

LETNO POROČILO ZA LETO 2025



INFORMACIJSKI
POOBLAŠČENEC

UVODNA BESEDA INFORMACIJSKE POOBLAŠČENKE GRADIMO MOSTOVE

Spoštovani,

pred vami je poročilo o delu Informacijskega pooblaščenca za leto 2025. Preteklo leto je zaznamoval izredno velik porast pritožb in prijav na vseh področjih naših pristojnosti, s tem pa so se povečale tudi potrebe po kadrovskih okrepitvah. Kot drugje v Evropi je porast deloma mogoče pripisati uporabi komercialnih umetnointeligenčnih storitev, s katerimi je mogoče prijavo pripraviti v trenutku in jo prav tako hitro tudi oddati organu. Pogosto se izkaže, da take prijave niso utemeljene, vendar mora njihova obravnava kljub temu potekati skladno s procesnimi zagotovili: strokovno, neodvisno in z inteligenco strokovnih sodelavcev. To seveda ni mogoče le v nekaj minutah in pomeni za organ veliko obremenitev.

Informacijski pooblaščenec se je v minulem letu kadrovske okrepil, vendar bodo zaradi izrazitega povečanja obsega zadev dodatne okrepitve potrebne tudi v prihodnje, zato je ključno, da so Informacijskemu pooblaščenču namenjena ustrezna proračunska sredstva, na kar aktivno opozarjamo pristojno ministrstvo. Tako zaključuje tudi Evropska komisija v poročilu o schengenski državi za Slovenijo za leto 2025 – državi nalaga, da mora zagotavljati ustrezna sredstva za to, da lahko Informacijski pooblaščenec izvaja redno, učinkovit nadzor. Zagotoviti mora tudi popolno proračunsko neodvisnost Informacijskega pooblaščenca, tako da se ima ta glede sredstev pravico obrniti neposredno na Državni zbor.

V lanskem letu je Računsko sodišče izvedlo revizijo našega poslovanja. Ta je bila v začetku leta 2026 zaključena s pozitivnim mnenjem. Ponosno torej lahko poudarim, da Informacijski pooblaščenec posluje zakonito in učinkovito.



"Že zdaj si lahko predstavljam dileme: Ali dokument o uporabi umetne inteligence pri zavezancu obstaja? Ali je mogoče razkriti model umetne inteligence? Gre za osebne podatke?"

Informacijski pooblaščenec je bil ustanovljen leta 2005 in od takrat intenzivno gradimo most med področjem dostopa do informacij javnega značaja in varstvom osebnih podatkov. V zadnjem letu smo začeli graditi še most med varstvom osebnih podatkov in regulacijo umetne inteligence. Informacijski pooblaščenec je namreč postal eden od organov za nadzor trga po Aktu o umetni inteligenci. V prihodnje nas čaka še gradnja mostu med umetno inteligenco in dostopom do informacij javnega značaja. Že zdaj si lahko predstavljam dileme: Ali dokument o uporabi umetne inteligence pri zavezancu obstaja? Ali je mogoče razkriti model umetne inteligence? Gre za osebne podatke? Obstaja prevladujoč javni interes za razkritje dokumentov o uporabi umetne inteligence v katerem od organov javnega sektorja?

Na področju dostopa do informacij javnega značaja smo lani obravnavali več kot 900 pritožb. Število pritožb narašča iz leta v leto – lani se je vnovič povečalo, in sicer za 20 %. Nekaj več kot 10 % vseh zahtev za dostop do informacij javnega značaja, ki jih prejme javni sektor, konča pod našimi rokami. Zakon o dostopu do informacij javnega značaja v praksi živi in je pomembno orodje za novinarje in druge prosilce, ki razkrivajo informacije in s tem prispevajo k preglednosti delovanja javnih institucij, oblasti, politike, države, vendar pa je prepogosto šele Informacijski pooblaščenec tisti, ki naloži razkritje dokumentov, do katerih je javnost upravičena.

Pri pridobivanju informacij je čas bistvenega pomena, vendar pa se čas do prejema informacije zlahka podaljša na več let, če so vloženi upravni spori. Kljub temu da je zakonodaja glede javnosti določenih informacij jasna in je že ustaljena tudi praksa odločanja Informacijskega pooblaščenca in sodišč, zavezanci vlagajo upravne spore in s tem podaljšujejo čas do razkritja informacij. Na mestu je vprašanje, koliko je taka informacija po več letih sploh še uporabna. Veliko število neutemeljenih pritožb v minulem letu

kaže tudi na povečano število t. i. zlorabe pravice. Pri posameznih zavezancih je bilo namreč kontinuirano vloženi več zahtev istega prosilca ali skupine prosilcev, te zahteve pa so zaradi števila in velikega obsega povzročile nerazumne obremenitve.

Namen ZDIJZ je odpiranje informacij, vendar pa tudi tehtanje in iskanje ravnotežja med različnimi pravicami in interesi, ki so določeni kot izjeme od prostega dostopa do podatkov in so lahko razkriti le ob testu prevladujočega interesa javnosti. Pogosto rečem, da je skoraj ni politično izpostavljene zadeve, ki se ne bi na tej ali oni točki znašla pred Informacijskim pooblaščenecem. Naše odločitve seveda niso nujno vsem všeč, običajno pomenijo, da se bo neki organ oz. njegov predstojnik moral soočiti z mnenjem javnosti ali celo z nadzornimi postopki glede pravilnosti svojega dela in odločitev. Včasih z našo odločitvijo ni zadovoljen prosilec, ko dokumenta z našimi pooblastili ne moremo odkriti ali pa ga ne moremo razkriti zaradi pretehtanih interesov, ki jih varujejo izjeme. Ne glede na to pa z veseljem ugotavljam, da morebitno nezadovoljstvo z našimi odločitvami ni odvisno od političnega pola, od prosilca, od organa. Naše odločitve so neodvisne, vedno temeljijo na strokovnosti, tehtnih argumentih ter sledijo ustaljeni praksi organa in sodišč. ZDIJZ v Sloveniji omogoča razvoj prakse, ki je zgled marsikateri državi. To potrjuje tudi poročilo evalvacije izvajanja Tromso konvencije Sveta Evrope o dostopu do uradnih dokumentov, ki jo je ratificirala Slovenija.

Na področju varstva osebnih podatkov smo v lanskem letu zabeležili še posebno skokovit porast postopkov, in to vseh, nadzornih, prekrškovnih in čezmejnih – gre za več kot 40-odstotno povečanje števila postopkov, kar pomeni zelo veliko dodatno obremenitev zaposlenih. Jeseni je močno odmeval primer ranljivosti ene od državnih zbirk podatkov, zaradi česar so bili podatki več kot 900.000 državljanov, med drugim njihov EMŠO in davčna števil-

ka, dostopni javnosti. Ob tem se je vnovič pokazalo, kako pomembno je ustrezno varovanje največjih zbirk podatkov v državi in kakšne so lahko škodljive posledice ob razkritju. Ukvarjali smo se tudi z mejami pristojnosti Informacijskega pooblaščenca, ko gre za obdelavo osebnih podatkov s strani medijev oz. pri dejavnostih v zvezi z izvrševanjem pravice svobode govora. Zakon o varstvu osebnih podatkov na to področje žal ni prinesel potrebne jasnosti in želim si, da svoje čim prej pove tudi sodna praksa.

Učinkovito izvajanje nadzora, sankcioniranje kršitev in obravnava pritožb so primarne zakonske pristojnosti Informacijskega pooblaščenca, veliko časa pa namenimo tudi posvetovalnim aktivnostim. Opažamo, da velika večina zavezancev želi delovati skladno s pravili, pa morda nima ustreznega znanja ali ne pozna dovolj dobro problematike, in tu so jim lahko v veliko pomoč konkretne usmeritve. Tudi v prihodnje ostaja to ena naših prioriteta, tako v smislu posvetovanj za organizacije iz zasebnega kot iz javnega sektorja. Naš trenutni izziv so omnibus uredbe, ki prihajajo iz EU kot odziv na kritiko, da EU preveč regulira in premalo inovira. Poenostavitve naj bi odvzele del birokratskega bremena, vendar me skrbi, da nekateri predlogi ustvarjajo dodatne pravne nejasnosti in bi lahko znižali standarde varovanja pravic v EU.

Ključna je tudi naš angažma v Evropskem odboru za varstvo podatkov. Pred kratkim smo se v Helsinški izjavi nadzorni organi v EU zavezali k temu, da z raznimi orodji in mehanizmi predvsem manjšim organizacijam pomagamo na poti k lažjemu doseganju skladnosti s pravili varstva osebnih podatkov. Evropski odbor ima izredno pomembno mesto v zagotavljanju skladnosti uporabe pravil s področja varstva osebnih podatkov v EU, zato sem ponosna, da bom k njegovim aktivnostim naslednjih pet let lahko prispevala tudi kot izvoljena podpredsednica.

V preteklem letu smo izdali skoraj 40 % več mnenj na zakonodajne predloge, ki niso ustrezno upoštevali varstva osebnih podatkov, še posebno na tem mestu opozarjam na področje digitalizacije velikih državnih zbirk podatkov. Upoštevanje pravil varstva osebnih podatkov lahko izboljša proces digitalizacije, zmanjša tveganja, da so podatki razkriti ali napačno obdelani, kar ima za posameznike negativne posledice. Tu ne gre le za varovanje zasebnosti posameznikov, kot smo večkrat opozorili pri sprejemanju Zakona o di-

gitalizaciji zdravstva. Napake pri obdelavi podatkov v zdravstvu lahko pomenijo tveganje za življenje posameznika, enako velja za nepremišljeno obdelavo podatkov z umetno inteligenco, dopuščanje obdelav podatkov za druge namene pa lahko pomeni, da nas zasledujejo oglasi za sporna zdravila vprašljive kakovosti, vse to pa izkorišča naša ranljivost. Še posebno je zaščita pred slednjim pomembna, ko govorimo o mladostnikih in starejših, ki so lažja tarča tovrstnih zlorab.

Z veseljem omenjam naše aktivnosti za mlade, za generacije, ki bodo živele z odločitvami, ki jih sprejemamo danes. Današnje igrišče je pogosto na spletu, žogi so se pridružile umetnointeligentne igrače, a pravila bi morala ostati ista – kako biti spoštljiv,

"Glede na to, da umetna inteligenca poleg prednosti prinaša tudi tveganja, je res pomembno, da se na vseh ravneh zavzemamo za razvoj zaupanja vrednega ekosistema umetne inteligence."

odgovoren, kako varovati zaupne podatke. Trenutno izvajamo EU-projekt PrivacyPRO, v katerem smo za mlade zasnovali družabno igro *Misija IP – postani varuh podatkov*, pripravili smo stripe, poučne video posnetke z igralcem Juretom Henigmanom, šolarje smo gostili v prostorih Informacijskega pooblaščenca ter izdelali gradiva za učne ure, ki jih lahko izvajajo učitelji. Varovanje otrok je ena od prioriteta mojega mandata tudi pri izvajanju nadzora. Pridružili smo se npr. 26 organom za varstvo zasebnosti z vsega sveta in skupaj smo pregledali več kot 900 storitev in aplikacij, ki jih uporabljajo otroci, ter opozorili na pomanjkljivosti. Našo odločitev, da morajo šole upoštevati privzeto varstvo osebnih podatkov ter podatkov otrok ne smejo posredovati tretjim osebam, je potrdilo tudi sodišče. Še vedno pa čakamo na odločitev sodišča glede največjega ponudnika informacijskih storitev v šolstvu, za katerega je Informacijski pooblaščenec odločil, da mora nehati z obdelavo osebnih podatkov za plačljivi del storitve.

V okvir naše pristojnosti od konca lanskega leta sodijo tudi sistemi UI, ki jih Akt o umetni inteligenci prepoveduje, npr. sistemi za družbeno točkovanje, za napovedovanje izvrševanja kaznivih dejanj in za sklepanje o čustvih na delovnem mestu in v izobraževanju. Pravila na tem področju se že uporabljajo. Nadzorovali bomo tudi visoko tvegane sisteme UI na

področju biometrije, izobraževanja, kaznivih dejanj, migracij, azila in nadzora nad mejami ter na področju pravosodja in volitev. Poleg nas bodo nadzor izvajali tudi Agencija za komunikacijska omrežja in storitve, Banka Slovenije, Agencija za zavarovalni nadzor in Tržni inšpektorat. V praksi to pomeni nov oddelek znotraj Informacijskega pooblaščenca ter povezovanje z drugimi organi v Sloveniji in na ravni EU v Odboru za UI.

Glede na to, da umetna inteligenca poleg prednosti prinaša tudi tveganja, je res pomembno, da se na vseh ravneh zavzemamo za razvoj zaupanja vrednega ekosistema umetne inteligence. Le tako nam bo kot družbi nova tehnologija resnično v korist. Ne smemo pozabiti na različne negativne posledice za pravice posameznikov, ki se lahko zgodijo zaradi pristranosti ali napak v podatkih, pa na posege v zasebnost in dostojanstvo. Vse več je govora tudi o negativnih vplivih na okolje. Enormna je poraba energije, elektrike, vode in energije za hlajenje – npr. za pozive, ki jih vnašamo v storitve ponudnikov generativne UI, katerih edini namen je pravzaprav zabava oz. ustvarjanje *brain rota*, kot pravijo najstniki danes.

Informacijski pooblaščenec bo v te teme tesno vpet kot nadzorni organ za varstvo osebnih podatkov ter po novem kot organ za nadzor trga za sisteme umetne inteligence, pa tudi preko obravnave pritožb s področja informacij javnega značaja. Pričakujem namreč, da bomo državljani radovedni glede tega, kako javne institucije uporabljajo umetno inteligenco in kaj to pomeni za nas in za naše okolje. Informacijski pooblaščenec bo tudi na tem področju spodbujal transparentnost in odgovornost javnih institucij.

Tudi v prihodnje bomo torej gradili mostove med različnimi področji našega delovanja, med pravom, tehnologijo, družbo in etiko, ter dosledno varovali neodvisnost institucije. Močne neodvisne nadzorne institucije z ustreznimi viri so namreč ključne za odprto in demokratično družbo. V organizacijskem smislu to pomeni spodbujanje interdisciplinarnosti, izobraževanja, kreativnosti, tudi preko povezovanja s študenti in različnimi fakultetami. Odlična popotnica pri gradnji vseh teh mostov so naše znanje, predanost in strokovnost zaposlenih, katerim gre – kot vsako leto – iskrena zahvala za vse opravljeno delo.

dr. Jelena Virant Burnik,
informacijska pooblaščenka



STRNJEN PREGLED LETA

DOSTOP DO INFORMACIJ JAVNEGA ZNAČAJA

Na področju dostopa do informacij javnega značaja je Informacijski pooblaščenec v letu 2025 obravnaval 1.301 zadevo, kar je 155 več kot v letu 2023 (13-odstotni porast) in največ od ustanovitve. Od leta 2016 (ko je bilo obravnavanih 822 zadev) se je število zadev na tem področju povečalo za kar 58 %. Kot že nekaj let zapored je tudi v letu 2025 naraslo število vseh prejetih pritožb, in sicer za 20 % (v letu 2024 je Informacijski pooblaščenec prejel skupaj 776 pritožb, v letu 2025 pa 920). Od tega je bil pretežni del pritožb vloženih zoper zavrnilne odločbe (601), 319 pa zaradi t. i. molka organa oz. neodzivnosti. V 381 primerih je Informacijski pooblaščenec odgovoril na zaprosila zavezancev in prosilcev glede procesnih vprašanj ter jih napotil na svojo prakso.

V skupnem deležu pritožb je delež pritožb zoper zavrnilne odločbe znašal 65 %, kar je več kot preteklo leto. Pri tem se je (podobno kot v letu 2024) vnovič zmanjšal delež prejetih pritožb zaradi molka, kar je pozitiven kazalnik, ki kaže na to, da so zavezanci manjkrat zamudili rok za posredovanje informacij javnega značaja. Po več letih naraščanja se je zmanjšalo tako število pritožb zaradi molka občin kot zaradi molka državnih organov, kar kaže na to, da sta bili ti dve skupini zavezancev v preteklem letu bolj odzivni. Žal je Informacijski pooblaščenec v letu 2025 zaznal tudi bistven porast pritožb zaradi molka zoper javne zavode, in sicer za 38 %. Tej skupini zavezancev bo treba v prihodnje nameniti (še) več pozornosti v smislu ozaveščanja in podpore pri delu.

Kot že vsa leta do zdaj je Informacijski pooblaščenec tudi v letu 2025 zoper poslovne subjekte pod prevladujočim vplivom vodil izjemno malo postopkov (16 zadev, kar je 1,7 % vseh pritožbenih zadev). To gre pripisati dejstvu, da so ti zavezanci za dostop do informacij javnega značaja zavezani le v ozkem delu svoje dejavnosti, ki ga zakon natančno določa (le glede pravnih poslov za izdatke, upravljanja s stvarnim premoženjem in izplačil poslovnim osebam), obenem pa ZDIJZ zanje določa široko obveznost proaktivne objave, po kateri morajo večino absolutno javnih informacij sami objaviti na svojih spletnih straneh.

V letu 2025 je Informacijski pooblaščenec v pritožbenih postopkih zoper zavrnilne odločbe izdal 540 odločb, kar je 64 več kot leto pred tem (ko je izdal 476 odločb). Ker se je skupno število prejetih pritožb (kot že nekaj let zapored) znova povečalo, se je čas reševanja pritožbenih zadev pri Informacijskem pooblaščenju podaljšal. Pritožbeni postopki namreč postajajo vse kompleksnejši in pogosto terjajo presojo obsežne dokumentacije in vključitev številnih stranskih udeležencev. Zanimiv je tudi podatek, da je Informacijski pooblaščenec večino prejetih pritožb kot neutemeljene zavrnil (300), pritožbam je, delno ali v celoti, ugodil v 149 primerih, v 91 primerih pa je zadeve vrnil prvostopenjskim organom v ponovni postopek, ker je ugotovil bistvene kršitve pravil postopka. To kaže na to, da je postopek za zavezance in prosilce (pre)zahteven in bi ob morebitni spremembi zakona kazalo stremeti k poenostavitvi postopka in s tem k skrajšanju časa reševanja.

Veliko število neutemeljenih pritožb kaže tudi na povečano število t. i. zlorabe pravice, ki jo je Informacijski pooblaščenec v letu 2025 obravnaval v 46 primerih. Pri tem je ugotovil, da se je v tem letu povečalo število zadev, pri katerih je bilo pri posameznih zavezancih kontinuirano vloženih več zahtev istega prosilca ali skupine prosilcev, te zahteve pa so zaradi števila in velikega obsega pri posameznih (zlasti manjših) zavezancih povzročile nerazumne obremenitve. Kljub temu da je Informacijski pooblaščenec v pretekli praksi že zavzel stališče, da je zlorabo pravice treba razlagati ozko, pa velja opozoriti, da se število neutemeljeno vloženih zahtev pri posameznih zavezancih povečuje in da imajo zavezanci v praksi zlasti težave z obrazložitvijo, da gre za zlorabo. Informacijski pooblaščenec je obravnaval 46 primerov ter v 26 primerih potrdil, da gre za zlorabo, v petih primerih je odločil, da zloraba ni podana, v preostalih 15 zadevah pa je odločbe organov odpravil in zadeve vrnil v ponovni postopek, ker je ugotovil, da organi zatrjevane zlorabe niso izkazali.

VARSTVO OSEBNIH PODATKOV

Na področju varstva osebnih podatkov je Informacijski pooblaščenec v letu 2025 največ pozornosti namenil učinkovitemu izvajanju nadzornih postopkov, svetovanju posameznikom, zavezancem ter pripravljavcem predpisov in preventivnim aktivnostim za delo z mladimi. Na področju nadzora nad uveljavlja-

njem varstva osebnih podatkov v praksi je Informacijski pooblaščenec v letu 2025 prejel 1365 prijav (štete so tako inšpekcijske prijave kot tudi prijave prijaviteljev s posebnim položajem, ki se nanašajo na prijave kršitev varstva osebnih podatkov prijaviteljev), kar je največ od ustanovitve. Na podlagi prijav prijaviteljev s posebnim položajem je bilo uvedenih 464 nadzornih postopkov, na podlagi inšpekcijskih prijav pa 102 inšpekcijska postopka, upravljavcem je bilo poslanih tudi 176 obvestil z usmeritvami, kako zagotoviti skladno obdelavo osebnih podatkov.

Dodatno je Informacijski pooblaščenec v 243 čezmejnih nadzornih postopkih sodeloval kot zadevni nadzorni organ na podlagi 60. člena Splošne uredbe (postopek čezmejnega sodelovanja) in obravnaval 270 zahtev za medsebojno pomoč po 61. členu Splošne uredbe. Informacijski pooblaščenec je obravnaval tudi 153 uradnih obvestil o kršitvi varnosti osebnih podatkov ter 22 primerov nedovoljenega sporočanja ali druge nedovoljene obdelave osebnih podatkov o pacientih. Zaradi v postopku ugotovljenih kršitev varstva osebnih podatkov je Informacijski pooblaščenec v letu 2025 uvedel 146 prekrškovnih postopkov. Poleg tega je prejel tudi 38 pritožb glede seznanitve z zdravstveno dokumentacijo na podlagi Zakona o pacientovih pravicah in osem pritožb glede zahtev za posredovanje osebnih podatkov po 41. členu Zakona o varstvu podatkov.

Področje nadzora nad zagotavljanjem varstva osebnih podatkov je v letu 2025 zaznamovalo predvsem izjemno povečanje števila prejetih prijav kršitev varstva osebnih podatkov, ki se je v primerjavi z letom 2024 povečalo za kar 60 %. Razloge za to je mogoče deloma pripisati tudi vedno bolj razširjeni uporabi generativnih orodij umetne inteligence (t. i. klepetalnikov umetne inteligence (*ang. AI chat-bot*)) pri iskanju informacij in pravnih nasvetov. Posamezniki namreč tudi na področju varstva osebnih podatkov nasvete vse pogosteje iščejo s tovrstnimi orodji, ki pogosto svetujejo prijavo na nadzorni organ za varstvo podatkov. Praksa kaže, da so ta priporočila glede na naravo vprašanja oz. težave pogosto neustrezna. Nadzorni organ posledično prejme več prijav, ki po vsebini ne sodijo v okvir njegovih pristojnosti, ali pa jih je treba rešiti z drugimi oblikami pravnega varstva. Število državnih nadzornikov se v letu 2025 ni povečalo, zato je povečana rast prejetih prijav pomenila velik pritisk na zaposlene. Ob enakem številu državnih nadzornikov bo to tudi v prihodnje neizpodbitno botrovalo nastajanju novih zaostankov.

Pri izvajanju nadzornih aktivnosti Informacijskega pooblaščenca pomemben izziv prinaša tudi povečanje njegovih pristojnosti na podlagi novih aktov digitalne agende EU in nejasne opredelitve ter razmejnitve teh pristojnosti glede na različne organe, pristojne za nadzor.

V prijavah, ki jih je v obravnavanem obdobju prejel in obravnaval Informacijski pooblaščenec, so prijavitelji najpogosteje zatrjevali sum nezakonitega razkrivanja in posredovanja osebnih podatkov neupravičenim osebam oz. nezakonito objavo osebnih podatkov. Po številu so sledile prijave, vložene zaradi nezakonitega izvajanja videonadzora, prijave zaradi suma kršitve pravic posameznikov, prijave nezakonitega ali prekomernega zbiranja osebnih podatkov, prijave uporabe osebnih podatkov za namene neposrednega trženja, prijave neustreznega zagotavljanja varnosti osebnih podatkov ter prijave nezakonitih vpogledov v zbirke osebnih podatkov.

Veliko prejetih prijav se je nanašalo na področje obdelav v okviru delovnih razmerij. Izpostaviti velja zlasti problematiko nadzora zaposlenih. Veliko števil prejetih prijav se je nanašalo na objave osebnih podatkov (tudi fotografij) v medijih. Za obravnavo tovrstnih prijav glede uveljavljanja pravic posameznikov pri obdelavi osebnih podatkov z namenom izvrševanja svobode izražanja so v skladu z določbo prvega odstavka 19. člena in tretjega odstavka 73. člena ZVOP-2 pristojna sodišča, in ne Informacijski pooblaščenec kot nadzorni organ. Sodišča odločajo v skladu z določbami zakonov, ki urejajo svobodo izražanja in sodno varstvo. Navedeno pomeni, da lahko prizadeti posameznik za uveljavljanje svojih pravic v zvezi z medijskim poročanjem (npr. izbris članka ali fotografije ali podatkov v članku) izkoristi sodno varstvo.

Pri obravnavi prijav Informacijski pooblaščenec ugotavlja, da v njih prijavitelji pogosto zatrjujejo enkratno preteklo kršitev (npr. nezakonit vpogled v njihove osebne podatke, posredovanje osebnih podatkov nepooblaščenemu uporabniku), ki v času vložitve prijave ne obstaja več. Taka prijava ne more biti predmet nadzornega postopka, v katerem se lahko obravnava le zatrjevane kršitve obdelave osebnih podatkov, 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 pretekle kršitve varstva osebnih podatkov obravnava zgolj v

okviru postopka o prekršku, ki ga uvede, če zazna zadostno stopnjo suma storitve katerega od prekrškov iz svoje pristojnosti.

Glede inšpekcijskih prijav je treba poudariti, da zatrjevane kršitve pogosto ne dosegajo standardov za uvedbo inšpekcijskega postopka z vidika javnega interesa, srečujemo pa se tudi s prijavi, ki so preveč splošne in brez kakršnih koli konkretnih indicov ali dokazov o obstoju nepravilnosti. V takih primerih ni smotno začeti postopka inšpekcijskega nadzora. Po eni strani gre za prijave, pri katerih ni zaznanih sistemskih težav, katerih ureditev bi bila v javnem interesu, ampak so razlogi za prijavo povsem zasebni, gre torej za posamezne primere z enkratnimi težavami, po drugi strani pa pri presplošnih prijavih praksa kaže, da uvedba inšpekcijskih postopkov ne prinaša zelenih rezultatov. Če iz navedb v prijavi ni mogoče v zadostni meri konkretizirati zatrjevane nepravilnosti, pa terja tudi nadpovprečno velik vložek sredstev.

