer so že na voljo gradiva, kot so smernice, infografike in vzorci, ki zavezancem lahko pomagajo pri doseganju skladnosti. Kot je bilo poudarjeno na letni mednarodni konferenci informacijskih pooblaščenec, si namreč večina zavezancev ne želi kršiti zakonodaje in se s tem izpostavljati sankcijam, imajo pa težave pri razumevanju zakonodaje in njeni implementaciji, zato so preventivne aktivnosti nadzornih organov zelo pomembne. Ob tem ne gre zanemariti, da so prav tako pomembne tudi nadzorne in kaznovalne aktivnosti nadzornih organov – ocenjujemo, da je odsotnost možnosti za izrekanje kazni po Splošni uredbi zaradi zamujanja ZVOP-2 močno negativno učinkovala na splošno raven skladnosti pri zavezancih, saj je vendarle pomemben element prisile izostal.

Z vidika skladnosti in preventive je Informacijski pooblaščenec skozi leta razvil obširen nabor instrumentov in orodij, s katerimi (poleg že omenjenih) vpliva na raven ozaveščenosti ter s tem razumevanja in spoštovanja zakonodaje, zato bo tudi v prihodnje izdajal smernice, infografike, mnenja, redno bo obveščal javnost prek svoje spletne strani, družabnih omrežij in novičnikov, še naprej bo sodeloval s partnerskimi organizacijami, podeljeval priznanja ob dnevu varstva osebnih podatkov, prav tako bo tudi organiziral brezplačna predavanja ter se udeleževal relevantnih strokovnih posvetov in konferenc.

Informacijski pooblaščenec sodeluje tudi v različnih delovnih skupinah EOVP in s tem prispeva k oblikovanju ključnih smernic, priporočil in odločitev v zvezi z varstvom osebnih podatkov. Predstavniki Informacijskega pooblaščenca so v letu 2023 aktivno sodelovali v 11 rednih ekspertnih podskupinah ter v 12 posebnih delovnih ter koordinacijskih skupinah oz. odborih glede specifičnih tematik ter na 15 plenarnih zasedanjih. Skupno so se udeležili 147 sestankov.

EOVP je v letu 2023 prispeval k razlagam številnih določb Splošne uredbe s smernicami in priporočili, npr. s smernicami o tehničnem obsegu 5. člena direktive o eZasebnosti in s smernicami o 37. členu 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.

Na področju svetovanja Evropski komisiji v zvezi z vprašanji varstva podatkov in priprave evropskih predpisov s področja varstva podatkov je EOVP v letu 2023 pripravil mnenje glede osnutka sklepa o ustreznosti okvira o zasebnosti podatkov EU-ZDA, ki izraža skrb glede izvajanja pravic posameznikov, nadaljnjih prenosov, glede obsega izjem in začasnega množičnega zbiranja podatkov ter glede delovanja mehanizma obrambe v praksi. Skupaj z Evropskim nadzornikom za varstvo podatkov je EOVP pripravil mnenje o predlogu uredbe o digitalnem evru kot digitalni valuti centralne banke. V mnenju so poudarjeni vidiki varstva osebnih podatkov pri uporabi digitalnega evra ter podana različna priporočila. Posamezniki naj bi vedno imeli možnost izbire pri plačevanju z digitalnim evrom ali denarjem. Skupaj z Evropskim nadzornikom za varstvo podatkov je EOVP pripravil tudi Mnenje o predlogu uredbe o določitvi dodatnih postopkovnih pravil v zvezi z izvrševanjem Uredbe (EU) 2016/679. Uredba naj bi podrobneje predpisala procesne korake in zagotovila pri čezmejnih postopkih nadzora, ki jih bodo morali upoštevati vodilni in zadevni organi. Sprejeta so bila tudi številna mnenja v postopkih skladnosti glede certifikacijskih in akreditacijskih mehanizmov.

Srečanja in s tem sodelovanje vseh nadzornih organov v okviru EOVP so bistvena za zagotavljanje doslednega izvajanja Splošne uredbe po vsej EU in za učinkovit nadzor na področju varstva osebnih podatkov. EOVP je pripravil tudi izjavo o tesnejšem sodelovanju nadzornih organov pri izvajanju strateških nadzornih primerov. V okviru svoje strategije za poostreno sodelovanje med nadzornimi

organi je EOVP ustanovil podporno skupino strokovnjakov (t. i. *Support Pool of Experts*), katere cilj je zagotoviti vsebinsko podporo članicam EOVP pri njihovih nadzorih. EOVP je v letu 2023 uvedel tudi novo delovno skupino ChatGPT, katere namen je usklajevanje pri vprašanjih skladnosti tega ponudnika generativne umetne inteligence s Splošno uredbo.

ODGOVORNA UREDNICA:

Mojca Prelesnik, informacijska pooblaščenka

AVTORJI BESEDIL:

Jože Bogataj, namestnik informacijske pooblaščenke

dr. Jelena Virant Burnik, vodja mednarodnega sodelovanja in razvoja

Jasna Duralija, svetovalka pooblaščenca

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

Matej Sironič, svetovalac pooblaščenca za varstvo osebnih podatkov

Ana Škrilin, študentka

mag. Andrej Tomšič, namestnik informacijske pooblaščenke

Barbara Žurej, svetovalka pooblaščenca za preventivo

OBLIKOVANJE:

Tomaž Brodgesell

Darko Mohar

LEKTORIRALA:

Katja Klopčič Lavrenčič

Informacijski pooblaščenec Republike Slovenije

Dunajska cesta 22

1000 Ljubljana

www.ip-rs.si

gp.ip@ip-rs.si

ISSN 2670-5788

Ljubljana, maj 2024



INFORMACIJSKI
POOBLAŠČENEC