Na področju nadzora nad zagotavljanjem varstva osebnih podatkov so nadzorne osebe pri Informacijskem pooblaščenca v letu 2025 skupaj rešile kar 1766 zadev, kar vključuje tudi zadeve, obravnavne v okviru čezmejnih postopkov po 60. členu Splošne uredbe. Poleg tega so nadzorne osebe zaključile 103 prekrškovne postopke ter pri tem izdale 134 prekrškovnih odločb, v katerih je bila kršiteljem v 89 primerih kot sankcija izrečena globa, v 45 primerih pa opomin. Rešenih pa je bilo tudi 23 pritožbenih primerov po Zakonu o pacientovih pravicah in 13 pritožb glede zahtev za posredovanje osebnih podatkov po 41. členu ZVOP-2 iz uradnih evidenc ali javnih knjig.

V letu 2025 je Informacijski pooblaščenec izdal več odločb zaradi nezakonite obdelave osebnih podatkov, ki so jih v zdravstvenih ustanovah izvedli zdravstveni delavci. Pri tem je šlo v večini primerov za nepooblaščen vpogled v osebne podatke pacientov v informacijskem sistemu posamezne zdravstvene ustanove in/ali v Centralnem registru podatkov o pacientih (CRPP). Kršiteljem je bila za take prekrške praviloma izrečena globa, zlasti ker je šlo pri tem praviloma za naklepne vpogled v osebne podatke in vpogled v zdravstvene osebne podatke. Informacijski pooblaščenec ocenjuje, da je povečano število obravnav navedenih prekrškov predvsem posledica večjega zavedanja pomembnosti varovanja osebnih podatkov tako na strani pacientov kot na strani nekaterih zdravstvenih ustanov ter

posledičnega obveščanja Informacijskega pooblaščenca v primeru zaznanega suma kršitev. Poleg teh je Informacijski pooblaščenec v prekrškovnih postopkih obravnaval tudi več primerov nezakonitih vpogledov, do katerih je prišlo s strani zaposlenih pri drugih upravljavcih, konkretno pri policiji in drugih državnih organih ter bankah.

Drugi vsebinsko obsežen sklop prekrškov, ki ga je v letu 2025 obravnaval Informacijski pooblaščenec, so predstavljali primeri nezakonite obdelave osebnih podatkov zaposlenih s strani delodajalcev, pri čemer je šlo v veliki večini primerov za izvajanje videonadzora delovnih prostorov v nasprotju z določbami ZVOP-2. Pri tem je šlo predvsem za primere, ko so delodajalci poleg zakonitega izvajanja videonadzora delovnih prostorov snemali tudi prostore, ki jih ne bi smeli, in na ta način prekomerno posegali v zasebnost zaposlenih. Informacijski pooblaščenec je v preteklem letu obravnaval tudi primer posebno hudega posega v zasebnost, ko je delodajalec na službene računalnike zaposlenih namestil poseben vohunski program, ki je na skrivaj spremljal in snemal vse dejavnosti zaposlenih na delovnem mestu, tj. ne samo na njihovih računalnikih, ampak tudi v pisarnah (zvočno snemanje telefonskih in osebnih pogovorov). Zaradi teže kršitve je Informacijski pooblaščenec kršitelju za prekršek, ki ga je s tem storil, izrekel najvišjo globo od začetka veljavnosti Splošne uredbe.

Pri drugih kršitvah varstva osebnih podatkov, v katerih je Informacijski pooblaščenec kršiteljem izdal odločbo in izrekel sankcijo, je šlo za kršitve zavarovanja osebnih podatkov, neustrezno uporabo piškotkov na spletnih straneh, razkrivanje osebnih podatkov nepooblaščenim osebam oz. nepooblaščenemu posredovanju osebnih podatkov, neustrezno informiranje posameznikov o obdelavi osebnih podatkov, kršitve pravic posameznikov iz Splošne uredbe in podobne primere.

Informacijska pooblaščenka dr. Jelena Virant Burnik je bila konec leta 2025 izvoljena za podpredsednico Evropskega odbora za varstvo podatkov, kar izkazuje zaupanje v njeno dolgoletno delo na tem področju in potrjuje prispevek Informacijskega pooblaščenca k razvoju in izboljšanju delovanja tega evropskega varuha podatkov.

Predstavniki Informacijskega pooblaščenca že vrsto let aktivno sodelujejo pri oblikovanju smernic, obveznih mnenj, odločitev in drugih dokumentov tega

odbora, pri čemer so v letu 2025 izstopale smernice o psevdonimizaciji in o obdelavi osebnih podatkov pri uporabi tehnologij za veriženje blokov (*angl. block-chain*). V zadnjih letih velik izziv za nadzor najkompleksnejših primerov predstavlja vprašanje prepleta in sovplivanja različnih aktov digitalne agende na zakonodajo s področja varstva osebnih podatkov, zato sta med pomembnejšimi dosežki EDPB v letu 2025 sprejem smernic o prepletu Akta o digitalnih storitvah in Splošne uredbe ter o prepletu Akta o digitalnih trgih in Splošne uredbe. Informacijski pooblaščenec je aktivno vlogo na svojem prioritetnem področju varstva otrok v digitalnem okolju prevzel tudi s sodelovanjem pri pripravi Izjave o preverjanju starosti, podrobno pa je v okviru Evropskega odbora za digitalne storitve spremljal tudi oblikovanje smernic Evropske komisije za zaščito mladoletnikov po 28. členu Akta o digitalnih storitvah (DSA).

Še eno pomembno področje, na katerem je Informacijski pooblaščenec posebej aktiven v okviru EDPB, je priprava mnenj na predloge zakonodajnih sprememb na ravni EU. V letu 2025 se je začela obravnavati dveh predlogov sprememb Splošne uredbe z omnibus zakonodajo. Med ključnimi dokumenti v letu 2025 je bila t. i. helsinška izjava, s katero so se članice EDPB zavezale, da si bodo še bolj prizadevale pomagati organizacijam za lažje doseganje skladnosti s Splošno uredbo, okrepile skladnost svojih nadzornih praks in še intenzivneje vključevale deležnike v delo EDPB. Zaposleni so se v letu 2025 udeležili več kot 170 sestankov v okviru 20 podskupin in drugih delovnih teles, 12 rednih plenarnih zasedanj ter enega izrednega in enega strateškega sestanka na najvišji ravni v Helsinkih na Finskem.

Z vidika skladnosti in preventive je Informacijski pooblaščenec skozi leta razvil obširen nabor instrumentov in orodij, s katerimi vplivamo na raven ozaveščenosti ter s tem razumevanja in spoštovanja zakonodaje. Informacijski pooblaščenec je v letu 2025 redno izdajal mnenja za splošno in strokovno javnost – izdal je 985 mnenj na zaprosila posameznikov in organizacij (od tega 847 pisnih, opravil pa je tudi 138 telefonskih svetovanj) ter izdal 117 pripomb na predpise. Opravljenih je bilo tudi 1446 telefonskih svetovanj.

Informacijski pooblaščenec je pripravil dve novi infografiki, razlago področja psevdonimizacije in novo ključno področje o tem na spletni strani ter infografiko o učinkovitem obvladovanju tveganj na področju varstva osebnih podatkov. Število izdanih mnenj na ocene učinka se je ustalilo, in sicer je Informacijski pooblaščenec v postopku predhodnega posvetovanja v letu 2025 izdal 30 mnenj.

Na dogodku ob evropskem dnevu varstva podatkov je Informacijski pooblaščenec podelil nagrado ambasador zasebnosti točki osveščanja o varni in odgovorni rabi interneta Safe.si. Podelitvi nagrad je sledila okrogla miza o stanju in izzivih varovanja zasebnosti in odgovorne uporabe digitalnih storitev pri otrocih ter o vključevanju izobraževalnih vsebin na to temo v učne načrte, dogodek pa se je zaključil s projekcijo filma *Lars je LOL*. Rdeča nit dogodka so bili namreč otroci in pomen ozaveščanja o varovanju zasebnosti v digitalnih okoljih, pri uporabi pametnih naprav.

Tudi v letu 2025 je Informacijski pooblaščenec izvajal preventivne aktivnosti za skladnost (*angl. privacy sweep*), izpostaviti je treba sodelovanji v usklajeni akciji sodelovanja v okviru EDPB, t. i. CEF (Coordinated Enforcement Framework) ter v okviru povezave Global Privacy Enforcement Network (GPEN). Tema usklajene akcije CEF je bila pravica do izbrisa, v akciji GPEN Privacy Sweep 2025 pa so predstavniki Informacijskega pooblaščenca pregledali 17 spletnih mest in aplikacij, ki so namenjene otrokom.

Informacijski pooblaščenec je v letu 2025 začel izvajati projekt PrivacyPRO, ki ga v okviru programa Državljeni, enakost, pravice in vrednote 2021–2027 sofinancira Evropska komisija. Projekt je namenjen povečanju ozaveščenosti in razumevanja načel varstva osebnih podatkov med otroki, učitelji, starši in skrbniki v Sloveniji, njegov namen pa je prispevati h kulturi varstva zasebnosti in osebnih podatkov že od zgodnjega otroštva. V letu 2025 so bile aktivnosti projekta primarno usmerjene v izdelavo izobraževalnih materialov za otroke, učitelje in starše. Ustvarili smo namizno igro *Misija IP: postani varuh podatkov* in istoimenske stripe, ki bodo od decembra 2025 do junija 2026 vsak mesec izhajali v reviji Pil. Posneli

smo sedem kratkih video vsebin z igralcem Juretom Henigmanom, v katerih otroke in mladostnike na zabaven način opozarja na pasti deljenja podatkov. Organizirali smo tudi dneve odprtih vrat, na katerih smo za osnovnošolce pripravili aktivnosti po modelu sobe pobegov ter jih na ta način seznanjali z varstvom osebnih podatkov. Za lažje poučevanje varstva osebnih podatkov v šolah smo pripravili tudi učno uro in posebna predavanja za učitelje, ki bodo izvedena v letu 2026.

PODROČJE UMETNE INTELIGENCE

Področje umetne inteligence je v letu 2025 zaznamoval začetek uporabe nekaterih delov Akta o umetni inteligenci, na primer določb glede modelov umetne inteligence za splošne namene in prepovedanih praks, sprejem Zakona o izvajanju uredbe (EU) o določitvi harmoniziranih pravil o umetni inteligenci (ZIUDHPUI) in predlog Digitalnega omnibusa za umetno inteligenco. Delo Informacijskega pooblaščenca na področju umetne inteligence v letu 2025 je bistveno sooblikoval sprejem nacionalnega zakona, ki je določil pristojne organe in kazni za kršitve Akta. Po eni strani je Informacijski pooblaščenec budno spremljal pripravo in sprejemanje ZIUDHPUI ter se nanj vseskozi odzival s svojimi mnenji in stališči (teh je bilo šest), po drugi strani pa se je na podlagi predvidene razdelitve pristojnosti kot bodoči organ za nadzor trga že začel pripravljati na izvajanje svojih prihodnjih pristojnosti, in sicer predvsem na področju prepovedanih praks, ki so se v letu 2025 že uporabljale.



Kazalo

UVODNA BESEDA INFORMACIJSKE POOBLAŠČENKE	3
STRNJEN PREGLED LETA.....	7
KAZALO	12
SEZNAM UPORABLJENIH KRATIC IN OKRAJŠAV ZAKONOV	13
1 O INFORMACIJSKEM POOBLAŠČENCU	14
1.1 NASTANEK IN OSEBNA IZKAZNICA INFORMACIJSKEGA POOBLAŠČENCA	14
1.2 KLJUČNA PODROČJA DELOVANJA IN PRISTOJNOSTI	17
1.3 ORGANIZIRANOST	19
1.3.1. IZOBRAŽEVANJE IN USPOSABLJANJE ZAPOSLENIH	20
1.4 MEDIJI IN KOMUNICIRANJE Z JAVNOSTMI.....	20
1.4.1 SPLETNA STRAN INFORMACIJSKEGA POOBLAŠČENCA.....	21
1.5 FINANČNO POSLOVANJE V LETU 2025.....	21
2 DOSTOP DO INFORMACIJ JAVNEGA ZNAČAJA.....	24
2.1 PRAVNA UREDITEV NA PODROČJU DOSTOPA DO INFORMACIJ JAVNEGA ZNAČAJA	24
2.2 ŠTEVILO VLOŽENIH PRITOŽB IN REŠENIH ZADEV	25
2.2.1 PRITOŽBE ZOPER ZAVRNILNE ODLOČBE IN IZDANE ODLOČBE	26
2.2.2 PRITOŽBE ZOPER MOLK	27
2.3 ŠTEVILO VLOŽENIH TOŽB IN PREJETIH SODB.....	28
2.4 STORJENI PREKRŠKI PO ZDIJZ, ZInfP IN ZMed.....	28
2.5 IZBRANI PRIMERI NA PODROČJU DOSTOPA DO INFORMACIJ JAVNEGA ZNAČAJA	28
2.6 AKTIVNOSTI IZOBRAŽEVANJA IN OZAVEŠČANJA	34
2.6.1 USPOSABLJANJE ZA OBČINE	34
2.6.2 DAN PRAVICE VEDETI	34
2.7 MEDNARODNO SODELOVANJE NA PODROČJU DOSTOPA DO INFORMACIJ JAVNEGA ZNAČAJA ..	34
2.7.1 SVETOVNA KONFERENCA ICIC V BERLINU	34
2.7.2 DELAVNICA PRAKTIČNIH PRIMEROV V ŠPANJI.....	35
2.7.3 SREČANJE INICIATIVE 2020.....	35
2.7.4 OBISK PREDSTAVNIKOV HRVAŠKEGA INFORMACIJSKEGA POOBLAŠČENCA	35
3 VARSTVO OSEBNIH PODATKOV.....	36
3.1 KONCEPT VARSTVA OSEBNIH PODATKOV V REPUBLIKI SLOVENIJI	36
3.2 NADZOR V LETU 2025	36
3.2.1 INŠPEKCIJSKI NADZOR	36
3.2.2 INŠPEKCIJSKI NADZOR V JAVNEM SEKTORJU	38
3.2.3 INŠPEKCIJSKI NADZOR V ZASEBNEM SEKTORJU	38
3.2.4 PRIJAVE KRŠITEV VARNOSTI OSEBNIH PODATKOV.....	38
3.2.5 PRITOŽBENI POSTOPKI PO 77. ČLENU SPLOŠNE UREDBE IN PO 33. ČLENU ZVOPOKD	39
3.2.6 OSTALI PRITOŽBENI POSTOPKI.....	41
3.2.7 SODELOVANJE PRI ČEZMEJNIH NADZORIH.....	41
3.2.8 PREKRŠKOVNI POSTOPKI	43
3.2.9 IZBRANI PRIMERI OBDELAVE OSEBNIH PODATKOV.....	45
3.3 DRUGI UPRAVNI POSTOPKI.....	52

3.3.1 DOPUSTNOST IZVAJANJA BIOMETRIJSKIH UKREPOV.....	52
3.3.2 PRENOS OSEBNIH PODATKOV V TRETJE DRŽAVE.....	52
3.4 PRIPRAVA MNENJ IN POJASNIL	53
3.4.1 SPLOŠNA POJASNILA	53
3.4.2 MNENJA NA PREDPISE.....	56
3.4.3 ZAHTEVA ZA OCENO USTAVNOSTI IN ZAKONITOSTI.....	57
3.4.4. OCENE UČINKOV NA VARSTVO OSEBNIH PODATKOV.....	58
3.5 SKLADNOST IN PREVENTIVA.....	60
3.5.1 AKTIVNOSTI ZA DOSEGANJE SKLADNOSTI IN PREVENTIVNA DEJAVNOST.....	60
3.5.2 POOBLAŠČENE OSEBE ZA VARSTVO PODATKOV	62
3.5.3 AKTIVNOSTI IZOBRAŽEVANJA IN OZAVEŠČANJA.....	62
3.6. MEDNARODNO SODELOVANJE.....	64
3.6.1 SODELOVANJE V EVROPSKEM ODBORU ZA VARSTVO PODATKOV	64
3.6.2 SODELOVANJE V DRUGIH NADZORNIH TELESIH EVROPSKE UNIJE.....	68
3.6.3 SODELOVANJE V DRUGIH MEDNARODNIH TELESIH.....	68
3.6.4. DRUGO MEDNARODNO SODELOVANJE	70
3.6.5 IZVAJANJE PRISTOJNOSTI PO DRUGIH AKTIH DIGITALNE ZAKONODAJE	71
4 UMETNA INTELIGENCA	74
4.1 REGULATORNI OKVIR NADZORA NAD SISTEMI UI V SKLADU Z AKTOM O UMETNI INTELIGENCI IN ZIUHPUI.....	74
4.2 NADZOR V LETU 2025	74
4.3 MNENJA NA ZAKONODAJO.....	75
4.4 PREVENTIVNE AKTIVNOSTI	75
4.5 MEDNARODNO SODELOVANJE.....	76
4.5.1 EVROPSKI ODBOR ZA UMETNO INTELIGENCO.....	76
4.5.2 NEFORMALNA SKUPINA PRISTOJNIH ORGANOV ZA NADZOR NAD SISTEMI UI (CA@AI)	77

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

ZIUETDS - Zakon o izvajanju Uredbe (EU) o enotnem trgu digitalnih storitev

ZIUEUP - Zakon o izvajanju uredbe (EU)

o evropskem upravljanju podatkov

ZIUHPUI - Zakon o izvajanju uredbe (EU) o

določitvi harmoniziranih pravil o umetni inteligenci

1 O INFORMACIJSKEM POOBLAŠČENCU

POD SVOJO STREHO ZDRUŽUJE DOSTOP DO INFORMACIJ JAVNEGA ZNAČAJA IN VARSTVO OSEBNIH PODATKOV, PO NOVEM TUDI NADZOR NAD UMETNO INTELIGENCO

1.1 NASTANEK IN OSEBNA IZKAZNIČA 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 pooblaščenca (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 s številnim pristojnosti tako na področju dostopa do informacij javnega značaja kot tudi na področju varstva osebnih podatkov.

Neodvisnost Informacijskega pooblaščenca 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. 4. 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. 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 (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 (ZVOP-OKD), ki se je začel uporabljati 31. 12. 2020. Splošna uredba 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 svobščine 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 okrepljeno tudi sodelovanje med nadzornimi organi v EU, še posebej s sodelovanjem Informacijskega pooblaščenca v okviru Evropskega odbora za varstvo podatkov (EDPB).

Dne 23. 10. 2025 je bil sprejet Zakon o izvajanju Uredbe (EU) o določitvi harmoniziranih pravil o umetni inteligenci (ZIUDHPUI), ki je začel veljati 21. 11. 2025. Zakon kot enega izmed organov, ki izvajajo naloge organov za nadzor trga po Uredbi (EU) 2024/1689 Evropskega parlamenta in Sveta z dne 13. 6. 2024 o določitvi harmoniziranih pravil o umetni intelligen-

ci in spremembi uredb (ES) št. 300/2008, (EU) št. 167/2013, (EU) št. 168/2013, (EU) 2018/858, (EU) 2018/1139 in (EU) 2019/2144 ter direktiv 2014/90/EU, (EU) 2016/797 in (EU) 2020/1828 (Akt o umetni inteligenci) določa Informacijskega pooblaščenca (IP), kar predstavlja najobsežnejši prevzem novih pristojnosti od začetka delovanja Informacijskega pooblaščenca kot neodvisnega državnega organa. V skladu z Aktom o umetni inteligenci in ZIUDHPUI je Informacijski pooblaščenec pristojen za nadzor nad prepovedanimi praksami (od 21. 11. 2025 dalje) in visoko tveganimi sistemi UI na področju biometrije, šolstva, preprečevanja, odkrivanja in preiskovanja kaznivih dejanj, meja, migracij in azila ter pravosodja in demokratičnih procesov.

Informacijska pooblaščenka **dr. Jelena Virant Burnik** je petletni mandat nastopila 17. 7. 2024.



Informacijska pooblaščenka in vodstvo

LETO 2025 V ŠTEVILKAH



54
zaposlenih




3.295.509,05
EUR proračuna

Varstvo osebnih podatkov


 **1226** ▲ **+45 %**
novih inšpekcijskih zadev
(nacionalnih in čezmejnih)

 **175**
uradnih obvestil o kršitvi
varnosti osebnih podatkov

 **465** ▲ **+152 %**
prejetih prijav prijaviteljev s
posebnim položajem

 **69**
pritožb po drugih zakonih


 **146** ▲ **+39 %**
postopkov o prekršku
294.390 €
skupna višina izrečenih glob


 **985**
pisnih mnenj


 **1446**
telefonskih pojasnil


 **117** ▲ **+39 %**
mnenj na predpise


 **30**
mnenj na
ocene učinka

 **8**
izdanih odločb
glede biometrije

 **4**
preventivne aktivnosti
za skladnost

 **2**
infografiki

 **67**
predavanj


 **1**
smernica


 **2**
uskklajeni akciji nadzora

 **EU projekt**
za ozaveščanje otrok

 **920** ▲ **+19 %**
vloženih pritožb

 **547** ▲ **+15 %**
odločitev

 **272**
pozivov zaradi molka


 **381**
pisnih prošenj za pojasnila


 **975**
telefonskih pojasnil


Informacije javnega značaja

Mednarodno sodelovanje

 **242** ▲ **+38 %**
postopkov sodelovanja
po 60. členu

 **299**
postopkov sodelovanja
po 61. členu

 **170**
sestankov ekspertnih skupin

 **14**
plenarnih zasedanj EOVP

 **40+**
mednarodnih sestankov

Umetna inteligenca

 **172**
sporočil in objav
na družbenih omrežjih



12
novičnikov

Odnosi z javnostjo



183 ▲ **+68 %**
odgovorov na
novinarska vprašanja



4
dogodki

1.2 KLJUČNA PODROČJA DELOVANJA IN PRISTOJNOSTI

Informacijski pooblaščenec svoje z zakonom določene naloge in pristojnosti opravlja na treh področjih:

- na področju dostopa do informacij javnega značaja,
- na področju varstva osebnih podatkov in
- na področju umetne inteligence (od 21. 11. 2025).

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 zoper odločbo, s katero je organ zavrgel ali zavrnil zahtevo ali drugače kršil pravico do dostopa ali ponovne uporabe informacije javnega značaja, ter v okviru postopka na drugi stopnji tudi za nadzor nad izvajanjem zakona, ki ureja dostop do informacij javnega značaja, in na njegovi podlagi izdanih predpisov.

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

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

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

Na področju varstva osebnih podatkov je Informacijski pooblaščenec pristojen predvsem za:

- inšpekcijski nadzor nad izvajanjem predpisov, ki urejajo varstvo ali obdelavo osebnih podatkov oz. prenos osebnih podatkov iz Republike Slovenije, ter opravljanje drugih nalog, ki jih določajo ti predpisi;
- odločanje v postopku prijav prijavitelja s posebnim položajem (gre za postopek, po katerem se odloča o tem, ali se osebni podatki konkretnega posameznika obdelujejo nezakonito oz. v nasprotju z zakonodajo o varstvu osebnih podat-

- kov oz. o pritožbi posameznika v zvezi z uveljavljanjem pravic pri upravljavcu osebnih podatkov po Splošni uredbi o varstvu podatkov in drugih predpisih s področja varstva osebnih podatkov),
- odločanje v prekrškovnih postopkih zaradi kršitve varstva osebnih podatkov,
- za odločanje v drugih upravnih postopkih (npr. odločanje o izvajanju biometričnih ukrepov na prvi stopnji, odločanje o pritožbi glede posredovanja podatkov po 41. členu ZVOP-2).

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. Skladno s tretjim odstavkom 55. člena Splošne uredbe Informacijski pooblaščenec ni pristojen za nadzor dejanj obdelave sodišč, kadar delujejo kot sodni organ.

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.

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. 4. 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 navedene v 76. členu ZVOPOKD.

Skladno s prvim odstavkom 77. člena ZVOPOKD Informacijski pooblaščenec ni pristojen za izvajanje nadzora in za prekrškovni nadzor glede obdelav osebnih podatkov, ki se obdelujejo v kazenskih zadevah sodišča.

Informacijski pooblaščenec ima pristojnosti tudi po naslednjih predpisih.

Na podlagi **Zakona o pacientovih pravicah (ZPacP)** Informacijski pooblaščenec deluje kot **pritožbeni** (deseti odstavek 41. člena, peti odstavek 42. člena in sedmi odstavek 45. člena) ter **inšpekcijski in prekrškovni** organ (četrti odstavek 85. člena določa, v katerih primerih Informacijski pooblaščenec izvaja inšpekcijski nadzor in vodi prekrškovne postopke). 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 **Zakonu o potnih listinah (ZPLD-1)** in **Zakonu o osebni izkaznici (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.

Zakon o elektronskih komunikacijah (ZEKom-2) določa pristojnosti Informacijskega pooblaščenca v 229. členu, in sicer Informacijski pooblaščenec izvaja inšpekcijski nadzor nad izvajanjem določb 216., 223. in 225. člena ZEKom-2 in najmanj enkrat letno opravlja inšpekcijski nadzor nad obdelavo podatkov iz 220. člena ZEKom-2. 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).

Zakon o centralnem kreditnem registru (ZCKR) ureja vzpostavitev centralnega kreditnega registra kot osrednje nacionalne zbirke podatkov o zadolženosti fizičnih oseb in poslovnih subjektov. V skladu s 26. členom ZCKR Banka Slovenije v zvezi z vzpostavitvijo in upravljanjem sistema izmenjave informacij (SISBON) 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 tem 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 s 31. členom ZCKR Informacijski pooblaščenec javno

objavi informacije v zvezi z ukrepi nadzora in sankcijami zaradi prekrška, ki jih je izrekel.

Zakon o potrošniških kreditih (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.

Zakon o kupcih in serviserjih nedonosnih kreditov bank (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.

Pristojnosti Informacijskega pooblaščenca na podlagi **Zakona o izvajanju Uredbe (EU) o enotnem trgu digitalnih storitev (ZIUETDS)** so nadzor nad tretjim odstavkom 26. člena Uredbe (EU) 2022/2065 Evropskega parlamenta in Sveta z dne 19. 10. 2022 o enotnem trgu digitalnih storitev in spremembi Direktive 2000/31/ES (Akt o digitalnih storitvah) v zvezi s prepovedjo predstavljanja oglasov ponudnikov spletnih platform na podlagi oblikovanja profilov, pri čemer se uporabljajo posebne vrste osebnih podatkov ter nadzor nad 28. členom Uredbe (EU) 2022/2065 v zvezi z zaščito mladoletnikov na spletu.

Informacijski pooblaščenec skladno s 5. členom **Zakona o izvajanju Uredbe (EU) o evropskem upravljanju podatkov (ZIUEUP)** deluje kot pritožbeni organ zoper odločbo, s katero je organ javnega sektorja odločil o zahtevi za ponovno uporabo zaščitnih podatkov organov javnega sektorja, in zoper sklep, s katerim je organ javnega sektorja zahtevo zavrgel.

Pristojnosti Informacijskega pooblaščenca opredeljujejo tudi pravila **schengenskega informacijskega sistema (in druga generacija sistema, t. i. SIS II)**¹, ki nacionalnim organom kazenskega pregona ter pravosodnim in upravnim organom omogočajo izmenjavo in dostop do podatkov o prestopu zunanji meja in vizumski politiki, v sistem pa so poleg tega vključeni tudi podatki o evropskem zapornem

¹ Pravni okvir SIS II vključuje: Uredbo (ES) št. 1987/2006 Evropskega parlamenta in Sveta z dne 20. 12. 2006 o vzpostavitvi, delovanju in uporabi druge generacije schengenskega informacijskega sistema (SIS II); Sklep Sveta 2007/533/PNZ z dne 12. 6. 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. 12. 2006 o dostopu služb držav članic, pristojnih za izdajo potrdil o registraciji vozil, do druge generacije schengenskega informacijskega sistema (SIS II).

nalogu, izročitvi, biometrični podatki in podatki o iskanju zaradi terorističnih aktivnosti. Informacijski pooblaščenec nadzira zakonitost obdelave osebnih podatkov v SIS II na svojem ozemlju in pri prenosu s svojega ozemlja, vključno z izmenjavo in nadaljnjo obdelavo dopolnilnih podatkov.

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

Na **področju umetne inteligence** je Informacijski pooblaščenec pristojen za:

- izvajanje nadzora ter odločanje v pritožbenih postopkih po zakonodaji digitalne agende Evropske unije (npr. Akt o digitalnih storitvah, Akt o evropskem upravljanju podatkov, Uredba o političnem oglaševanju);
- nadzor nad izvajanjem Akta o umetni inteligenci v delu glede prepovedanih praks sistemov umetne inteligence in glede visoko tveganih sistemov umetne inteligence na področju biometrije, šolstva, preprečevanja, odkrivanja in preiskovanja kaznivih dejanj, mej, migracij in azila, demokratičnih procesov ter pravosodja,
- odločanje v prekrškovnih postopkih zaradi kršitve Akta o umetni inteligenci.

1.3 ORGANIZIRANOST

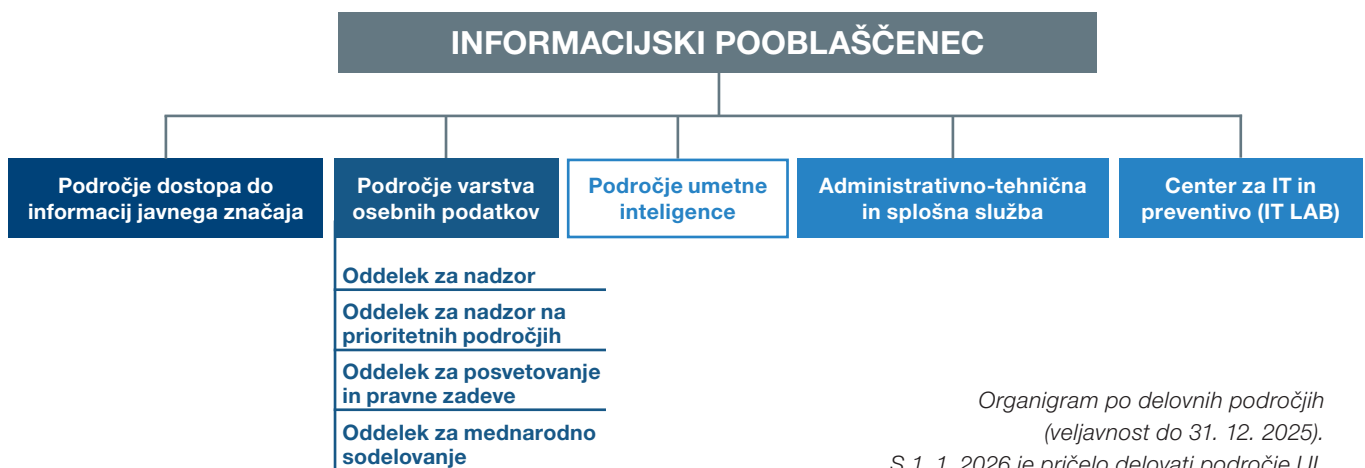
Informacijski pooblaščenec opravlja naloge iz svoje pristojnosti na sedežu v Ljubljani.

Notranjo organizacijo organa določata Akt o notranji organizaciji in sistemizaciji delovnih mest pri Informacijskem pooblaščenecu ter njegova priloga Sistemizacija delovnih mest pri Informacijskem pooblaščenecu. Sistemizacija delovnih mest je prilagojena nalogam in delovnim procesom Informacijskega pooblaščenca ter je oblikovana tako, da zagotavlja čim učinkovitejšo izrabo človeških virov.

V letu 2025 je Informacijski pooblaščenec začel izvajati nove pristojnosti po Zakonu o izvajanju uredbe (EU) o evropskem upravljanju podatkov, v katerem je bila predvidena finančna posledica dveh (2) dodatnih zaposlenih, zaradi česar je bil kadrovski načrt v začetku leta 2025 povečan s 53 na 55 zaposlenih.

V skladu z omenjenimi spremembami in v okviru veljavnega kadrovskega načrta so bili na dan 31. 12. 2025 pri Informacijskem pooblaščenecu zaposleni: **1 funkcionar in 53 javnih uslužbencev, od tega 47 na uradniških delovnih mestih za nedoločen čas in 6 na strokovno tehničnih delovnih mestih (5 za nedoločen čas in 1 za določen čas).**

Zaradi novih pristojnosti na področju umetne inteligence je bilo treba reorganizirati obstoječo organizacijsko strukturo Informacijskega pooblaščenca, kar je bilo s sprejemom novega Akta o notranji organizaciji in sistemizaciji delovnih mest izvedeno v decembru 2025, z začetkom veljavnosti 1. 1. 2026.



Organigram po delovnih področjih
(veljavnost do 31. 12. 2025).
S 1. 1. 2026 je pričelo delovati področje UI.

Kljub kadrovske okrepitvi v letu 2025 se na vseh področjih poslovanja kaže še nadaljnja potreba po zagotavljanju dodatnega kadra, saj z obstoječo kadrovske sestavo še vedno ni mogoče slediti povečanemu prirpadu zadev in obsegu pristojnosti. Število zaposlenih je treba povečati na vseh treh strokovnih področjih (popolnitev področja umetne inteligence, nadomestitev uslužbencev na področju varstva osebnih podatkov, ki prevzemajo naloge s področja novih pristojnosti, in okrepitev področja varstva osebnih podatkov in področja informacij javnega značaja) kot tudi v podpornih službah organa (področje kadrovskega poslovanja, IT-podpora).

Informacijski pooblaščenec je v letu 2025 v svoj delovni proces aktivno vključeval tudi študente, kar se je izkazalo za izjemno dobro prakso tako z vidika pomoči pri obvladovanju pripada zadev kot tudi z vidika motiviranja mladih za poznejšo redno zaposlitev. Informacijski pooblaščenec bo z vključevanjem študentov na podlagi študentskega dela nadaljeval tudi v prihodnje.

1.3.1. IZOBRAŽEVANJE IN USPOSABLJANJE ZAPOSLENIH

Zaradi kompleksnosti zakonodajnih in tehnoloških novosti je nujno potrebno periodično in dodatno izobraževanje oz. usposabljanje zaposlenih na strokovnih področjih, za katere je pristojen Informacijski pooblaščenec, in na vseh drugih področjih poslovanja oz. upravljanja organa. Izobraževanje in usposabljanje javnih uslužbencev je ključno za razvoj kompetenc, ki pripomorejo k uspešnemu opravljanju delovnih nalog in s tem prispevajo k izboljšanju delovnih procesov, učinkovitosti in uspešnosti poslovanja Informacijskega pooblaščenca kot celote. Z udeležbo na kakovostnih izobraževalnih vsebinah, ki praviloma vključujejo najnovejše teoretične in praktične pristope k predstavljenim vsebinam, se med javnimi uslužbenci krepi profesionalizem in strokovnost.

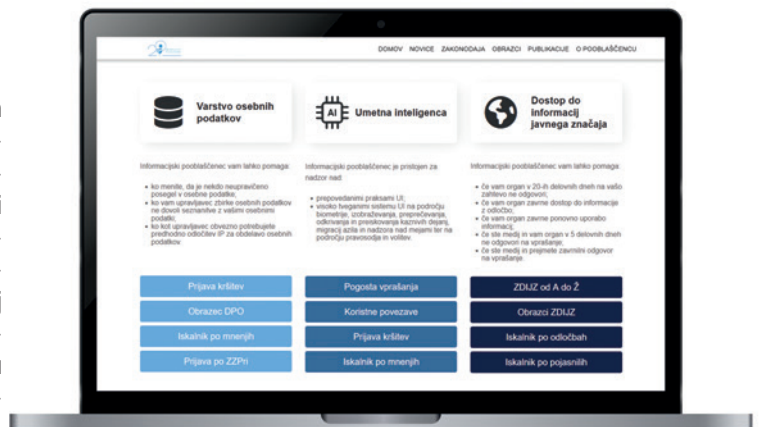
Informacijski pooblaščenec je v okviru finančnih sredstev, predvidenih v Načrtu izobraževanja, usposabljanja in izpopolnjevanja zaposlenih, spodbujal vse opisane oblike izobraževanj in usposabljanj, še posebej pa izobraževanja v mednarodnem okolju, saj se tako prenašajo najboljše prakse in pristopi drugih držav, omogoča se izmenjava izkušenj, povečujejo se možnosti za sodelovanje v skupnih projektih. Javni uslužbenci, ki imajo stik z mednarodnim okoljem, bolje razumejo globalne izzive s področij, za katera je pristojen Informacijski pooblaščenec.

V okviru izobraževanja in usposabljanja se je v letu 2025 z rednimi informativnimi vsebinami na skupnih kolegijih in sestankih skrbelo za ustrezen pretok informacij in znanja med zaposlenimi znotraj organa.

Z oblikami t. i. neformalnega mentorstva se je v letu 2025 uvajalo novo zaposlene, da so se učinkoviteje spoznali z nalogami in pristojnostmi Informacijskega pooblaščenca, delovnimi procesi, delovanjem informacijskega sistema in drugimi vsebinami, pomembnimi za uspešno opravljanje dela.

1.4 MEDIJI IN KOMUNICIRANJE Z JAVNOSTMI

Tudi v letu 2025 je Informacijski pooblaščenec intenzivno sodeloval z mediji ter krepil transparentno komuniciranje z javnostmi. Odzval se je na **183 novinarskih vprašanj**, kar predstavlja več kot 60 % porast od prejšnjega leta, zaradi česar je bila zaposlena nova svetovalka za odnose z javnostmi.



Mediji so se na Informacijskega pooblaščenca najpogosteje obračali z vprašanji glede razlage obveznosti zavezancev, stališč ob predlaganih spremembah zakonodaje ter obravnave aktualnih dogodkov, povezanih z varstvom osebnih podatkov, z umetno inteligenco in z dostopom do informacij javnega značaja. Pomemben del novinarskih poizvedb se je nanašal tudi na primere, ki so sprožili širšo javno razpravo ali izpostavili domnevne kršitve pravic posameznikov; nanje se je Informacijski pooblaščenec odzival z jasnimi pojasnili in strokovnimi stališči.

Informacijski pooblaščenec je v letu 2025 objavil **172 spletnih novic**, od tega **53 na spletni strani** in **119 na družbenih omrežjih LinkedIn in Facebook**, kjer predvsem opozarja na pomembne novo-

sti na področju varovanja zasebnosti ter objavlja povezave do relevantnih novosti. Na omrežju LinkedIn, ki je namenjeno strokovni javnosti, objave Informacijskega pooblaščenca spremlja več kot 2000 sledilcev, na omrežju Facebook, ki je namenjeno predvsem splošni javnosti, pa dobrih 2200 sledilcev. V letu 2025 je Informacijski pooblaščenec objavil 25 sporočil več kot leto poprej, in sicer je objavil 64 sporočil na omrežju LinkedIn in 55 objav na omrežju Facebook ter poslal 12 novičnikov, ki naročnikom omogočajo strnjen pregled najpomembnejših objav, mnenj in priporočil. Pomemben del komunikacije so predstavljale tudi ozaveščevalne aktivnosti, med njimi objave o varni rabi gesel in lokacijskih podatkov ter o tveganjih pri uporabi umetne inteligence, objavljeni so bili tudi novi izobraževalni materiali.

Poleg pisnih objav je Informacijski pooblaščenec sodeloval v približno **20 radijskih in televizijskih oddajah**, ki so bile posvečene aktualnim temam, odgovarjal je na vprašanja gledalcev in poslušalcev ter prispeval k boljši ozaveščenosti javnosti o pravicah in obveznostih na področju varstva osebnih podatkov.

1.4.1 SPLETNA STRAN INFORMACIJSKEGA POOBLAŠČENCA

Informacijski pooblaščenec redno posodablja svojo spletno stran z novimi vsebinami, ki so lahko v pomoč zavezancem pri razumevanju in izpolnjevanju zahtev zakonodaje. Zlasti so uporabne informacije o ključnih področjih zakonodaje, kjer so posamezne ključne teme obdelane na razumljiv način, uporabnik pa ima na enem mestu podane vse pomembne informacije o tem področju, napotitve na relevantne člene ter povezave do uporabnih gradiv, kot so smernice (Informacijskega pooblaščenca in EDPB), infografike, vzorci in obrazci.

Konec leta 2025 smo prenovili in posodobili spletno stran Informacijskega pooblaščenca, da odseva novo

strukturo področij njegovega delovanja – dodali smo podstran, namenjeno umetni inteligenci, na kateri javnost lahko najde odgovore na najpogostejša vprašanja, koristne povezave na drugo gradivo, osnovne informacije o prijavi kršitev, objavljena mnenja in smernice Informacijskega pooblaščenca².

Informacijski pooblaščenec je prek spletne strani zavezance opozarjal na dolžnosti in podajal priporočila za posameznike.

Med slednjimi velja izpostaviti npr. priporočila za posameznike po razkritju obsežnega odtekanja podatkov o EMŠO, davčnih številkah, imenih in priimkih ter naslovih posameznikov ob incidentu, ki ga je jeseni 2025 utrpela Uprava za varno hrano veterinarstvo in varstvo rastlin.

1.5 FINANČNO POSLOVANJE V LETU 2025

Finančna sredstva za delovanje 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 nalog je imel Informacijski pooblaščenec za leto 2025 skupni veljavni proračun v višini 3.295.509,05 EUR. Skupaj prevzete obveznosti Informacijskega pooblaščenca na dan 31. 12. 2025 so znašale 3.267.826,35, od tega na integralnih postavkah v višini 3.187.529,11 EUR.



Informacijski pooblaščenec je v sporočilih za javnost pojasnil, kakšnim tveganjem smo izpostavljeni, če pridejo naši osebni podatki (EMŠO, davčna številka, ime in priimek, kraj bivanja) v roke spletnim kriminalcem, kaj vse je danes mogoče s temi podatki storiti na spletu, kako nezaščiten in ranljiv je posameznik, ki so mu bili ukradeni omenjeni osebni podatki, in kako se lahko posameznik zaščiti. Opozoril je, da je priporočljivo uporabljati standardne dobre prakse glede informacijske varnosti, kot je izbira varnih gesel, redno preverjanje bančnih in drugih izpiskov ter podatkov o naših statusih, opravljenih nakupih in storitvah ter dobršna mera dojemljivosti in pozornosti pri prepoznavanju nenavadnih situacij in dogodkov, ki lahko kažejo na to, da se je nekdo izkazoval za nas bodisi za pridobitev protipravne koristi bodisi za ustvarjenje potvorjenih dejstev o naših dejavnostih, komunikacijah, lokacijah ali statusih.

² <https://www.ip-rs.si/umetna-inteligenca/>

Proračun Informacijskega pooblaščenca.

	Veljavni proračun v EUR	Prevzete obveznosti v EUR	Razpoložljiv proračun v EUR konec leta
INFORMACIJSKI POOBLAŠČENEC	3.295.509,05	3.267.826,35	27.682,70
OPRAVLJANJE DEJAVNOSTI	3.201.818,00	3.187.529,11	14.288,89
PP 1267 Plače	2.677.445,00	2.669.474,52	7.970,48
PP 1271 Materialni stroški	504.373,00	501.275,13	3.097,87
PP 1273 Investicije	20.000,00	16.779,46	3.220,54
NAMENSKA SREDSTVA	12.327,92	0,00	12.327,92
7459 Namenska sr. kupnine	12.327,92	0,00	12.327,92
7460 Stvarno premoženje – sr. odškodnine	0,00	0,00	0,00
DONACIJE – EU projekti	81.363,13	80.297,24	1.065,89
PP 9958 Mednarodna spl. str.	0,14	0,00	0,14
PP130134 projekt Taiex	1.052,99	0,00	1.052,99
PP251069 PrivacyPRO	80.310,00	80.297,24	12,76

Vir izpis DPS-06-20, 27. 1. 2026

Informacijski pooblaščenec je v letu 2025 razpolagal z:

- namenskimi sredstvi v višini 12.327,92 EUR (prenos iz leta 2024 v višini 7.317,92 EUR in prihodek od prodaje vozila v višini 5.010,00 EUR),
- sredstvi z naslova projekta Taiex v višini 1.052,99 (prenos iz leta 2024 v višini 2,99 EUR in priliv v višini 1.050,00 EUR v letu 2025) in
- založenimi sredstvi v višini 2.000,00 EUR (prenos iz leta 2024 v višini 1.000 EUR in priliv v letu 2025 v višini 1.000,00 EUR).

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

V letu 2025 je bilo finančno poslovanje razdeljeno na ukrep in projekte:

Ukrep 1215-18-0001 vključuje integralni proračunski postavki plače 1267 in materialni stroški 1271. Znesek veljavnega proračuna na ukrepu je ob koncu leta 2025 znašal 3.181,818,00 EUR, medtem ko so prevzete obveznosti ob koncu leta znašale 3.170.749,65 EUR.

Poraba sredstev za plače zaposlenih, evidentirana na PP 1267

V letu 2025 je bila poraba sredstev za plače zaposlenih v okviru proračunske postavke 1267 realizirana v višini 2.669.474,52 EUR, kar predstavlja 99,70 % veljavnega proračuna, ki je znašal 2.677.445,00 EUR.

- **Poraba sredstev za materialne stroške, evidentirane na PP 1271**

Materialni stroški, evidentirani na proračunski postavki 1271, zagotavljajo sredstva za nemoteno poslovanje IP.

Poraba sredstev za blago in storitve, evidentirane na proračunski postavki 1271 (skupina 402), je bila v letu 2025 v skladu z načrtovanimi sredstvi in je znašala 501.275,13 EUR, kar predstavlja 99,38 % celotnega veljavnega proračuna na tej postavki, ki je ob koncu leta znašal 504.373,00 EUR.

Projekt 1215-21-0001, PP 1273 Investicije

Veljaven proračun na proračunski postavki 1273 Investicije in investicijsko vzdrževanje (skupina 420) je ob koncu leta 2025 znašal 20.000,00 EUR. Poraba sredstev je bila realizirana v višini 16.779,46 EUR, kar predstavlja 83,90 % veljavnega proračuna.

Projekt 1215-21-0001, PP 7459 Namenska sredstva kupnine in PP 7460 Stvarno premoženje – sredstva odškodnin.

V leto 2025 je bilo prenesenih **7.317,92 EUR** finančnih sredstev kupnin. V letu 2025 je bilo prodano službeno vozilo. Na proračunski postavki 7459 v letu 2025 ni bilo porabe sredstev. Znesek v višini 12.327,92 EUR se prenese v leto 2026.

Projekt 1215-16-0001, PP 130134 projekt Taiex

TAIEX (*Technical Assistance and Information Exchange*) je instrument EU, ki nudi podporo državam prejemnicam pomoči pri prilagajanju nacionalne zakonodaje zakonodaji EU in njenemu izvajanju.

V leto 2025 je bilo na postavki Taiex prenesenih 2,99 EUR finančnih sredstev. V letu 2025 je bil z naslova študijskega obiska junija nakazan priliv v višini 1.050,00 EUR. Znesek v višini 1.052,99 EUR se prenese v leto 2026.

Projekt 1215-25-0003: PP 251069 IP PrivacyPRO – Postani strokovnjak za varstvo osebnih podatkov

Informacijski pooblaščenec je 19. 9. 2024 podpisal pogodbo o izvajanju in financiranju projekta (Grant Agreement) z Evropsko komisijo.

Informacijski pooblaščenec bo v letih 2025, 2026 in 2027 samostojno izvajal projekt: »Become a PrivacyPRO(tector)«, s krajšim nazivom »PrivacyPRO«, št. projekta 101193212 (101193212 – PrivacyPRO – CERV-2025-DATA). Projekt je namenjen izobraževanju otrok in njihovih staršev, učiteljev, socialnih delavcev ter ostalih posameznikov, ki delajo z otroki, glede varstva osebnih podatkov otrok. Projekt financira Evropska komisija v okviru Programa »Državljeni, enakost, pravice in vrednote 2021–2027«. Veljaven proračun na proračunski postavki 251069 je ob koncu leta 2025 znašal 80.310,00 EUR. Poraba sredstev je bila realizirana v višini 80.297,24 EUR, kar predstavlja 99,98 % veljavnega proračuna.

Ocena ustreznosti finančnih sredstev

Proračun Informacijskega pooblaščenca 2018–2025.

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
2024	2.796.248,05 EUR
2025	3.295.509,05 EUR

Neodvisni državni organi, kot je Informacijski pooblaščenec, imajo v sodobnih demokratičnih družbah ključno vlogo pri varovanju in krepitvi demokratičnih vrednot ter pri zagotavljanju spoštovanja človekovih pravic. V zadnjih letih se Informacijski pooblaščenec sooča z nenehnim povečevanjem števila zadev in nalog, ki izhajajo tako iz nacionalnih kot tudi evropskih pravnih obveznosti. To neposredno vpliva na povečevanje potreb po dodatnih kadrovskih virih ter posledično tudi na rast stroškov dela.

Da bi Informacijski pooblaščenec lahko še naprej učinkovito izvrševal svoje številne pristojnosti, je nujna zagotovitev finančnih sredstev v obsegu, ki omogoča stabilno in nemoteno delovanje samostojnega in neodvisnega državnega organa z ustrezno strokovno, administrativno in tehnično podporo.

Že Splošna uredba izrecno določa, da mora vsaka država članica zagotoviti, da ima vsak nadzorni organi na voljo človeške, tehnične in finančne vire, prostore ter infrastrukturo, ki jih potrebuje za učinkovito opravljanje svojih nalog in izvajanje pooblastil, tudi tistih, ki se nanašajo na medsebojno pomoč, sodelovanje in udeležbo v odboru (52. člen). Informacijski pooblaščenec je o tem, ali ima za svoje delovanje zagotovljena zadostna sredstva, dolžan obveščati tudi Evropski odbor za varstvo podatkov (EDPB).

Država je zavezana zagotavljati implementacijo in učinkovito izvajanje evropske zakonodaje, kar vključuje tudi zagotovitev ustreznih sredstev za delovanje nadzornih organov. Le tako lahko ti prilagodijo svoje organizacijske strukture, zagotovijo ustrezno usposobljen kader ter izvajajo predvidene nadzorne postopke. Na pomen zadostnih finančnih virov za svoje delovanje je Informacijski pooblaščenec ves čas opozarjal tudi v postopkih implementacije varstva osebnih podatkov in umetne inteligence.

Revizija pravilnosti poslovanja Informacijskega pooblaščenca

Leta 2025 je Računsko sodišče RS pričelo redno revizijo pravilnosti poslovanja Informacijskega pooblaščenca na podlagi Zakona o računskem sodišču in Poslovnika Računskega sodišča Republike Slovenije. Sklep o izvedbi revizije je bil izdan 6. maja 2025. Revizija se je izvajala v skladu z mednarodnimi revizijskimi standardi in Napotilom za izvajanje revizij.

V reviziji je Računsko sodišče preverjalo skladnost poslovanja s predpisi ter predvsem pravilnost porabe javnih sredstev, zlasti za:

1. določanje, obračunavanje in izplačevanje plač ter drugih stroškov, povezanih z delom, ter
2. nabave blaga, materiala in storitev ter osnovnih sredstev.

Revizija je bila zaključena v začetku leta 2026 s pozitivnim mnenjem o skladnosti poslovanja Informacijskega pooblaščenca.

2 DOSTOP DO INFORMACIJ JAVNEGA ZNAČAJA

JAVNOST IMA PRAVICO VEDETI

2.1 PRAVNA UREDITEV NA PODROČJU DOSTOPA DO INFORMACIJ JAVNEGA ZNAČAJA

Pravica dostopa do informacij javnega značaja je zagotovljena z 39. členom Ustave Republike Slovenije. Ta v drugem odstavku določa, da ima vsakdo pravico dobiti informacijo javnega značaja, za katero ima v zakonu utemeljen pravni interes, razen v primerih, ki jih določa zakon. ZDIJZ sledi usmeritvam mednarodnih aktov in EU. Njegov namen je zagotoviti javnost in odprtost delovanja javne uprave ter vsakomur omogočiti dostop do informacij javnega značaja in njihovo ponovno uporabo. 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 v letu 2022.

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

Kdo so zavezanci za posredovanje informacij javnega značaja?

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

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

Zavezanci so informacije javnega značaja dolžni zagotavljati na dva načina: z objavo na spletu in z

omogočanjem dostopa na podlagi individualnih zahtev. Za vsako od skupin zavezancev je pojem »informacija javnega značaja« (torej informacija, ki jo morajo posredovati prosilcu) definiran drugače; pri zavezancih iz druge skupine je ožji. Medtem ko **za organe na splošno velja, da so vsi dokumenti, zadeve, dosjeji, registri, evidence in dokumentarno gradivo, s katerim razpolagajo** (ne glede na to, ali jih je organ izdelal sam, v sodelovanju z drugim organom ali jih je pridobil od drugih oseb), **informacije javnega značaja, razen izjem, za poslovne subjekte pod prevladujočim vplivom oseb javnega prava velja ravno obraten miselni proces: informacije javnega značaja so le tisti dokumenti, zadeve, dosjeji, registri, evidence in dokumentarno gradivo, ki jih kot take določa ZDIJZ** (npr. informacije, povezane s sklenjenimi pravnimi posli, ter informacije o članih poslovnega organa, organa upravljanja in organa nadzora). Za te zavezance velja tudi časovna omejitev, saj se dolžnost posredovanja nanaša le na informacije, nastale v času pod prevladujočim vplivom. Zavezanci, ki izpolnjujejo kriterije za umestitev v obe skupini (npr. gospodarske družbe v 100-odstotni lasti občine, ki so hkrati tudi izvajalke javne službe), so zavezani posredovati obe vrsti informacij javnega značaja. Tisti poslovni subjekti pod prevladujočim vplivom oseb javnega prava, ki hkrati ne sodijo med organe, lahko uporabijo t. i. poenostavljeni postopek odločanja o zahtevah (npr. ne izdajo zavrnilne odločbe, ampak vlagatelja pisno obvestijo o razlogih, zaradi katerih informacije ne bodo posredovali). 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 informacij 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.

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?

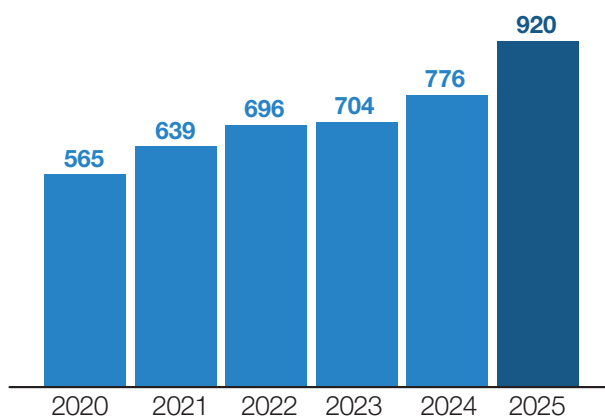
Če poda zahtevo za posredovanje informacij medij na podlagi 11. člena ZMed, je postopek nekoliko drugačen, saj **informacije po ZMed niso enake informacijam javnega značaja po določbah ZDIJZ.** Informacije za medije so širši pojem kot informacije javnega značaja, saj med prve sodi tudi priprava odgovorov na vprašanja (torej pojasnila, razlage, analize, komentariji). Če medij zahteva odgovor na vprašanje, se njegova vloga obravnava po določbah ZMed, če pa zahteva dostop do doku-

menta, 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 petih delovnih dneh** od prejema vprašanja, pri čemer sme odgovor zavrniti le, če so zahtevane informacije izvzete iz prostega dostopa po ZDIJZ ali če odgovor ni vezan na delovno področje zavezanca. Medij lahko po prejemu odgovora zahteva dodatna pojasnila, ki mu jih mora zavezanec posredovati najpozneje v treh delovnih 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 pri Informacijskem pooblaščenca je dovoljena, kadar odgovor na vprašanje izhaja iz dokumenta.

2.2 ŠTEVILO VLOŽENIH PRITOŽB IN REŠENIH ZADEV

Leta 2025 je Informacijski pooblaščenec vodil 920 pritožbenih postopkov, od tega 601 postopek zoper zavrnilne odločbe organov in 319 postopkov zaradi t. i. molka organa oz. neodzivnosti. Zoper poslovne subjekte pod prevladujočim vplivom je Informacijski pooblaščenec vodil 16 pritožbenih postopkov, od tega tri zaradi molka in 13 zoper zavrnilne odločbe poslovnih subjektov pod prevladujočim vplivom.

Število vseh vloženi pritožb po letih.



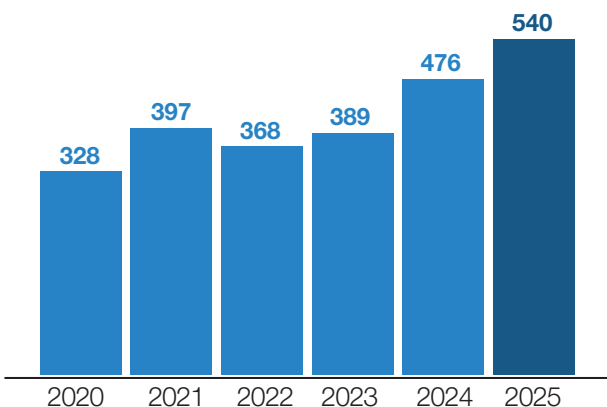
Leta 2025 je Informacijski pooblaščenec odgovoril na 381 pisnih prošenj za neformalno pomoč ali mnenje, ki jih je prejel od zavezancev prve stopnje in prosilcev, odgovoril pa je tudi na 975 zapisil v okviru telefonskih dežurstev. Vsem je odgovoril v

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 zavrnilli zahteve po dostopu do informacij javnega značaja, je Informacijski pooblaščenec v letu 2025 vsebinsko obravnaval 601 pritožbo. Izdal je 540 odločb, kar je 64 več kot leto pred tem in 64 % več kot v letu 2020. Dve pritožbi prosilcev je Informacijski pooblaščenec s sklepom zavrgel (pritožbi sta bili nedovoljeni oz. prepozni), v petih primerih pa je zaradi umika pritožbe prosilca izdal sklep o ustavitvi postopka. Med reševanjem pritožb je na terenu opravil 21 ogledov *in camera* (tj. ogledov brez prisotnosti stranke, ki zahteva dostop do informacije javnega značaja), na katerih je ugotavljal dejansko stanje pri organu.

Število izdanih odločb po letih.



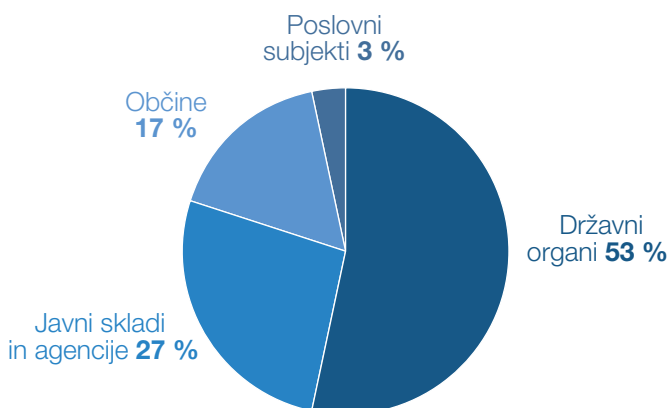
Informacijski pooblaščenec je v izdanih odločbah (540):

- pritožbo zavrnil (299),
- pritožbi delno ali v celoti ugodil oz. rešil zadevo v korist prosilca (146),
- pritožbi ugodil in zadevo vrnil prvostopenjskemu organu v ponovno odločanje (91),
- 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:

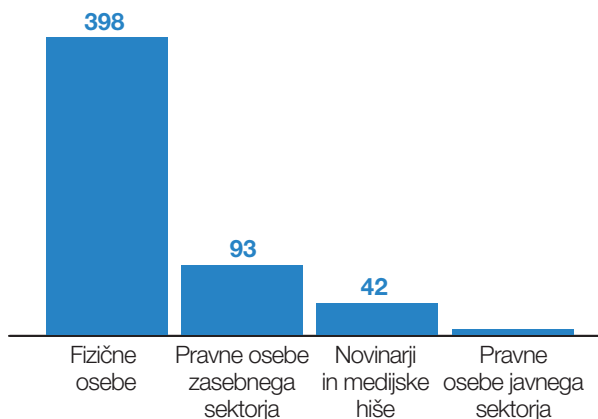
- državni organi 288, od tega ministrstva in organi v sestavi ter upravne enote 205, sodišča, vrhovno državno tožilstvo in državno odvetništvo pa 83,
- javni skladi, zavodi, agencije, izvajalci javnih služb, nosilci javnih pooblastil in druge pravne osebe javnega prava 144,
- občine 91,
- poslovni subjekti pod prevladujočim vplivom države, občin ali drugih oseb javnega prava 17.

Zoper katere zavezance so bile vložene pritožbe?



V 398 primerih so bili prosilci fizične osebe, v 93 primerih so se pritožile pravne osebe zasebnega sektorja, v 42 primerih novinarji in medijske hiše, v sedmih primerih pa so se pritožile pravne osebe javnega sektorja.

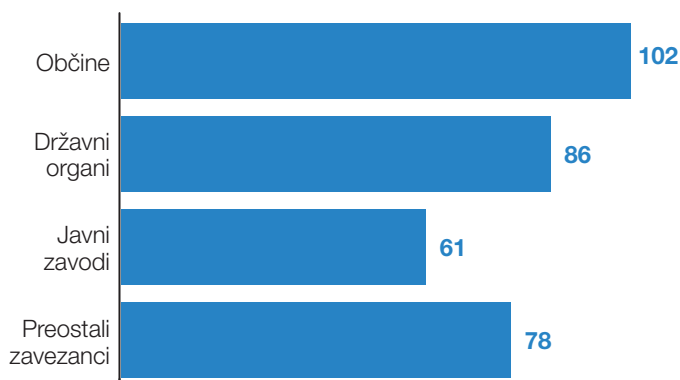
Kdo so bili pritožniki v postopkih dostopa do informacij?



2.2.2 PRITOŽBE ZOPER MOLK

V letu 2025 je Informacijski pooblaščenec prejel 319 pritožb zaradi molka, od tega 316 zaradi molka organov in tri zaradi neodziva poslovnih subjektov pod prevladujočim vplivom. Največ pritožb zaradi molka je bilo zabeleženih zoper občine (102), kar predstavlja triodstotno povečanje v primerjavi z letom 2024, ko je bilo teh pritožb 99. Sledile so pritožbe zoper molk državnih organov (86), kjer se je število primerov zmanjšalo za 14,7 %, saj je bilo v letu 2025 obravnavanih 75 primerov. Zoper javne zavode je bilo v letu 2025 podanih 61 pritožb zaradi molka, kar pomeni 38,6-odstotni porast v primerjavi z letom 2024, ko je bilo takih primerov 44. 78 pritožb zaradi molka je Informacijski pooblaščenec prejel zoper preostale zavezanca (torej zoper izvajalce javnih služb ali nosilce javnega pooblastila, javna podjetja, druge subjekte javnega prava, druge državne organe, javne agencije, sodišča in javne sklade).

Zoper katere zavezanca so bile vložene pritožbe?

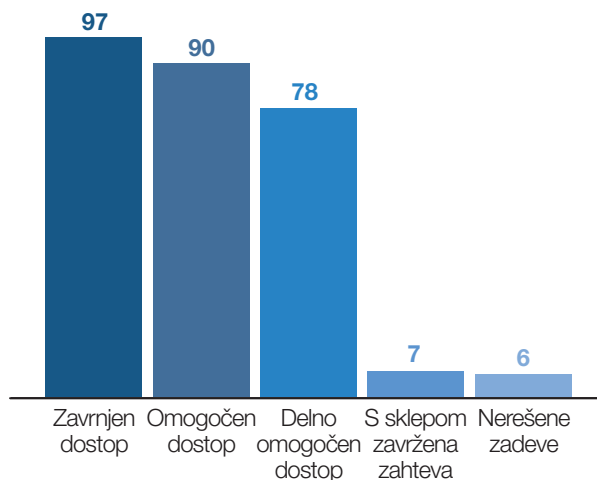


Največ pritožb zaradi molka organa je bilo vloženi s strani fizičnih oseb, in sicer kar 72,7 % (232 primerov). Novinarji oz. mediji so vložili 16 % pritožb zaradi molka (51 primerov), pravne osebe zasebnega prava pa 11 % (35 primerov). V le 0,3 % (v enem primeru) so pritožbo zaradi molka vložile pravne osebe javnega prava. Po preizkusu formalnih predpostavk Informacijski pooblaščenec v 41 primerih postopka zaradi molka ni uvedel. Od tega je v 14 primerih pritožbo zavrgel s sklepom, v 12 primerih zaradi preuranjenosti, v enem primeru zaradi pomanjkljivosti pritožbe, ki je prosilec ni dopolnil, v enem primeru pa je bila pritožna nedovoljena. V 14 primerih je prosilec pritožbo umaknil, ker je od zavezanca že prejel zahtevano informacijo. V 13 primerih je postopek zaradi molka 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 272 primerih zavezanca pozval, naj čim prej odloči o zahtevi prosilca. Po pozivu Informacijskega pooblaščenca so zavezanca zahtevano informacijo v 90 primerih posredovali, v 97 primerih so zavrnil dostop z izdajo zavrnilne odločbe, v 78 primerih pa so dostop delno omogočili (tako da so določene podatke zakrili ali pa so omogočili dostop samo do nekaterih informacij, preostale pa so zavrnil). V sedmih primerih je zavezanec zahtevo prosilca s sklepom zavrgel. Šest zadev je še odprtih in v fazi reševanja.

Kako so ravnali zavezanca po pozivu Informacijskega pooblaščenca zaradi molka?



V okviru zahtev za dostop do informacij javnega značaja pri poslovnih subjektih pod prevladujočim vplivom je Informacijski pooblaščenec vodil tri pritožbene postopke zaradi molka zavezanca, in sicer je, po pozivu zaradi molka, zavezanec v enem primeru prosilcu dostop omogočil, v enem primeru je zahtevi delno ugodil, v enem primeru pa je zahtevo prosilca zavrgel.

Med 319 primeri molka je bilo 45 primerov povezanih z Zakonom o medijih, pri čemer je največkrat, v 14 primerih, šlo za organe državne uprave.

2.3 ŠTEVILO VLOŽENIH TOŽB IN PREJETIH SODB

Pritožba zoper odločbo Informacijskega pooblaščenca ni dopustna, mogoče pa je sprožiti upravni spor. Leta 2025 je bilo na Upravnem sodišču RS vloženi 42 tožb zoper odločbe Informacijskega pooblaščenca (zoper 7 % izdanih odločb), kar je manj kot preteklo leto (12,6 %). 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 2025 odločilo o 44 tožbah, ki so bile vložene zoper odločbe Informacijskega pooblaščenca, in:

- tožbo zavrnilo – 24,
- tožbi ugodilo, izpodbijano odločbo oz. del odločbe odpravilo in zadevo vrnilo Informacijskemu pooblaščenca v ponovno odločanje – 10,
- tožbi ugodilo in samo odločilo o zahtevi – 1,
- postopek s sklepom ustavilo, prekinilo ali tožbo zavrglo – 7.

Leta 2025 je Vrhovno sodišče RS odločilo o eni reviziji zoper sodbo Upravnega sodišča in revizijo zavrnilo.

2.4 STORJENI PREKRŠKI PO ZDIJZ, ZInfP IN ZMed

Leta 2025 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

Analize o prestrukturiranju družb Termoelektrarna Šoštanj in Premogovnik Velenje so informacije javnega značaja po drugem odstavku 4.a člena ZDIJZ

Prosilec je na Holding slovenske elektrarne d.o.o. naslovil zahtevo za dostop do analiz, povezanih s prestrukturiranjem termo divizije skupine HSE. Zavezanec je dostop zavrnil z utemeljitvijo, da zahtevane informacije ne izpolnjujejo pogojev iz prvega odstavka 4.a člena ZDIJZ. Informacijski pooblaščenec je v pritožbenem postopku temu pritrdil, hkrati pa je ugotovil, da gre za informacije javnega značaja po drugem odstavku 4.a člena ZDIJZ. Zavezanec je namreč za izdelavo zahtevanih analiz predhodno sklenil pravni posel, torej pogodbo za svetovanje, kar v konkretnem primeru pomeni, da je zahtevana »povezava« podana, zato je izpolnjena prva predpostavka definicije informacije javnega značaja iz drugega odstavka 4.a člena ZDIJZ. Za razkritje obravnavanih analiz mora biti izkazan tudi drugi pogoj, torej obstoj javnega interesa. Informacijski pooblaščenec je ugotovil, da je v povezavi z izdelanimi analizami prišlo do predčasnega sprejema ukrepov, ki bodo nedvomno imeli dodatne finančne posledice za državni proračun, v breme davkoplačevalcev, ključen pa je učinek ukrepov za prebivalce Šaleške doline, tako z ekonomskega oz. socialnega vidika kakor tudi glede vprašanja zagotavljanja toplotne energije za ogrevanje Šaleške doline. Prost dostop do vsebine zahtevanih analiz bi zato pomembno prispeval h kakovostni javni razpravi, kako bo prihodnost družb Termoelektrarna Šoštanj (TEŠ) in Premogovnik Velenje (PV), ki sta v Sloveniji že več let družbeno pereča tema, vplivala na prebivalce Šaleške doline, pa tudi širše. V danem primeru in danih okoliščinah, ko je država s posebnim zakonom in dodatnimi sredstvi posegla v delovanje TEŠ, je zato javni interes glede podatkov iz zahtevanih analiz o prestrukturiranju družb TEŠ in PV izkazan v interesu vseh zaposlenih v družbah TEŠ in PV (zaradi morebitne ukinitve delovnih mest, kar bi močno vplivalo na lokalno gospodarstvo in socialni status prebivalcev) ter vseh uporabnikov toplotne energije v Šaleški dolini, pa tudi vseh davkoplačevalcev v Republiki Sloveniji zaradi dodatne porabe javnih sredstev, ki jih bo država namenila za energetske investicije. Javni interes po dostopu do zahtevanih informacij je torej kompleksen splet potrebe po informacijah o pravičnem prehodu in opustitvi rabe premoga, o vplivu na okolje in o ekonomskih posledicah, pomembno vprašanje pa je tudi, kakšna je dolgoročno trajnostna strategija države. Informacijski pooblaščenec je zato zaključil,

da so izpolnjeni pogoji iz drugega odstavka 4. člena ZDIJZ, zato je dostop javnosti do zahtevanih analiz dopusten ter nikakor ne more pomeniti preobsežnega in nesorazmernega posega v interese zavezanca.

KLJUČNE BESEDE: poslovna skrivnost, test interesa javnosti, številka odločbe 09021-9/2024

Poročanje v zvezi z vzpostavitvijo sekcijskega merjenja hitrosti vsebuje podatke o porabi javnih sredstev, ki so absolutno javni, in je hkrati tema, ki zadeva širši javni interes

DARS d.d. je s sklicevanjem na poslovno skrivnost (2. točka prvega odstavka 6. člena ZDIJZ) zavrnil odgovore na novinarska vprašanja glede poročanja po pogodbi v zvezi z vzpostavitvijo sekcijskega merjenja hitrosti na avtocestah. Informacijski pooblaščenec je v pritožbenem postopku ugotovil, da pogoji, ki jih določa Zakon o poslovni skrivnosti (ZPosS), v obravnavanem primeru niso izpolnjeni, saj dokument, ki vsebuje zahtevane informacije, predstavlja poročanje izvajalca o fazi postopka pridobivanja certifikata, ki ne pomeni strokovnega znanja, izkušenj in dragocenih informacij, ki bi omogočale večjo konkurenčnost na trgu. Poleg tega obravnavani dokument vsebuje podatke o porabi javnih sredstev, ki so javni na podlagi 1. alineje tretjega odstavka 6. člena ZDIJZ. Zahtevani podatki sicer ne izkazujejo neposredno izplačila javnih sredstev, vendar se nanašajo na izvajanje pogodbe, sklenjene na podlagi izvedenega javnega naročila za dodelitev javnih sredstev. Le z razkritjem teh podatkov je omogočeno doseganje namena nadzora javnosti, ki naj bi ga institut transparentnosti zasledoval, to pa je spodbujanje oz. zagotavljanje smotrne porabe javnih sredstev in učinkovito izvajanje javnih funkcij. Informacijski pooblaščenec je ugotovil, da je za razkritje podan tudi prevladujoč javni interes, saj se zahtevane informacije tičejo varnosti ljudi v cestnem prometu, od te pa je odvisna kakovost življenja vseh državljanov. Ker gre za temo, ki je v danem trenutku aktualna, bi razkritje zahtevanih dokumentov javnosti pripomoglo k širši razpravi o pomembni družbeni temi. Bistveno je tudi to, da je prosilec novinar medija, ki ima dolžnost posredovati informacije o vseh zadevah, ki zadevajo javnost. S tem prosilec kot medij udejanja aktivni vidik svoje ustavne pravice do svobode izražanja, ki se kaže v varovanju svobode posredovanja informacij in mnenj. Gre torej za razkritje informacij, ki bi koristile javnemu vedenju, s čimer bi se omogočilo nadzor in sodelovanje javnosti pri temah, nad katerimi bi morala zelo skrbno bdeti. Informacijski pooblaščenec je zato odločil, da je organ prosilcu dolžan posredovati dokument, ki se nanaša na poročanje glede vzpostavitve sekcijskega merjenja hitrosti.

KLJUČNE BESEDE: varstvo upravnega postopka, številka odločbe 090-166/2025

Za razkritje imen in priimkov obtoženih je podan prevladujoč interes javnosti, ker gre za kazniva dejanja, storjena v povezavi z izvajanjem oz. zlorabo delovne obveznosti posameznikov in njihovega položaja na delovnem mestu v gospodarski družbi

Okrožno sodišče v Ljubljani je zahtevi medija za posredovanje sodne odločbe v kazenski zadevi delno ugodilo in mu posredovalo anonimizirano sodno odločbo, pri čemer se je sklicevalo na varstvo osebnih podatkov (3. točka prvega odstavka 6. člena ZDIJZ). V pritožbenem postopku je Informacijski pooblaščenec ugotovil, da imena in priimki sodnice, sodne zapisničarice in državnega tožilca niso varovani osebni podatki, ker gre za podatke, povezane z opravljanjem javne funkcije ali delovnega razmerja javnega uslužbenca (1. alineja tretjega odstavka 6. člena ZDIJZ). Osebni podatki odvetnikov tudi niso varovani, saj v dokumentu ne nastopajo v svoji zasebnopravni sferi, temveč kot poslovni subjekti, zato se določila Splošne uredbe o varstvu osebnih podatkov nanje ne raztezajo. Prav tako v krog varstva osebnih podatkov ne sodi navedba zastopnikov pravnih oseb, ki so javno objavljeni v Poslovnem registru. Imena in priimki, elektronski naslovi ter podatki o transakcijskih računih ostalih fizičnih oseb, ki so navedeni v zahtevani sodbi, so varovani osebni podatki, ker ni podlage za njihovo razkritje. Enako velja za osebne okoliščine, ki se nanašajo na obtožene osebe. Za razkritje imen in priimkov obtoženih oseb v obravnavani kazenski zadevi pa je podan prevladujoč javni interes. Kazniva dejanja so bila namreč storjena v povezavi z izvajanjem oz. zlorabo delovne obveznosti posameznikov in njihovega položaja na delovnem mestu v gospodarski družbi. Družbena občutljivost za pojave (obsodilne sodbe) nepravilnih ali nezakonitih ravnanj je pričakovana in primerna, saj se s tem kaže tudi občutljivost družbe na kazniva dejanja zoper gospodarstvo. Odziv je še toliko večji v primerih škodljivih ravnanj, ki neposredno prizadenejo večjo skupnost, oz. situacij, ki so blizu večjemu številu posameznikov oz. se v njih za oškodovance lahko prepozna večje število posameznikov. Pri razkrivanju tovrstnih podatkov moramo upoštevati tudi različne vidike obravnavanja kaznivih dejanj, ki so lahko ekonomski, kulturni, politični, pravni in drugi. Lahko povzročajo ekonomsko škodo, zmanjšujejo obseg socialnih pravic, kakovost bivanja v družbi ipd. Zato je potreba po transparentnosti pri preprečevanju teh posledic toliko večja. Javnost je bila z zaključkom konkretnega kazenskega postopka na prvi stopnji seznanjena z javno razglasitvijo zahtevane sodbe in tudi preko medijev. V tem pogledu se kaže pravica javnosti, da bdi nad delom pravosodnih organov, v konkretnem primeru sodišč, ki vodijo kazenske postopke, predvsem z vi-

dika seznanitve s celotno odločitvijo sodišča. Glede na to, da se zahtevane informacije nanašajo na temo, ki je aktualna, bi razkritje zahtevanih informacij javnosti pripomoglo k širši razpravi o pomembni družbeni temi, torej je izpolnjena tudi časovna komponenta javnega interesa. Pri tem je bistveno tudi to, da je prosilec medij, ki ima dolžnost posredovati informacije v vseh zadevah, ki zadevajo javnost. Upoštevajoč vse navedeno je Informacijski pooblaščenec ob tehtanju koristi, ki jih mediju in javnosti prinaša dostop do informacij javnega značaja, ter interesov za varovanje osebnih podatkov zaključil, da javni interes za razkritje imen in priimkov obtoženih oseb prevlada, zato jih je organ dolžan posredovati mediju.

KLJUČNE BESEDE: osebni podatek, številka odločbe 090-228/2025

Interes javnosti za razkritje razlogov za odvzem licence zdravnikom prevlada nad izjemo varstva osebnih podatkov

Medij je od Zdravniške zbornice Slovenije zahteval kopije dokumentov glede odvzema licence zdravnikom. Organ mu je posredoval zahtevane odločbe, pri čemer je s sklicevanjem na izjemo varstva osebnih podatkov (3. točka prvega odstavka 6. člena ZDIJZ) prekril razloge za odvzem licence. Informacijski pooblaščenec je v pritožbenem postopku ugotovil, da je te podatke mogoče šteti za osebne podatke posameznikov, vendar so ti prosto dostopni, ker gre za podatke, za razkritje katerih je podan javni interes. V delu, v katerem organ odloča o odvzemu zdravniške licence, gre za pristojnosti organa v zvezi z izvajanjem javnih pooblastil na področju licenc zdravnikov. Vsebina in obrazložitev upravne odločbe, v zvezi s katero organ izvaja javno pooblastilo, je bistvenega pomena za demokratičen nadzor nad delovanjem organa. Vsa vprašanja, povezana z izvajanjem sistema podeljevanja in odvzema licenc ter drugih oblik sankcioniranja dela zdravnikov, so splošna družbena vprašanja in zadevajo širok krog javnosti. Pri presoji v obravnavani zadevi je odločilno to, da je zdravstvo področje, ki je v javnem interesu, saj zadeva vsakogar, ter da je zdravje dobrina, ki je med najpomembnejšimi v življenju posameznika, poklic zdravnika pa je na ravni države izrazito reguliran poklic. Razlogi za odvzem licence so posledično v interesu javnosti, saj gre za področje, ki je po sami vsebini v širšem interesu celotne družbe, prav tako pa gre tudi za nadzor javnosti nad izvrševanjem javnega pooblastila, ki je bilo v tem delu podeljeno organu. Tudi z vidika pacientovih pravic, zaradi uresničevanja pravice do samostojnega odločanja o zdravljenju in pravice do sodelovanja v procesu zdravljenja, je pomembno, da so ljudje obveščeni o določenih vidikih zdravljenja, kar

sestoji tudi iz informacij o preteklem delovanju zdravnika, informacij o tem, kdaj in na katerem področju je pridobil licenco za samostojno opravljanje zdravniške službe, pa tudi o tem, kdaj in iz katerih razlogov mu je bila licenca morebiti odvzeta. Ni zanemarljivo niti dejstvo, da podatke zahteva medij, za katerega je dostop do informacij ključnega pomena za izvajanje vloge »javnega čuvaja«. Informacijski pooblaščenec je zaključil, da je v zvezi z razkritjem razlogov za odvzem zdravniške licence, ne glede na obstoj izjeme varstva osebnih podatkov, v obravnavani zadevi podan interes javnosti, da se z navedenimi informacijami seznanijo. Obravnavane odločbe o odvzemu licence vsebujejo tudi podrobnejše podatke o obravnavi pacientov, podatki o pacientih pa za seznanitev javnosti z razlogi za odvzem licence niso bistveni, zato niso prosto dostopna informacija. Prav tako javnosti niso dostopni naslov in datum rojstva zdravnikov. Ti osebni podatki namreč ne kažejo na okoliščine, ki bi jih bilo treba razkriti na podlagi interesa javnosti.

KLJUČNE BESEDE: osebni podatek, test interesa javnosti, številka odločbe 090-236/2025

Poročilo o izvajanju aktivnosti Stanovanjskega sklada RS glede odprave napak je absolutno javno, ker vsebuje podatke o porabi javnih sredstev, hkrati pa je za njegovo razkritje podan javni interes

Stanovanjski sklad RS je zavrnil zahtevo prosilke za dostop do poročila o izvajanju aktivnosti glede odprave napak po pravnomočnih sodbah. Informacijski pooblaščenec je po proučitvi pritožbe ugotovil, da izjema varstva sodnega postopka (8. točka prvega odstavka 6. člena ZDIJZ), ki jo je zahteval organ, ni podana, ker zahtevani dokument ni del sodnega spisa in je nastal zaradi potreb organa. Ker že odsotnost enega pogoja onemogoča sklicevanje na navedeno izjemo, se Informacijski pooblaščenec ni spuščal v presojo izpodbijane odločbe glede škodnega testa, ki ga je organ dolžan izvesti pri izkazovanju obstoja pogoja, da bi razkritje podatka škodovalo izvedbi sodnega postopka. Zahtevana izjema varstva sodnega postopka tako ni podana. Prav tako ni podana izjema notranjega delovanja (11. točka prvega odstavka 6. člena ZDIJZ), saj zahtevano poročilo ne vsebuje mnenj in stališč, ampak gre za poročilo o do zdaj izvedenih aktivnostih organa in načrtu za (nadaljnje) saniranje napak pri stanovanjskih naseljih po pravnomočnih sodbah. V dokumentu tako ne gre za izmenjavo ali izražanje kritičnih mnenj ali predloge strateških usmeritev, na podlagi katerih bi se oblikovala notranja politika organa. Poleg tega je bilo to poročilo posredovano Ministrstvu za solidarno prihodnost, torej je šlo za komunikacijo organa z dru-

gim (zunanjim) subjektom. Ker obravnavano poročilo ne predstavlja dokumenta za notranjo rabo organa, ni izpolnjen že prvi pogoj za izjemo notranjega delovanja, zato se Informacijski pooblaščenec ni spuščal v presojo morebitne škode, ki bi nastala z razkritjem, temveč je zaključil, da zahtevano poročilo ne predstavlja zatrjevane izjeme. Dodatno je Informacijski pooblaščenec utemeljil še, da je za razkritje zahtevanega poročila podana pravna podlaga v 1. alineji tretjega odstavka 6. člena ZDIJZ. Vsebuje namreč podatke glede sanacije napak po pravnomočnih sodbah na nepremičninah, ki jih je organ kot javni sklad kupil od gradbenih izvajalcev. Organ je javni nepremičninski in finančni sklad, ki kot nacionalno pomembna institucija na raznovrstne načine izpolnjuje stanovanjske potrebe prebivalcev Slovenije. Poleg tega je organ izvajalec nacionalne stanovanjske politike. V obravnavanem primeru gre torej za porabo javnih sredstev, s katerimi organ razpolaga. Skladno s sodno prakso poraba javnih sredstev ni zgolj »trošenje«, pač pa vse oblike razpolaganja z javnimi sredstvi, zato je treba dostop do zahtevanega poročila dovoliti tudi iz tega razloga. Informacijski pooblaščenec je še ocenil, da je v konkretnem primeru javni interes glede razkritja poročila močnejši od javnega interesa oz. interesa drugih oseb za omejitev dostopa (drugi odstavek 6. člena ZDIJZ). Pri tem je poudaril, da gre pri izvajanju nacionalne stanovanjske politike na način, da organ med drugim posluje z nepremičninami z namenom zagotavljanja javnega interesa ter investira v gradnjo stanovanj in stavbna zemljišča, za porabo javnih sredstev, zato je zagotovo velik interes javnosti, da izve, ali so javna sredstva dejansko porabljena za stanovanja, ki izpolnjujejo zahtevane gradbene standarde. Prav tako je javnosti znano, da so v stanovanjih, na katera se nanaša zahtevano poročilo, napake, zaradi katerih so kupci sprožili sodni postopek zoper organ. Zato je upravičen interes javnosti, da izve, kakšno kvaliteto stanovanj ponuja na trgu organ kot izvajalec nacionalne stanovanjske politike, ki mora delovati izključno v javnem interesu. V javnem interesu je zagotovo, da organ na trg ponudi stanovanja za ceno, ki je ugodnejša od tiste, ki jo ponuja tržni nepremičninski trg, ne da bi pri tem trpela kvaliteta. Prav dejstev, ki bi lahko potencialno ogrozila ugled organa, ni mogoče zakriti pred javnostjo, saj je v takih primerih interes javnosti za pridobitev informacij toliko bolj izražen zaradi okoliščine, da gre za zavezanca za posredovanje informacij.

KLJUČNE BESEDE: notranje delovanje, test interesa javnosti, varstvo sodnega postopka, številka odločbe 090-275/2025

Podatki, navedeni v vetrni študiji za vetrno elektrarno, lahko pomembno prispevajo h kakovostni javni razpravi, zato je podan prevladujoč interes javnosti za razkritje teh podatkov na podlagi drugega odstavka 4.a člena ZDIJZ

Družba Dravske elektrarne Maribor d.o.o. je zavrnila zahtevo za dostop do študije vetra za vetrno elektrarno s sklicevanjem na varstvo poslovne skrivnosti. V pritožbenem postopku je Informacijski pooblaščenec ugotovil, da zahtevana informacija izpolnjuje prvi pogoj po drugem odstavku 4.a člena ZDIJZ, torej da je zavezanec za izdelavo zahtevane študije predhodno sklenil pravni posel. Za razkritje dela zahtevane študije pa je izkazan tudi drugi pogoj, to je javni interes. Zavezanec je s svojimi navedbami izkazal, da so v konkretnem primeru izpolnjene vse zahteve, ki za opredelitev poslovne skrivnosti izhajajo iz ZPosS, zato je Informacijski pooblaščenec presojal, ali je javni interes za razkritje močnejši od izkazane izjeme varstva poslovne skrivnosti. Pri tem je sledil navedbam zavezanca, da same meritve in konkretne analize ni mogoče povezati z zatrjevanimi vplivi na zdravje ljudi in na okolje. Temu so bile namenjene druge študije in analize, ki so javno dostopne. Posledično ni bilo mogoče narediti povezave v smislu 2. alineje tretjega odstavka 6. člena ZDIJZ. Javni interes, ki je v primeru drugega odstavka 4.a člena ZDIJZ podlaga za razkritje, pa seveda ni nujno povezan samo z okoljskimi podatki, temveč lahko o javnem interesu govorimo tudi takrat, kadar so zahtevane informacije pomembne za kvalitetno javno razpravo, kadar je govora o pomembnih družbenih temah, kar umeščanje vetrnih elektrarn v prostor zagotovo je. Informacijski pooblaščenec se je strinjal s prosilcem, da gre za takšne vrste informacij, ki morajo biti javnosti dostopne vsaj v svojem zaključku, saj je le s tem zagotovljena celostna strokovna in civilna presoja oz. javna razprava o izgradnji vetrnih elektrarn tudi z vidika ekonomske upravičenosti, kar nedvomno krepi legitimnost odločitve. Morebitna postavitev vetrne elektrarne namreč zagotovo ne bo učinkovala samo na zavezanca, temveč tudi na okolico in na ljudi, ki bodo živeli v njeni bližini. Informacijski pooblaščenec je zato odločil, da je v danem primeru prosilcu treba omogočiti dostop do zaključka zahtevane študije, v katerem so povzete ključne ugotovitve, s čimer se lahko pomembno prispeva h kakovostni javni razpravi, hkrati pa se ne poseže v tiste dele študije, ki vsebujejo specifično strokovno znanje ter poslovne informacije.

KLJUČNE BESEDE: okoljski podatki, številka odločbe 09021-6/2025

Podatki o pošiljkah odpadkov so okoljski podatki in zato ne predstavljajo poslovnih skrivnosti

Stranski udeleženec je izpodbijal odločbo Agencije RS za okolje, ker je menil, da je organ nekatere podatke napačno klasificiral kot podatke o odpadkih in posledično ugodil zahtevi prosilca za dostop do podatkov o pošiljkah odpadkov. Informacijski pooblaščenec je ugotovil, da so predmet pritožbe podatki, ki jih organ hrani v informacijskem sistemu o ravnanju z odpadki; slednji je bil vzpostavljen za zagotavljanje sledljivosti pošiljk odpadkov ter spremljanja nastajanja odpadkov in ravnanja z njimi, in sicer na podlagi Uredbe o odpadkih. Pri tolmačenju predpisov, kdaj je mogoče podatke šteti za podatke, povezane z okoljem, je treba zavzeti široko razlago, kar velja tudi za sam pojem odpadka. Podatki o pošiljkah odpadkov (podatek o tem, ali je bila pošiljka sprejeta, datum oddaje in prevzema pošiljke odpadkov ter kraj oddaje in prevzema pošiljke odpadkov) omogočajo sledljivost pošiljk odpadkov in spremljanje nastajanja odpadkov ter ravnanja z njimi, zato gre za podatke, ki se neposredno tičejo odpadkov in ravnanja z odpadki, kar pomeni, da gre za okoljske podatke v smislu Zakona o varstvu okolja (ZVO-2). Ta temelji na načelu javnosti, ki poleg splošne določbe, da so okoljski podatki javni, javnosti daje tudi vrsto drugih pravic, ki pa 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 zaključil, da so obravnavani podatki o pošiljkah odpadkov izjema od izjem iz 2. alineje tretjega odstavka 6. člena ZDIJZ, zato v skladu s tretjim odstavkom 2. člena ZPosS ne morejo predstavljati poslovne skrivnosti proizvajalcev ter posledično ne predstavljajo izjeme po 2. točki prvega odstavka 6. člena ZDIJZ, ki jo je sicer zatrjeval stranski udeleženec.

KLJUČNE BESEDE: okoljski podatki, številka odločbe 090-478/2025/3

Pri javnih funkcionarjih je treba upoštevati pravico do tajnosti pisem, kadar gre za dejavnost, ki jo je posameznik, ki sicer opravlja javno funkcijo, izvajal v okviru svojega zasebnega življenja

Mestna občina Ljubljana je zavrnila zahtevo prosilca za dostop do pisma, ki ga je župan poslal predsedniku druge države. V pritožbenem postopku je Informacijski pooblaščenec ugotovil, da organ zahtevanega pisma nima v posesti, ker kot zasebno županovo pismo ni bilo evidentirano v evidenco dokumentarnega gradiva. Niti uradna oseba organa niti Informacijski pooblaščenec

nimata pristojnosti pregledovati elektronskih poštnih predalov posameznih javnih uslužbencev oz. funkcionarjev, zato jih tudi ne moreta »prisiliti« v morebitno izročitev zahtevanih informacij. Z vpogledom v elektronsko pošto javnih funkcionarjev ali javnih uslužbencev z namenom ugotovitve, ali z zahtevanimi informacijami razpolagajo, bi namreč posegli v ustavno zavarovano pravico do komunikacijske zasebnosti javnega uslužbenca oz. javnega funkcionarja. Četudi bi organ razpolagal z materializirano obliko zahtevanega pisma, pa iz izjav župana izhaja, da gre za njegovo osebno pismo in da se ne nanaša na delovno področje organa. V pismu je župan namreč izrazil svoje osebno mnenje, za kar ni imel nobenega pooblastila ne organa ne države. Zgolj na podlagi dejstva, da je zahtevano pismo vsebovalo glavo organa, ni mogoče zaključiti, da pismo sodi v delovno področje organa, ker je za to presojlo odločilna dejanska vsebina pisma, ki pa ne sodi v delovno področje organa. Informacijski pooblaščenec je izvedel tudi test praktične konkordance in ugotovil, da je interesu splošne javnosti v danih okoliščinah v zadostni meri zadoščeno že z informacijami, ki jih je v zvezi z zahtevanim pismom podal župan na novinarski konferenci in na podlagi katerih se lahko splošna javnost v zadostni meri seznanila z načinom delovanja obravnavanega posameznika. Razkrivanje vsebine izvornika zahtevanega pisma v konkretnem primeru bi po oceni Informacijskega pooblaščenca pomenilo nesorazmeren poseg v pravico do tajnosti pisem posameznika, ki ga je pripravil. Informacijski pooblaščenec je tako tudi na podlagi izvedbe testa sorazmernosti ugotovil, da zahtevanega pisma ni mogoče uvrstiti v delovno področje organa. Informacijski pooblaščenec je zaključil, da prosilčevi zahtevi ni mogoče ugoditi, saj organ ne razpolaga z zahtevanim pismom, ki po vsebini niti ne sodi v delovno področje organa, kar pomeni, da niso izpolnjeni pogoji za informacijo javnega značaja iz 4. člena ZDIJZ.

KLJUČNE BESEDE: ali dokument obstaja, številka odločbe 090-285/2025/5

Imena in priimki prejemnikov izjemnih pokojnin niso varovani osebni podatki

Medij je zahteval, da mu Zavod za pokojninsko in invalidsko zavarovanje Slovenije posreduje imena in priimke prejemnikov izjemnih pokojnin v letu 2022. Informacijski pooblaščenec je v pritožbenem postopku ugotovil, da je organ zahtevo neutemeljeno zavrnil, ker razpolaga s seznamom prejemnikov izjemnih pokojnin, priznanih v skladu z Zakonom o izjemnem priznanju in odmeri starostne pokojnine osebam, ki imajo posebne zasluge (ZIPO), seznam pa vsebuje osebne podatke, ki jih je dopustno razkriti javnosti na podlagi določb

ZIPO. Ta namreč določa, da se odločba o izjemnem priznanju in odmeri starostne oz. družinske pokojnine objavi v Uradnem listu Republike Slovenije, kar pomeni, da podatki o tem, kdo so uživalci izjemnih pokojnin, ne pomenijo izjeme od prostega dostopa do informacij javnega značaja po 3. točki prvega odstavka 6. člena ZDIJZ, saj ne predstavljajo t. i. varovanih osebnih podatkov. Poleg tega so obravnavani podatki povezani s porabo javnih sredstev, ker se sredstva za izjemne pokojnine zagotavljajo iz državnega proračuna, zato se dostop do njih dovoli tudi na podlagi tretjega odstavka 6. člena ZDIJZ.

KLJUČNE BESEDE: ali gre za delovno področje, osebni podatki, številka odločbe 090-42/2025

Kinološka zveza Slovenije ni zavezanec za posredovanje informacij javnega značaja

Kinološka zveza Slovenije je na zahtevo prosilca za posredovanje informacij odgovorila, da ni zavezanec po ZDIJZ. Informacijski pooblaščenec je zavrnil pritožbo prosilca zoper navedeni odgovor, ker je ugotovil, da Kinološka zveza Slovenije ni vpisana v Register zavezancev za informacije javnega značaja. Dalje je ugotovil, da je organizirana kot društvo v skladu z Zakonom o društvih (ZDru-1) in je pravna oseba zasebnega prava, ki ni niti izvajalec javne službe niti nosilec javnih pooblastil. Navedeno pomeni, da ne gre za subjekt, ki bi bil zavezan kot organ po 1. členu ZDIJZ. Ob tem je Informacijski pooblaščenec pojasnil, da so javne službe tiste dejavnosti, ki se morajo zaradi različnih razlogov izvrševati v javnem interesu pod posebnim režimom, ker jih na trgu ni mogoče zadovoljiti ali ne smemo dopustiti, da se zadovoljijo na trgu. Krovni zakon, ki ureja gospodarske javne službe in določa način ter oblike izvajanja gospodarskih javnih služb, je Zakon o gospodarskih javnih službah (ZGJS). Negospodarske oz. socialne javne službe pa se izvajajo v skladu z Zakonom o zavodih (ZZ). Upošteva se navedeno je Informacijski pooblaščenec zaključil, da področje delovanja Kinološke zveze Slovenije ni opredeljeno kot izvajanje javne službe. Ugotovil je tudi, da Kinološka zveza Slovenije ni poslovni subjekt pod prevladujočim vplivom oseb javnega prava, torej da ni zavezana niti po 1.a členu ZDIJZ.

KLJUČNE BESEDE: ali je organ zavezanec, številka odločbe 090-48/2025

Podatki o prestajanju kazni zapora oz. o načinu izvrševanja kazenskih sankcij niso neposredno v povezavi z opravljanjem javne funkcije ali s porabo javnih sredstev

Prošilec je od Okrožnega sodišča v Murski Soboti zahteval podatke glede izvršitve pravnomočne sodbe, in sicer v zvezi s poimensko navedenim obsojencem. Organ je njegovo zahtevo zavrnil iz razloga varstva osebnih podatkov (3. točka prvega odstavka 6. člena ZDIJZ). Temu je sledil tudi Informacijski pooblaščenec, ki je v pritožbenem postopku ugotovil, da zahtevani podatki ne predstavljajo podatkov, ki bi bili neposredno povezani s porabo javnih sredstev ali z opravljanjem javne funkcije v smislu določbe tretjega odstavka 6. člena ZDIJZ. Pojem »podatki, povezani s porabo javnih sredstev ali z opravljanjem javne funkcije« je namreč odprt pravni pojem, ki ga je v vsakem posameznem primeru treba napolniti z vsebino. Na podlagi 1. alineje tretjega odstavka 6. člena ZDIJZ so praviloma javni tisti podatki, ki so neposredno povezani s porabo javnih sredstev, z opravljanjem javne funkcije ali delovnega razmerja javnega uslužbenca, ne pa tudi tisti podatki, ki so s tem povezani zgolj posredno. Posameznik, na katerega se nanaša obravnavana zahteva prosilca, je sicer res bil obsojen zaradi kaznivega dejanja, ki je bilo storjeno v zvezi z opravljanjem javne funkcije, vendar sami podatki v zvezi s prestajanjem kazni zapora, tudi podatki o tem, ali je obsojeni vložil prošnjo za alternativno prestajanje kazni, kako je bila ta obravnavana itd., niso več v neposredni zvezi s porabo javnih sredstev niti z opravljanjem javne funkcije. Informacijski pooblaščenec je vpogledal v zahtevani dokument in ugotovil, da vsebuje številne objektivne in subjektivne navedbe v zvezi z obsojencem, ki izvirajo iz njegove zasebnopravne sfere in niso v neposredni zvezi z opravljanjem funkcije, nanjo pa neposredno tudi ne vplivajo. Ob tem je relevantna tudi okoliščina, da posameznik javne funkcije ne opravlja več, kot tudi okoliščina, da je bila javnost o tem primeru že obširno seznanjena, organ pa je prosilcu predhodno tudi že omogočil dostop do pravnomočne sodbe v tej zadevi, iz katere izhajajo vse okoliščine, ki vplivajo ali bi lahko vplivale na izvajanje javne funkcije.

KLJUČNE BESEDE: javni uslužbenci in funkcionarji, številka odločbe 090-469/2025

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 USPOSABLJANJE ZA OBČINE

Informacijski pooblaščenec je maja 2025 uspešno izvedel spletno usposabljanje s področja dostopa do informacij javnega značaja, ki je bilo namenjeno občinam in ki se ga je udeležilo več kot 100 udeležencev. V prvem delu usposabljanja so bile predstavljene najpogostejše postopkovne dileme dostopa do informacij javnega značaja, drugi del pa je bil namenjen zakonskim izjemam od prostega dostopa, zlasti izjemi varstva osebnih podatkov, poslovne skrivnosti in izjemi dokumentov v postopku nastajanja. Primeri iz prakse Informacijskega pooblaščenca in sodne prakse so bili

osvetljeni z vidika aktualnih vprašanj, ki se nanašajo na delo občin, s čimer so uporabniki pridobili konkretne informacije za lažje delo v praksi. Ker je bilo usposabljanje s strani uporabnikov dobro sprejeto, si bo Informacijski pooblaščenec podobne dogodke prizadeval izvajati tudi v prihodnje.



2.6.2 DAN PRAVICE VEDETI

V zadnjem tednu septembra po vsem svetu potekajo aktivnosti, ki zaznamujejo svetovni dan pravice vedeti (28. september). V tem okviru je Informacijski pooblaščenec 24. 9. 2025 organiziral strokovni posvet na temo uresničevanja in omejevanja pravice dostopa do informacij javnega značaja, na katerem je potekala razprava o izzivih in dobrih praksah zavezancev, predstavljena je bila Konvencija Sveta Evrope o dostopu do uradnih dokumentov ter procesne novosti s področja upravnega postopka. Udeleženci posveta so se strinjali, da ima področje dostopa do informacij javnega značaja v Republiki Sloveniji dobro pravno podlago, ki se v večini primerov ustrezno izvaja tudi v praksi. Kljub temu še vedno obstaja prostor za izboljšave, in sicer bi bilo treba postopke odločanja o zahtevah voditi hitreje



Dogodek ob dnevu pravice vedeti, Ljubljana, 24. 9. 2025.

in še več ozaveščati prosilce ter organe o pomenu te pravice. Hiter razvoj modernih tehnologij prinaša nove izzive tudi na tem področju. Pripravljeni moramo biti na reševanje konfliktov interesov, ki bodo iz tega izhajali, to pa lahko dosežemo le s strokovnim sodelovanjem med vsemi deležniki, zato se moramo še naprej truditi ohraniti in spodbujati konstruktiven dialog na tem področju. Z deljenjem dobrih praks, z odprtim razmišljanjem o še nerešenih izzivih in z opozarjanjem na morebitne šibke točke postopka dostopa do informacij javnega značaja bomo lahko skupaj okrepili moč pravice vedeti in posledično vseh drugih pravic, katerih izvrševanje je z njo pogojeno.

2.7 MEDNARODNO SODELOVANJE NA PODROČJU DOSTOPA DO INFORMACIJ JAVNEGA ZNAČAJA

2.7.1 SVETOVNA KONFERENCA ICIC V BERLINU

Od 23. do 25. junija je v Berlinu zvezni nemški pooblaščenec za varstvo osebnih podatkov in informacije javnega značaja gostil 16. mednarodno konferenco informacijskih pooblaščenecv (ICIC) z naslovom *Dostop do okoljskih podatkov v digitalni dobi (Access to Environmental Information in a Digital Era)*. Konference so se udeležili informacijski pooblaščeneci in druge institucije, ki izvajajo pristojnosti s področja dostopa do informacij javnega značaja. V okviru konference so bile izvedene okrogle mize, na katerih so udeleženci razpravljali o kritičnih vprašanjih v zvezi z dostopom do informacij ranljivih skupin in o primernih ukrepih, da bi se jim informacije zagotovile. Velik poudarek je bil namenjen tudi dostopu do okoljskih podatkov ter pomembnosti transparentnega delovanja in obveščeni javnosti na tem področju. Poudarjen je bil pomen civilne družbe in medijev pri spodbujanju dostopa do informacij in transparentnosti, konference pa so se udeležili tudi predstavniki nevladnih organizacij in novinarji z vsega sveta. Konference sta se udeležila tudi dva predstavnika Informacijskega pooblaščenca.

2.7.2 DELAVNICA PRAKTIČNIH PRIMEROV V ŠPANIJI

V Prishtini na Kosovu se je 7. in 8. aprila 2025 odvijala delavnica z naslovom *Case handling Workshop on Freedom of Information*, ki jo je gostil kosovski pooblaščenec za dostop do informacij javnega značaja in varstvo osebnih podatkov (Agjencia për Informim dhe Privatësi) pod okriljem ICIC. Gre že za peto mednarodno delavnico na temo reševanja konkretnih primerov iz prakse organov, pristojnih za nadzor nad dostopom do informacij javnega značaja. Delavnice so se udeležili predstavniki iz 15 evropskih nadzornih organov, iz Španije, Portugalske, Švice, Črne gore, Severne Makedonije, Škotske, Združenega kraljestva, Albanije, Hrvaške, Madžarske, Avstrije, Estonije, Slovenije in Nemčije. Predstavljene so bile različne nacionalne ureditve postopkov dostopa do informacij javnega značaja, predvsem konkretni primeri iz prakse. Udeleženci so se osredotočili na dileme, težave in ovire, s katerimi se srečujejo uradne osebe pri vodenju in odločanju v pritožbenih postopkih. Posebna pozornost je bila namenjena tudi primerom in izkušnjam s področja javnih naročil, varstva poslovnih skrivnosti ter varstvu avtorskih in sorodnih pravic v postopkih dostopa do informacij javnega značaja. Predstavniki Informacijskega pooblaščenca sta na delavnici sodelovali s prispevkom.

2.7.3 SREČANJE INICIATIVE 2020

Oktober 2025 je v Prizrenu na Kosovu potekalo 6. srečanje Iniciative 2020, ki sta se ga udeležili namestnica informacijske pooblaščenke mag. Kristina Kotnik Šumah in generalna sekretarka Mojca Komac Adlešič. Združenje je bilo ustanovljeno oktobra 2020 na pobudo Informacijskega pooblaščenca Republike Slovenije, vanj pa so povezani organi s področja dostopa do informacij javnega značaja iz Slovenije, Hrvaške, Bosne in Hercegovine, Črne gore, Srbije, Kosova in Severne Makedonije. Namen združenja je sodelovanje in izmenjava dobrih praks pri promociji in varstvu pravice dostopa do informacij javnega značaja. Na srečanju so udeleženci razpravljali o usklajevanju nacionalnih

zakonodaj z evropskimi in mednarodnimi standardi, vključno s Tromsø konvencijo Sveta Evrope, ter o vplivu digitalizacije in novih tehnologij na to področje. Izpostavljena je bila problematika naraščajočih pritožb zaradi molka ter potreba po krepitvi mehanizmov za spremljanje in nadzor na področju proaktivne transparentnosti. Članice so opozorile na naraščajoči obseg svojih nalog in pristojnosti ter s tem povezano potrebo po zagotavljanju zadostnih finančnih in kadrovskih virov, da bi lahko svoje naloge učinkovito izvajale. Članice so se dogovorile, da bo naslednje srečanje v letu 2026 gostila Slovenija.



Šesto srečanje Iniciative 2020, Prizren, 13.–15. oktober 2025.

2.7.4 OBISK PREDSTAVNIKOV HRVAŠKEGA INFORMACIJSKEGA POOBLAŠČENCA

V okviru študijskega obiska je Informacijski pooblaščenec gostil ekipo hrvaškega Pooblaščenca za dostop do informacij javnega značaja (Poverenik za informiranje), sledil pa je obisk predstavnikov Informacijskega pooblaščenca v Zagrebu. Gre za neodvisen državni organ, ki v Republiki Hrvaški deluje kot drugostopenjski, pritožbeni organ v postopkih dostopa do informacij javnega značaja. Ekipi sta izmenjali izkušnje s področja postopkovnih dilem, dostopa do okoljskih podatkov, izjeme poslovne skrivnosti in izjeme varstva osebnih podatkov. Ugotovili sta, da se v praksi obeh pojavljajo podobne procesne in vsebinske dileme. Strinjali sta se, da sta strokovna razprava in izmenjava dobrih praks za obe ekipe koristni in da bosta tovrstno sodelovanje nadaljevali tudi v prihodnje.



Obisk hrvaškega Pooblaščenca za dostop do informacij javnega značaja, Ljubljana, 23. maj 2025.

3 VARSTVO OSEBNIH PODATKOV

V NAŠIH PODATKIH STA MOČ IN BOGASTVO.
OHRANIMO NADZOR NAD NJIMI.

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, ki zagotavlja varstvo osebnih podatkov, določa, da mora biti zbiranje, obdelovanje, namen uporabe, nadzor in varstvo tajnosti določeno z zakonom, 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.

Normativni okvir varstva osebnih podatkov v Sloveniji določajo naslednji sistemski akti:

- 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),
- Zakon o varstvu osebnih podatkov (ZVOP-2), ki je začel veljati 26. 1. 2023, in
- Zakon o varstvu osebnih podatkov na področju obravnavanja kaznivih dejanj (ZVOPOKD), ki je začel veljati 31. 12. 2020.

V letu 2025 pričete nove zadeve zaradi zatrjevane kršitve varstva osebnih podatkov.

3.2 NADZOR V LETU 2025

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 pooblaščenecu (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 obdelavo 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 oseb za varstvo osebnih podatkov, evidence dejavnosti obdelav);

Skupaj: 1226 zadev

Javni sektor: 228 zadev

Zasebni sektor: 998 zadev

Inšpekcijske
prijave **189**

Ex offo **39**

Inšpekcijske
prijave **692**

Predlogi za
 uvedbo nadzornega
 postopka, prejeti s
 strani tujih nadzornih
 organov **243**

Ex offo **63**

- 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.

Informacijski pooblaščenec je leta 2025 zaradi zatrjevane kršitve varstva osebnih podatkov obravnaval 1.226 novih inšpekcijskih zadev, od tega 228 zoper javni in 998 zoper zasebni sektor.

Inšpekcijske prijave, ki jih je prejel Informacijski pooblaščenec, so se nanašale na sume kršitev več določb Splošne uredbe in ZVOP-2, kot izhaja iz spodnje grafične predstavitev.

Nezakonito izvajanje videonadzora 274	
Nezakonito razkrivanje, posredovanje in nezakonita objava 213	
Nezakonita obdelava osebnih podatkov pri izvajanju neposrednega trženja 70	
Priskotki 30	Neustrezno zavarovanje osebnih podatkov 58
	Nezakonit vpogled v osebne podatke 45
Kršitev pravice do informacij 23	Nezakonito zbiranje oziroma zahtevanje osebnih podatkov 93
	Drugo 75

Na podlagi obravnave vseh inšpekcijskih zadev je Informacijski pooblaščenec 73 prijaviteljev napotil na pravice, ki jih morajo pri upravljavcih osebnih podatkov posamezniki uveljavljati sami, največkrat na pravico do seznanitve z lastnimi osebnimi podatki, na pravico do ugovora in na pravico do izbrisa podatkov. 106 prijaviteljev je obvestil, da postopka inšpekcijskega nadzora ne bo uvedel, ker iz prijave ne izhaja sum kršitve določb Splošne uredbe in/ali ZVOP-2. V 254 primerih Informacijski pooblaščenec postopka ni uvedel, ker niso bili predloženi ustrezni in zadostni dokazi, ki bi zatrjevano kršitev utemeljevali, v 123 primerih pa za ukrepanje ni bil pristojen. V 75 primerih inšpekcijski postopek ni bil uveden, ker je kršitelj nepravilnosti že odpravil. V 109 primerih pa Informacijski pooblaščenec inšpekcijskega postopka ni uvedel, ker je šlo za enkratna dejanja oziroma kršitve varstva osebnih podatkov v preteklosti, takih kršitev pa se z inšpekcijskimi ukrepi za nazaj ne da preprečiti ali odpraviti. V primeru, da je iz teh prijav izhajala kršitev, je te obravnaval v okviru pristojnosti, ki jih ima kot prekrškovni organ, in sicer z uvedbo prekrškovnega postopka oz. izrekom ukrepov v skladu z Zakonom o prekrških (ZP-1) (več v poglavju 3.2.9).

Na podlagi 70 % inšpekcijskih prijav, prejetih v letu 2025, Informacijski pooblaščenec inšpekcijskega postopka ni uvedel, saj iz prijave ni izhajal javni interes za uvedbo inšpekcijskega postopka oz. prijavi niso bili priloženi ustrezni dokazi, iz katerih bi izhajal zadosten sum kršitve varstva osebnih podatkov. Informacijski pooblaščenec inšpekcijskega postopka prav tako ni uvedel v primerih, ko so bile nepravilnosti že odpravljene, ali na podlagi tistih prijav, pri katerih je šlo za zatrjevanje preteklih kršitev, ki se jih z ukrepi inšpekcijskega postopka ne da odpraviti; v takih primerih je zatrjevano kršitev, ob obstoju zadostnih dokazov, obravnaval v okviru svojih prekrškovnih pristojnosti.

V primerih prijav, iz katerih je sicer izhajal sum kršitve varstva osebnih podatkov, ki pa ni dosegel praga za uvedbo inšpekcijskega postopka, je bilo upravljavcem v smislu preventivnega delovanja poslano obvestilo z usmeritvami, kako zagotoviti skladno obdelavo podatkov. Informacijski pooblaščenec je v letu 2025 različnim upravljavcem poslal 176 takih obvestil, v katerih jih je obvestil o prejeti prijavi kršitve varstva podatkov ter jim posredoval napotke za zagotovitev skladnosti s predpisi.

Informacijski pooblaščenec je prejel tudi šest prijav, ki so jih prijavitelji podali po Zakonu o zaščiti prijaviteljev.

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 2025 obravnaval **228 novih zadev**. Zoper zavezanca v javnem sektorju je prejel 189 novih inšpekcijskih prijav. Na podlagi teh prijav ter po lastni presoji je skupaj uvedel 39 novih inšpekcijskih postopkov.

Informacijski pooblaščenec je leta 2025 zavezancem v javnem sektorju izdal šest t. i. predodločb³ ter eno ureditveno odločbo, medtem ko so večino kršitev zavezanci odpravili prostovoljno že po prejemu poziva in usmeritev s strani državnega nadzornika za varstvo osebnih podatkov.

Leta 2025 je bilo v javnem sektorju 58 inšpekcijskih postopkov zaključenih z izdajo sklepa o ustavitvi postopka. Informacijski pooblaščenec je 39 postopkov ustavil, ker so zavezanci ugotovljene nepravilnosti odpravili, v 12 postopkih ni zaznal kršitev določb Splošne uredbe ali ZVOP-2, štiri postopke je ustavil zato, ker je šlo za kršitve, ki so predstavljale enkratna dejanja v preteklosti, ki jih z inšpekcijskimi ukrepi za nazaj ni bilo več mogoče odpraviti, v treh primerih pa ni bilo predloženih dovolj dokazov za nadaljevanje postopka.

3.2.3 INŠPEKCIJSKI NADZOR V ZASEBNEM SEKTORJU

Informacijski pooblaščenec je zoper zavezanca v zasebnem sektorju obravnaval **998 novih zadev**. Zoper zavezanca v zasebnem sektorju je prejel 692 novih inšpekcijskih prijav. Na podlagi teh prijav ter po lastni presoji je skupaj uvedel 63 novih inšpekcijskih postopkov. Dodatno je uvedel še 243 postopkov po iniciativi nadzornih organov v EU v okviru čezmejnega sodelovanja – v teh je Informacijski pooblaščenec sodeloval kot zadevni nadzorni organ (več v poglavju 3.2.8).

Informacijski pooblaščenec je leta 2025 zavezancem v zasebnem sektorju izdal 25 t. i. predodločb ter dve ureditveni odločbi, medtem ko so večino kršitev zavezanci odpravili prostovoljno že po prejemu poziva in usmeritev s strani državnega nadzornika za varstvo osebnih podatkov.

Leta 2025 je Informacijski pooblaščenec pri zavezancih v zasebnem sektorju s sklepom ustavil 185 postopkov: 135 postopkov je ustavil po tem, ko so zavezanci ugotovljene nepravilnosti odpravili, 24 po-

stopkov je ustavil, ker ni zaznal kršitev določb Splošne uredbe ali ZVOP-2, 10 postopkov je zaključil, ker v zvezi z ugotovljenimi prekrški ni bilo mogoče izreči inšpekcijskih ukrepov, saj je šlo za enkratna dejanja v preteklosti, v 16 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 2023 zoper inšpekcijsko odločbo, s katero je bilo upravljavcu naloženo prenehanje izvajanja video-nadzora. Sodišče je tožbi ugodilo, odločbo razveljavilo in vrnilo zadevo Informacijskemu pooblaščenec v ponovno odločanje.

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 2025 prejel **152 uradnih obvestil o kršitvi varnosti osebnih podatkov**: 79 obvestil so poslali zavezanci iz zasebnega sektorja (npr. banke, trgovska podjetja, zavarovalnice), 73 pa zavezanci iz javnega sektorja (predvsem zdravstvene in izobraževalne ustanove, pa tudi ministrstva in centri za socialno delo).

Kršitve varnosti osebnih podatkov (152) so se nanašale na posredovanje dokumentov z osebnimi podatki (npr. zdravniških izvidov, računov, dokumentov v upravnih postopkih, debetnih kartic) napačnim osebam kot posledica nenamerne človeške napake ali netočnih podatkov v zbirkah osebnih podatkov (npr. e-naslovov strank), na neustrezno zagotavljanje varnosti osebnih podatkov, hekerske vdore oziroma kibernetiski napad, na nezakonito razkritje osebnih podatkov nepooblaščenim osebam, nepooblaščen dostop do osebnih podatkov oziroma njihova obdelava s strani zaposlenih, nezakonite objave osebnih podatkov, nezakonito uporabo osebnih podatkov za druge namene, izgubo ali krajo prenosnega računalnika ali drugih nosilcev osebnih podatkov (USB-klju-

³ 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 obvestiti o 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). V praksi to 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.

Kršitve varnosti osebnih podatkov v letu 2025.



ček, zdravstveni karton, zvezek z osebnimi podatki strank), na razkritje osebnih podatkov zaradi napake v aplikaciji oziroma tehnične napake oziroma 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).

Informacijski pooblaščenec je v letu 2025 prejel **eno obvestilo o kršitvi varnosti osebnih podatkov po 52. členu ZVOPOKD**.

3.2.5 PRITOŽBENI POSTOPKI PO 77. ČLENU SPLOŠNE UREDBE IN PO 33. ČLENU ZVOPOKD

Posamezniki lahko v primeru suma kršitev obdelav osebnih podatkov, ki se nanašajo nanje, ali v primeru kršitev v zvezi z uveljavljanjem njihovih pravic podajo prijavo po 30. členu ZVOP-2 kot prijavitelji s posebnim položajem, s čimer se zagotavlja pravica do pritožbe po 77. členu Splošne uredbe (pritožba zaradi kršitve varstva osebnih podatkov). Informacijski pooblaščenec vodi nadzorne postopke na zahtevo prijavitelja s posebnim položajem tudi v primeru, ko gre za obdelave na področju obravnavanja kaznivih dejanj, in sicer na podlagi 33. člena ZVOPOKD.

Pri tovrstnih prijavih gre za nadzorni postopek posebne vrste, v katerem ima tudi prijavitelj položaj stranke, zaradi česar mora njegova prijava (poleg sestavin, ki jih zahteva ZVOP-2) vsebovati tudi vse sestavine, ki jih za vlogo določa Zakon o splošnem upravnem postopku (ZUP). V tem postopku lahko Informacijski pooblaščenec uporabi vsa nadzorna

pooblastila (npr. vsa preiskovalna in popravljalna pooblastila iz 58. člena Splošne uredbe) in izreka vse nadzorne ukrepe, ki mu jih omogočajo predpisi (ZVOP-2, Splošna uredba, ZVOPOKD, ZUP in področni zakoni), vsaka stranka pa krije svoje stroške postopka. V primeru ugotovljenih kršitev lahko Informacijski pooblaščenec izreka sankcije v skladu s Splošno uredbo in ukrepa v skladu s svojimi prekrškovnimi pooblastili.

Pri obravnavi prijav prijaviteljev s posebnim položajem in pritožb zoper odločitve v zvezi z uveljavljanjem pravic so prijave oziroma vloge pogosto nepopolne. 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, saj se skladno s 30. in 34. členom ZVOP-2 oziroma 33. do 38. členom ZVOPOKD v tem postopku obravnava le kršitve obdelave osebnih podatkov prijavitelja s posebnim položajem, ki v trenutku vložitve prijave še obstajajo. Nadzorni postopek Informacijski pooblaščenec praviloma uvede le v primeru, ko iz prijave izhaja, da je treba upravljavcu naložiti sprejem ukrepov (npr. odrediti izbris podatkov ali posredovanje podatkov posamezniku, sprejem organizacijskih in tehničnih ukrepov za zagotavljanje varnosti osebnih podatkov), s katerimi se bo odpravila kršitev ali se bodo preprečevale podobne možne kršitve v prihodnosti. Ugotavljanje preteklih kršitev varstva osebnih podatkov lahko posameznik skladno z določbami 11. člena ZVOP-2 oz. 12. člena ZVOPOKD s tožbo zahteva od sodišča.

Posamezniki so v letu 2025 skupno vložili 302 prijavi (v 111 primerih zoper upravljavce javnega sektorja in v 191 primerih zoper upravljavce zasebnega sektorja), s katerimi so zahtevali ugotovitev, da se njihovi osebni podatki obdelujejo nezakonito oz. v nasprotju s Splošno uredbo oz. ZVOP-2. Po ZVOPOKD je Informacijski pooblaščenec v letu 2025 prejel eno tovrstno prijavo.

Prijave posameznikov, s katerimi so zahtevali ugotovitev, da se njihovi osebni podatki obdelujejo nezakonito.



V okviru teh postopkov je Informacijski pooblaščenec izdal skupno 15 odločb, s katerimi je v devetih primerih ugotovil kršitev Splošne uredbe oz. ZVOP-2, v šestih primerih pa je ugotovil, da kršitev ni. V 213 primerih je postopek s sklepom ustavil ali vlogo zavrgel zaradi postopkovnih pomanjkljivosti.

V primeru prijav in pritožb v zvezi z uveljavljanjem pravic prejme Informacijski pooblaščenec največ vlog, ki se nanašajo na pravico posameznika do seznanitve z lastnimi osebnimi podatki ter pravico do izbrisa (t. i. pravica do pozabe). Pravica do seznanitve z lastnimi osebnimi podatki je zagotovljena vsakemu posamezniku v tretjem odstavku 38. člena Ustave RS, v 15. členu Splošne uredbe ter v 24. členu ZVOPOKD. Postopkovna pravila so urejena v 11. in 12. členu Splošne uredbe, v 12. do 21. členu ZVOP-2 ter v 18. do 22. in v 25. členu ZVOPOKD.

Informacijski pooblaščenec je v letu 2025 prejel 162 prijav posameznikov v zvezi s kršitvami njihovih pravic. Med njimi so bile 104 prijave zaradi kršitve pravice do seznanitve z lastnimi osebnimi podatki, 14 prijav zaradi kršitve pravice do popravka, 42 prijav zaradi kršitve pravice do izbrisa ter po ena prijava zaradi kršitve pravice do omejitve in pravice do ugovora obdelavi po Splošni uredbi. Posamezniki se vedno bolj zavedajo zlasti 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.

Prijave posameznikov v zvezi s kršitvami njihovih pravic v letu 2025.



Vložene prijave so v 75 primerih zadevale upravljavce iz javnega sektorja (zlasti ministrstva in organe v njihovi sestavi, šole in javne zdravstvene zavode), 87 prijav pa se je nanašalo na upravljavce iz zasebnega sektorja (npr. banke, zavarovalnice, operaterje elektronskih komunikacij, trgovska podjetja in druge gospodarske družbe).

Leta 2025 je Informacijski pooblaščenec, vključno s postopki, začeti pred letom 2025, izdal 41 upravnih odločb v zvezi s pravicami po Splošni uredbi. V 24 odločbah je ugotovil, da je v trenutku vložitve prijave obstajala kršitev Splošne uredbe oz. ZVOP-2, s 17 odločbami pa je ugotovil, da kršitev ni bilo. Informacijski pooblaščenec je s sklepom zaključil 60 postopkov v zvezi z uveljavljanjem pravic po Splošni uredbi bodisi zaradi postopkovnih pomanjkljivosti bodisi zaradi umika prijave po tem, ko je upravljavec izpolnil svoje obveznosti.



Na področju obravnavanja kaznivih dejanj ter izvrševanja kazenskih sankcij je v letu 2025 Informacijski pooblaščenec prejel 17 pritožb posameznikov v zvezi s kršitvami pravice do seznanitve z lastnimi osebnimi podatki po ZVOPOKD in dve pritožbi glede kršitve drugih pravic. V zvezi s pritožbami po ZVOPOKD je Informacijski pooblaščenec izdal pet odločb, in sicer eno ugodilno in tri zavrnilne.

3.2.6 OSTALI PRITOŽBENI POSTOPKI

Informacijski pooblaščenec na pritožbeni stopnji odloča tudi o posebnih pravicah glede seznanitve z zdravstveno dokumentacijo po Zakonu o pacientovih pravicah (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 v letu 2025 nanašalo 38 pritožb (od tega 28 na pravico do seznanitve z lastno zdravstveno dokumentacijo in 10 na pravico do seznanitve z zdravstveno dokumentacijo po pacientovi smrti).

Glede pritožb, ki jih je Informacijski pooblaščenec vodil po ZPacP, je bilo izdanih 15 odločb, od tega je bilo izdanih 10 odločb glede pravice do seznanitve z lastno zdravstveno dokumentacijo po 41. členu ZPacP ter pet odločb glede seznanitve z zdravstveno dokumentacijo po pacientovi smrti. Osem vlog je bilo zaključenih s sklepom bodisi zaradi nepopolne vloge bodisi zato, ker je izvajalec zdravstvene dejavnosti zahtevo v celoti izpolnil.

Informacijski pooblaščenec 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 2025 je Informacijski pooblaščenec prejel osem tovrstnih pritožb. Glede vseh zahtev za posredovanje osebnih podatkov tako iz uradnih evidenc ali javnih knjig kot iz drugih zbirk ima posameznik na voljo sodno varstvo.

3.2.7 SODELOVANJE PRI ČEZMEJNIH NADZORIH

Kadar je obdelava osebnih podatkov čezmejna, torej če zadeva več držav članic EU in Evropske gospodarske skupnosti (EGS) (Islandija, Norveška in Lihtenštajn), Splošna uredba zapoveduje sodelovanje med nadzornimi organi teh držav članic. Sodelovanje se uresničuje prek naslednjih mehanizmov:

- 1. 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),
- 2. medsebojna pomoč** med organi za varstvo osebnih podatkov v državah članicah EU in EGS (61. člen Splošne uredbe),
- 3. skupno ukrepanje** organov za varstvo osebnih podatkov v državah članicah EU in EGS (62. člen Splošne uredbe).

1. Postopki po načelu »vse na enem mestu«

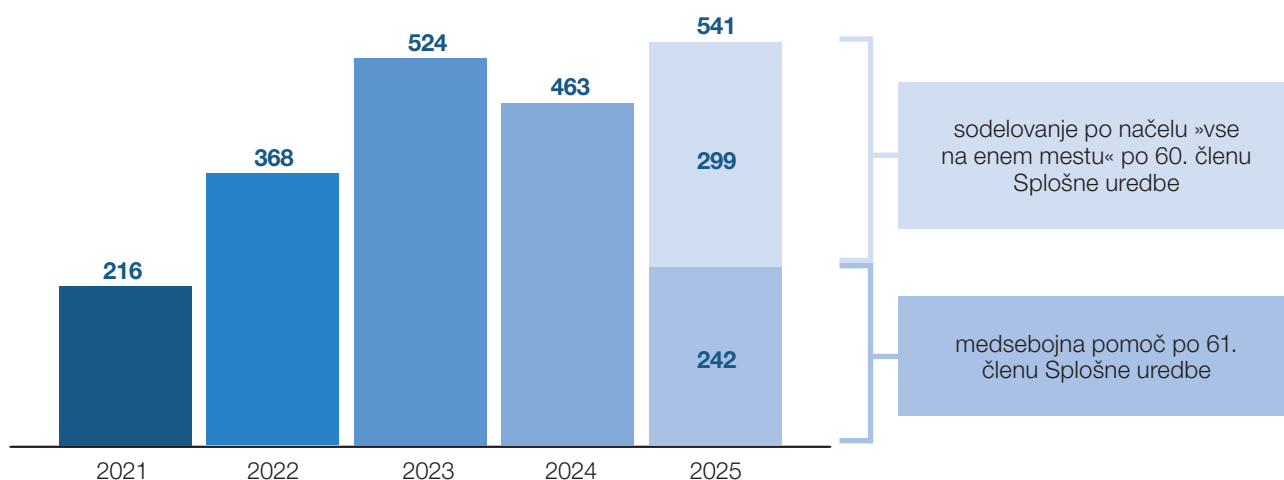
Nadzorni organi glede na kraj ustanovitve upravljavca določijo, kdo med njimi bo vodilni nadzorni organ; zelo pogosto je to irski nadzorni organ, pa tudi nadzorni organi Luksemburga, Francije, Nizozemske, Nemčije, Francije in Avstrije, saj imajo v teh državah pogosto glavno ustanovitev upravljavci, ki poslujejo čezmejno. Drugi organi pa v čezmejnem postopku sodelujejo 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. Najpogosteje obdelava pomembno vpliva na posameznike v več državah v primerih priljubljenih ponudnikov komunikacijskih spletnih storitev in družabnih omrežij, spletnih storitev (aplikacij za zmenke, spletnih iger, ponudnikov pretočnih storitev), ponudnikov somobilnosti in v primerih letalskih prevoznikov.

Vodilni organ v postopku nadzora vodi nadzor nad upravljavcem, usmerja sodelovanje z drugimi organi ter pripravi osnutek odločbe, zadevni organi pa lahko izrazijo svoje zadržke ali strinjanje. V primeru nestrinjanja, ki se izrazi kot formalni ugovor, med vodilnim in zadevnimi organi o sporu odloči Evropski odbor za varstvo osebnih podatkov (EDPB).

Čezmejni primeri po načelu »vse na enem mestu« so zadevali različne najpogostejše kršitve, od kršitev glede ustreznega zavarovanja podatkov (med prizadetimi so bili tudi uporabniki iz Slovenije), kršitev glede izvajanja pravic posameznikov, dostopa do podatkov in izbrisa podatkov, pretiranih zahtev po podatkih za identifikacijo strank, posredovanja podatkov tretjim osebam, obdelave osebnih podatkov brez ustrezne pravne podlage do neustreznega informiranja o obdelavi osebnih podatkov itd.

V letu 2025 je bil Informacijski pooblaščenec udeležen v 541 postopkih sodelovanja v zvezi z upravljavci, ki izvajajo čezmejno obdelavo osebnih podatkov, in sicer v 242 postopkih po 60. členu Splošne uredbe in v 299 postopkih po 61. členu Splošne uredbe. V postopkih po 60. členu je Informacijski pooblaščenec podrobneje spremljal 29 čezmejnih primerov nadzora ter proučil in po potrebi sporočil svoje nestrinjanje z osnutkom odločitve vodilnega nadzornega organa. V enem primeru je bil v vlogi domnevnega vodilnega organa.

Sodelovanje Informacijskega pooblaščenca v čezmejnih postopkih nadzora v letu 2025.



Informacijski pooblaščenec je prejel tudi 25 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 nadzornim organom. V takem primeru je Informacijski pooblaščenec zadolžen za celotno komunikacijo s prijaviteljem, vodilni nadzorni organ glede na ustanovitev upravljavca pa je pristojen za izvedbo nadzora in sprejem ukrepov zoper takšnega upravljavca.

V letu 2025 je bil Informacijski pooblaščenec v enem primeru čezmejnega sodelovanja označen kot domnevni vodilni nadzorni organ, ki naj bi vodil postopek nadzora zoper upravljavca, ki ima glavno ali edino ustanovitev v Sloveniji, vendar se je po preverjanju dejstev in okoliščin ugotovilo, da Informacijski pooblaščenec v tem primeru ni dejanski vodilni nadzorni organ.

V letu 2025 je bilo v čezmejnih postopkih, v katerih je sodeloval Informacijski pooblaščenec, izdanih 235 osnutkov odločitev po 60. členu Splošne uredbe. 236 postopkov je bilo končanih s končno odločitvijo po 60. členu Splošne uredbe. V primerjavi z letom 2024 je porast števila izdanih odločitev 71-odstoten. Na spletni strani Evropskega odbora za varstvo podatkov je dostopen javni register končnih odločitev v postopkih čezmejnega sodelovanja po 60. členu.⁴

2. Medsebojna pomoč

Informacijski pooblaščenec je leta 2025 sodeloval tudi v 298 postopkih zagotavljanja medsebojne pomoči med nadzornimi organi po 61. členu Splošne uredbe. Prejel je 270 zahtev drugih organov, podal pa je 28 zahtev, s katerimi je izmenjal informacije in prošnje za ukrepanje v konkretnih čezmejnih postopkih.

Splošna uredba predvideva tudi neformalno sodelovanje med nadzornimi organi z namenom zagotavljanja skladnosti in skupnega razumevanja Splošne uredbe. V tem smislu je Informacijski pooblaščenec odgovoril na 45 zaprosil za mnenja ter drugim organom podal dve takšni zaprosili. Zaposila za tolmačenje so se nanašala na obdelavo osebnih podatkov v kontekstu bank in zavarovalnic, na uporabo umetne inteligence za preverjanje starosti, na varstvo otrok in objavljanje njihovih podatkov s strani staršev vplivnežev, na namestitve kamer, na delovna razmerja idr.

3.2.8 PREKRŠKOVNI POSTOPKI

Informacijski pooblaščenec je zaradi suma kršitev določb o varstvu osebnih podatkov v letu 2025 uvedel 146 novih postopkov o prekršku, od tega 63 zoper pravne osebe javnega sektorja in njihove odgovorne osebe, 61 zoper pravne osebe zasebnega sektorja in njihove odgovorne osebe, 22 pa zoper odgovorne osebe državnih organov in samoupravnih lokalnih skupnosti in posameznike.

Kršitve varstva osebnih podatkov v letu 2025.



⁴ https://edpb.europa.eu/our-work-tools/consistency-findings/register-for-article-60-final-decisions_en

Informacijski pooblaščenec je v prekrškovnih postopkih v letu 2025 izrekel:

- 89 glob,
- 45 opominov,
- izdal je dva plačilna naloga in
- 42 opozoril.

Štiri postopke o prekršku je Informacijski pooblaščenec ustavil.

Na podlagi napovedi zahtev za sodno varstvo zoper odločbe, s katerimi je Informacijski pooblaščenec izrekel globe oz. opomine, so bile izdane štiri odločbe z obrazložitvijo; po njihovem prejemu so vsi kršitelji vložili zahtevo za sodno varstvo. Relativno majhen delež vloženih zahtev za sodno varstvo, to je zgolj za 5,5 % izdanih odločb o prekršku, kaže na to, da storilci storjene prekrške priznavajo in se zavedajo svoje odgovornosti.

Informacijski pooblaščenec je v letu 2025 kršiteljem izrekel globe v skupni višini 294.390 EUR.

Pristojnost za izrekanje glob zaradi ugotovljenih kršitev določb Splošne uredbe je Informacijski pooblaščenec dobil z uveljavitvijo ZVOP-2, prve tovrstne globe pa je izrekel v letu 2025, in sicer je bilo teh glob 14, njihova skupna višina pa je znašala 177.020 EUR.

Zaradi kršitev določb ZVOP-2 je bilo izrečenih 59 glob v skupni višini 110.220 EUR, zaradi kršitve določb ZEKom-2 pa šest glob v skupni višini 6.650 EUR.

Leta 2025 je Informacijski pooblaščenec prejel sedem sodb, s katerimi so okrajna sodišča odločila o zahtevah za sodno varstvo, ki so jih storilci vložili zoper odločbe o prekrških, izdane v letih 2022, 2023 in 2024:

- zahtevi za sodno varstvo je bilo v celoti ugodeno; odločba se je v celoti spremenila tako, da se je postopek ustavil – 3 (v enem od teh postopkov je zadeva pred sodiščem zastarala),
- zahtevi za sodno varstvo je bilo delno ugodeno – 2,
- zahteva za sodno varstvo je bila zavrnjena kot ne-utemeljena – 2.

Informacijski pooblaščenec je v letu 2025 skupno zaključil 1727 nadzornih zadev (med njimi tudi zadeve, pričete v predhodnih letih). Zaključenih je bilo 1162 zadev v okviru inšpekcijskega nadzora, 329 postopkov, ki so bili pričeti na podlagi prijav prijaviteljev s posebnim položajem, ter 236 čezmejnih postopkov. Poleg tega je bilo zaključenih 118 prekrškovnih zadev ter 47 ostalih pritožbenih postopkov.

Zaključene zadeve v letu 2025.

Zadeve, obravnavane v okviru inšpekcijskega nadzora: **1162**



Postopki na podlagi prijav prijaviteljev s posebnim položajem: **329**



Čezmejni postopki: **236**



Zaključene prekrškovne zadeve **118**

Zaključeni ostali pritožbeni postopki **47**

3.2.9 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.

Paketni izvozi osebnih podatkov iz centralnega registra prebivalstva brez jasne zakonske podlage.

V inšpekcijskem postopku je bilo ugotovljeno, da je upravljavec centralnega registra prebivalstva (CRP) občinam omogočal *on-line* dostop do podatkov ter avtomatizirano paketno izvažanje osebnih podatkov preko aplikacije eObčine, pri čemer so se izvozi izvajali brez posamične zahteve in brez presoje, ali občina podatke v konkretnem primeru potrebuje za izvajanje posamezne naloge iz 21. člena ZLS. Upravljavec zaradi takšnega načina dostopa ni imel nadzora nad nadaljnjo obdelavo podatkov, saj so občine podatke po izvozu vključevale v lastne informacijske sisteme in ustvarjale nove zbirke osebnih podatkov, za kar pravna podlaga ne obstaja. Ugotovljeno je bilo tudi, da so se nadalje podatki uporabljali za namene, ki niso določeni v zakonodaji.

Informacijski pooblaščenec je ugotovil, da takšen način posredovanja podatkov nima jasne zakonske podlage in ni skladen z 38. členom Ustave RS ter načeli zakonitosti, omejitve namena in odgovornosti po 5. členu Splošne uredbe. Informacijski pooblaščenec je zato upravljavcu CRP odredil uskladitev dostopov ter dolžnosti preverjanja vsakokratnega zakonitega namena in onemogočanje posredovanja podatkov, ki ni v skladu z veljavno zakonodajo.

Zunanji izvajalec šolske prehrane nima pravne podlage za vpogled v finančno stanje posameznika ali njegovo zgodovino obrokov.

Inšpekcijski nadzor pri zavezancu s področja izobraževanja je razkril kršitev načela najmanjšega obsega podatkov pri zagotavljanju šolske prehrane. Zavezanec je zunanjemu izvajalcu prek informacijskega sistema omogočil dostop do preširokega nabora podatkov dijakov (subvencije, stanje dobroimetja, zgodovina obrokov), čeprav bi za namen razdeljevanja hrane po 17. členu ZŠolPre-1 zadostovala le ime in priimek. Ker zavezanec že ob zasnovi sodelovanja ni zagotovil stroge omejitve dostopa le do tistih podatkov (ime in priimek), ki so nujni za namen obdelave, so bile izvajalcu omogočene zlorabe in spreminjanje podatkov. Poleg tega so bile dostopne pravice dodeljene s privzetim profilom, ki je bil nastavljen preši-

roko, ne da bi ga zavezanec tehnično omejil na nujno potrebne podatke. Pravilno ravnanje bi zahtevalo dosledno implementacijo vgrajenega in privzetega varstva podatkov (25. člen Splošne uredbe), kar pomeni, da bi moral zavezanec že ob sklenitvi pogodbe s tehničnimi nastavitvami zagotoviti, da izvajalec vidi le podatke, nujno potrebne za opravljanje storitve.

Ker je zavezanec ob zaznavi zlorabe sodelovanje z izvajalcem takoj prekinil in uvedel nove, varnejše protokole, je Informacijski pooblaščenec postopek inšpekcijskega nadzora ustavil, zaradi ugotovljenih nepravilnosti pa je pravni in odgovorni osebi izrekel opomin.

Kršitelja sta na izrečeni prekrškovni ukrep vložila zahtevo za sodno varstvo, sodišče pa je zahtevo zavrnilo in potrdilo odločitev Informacijskega pooblaščenca. Sodišče je poudarilo, da bi pravilna uporaba načela vgrajenega in privzetega varstva osebnih podatkov takšne zlorabe in goljufije preprečila ter da morajo upravljavci aktivno poskrbeti za izklop nepotrebnih funkcionalnosti v sistemih, ne glede na to, ali jih informacijska rešitev privzeto ponuja ali ne.

Nezadostni tehnični ukrepi in zanašanje na "skrite" URL-je omogočili nepooblaščen dostop do osebnih podatkov udeležencev dobrodelnega teka.

Varnost osebnih podatkov mora biti zagotovljena z ustreznimi tehničnimi in organizacijskimi ukrepi, ki preprečujejo nepooblaščen dostop do podatkov, objavljenih v spletnih okoljih. Inšpekcijski nadzor je pokazal, da upravljavec spletne strani za prijave na športno prireditev tega ni zagotovil, saj so bila potrdila o prijavi z osebnimi podatki udeležencev shranjena na javno dostopnem strežniku brez kakršne koli avtentikacije. Do podatkov je bilo mogoče dostopati prek URL povezav, ki niso bile generirane z zadostno stopnjo naključnosti, kar je omogočalo enostavno ugibanje zaporednih kod in s tem vpogled v potrdila drugih udeležencev.

Informacijski pooblaščenec je ugotovil, da takšna zasnova sistema pomeni kršitev obveznosti iz 32. člena Splošne uredbe, ki upravljavcem nalaga, da morajo zagotoviti varnost obdelave osebnih podatkov, zlasti pri spletnih storitvah, kjer je tveganje za razkritje podatkov povečano. Upravljavec bi moral že ob zasnovi rešitve zagotoviti ustrezno zaščito dostopa, na primer z avtentikacijo ali z uporabo enkratnih, nepredvidljivih povezav, ki jih ni mogoče uganiti. Ker teh ukrepov ni zagotovil, je prišlo do nepooblaščenega razkritja osebnih podatkov več udeležencev.

Ugotovljeno kršitev varnosti podatkov je Informacijski pooblaščenec obravnaval tudi v okviru prekrškovnega postopka in odgovorni osebi izrekel globo v višini 400 EUR, pravni osebi pa globo v višini 16.250 EUR.

Visoka globa zaradi prikritega izvajanja nadzora zaposlenih.

Inšpekcijski nadzor, ki ga je Informacijski pooblaščenec uvedel na podlagi prijave in izvedel z nenapovedanim prihodom v podjetje s področja kovinsko-predelovalne industrije, je razkril izvajanje prikritega nadzora nad zaposlenimi s pomočjo programske opreme Spyrix Employee Monitoring. Informacijski pooblaščenec je v inšpekcijskem nadzoru temeljito pregledal delovne postaje zaposlenih in pri tem ugotovil, da je zavezanec z namenom varovanja poslovne skrivnosti na računalnike nekaterih zaposlenih namestil vohunsko programsko opremo, ki je več kot leto dni snemala in shranjevala vse aktivnosti, ki so jih zaposleni izvajali na službenih računalnikih. Snemanje in shranjevanje aktivnosti je potekalo na način, da je vohunska programska oprema večkrat na minuto zabeležila posnetek zaslona računalnika ter zvočni posnetek morebitnega pogovora zaposlenega s sodelavci ali drugimi osebami. Zavezanec je s tem pridobil popoln vpogled v izvajanje delovnih aktivnosti zaposlenih in njihovo zasebno življenje, vključno z vsebino komunikacije zaposlenih preko zasebne elektronske pošte in popolnoma zasebnih pogovorov. Informacijski pooblaščenec je v postopku ugotovil, da zavezanec za tovrstno obdelavo ni izpolnjeval nobenega pogoja za zakonito obdelavo osebnih podatkov iz prvega odstavka 6. člena Splošne uredbe, s čimer je kršil temeljno načelo obdelave osebnih podatkov, tj. načelo zakonitosti.

Zaradi ugotovljene kršitve je Informacijski pooblaščenec v skladu s kriteriji iz Splošne uredbe pravni osebi izrekel globo v višini 71.474 EUR, odgovorni osebi pravne osebe pa globo v višini 4.000 EUR.

Snemanje računalniških zaslonov, vseh notranjih prostorov in omogočanje neposrednega spremljanja posnetkov vodstvu z namenom izvajanja nadzora nad delom zaposlenih je nezakonito.

Inšpekcijski nadzor pri zavezancu s področja stavbnega pohištva je razkril nezakonito izvajanje videonadzora v delovnih prostorih. Informacijski pooblaščenec je ugotovil, da je zavezanec z desetimi kamerami snemal prodajni salon, pisarne in proizvodne prostore, pri čemer je bila ena od kamer usmerjena neposredno v zaslon računalnika zaposlene.

Poleg tega je bil vodstvu omogočen neposreden vpogled v živo slike vseh kamer.

Zavezanec v inšpekcijskem postopku ni izkazal nujnosti za snemanje notranjih prostorov v takšnem obsegu niti ni preveril možnosti milejših ukrepov, kot so na primer pisna navodila zaposlenim ali neposreden nadzor s strani vodij. Pri takem videonadzoru, ki je usmerjen neposredno v delovna mesta, gre za kršitev 78. člena ZVOP-2, saj njegov namen ni varovanje ljudi in premoženja, temveč nadzor nad delom zaposlenih.

Zaradi ugotovljenih kršitev 78. člena ZVOP-2 je bilo zavezancu odrejeno, da videonadzor omeji le na območja, kjer je to nujno (npr. sef), ker varnosti ljudi oz. premoženja na teh območjih ne more zagotavljati z drugimi milejšimi sredstvi, kot so na primer pisna navodila zaposlenim in neposreden nadzor vodje. Zaradi ugotovljenih kršitev je bila pravni osebi izrečena globo v višini 12.000 EUR, odgovorni osebi pa globo v višini 2.000 EUR.

Vnaprej označena okenca (angl. pre-ticked boxes) za podajo privolitve niso zakonita.

Inšpekcijski nadzor nad spletno stranjo ponudnika informacijskih storitev je razkril systemske pomanjkljivosti pri zagotavljanju preglednosti obdelave osebnih podatkov. Upravljavec posameznikom ob zbiranju podatkov prek spletnih obrazcev ni zagotovil informacij po 13. členu Splošne uredbe, poleg tega so bila polja za strinjanje s pogoji uporabe in prejemanjem obvestil vnaprej označena. Takšna praksa je v nasprotju z načelom preglednosti in prostovoljnosti privolitve po Splošni uredbi. Informacije o obdelavi podatkov (npr. namen, pravna podlaga, identiteta upravljavca) morajo biti namreč dostopne neposredno ob obrazcih, ki zahtevajo vnos podatkov, polja za privolitve pa morajo biti privzeto prazna. Privolitev mora biti podana z aktivnim dejanjem posameznika, sicer ne velja za prostovoljno in izrecno.

Zavezanec je med postopkom posodobil politiko zasebnosti in nepravilnosti odpravil, zaradi ugotovljenih kršitev pa je bila pravni osebi izrečena globo v višini 4.800 EUR, odgovorni osebi pa globo v višini 300 EUR.

Nezakonito sledenje preko spletnih piškotkov.

Inšpekcijski nadzor nad spletno stranjo trgovskega podjetja je razkril systemske pomanjkljivosti pri upravljanju spletnih piškotkov, ki niso bili skladni

z 225. členom ZEKom-2 ter določili Splošne uredbe. V postopku je bilo ugotovljeno, da upravljavec spletne strani uporabnikom ni omogočil takojšnje zavrnitve sledenja, saj je bila ta možnost dostopna šele v drugem koraku nastavitvev, kar po zakonodaji izniči prostovoljnost privolitve. Posebej kritična je bila ugotovitev, da so določeni analitični in oglaševalski piškotki tretjih oseb na napravah uporabnikov ostali aktivni tudi po tem, ko so ti sledenje izrecno zavrnili ali preklicali. Poleg tega upravljavec za večje število piškotkov ni zagotovil obveznih informacij o namenu obdelave in času hrambe podatkov.

Ugotovljene kršitve je Informacijski pooblaščenec obravnaval tudi v okviru svojih prekrškovnih pristojnosti in pravni osebi izrekel globo v višini 2.500 EUR, odgovorni osebi pravne osebe pa globo v višini 500 EUR.

Tehnični dostop do osebnih podatkov ne pomeni avtomatične pravice do vpogleda.

Informacijski pooblaščenec je bil z obvestilom, ki mu ga je zdravstvena ustanova poslala skladno s 46. členom ZPacP, obveščen, da je izvedeni izredni notranji nadzor razkril večkratne neupravičene vpogleda v zdravstveno dokumentacijo pacienta s strani zaposlene zdravstvene delavke. Zaposlena je v treh ločenih dneh opravila več deset dostopov do pacientove kartoteke, čeprav pacienta ni obravnavala in za vpogleda ni imela nobene strokovne potrebe. Dostop je bil opravljen z njenim osebnim geslom in prek službenega računalnika, kar pomeni zavestno obdelavo podatkov brez pravne podlage.

Zdravstveni podatki sodijo med posebej varovane osebne podatke, zato je dopusten le tisti dostop, ki je nujen za konkretno zdravstveno obravnavo. Dostop je dovoljen le, če je nujen za izvajanje konkretnih delovnih nalog, določenih s pogodbo o zaposlitvi ali drugim aktom. Vsak vpogled, ki presega te okvire, na primer iz osebnega interesa ali radovednosti, je nezakonit in predstavlja kršitev zakonodaje o varstvu osebnih podatkov, poleg tega pa tudi zlorabo zaupanja v zdravstveni sistem.

Informacijski pooblaščenec je v prekrškovnem postopku ugotovil kršitev načela zakonitosti, načela omejitve namena in načela najmanjšega obsega podatkov po Splošni uredbi ter zato odgovorni osebi zaradi treh istovrstnih prekrškov v steku izrekel globo v višini 950 EUR.

Nezakonit videonadzor notranjosti najemniškega stanovanja.

Najemodajalec je več kot leto in pol izvajal videonadzor na notranjem hodniku najemniškega stanovanja. Kamera je bila nameščena na način, da je bil ob odprtih vratih omogočen vpogled tudi v druge bivalne prostore. Najemodajalec se je kot upravljavec pri tem skliceval na privolitve najemnikov, ki naj bi bile podane s sklenitvijo najemne pogodbe, preko katere so bili najemniki seznanjeni s Hišnim redom, ki je določal tudi, da se zaradi zagotavljanja varnosti v stanovanju izvaja snemanje skupnih prostorov.

Informacijski pooblaščenec je v postopku ugotovil, da obdelava osebnih podatkov stanovalcev, do katere pride na podlagi videonadzora v stanovanju, ki se oddaja, v nobenem primeru ne more biti zakonita. Upravljavec namreč take obdelave podatkov ne more utemeljevati na svojem zakonitem interesu (točka f prvega odstavka 6. člena Splošne uredbe), saj njegov ekonomski interes ne more prevladati nad temeljnimi človekovimi pravicami in svoboščinami posameznikov ter pravico do varstva njihove zasebnosti in nedotakljivosti stanovanja. Iz narave najemnega razmerja tudi izhaja, da najemnik kot šibkejša stranka tega razmerja prostovoljne privolitve (točka a prvega odstavka 6. člena Splošne uredbe) v obdelavo svojih podatkov ne more dati.

Upravljavec je v postopku navajal tudi, da s takšnim videonadzorom preprečuje tatvine, poškodbe lastnine, nedovoljene vstope v objekt in krajo koles v skupnih prostorih. Te argumente je Informacijski pooblaščenec zavrnil kot nesorazmeren ukrep, saj se isti cilj (varovanje ljudi in premoženja v stanovanju) lahko doseže z mnogo manj invazivnimi ukrepi v pričakovano zasebnost, kot je videonadzor skupnega hodnika v stanovanju, na primer z zaklepanjem stanovanja, alarmom, shranjevanjem koles v zaklenjeni kolesarnici ipd.

Zaradi nezakonitega, zavestnega in dolgotrajnega videonadzora je Informacijski pooblaščenec najemodajalcu izrekel globo v višini 16.000 EUR, pri čemer sta bila v postopku določitve višine globe kot olajševalni okoliščini upoštevana tako upravljavčevo sodelovanje v postopku kot tudi dejstvo, da je upravljavec kamere odstranil takoj po prejemu poziva Informacijskega pooblaščenca.

Izbris osebnih podatkov iz Schengenskega informacijskega sistema.

Schengenski informacijski sistem (SIS) državam članicam omogoča enotno izvajanje politike vstopov v schengenski prostor. Pravo EU določa pogoje za vpis in izbris ukrepa prepovedi vstopa za tujca, ki nima pravice prebivati na območju EU. Če je prepoved vstopa vpisana za osebo, ki ima veljavno dovoljenje za prebivanje v drugi državi članici, mora država razpisnica izvesti posvetovalni postopek z državo, ki je dovoljenje izdala. Če ta dovoljenje ohrani v veljavi, mora država razpisnica prepoved vstopa izbrisati iz SIS.

V zadevi, ki jo je obravnaval Informacijski pooblaščenec, je bila prepoved vstopa v Slovenijo določena kot stranska sankcija, če tujec po ustavitvi postopka za izdajo dovoljenja za delo ne bi zapustil območja EU in schengenskega prostora. Upravni akt pri tem ni upošteval, da je imel tujec v času njegove izvršljivosti veljavno dovoljenje za prebivanje v drugi državi članici EU. Na tej podlagi je slovenska policija v SIS vpisala prepoved vstopa. Zahtevo posameznika za izbris ukrepa je zavrnila z obrazložitvijo, da je prepoved določena z aktom drugega organa in da policija nastopa zgolj kot izvrševalka ukrepa.

V nadzornem postopku je Informacijski pooblaščenec ugotovil, da policija razpisa ni izbrisala, čeprav je že razpolagala z informacijo, da država izdajateljica dovoljenja za prebivanje tega ohranja v veljavi. S tem je kršila obveznosti iz 29. člena Uredbe (EU) 2018/1861 ter posamezniku nezakonito zavrnila pravico do izbrisa po 17. členu Splošne uredbe. Informacijski pooblaščenec je zato prijavi posameznika ugodil in odredil takojšen izbris ukrepa iz sistema SIS. Ob tem je poudaril, da sta vpis in izbris podatkov v SIS samostojni vsebinski odločitvi upravljavca, ki mora pri svojem ravnanju upoštevati primarnost prava EU in zagotoviti učinkovito varstvo pravic posameznikov.

Dostop starša do otrokove zdravstvene dokumentacije in meja koristi otroka.

Starš je pri izvajalcu zdravstvene dejavnosti vložil zahtevo za pridobitev kopije celotne zdravstvene dokumentacije mladoletnega otroka za večmesečno obdobje. Zdravstvena ustanova je zahtevo zavrnila, ker je ocenila, da so podane okoliščine iz 20. člena ZVOP-2, ki omogočajo omejitev dostopa zakonitemu zastopniku, kadar bi razkritje podatkov lahko škodovalo otrokovim koristim. Pri tem se je sklicevala na

informacije centra za socialno delo o omejitvah stikov med staršem in otrokom zaradi domnevnega kaznivega dejanja. Starš je zoper odločitev vložil pritožbo pri nadzornem organu.

V postopku je bilo ugotovljeno, da je zdravstvena ustanova odločitev sprejela brez konkretne presoje posameznih zapisov in brez tehtanja, ali bi razkritje posameznih podatkov dejansko lahko negativno vplivalo na otroka. Informacijski pooblaščenec je presodil, da omejeni stiki ali pretekli postopki sami po sebi ne pomenijo avtomatične podlage za zavrnitev dostopa. Izjema po 20. členu ZVOP-2 se lahko uporabi le, če obstajajo konkretne in objektivne okoliščine, ki kažejo na neposredno ali posredno škodo za otroka, pri čemer mora biti presoja opravljena za vsak dokument posebej.

Na podlagi pregleda dokumentacije je informacijski pooblaščenec ugotovil, da je večina zapisov predstavljala informacije o običajnih zdravstvenih obravnavah, ki niso bile v nikakršni zvezi z domnevno zlorabo ali nasiljem, zato ne morejo škodovati otrokovim interesom. V teh delih je pritožbi ugodil in odredil posredovanje dokumentacije. Informacijski pooblaščenec pa je pritožniku zavrnil dostop do dela zapisov, ki so vsebovali informacije, za katere je presodil, da bi seznanitev pritožnika z njimi lahko škodila otrokovim interesom, saj bi lahko negativno vplivala na otrokovo duševno stanje, ogrozila njegov občutek varnosti ali njegovo sodelovanje pri zdravstveni oskrbi.

Omejitve pravice do popravka zdravstvene dokumentacije.

Posameznik je pri upravljavcu vložil zahtevo za popravek zdravstvene dokumentacije, ker izdani izvid po opravljenem pregledu po njegovi presoji ni ustrezno odražal njegovega zdravstvenega stanja. Upravljavec je zahtevo zavrnil, saj je presodil, da pravica do popravka po 16. členu Splošne uredbe omogoča popravek netočnih ali dopolnitev nepopolnih osebnih podatkov, ne pa poseganja v strokovne ugotovitve zdravnika. Posameznik je zato pri nadzornem organu vložil prijavo zaradi domnevne kršitve te pravice.

V postopku je bilo ugotovljeno, da je posameznik želel, da se dodatne informacije o poškodbah vnesejo v diagnostični del izvida. Nadzorni organ je pojasnil, da je popravek mogoč le v delu izvida, ki predstavlja neposreden zapis pacientovih izjav (anamneza), če je ta zapis nepopoln ali napačen. Pravica do popravka pa se ne nanaša na subjektivne strokovne zapise zdravnika, če ti odražajo dejanske ugotovitve zdrav-

nika, kot so diagnoza, opis klinične slike, interpretacija izvidov, opis razvoja bolezni, mnenje ali predlagana terapija, saj strokovna pravilnost ugotovitev zdravnika ne more biti predmet presoje v okviru pravice do popravka 16. člena Splošne uredbe.

Posameznik je zahteval spremembo oziroma dopolnitev diagnoze, ne pa dopolnitve anamneze, zato pogoji za uveljavljanje pravice do popravka niso bili izpolnjeni. Informacijski pooblaščenec je posledično ugotovil, da upravljavec v trenutku vložitve prijave ni kršil 16. člena Splošne uredbe. Prijavo je zavrnil in potrdil pravilnost upravljavčeve odločitve. Posamezniku je bilo pojasnjeno, da lahko pri upravljavcu vloži novo zahtevo, če želi dopolnitev dela izvida, ki se nanaša na anamnezo, medtem ko strokovnih ugotovitev zdravnika v okviru pravice do popravka ni mogoče spreminjati.

Neizkazana identiteta vlagateljice pri zahtevi za dostop do videoposnetka.

Posameznik je od upravljavca parkirišča zahteval dostop do videoposnetka domnevnega škodnega dogodka in drugih osebnih podatkov. Upravljavec je zahtevo zavrnil, ker ni mogel z gotovostjo potrditi, da je oseba na posnetku ista kot vlagatelj zahteve. V postopku pred Informacijskim pooblaščenecem je bilo ugotovljeno, da je upravljavec posameznika na podlagi posnetka in poizvedb sprva prepoznal kot možnega udeleženca dogodka. Posameznik je udeležbo v dogodku izrecno zanikal in navedel, da tistega dne ni bil na kraju dogodka. Upravljavec je posamezniku dvakrat omogočil osebni vpogled v posnetek, kar bi omogočilo preverjanje istovetnosti (identitete), vendar je posameznik to možnost zavrnil. Prav tako ni predložil nobenega dokaza, da se zahtevani podatki nanašajo nanj.

Informacijski pooblaščenec je v svoji odločitvi poudaril, da mora upravljavec pred odobritvijo dostopa do osebnih podatkov zagotoviti, da se ti podatki dejansko nanašajo na vlagatelja zahteve, identiteta pa mora biti potrjena z gotovostjo. Kadar obstaja utemeljen dvom, lahko upravljavec zahteva dodatne informacije za potrditev identitete. Vlagatelj ni izkazal, da je oseba na posnetku, in ni sprejel ponujenih načinov identifikacije, zato upravljavec ni mogel zanesljivo ugotoviti, da gre za njegove osebne podatke. Informacijski pooblaščenec je zato ugotovil, da upravljavec z zavrnitvijo dostopa ni kršil pravice do dostopa po 15. členu Splošne uredbe, in je prijavo zavrnil.

Razkritje identitete zdravnika zaradi nezakonitega vpogleda v zdravstvene podatke.

Posameznik je od Zavoda za zdravstveno zavarovanje Slovenije zahteval podatke o tem, kdo je vpogledoval v njegove zdravstvene podatke. Upravljavec je posredoval podatke o izvajalcih zdravstvene dejavnosti, ne pa tudi podatkov o konkretnemu zdravniku, za katerega je prijavitelj zatrjeval sum nezakonitega vpogleda.

V nadzornem postopku je prijavitelj zahtevo omejil izključno na podatke o vpogledih tega zdravnika. Informacijski pooblaščenec je na podlagi sodne prakse Sodišča EU glede presoje obsega pravic posameznika v zvezi s seznanitvijo s podatki o notranjih uporabnikih podatkov pri upravljavcu (sodba v primeru št. C 579/21 Sodišča EU) presodil, da je posameznik izjemoma upravičen tudi do podatkov o notranjem uporabniku, saj je bila obdelava izvedena brez pravne podlage oz. izven delovnih nalog, zaradi česar tak uporabnik nastopa kot *de facto* zunanji uporabnik. Na podlagi izvedene notranje revizije izvajalca zdravstvene dejavnosti je bilo ugotovljeno, da je zdravnik na določen dan brez pravne podlage vpogledal v sistem zdravstvenega zavarovanja. Pri tem je šlo za nezakonito obdelavo, zato je prijavitelj upravičen do podatkov o tej obdelavi, vključno s podatkom o identiteti zdravnika, časom vpogleda in funkcijo sistema. V preostalem delu je Informacijski pooblaščenec ugotovil, da upravljavec ni kršil 15. člena Splošne uredbe.

Omejitev pravice do dostopa zaradi varstva žrtve v postopku obravnave nasilja v družini.

Posameznik je uveljavljal pravico do dostopa do osebnih podatkov, ki so nastali v postopku obravnave nasilja v družini. Organ je zahtevo zavrnil, ker bi razkritje podatkov poseglo v pravice druge osebe, ki je bila v postopku obravnavana kot žrtev. Posameznik je zato vložil pritožbo.

V postopku je bilo ugotovljeno, da dokument vsebuje osebne podatke obeh udeleženi, vendar se vsebinski del nanaša predvsem na osebne okoliščine žrtve. Informacijski pooblaščenec je poudaril, da mora upravljavec v takih primerih presojati, ali bi razkritje podatkov negativno vplivalo na pravice druge osebe. Ker gre za obravnavo nasilja v družini, je žrtev v neenakem položaju in je upravičeno pričakovala, da bodo podatki, razkriti pristojnemu organu, ostali zauzupni, kar določa tudi veljavna zakonodaja.

Informacijski pooblaščenec je ocenil, da bi razkritje dokumenta neprimerno bolj poseglo v pravice žrtve kot v pravice prosilca. Razkritje bi lahko ogrozilo njeno zasebnost ter porušilo zaupanje v postopke organa, ki temeljijo na varovanju integritete in dostojanstva oseb v stiski. Ker podatkov ni bilo mogoče izločiti ali anonimizirati na način, ki bi zaščitil žrtev, je presodil, da je omejitev dostopa utemeljena na četrtem odstavku 15. člena Splošne uredbe in predpisih, ki urejajo zaupnost v socialnovarstvenih postopkih. Na tej podlagi je Informacijski pooblaščenec ugotovil, da organ s tem, ko je zavrnil vpogled, ni kršil pravice do dostopa. Pritožba je bila zato zavrjena.

Omejitev pravice do seznanitve zaradi tajnih podatkov v pristojnosti obveščevalnovarnostne službe.

Posameznik je od obveščevalnovarnostne službe zahteval kopije vseh dokumentov, ki vsebujejo njegove osebne podatke. Upravljavec je del dokumentov posredoval, preostale pa zavrnil, ker so bili označeni s stopnjo tajnosti v skladu z Zakonom o tajnih podatkih (ZTP). Posameznik je zoper odločitev vložil prijavo pri nadzornem organu. V postopku je bilo ugotovljeno, da gre za podatke s področja obveščevalnovarnostnih dejavnosti, v zvezi s katerimi se Splošna uredba ne uporablja. V teh primerih se izvrševanje pravice do seznanitve z lastnimi osebnimi podatki, ki je tudi ustavno opredeljena pravica, presoja po ZVOP-2 in specialnih predpisih. Informacijski pooblaščenec je pri ogledu dokumentarnega gradiva ugotovil, da zahtevani dokumenti obstajajo, vendar so vsi označeni s stopnjo tajnosti »TAJNO« na podlagi veljavnih ocen možnih škodljivih posledic. Dokumenti so bili pravilno označeni in varovani v skladu z ZTP, Informacijski pooblaščenec pa ni zaznal okoliščin, ki bi vzbujale dvom o zakonitosti njihove opredelitve kot tajnih.

ZTP določa, da tajni podatki niso dostopni nepooblaščenim osebam in da je dostop mogoč le za osebe z ustreznim dovoljenjem in službeno potrebo. Posameznik teh pogojev ne izpolnjuje, zato do dokumentov, ki so hkrati njegovi osebni podatki, ni upravičen. Dodatno Zakon o Slovenski obveščevalnovarnostni agenciji (ZSOVA) omejuje vpogled v podatke, ki bi lahko onemogočili ali otežili izvajanje nalog agencije. Informacijski pooblaščenec je v postopku ugotovil tudi, da je upravljavec pravilno prekril osebna imena, ki so bila prav tako opredeljena kot tajni podatki. Na podlagi navedenega je Informacijski pooblaščenec prijavo zavrnil in ni ugotovil kršitev ZVOP-2.

Obdelava osebnih podatkov v okviru svobode izražanja – zahteva za izbris objav zavržena.

Posameznica je od upravljavca spletnega foruma zahtevala izbris svojih objav, ker naj bi vsebovale osebne podatke, kot so podatki o izobrazbi, prejšnjem delodajalcu in zdravljenju. Upravljavec je pojasnil, da je njen uporabniški račun anonimiziral, odstranil povezavo z elektronskim naslovom ter izbrisal tiste dele objav, ki bi lahko razkrili njeno identiteto. Preostale objave po preverjanju niso vsebovale osebnih podatkov.

V nadzornem postopku je bilo ugotovljeno, da je upravljavec izvedel anonimizacijo uporabniškega profila in izbrisal vse povezovalne podatke, ki bi omogočali identifikacijo posameznice. Forum predstavlja javno dostopen prostor za izmenjavo informacij, ki so povezane z dejavnostjo upravljavca, zato objave pomenijo del uresničevanja svobode izražanja tako uporabnikov kot upravljavca. Informacijski pooblaščenec je na tej podlagi presodil, da se obdelava osebnih podatkov v okviru javnih objav na forumu presoja po pravilih o svobodi izražanja. ZVOP-2 pa določa, da se o izbrisu osebnih podatkov, ki se obdelujejo v okviru svobode izražanja, odloča v sodnem postopku, ne v upravnem postopku pred nadzornim organom. Odločanje o zahtevi za izbris v tem primeru ni upravna zadeva, zato Informacijski pooblaščenec o njej ni pristojen odločati in je moral prijavo zavreči. Odločanje o izbrisu objav, ki so del uresničevanja svobode izražanja, namreč ne sodi v njegovo pristojnost.

Onemogočanje dostopa do uporabniškega računa na družbenem omrežju.

Prijavitelj je vložil prijavo zoper družbo Meta Platforms Ireland Ltd, saj naj bi mu bil neupravičeno in avtomatsko onemogočen dostop do uporabniškega računa na družbenem omrežju Facebook. Posameznik je zahteval, da je neznana oseba njegov račun na Facebooku neupravičeno povezala z uporabniškim računom na drugi spletni platformi. Zaradi domnevne kršitve pogojev uporabe na povezanem uporabniškem računu naj bi bil prijavitelju onemogočen tudi dostop do njegovega računa na Facebooku, ki ga je neuspešno skušal povrniti. Prijavitelj se je obrnil na Informacijskega pooblaščenca in ga prosil za posredovanje pri ponovni vzpostavitvi dostopa do računa.

Informacijski pooblaščenec se je odločil, da ne bo uvedel postopka nadzora, saj je pristojen zgolj za nadzor nad zakonitostjo obdelave osebnih podatkov posameznikov, iz prijave pa je izhajalo, da se ta primarno nanaša na onemogočen dostop do uporabniškega računa, ne na varstvo osebnih podatkov. Ker pa bi lahko šlo za morebitno kršitev Akta o digitalnih storitvah, je Informacijski pooblaščenec prijavo odstopil v reševanje Agenciji za komunikacijska omrežja in storitve Republike Slovenije. Pravice dostopa do osebnih podatkov iz 15. člena Splošne uredbe namreč ni mogoče enačiti z dostopom do uporabniškega računa, ki je bil onemogočen. Če je osrednje vprašanje dostop do uporabniškega računa, je za obravnavo prijav, ki se nanašajo na pravice in možnosti po Aktu o digitalnih storitvah, pristojna Agencija za komunikacijska omrežja in storitve Republike Slovenije, ne Informacijski pooblaščenec.

Nepooblaščen dostop do osebnih podatkov drugih uporabnikov v aplikaciji Easypark.

Informacijski pooblaščenec je sodeloval v čezmejnem postopku, ki ga je vodil švedski nadzorni organ za varstvo osebnih podatkov (v nadaljevanju: IMY) zoper upravljavca Easypark AB. IMY je prejel več pritožb uporabnikov iz različnih držav članic, ki so lahko v aplikaciji Easypark dostopali do osebnih podatkov drugih uporabnikov, kot so ime, naslov, e-pošta, številka registracije in lokacija parkirišča. Eden izmed uporabnikov je lahko dostopal celo do podatkov o plačilnih sredstvih drugega uporabnika in jih zlorabil za plačilo parkirnine.

IMY je pojasnil, da so bili računi uporabnikov vezani na njihove telefonske številke. Če uporabnik ni obvestil upravljavca Easypark AB o menjavi telefonske številke, je lahko do njegovega računa dostopal vsakokratni novi uporabnik zamenjane številke. V osnutku odločbe je tako ugotovil, da Easypark AB ni sprejel ustreznih tehničnih ukrepov, zaradi česar je kršil prvi odstavek 32. člena Splošne uredbe o varnosti podatkov. Ugotovil je še, da so podatki o lokaciji in času parkiranja lahko razkrili, kdaj se je posameznik nahajal npr. ob šoli ali v bolnišnici, vendar je zaradi majhnega števila pritožb ocenil, da to ni bistveno prispevalo k teži kršitve.

Informacijski pooblaščenec je v komentarjih izpostavil, da število pritožb nadzornega organa ne bi smelo odvrniti od presoje, ali je morda podana tudi kršitev načela celovitosti in zaupnosti iz točke f prvega odstavka 5. člena Splošne uredbe. Preveriti bi bilo treba, koliko uporabnikov je bilo prizadetih, ne le to, koliko jih je obvestilo nadzorni organ. Informacijski pooblaščenec je opozoril tudi na resnost kršitve v primeru, ko je uporabnik zlorabil tuja plačilna sredstva, saj problematika ni omejena le na varstvo osebnih podatkov.

IMY je po prejetih komentarjih obrazložitev nadgradil z izpostavljenimi vidiki kršitev in v končni odločitvi upravljavcu Easypark AB izrekel opomin zaradi kršitve prvega odstavka 32. člena Splošne uredbe.

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.

Oseba zasebnega sektorja, ki namerava obdelovati biometrične osebne podatke, mora Informacijskemu pooblaščenцу pred začetkom obdelave posredovati opis nameravanih obdelav in razloge za njihovo uvedbo⁵.

Informacijski pooblaščenec leta 2025 ni prejel nobene vloge za izdajo dovoljenja za uvedbo biometrijskih ukrepov v javnem sektorju, je pa prejel 12 vlog za izdajo dovoljenja za uvedbo biometrijskih ukrepov v zasebnem sektorju, od tega se jih je osem nanašalo na varstvo točnosti identitete strank vlagatelja. Uvedbo biometrijskih ukrepov zaradi varstva točnosti identitete strank vlagatelja je Informacijski pooblaščenec v šestih primerih odobril, v enem jo je zavrnil, v enem postopku pa je vlagatelj zahtevo umaknil, zato je bil postopek s sklepom ustavljen. Informacijski pooblaščenec je v dveh primerih zavrnil tudi uvedbo biometrijskih ukrepov, ki so jo želeli izvesti z namenom varstva premoženja, v enem primeru pa je zavrnil uvedbo biometrijskih ukrepov z namenom opravljanja dejavnosti in varovanja poslovnih skrivnosti.

Dejanja obdelave biometričnih osebnih podatkov v zasebnem sektorju morajo biti 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). Slovenska akreditacija je septembra 2025 vzpostavila shemo akreditiranja certifikacijskih organov za proizvode, procese, storitve po SIST EN ISO/IEC 17065 za certificiranje postopkov obdelave osebnih podatkov. Zahteve za akreditacijo vključujejo vzpostavitev sistema po SIST EN ISO/IEC 17065:2012 ter implementacijo relevantnih členov Splošne uredbe o varstvu podatkov in ZVOP-2 ter določil Dodatnih akreditacijskih zahtev Informacijskega pooblaščenca za telesa za certificiranje v skladu s točko b prvega odstavka 43. člena in tretjim odstavkom 43. člena Splošne uredbe o varstvu podatkov v povezavi z ISO/IEC 17065. Certifikacijski organi, ki želijo pridobiti akreditacijo na ome-

njenem področju, na Slovensko akreditacijo posredujejo prijavo za akreditacijo po tem, ko pripravijo posebno shemo certificiranja in le-to odobri Informacijski pooblaščenec. Do konca leta 2025 Slovenska akreditacija ni prejela še nobene take vloge.

3.3.2 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:

- 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);
- izvoznik podatkov zagotovi ustrezne zaščitne ukrepe na podlagi 46. in 47. člena;
- gre za posebne primere, določene 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 potrebno. Na spletni strani Informacijskega pooblaščenca so objavljene smernice⁶, v katerih je podrobno predstavljena ureditev prenosov osebnih podatkov v tretje države in mednarodne organizacije po Splošni uredbi in po ZVOP-2.

Informacijski pooblaščenec v letu 2025 ni prejel nobene vloge v zvezi s prenosom podatkov v tretje države.

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 prenašajo v ameriška podjetja v skladu z okvirom za varstvo zasebnosti podatkov med EU in ZDA.

Splošno sodišče EU je septembra 2025 zavrnilo tožbo francoskega državljana Philippa Latomba za razveljavitev sklepa o ustreznosti za ZDA. Tožnik je zoper odločitev vložil pritožbo, o kateri bo v prihodnje odločalo Sodišče EU.

⁵ https://www.ip-rs.si/fileadmin/user_upload/doc/obrazci/ZVOP/Prijava_biometrijskih_ukrepov_-_zahteva_za_izdajo_odlocbe_Informacijskega_pooblasenca__Obrazec_BIOM_doc

⁶ <https://www.ip-rs.si/publikacije/priro%C4%BDniki-in-smernice/smernice-po-splo%C5%A1ni-uredbi-o-varstvu-podatkov-gdpr/smernice-glede-prenosa-osebni-podatkov-v-tretje-dr%C5%BEave-in-mednarodne-organizacije-po-splo%C5%A1ni-uredbi-o-varstvu-podatkov>

3.4 PRIPRAVA MNENJ IN POJASNIL

3.4.1 SPLOŠNA POJASNILA

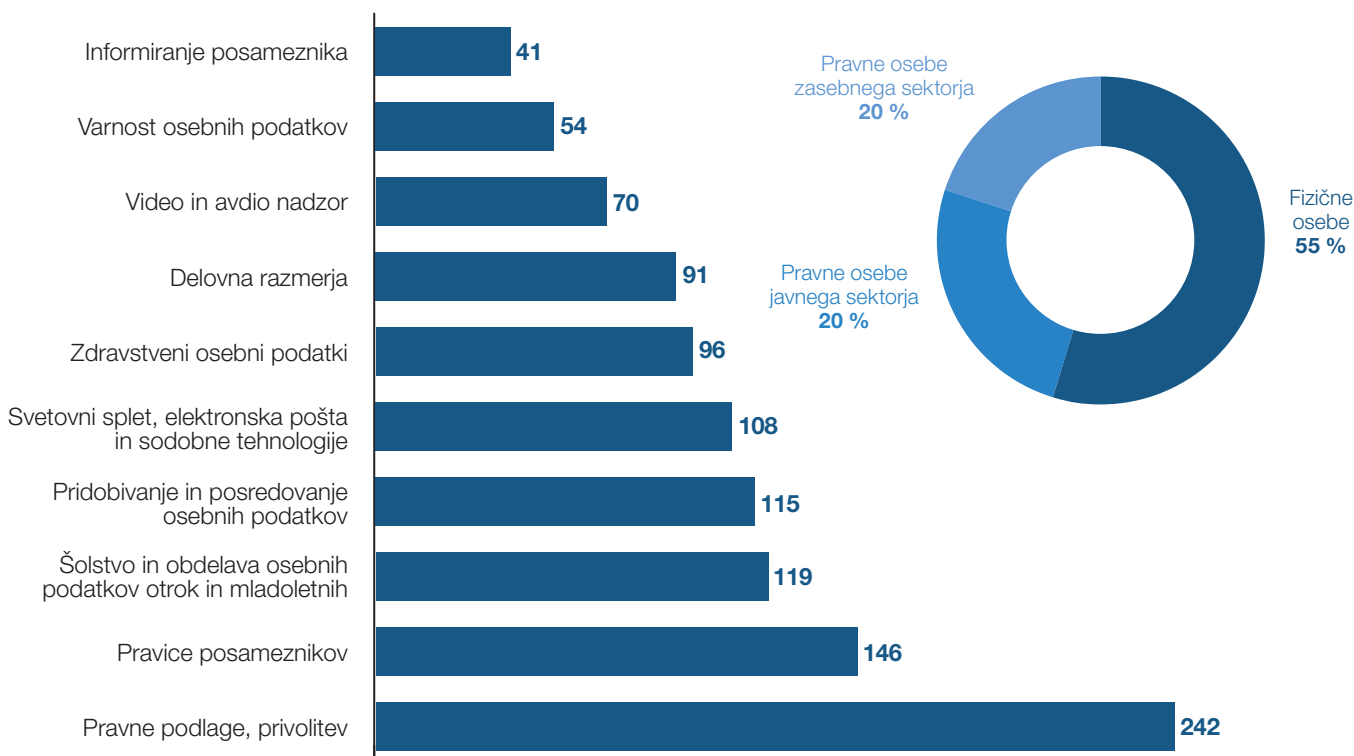
Na podlagi 57. člena Splošne uredbe, 76. člena ZVOPOKD in 56. člena ZVOP-2 Informacijski pooblaščenec izdaja neobvezna mnenja, pojasnila in stališča o vprašanih s področja varstva osebnih podatkov, s katerimi prispeva k ozaveščenosti upravljavcev in obdelovalcev ter širše javnosti.

Leta 2025 je Informacijski pooblaščenec svetoval 2.431 posameznikom in pravnim osebam, ki so se nanj obrnile z vprašanji s področja varstva osebnih podatkov.

Informacijski pooblaščenec je pripravil **985 mnenj in napotitev na mnenja (od tega 847 pisnih mnenj, v 138 primerih je prosilcem svetoval po telefonu)**. Vsa mnenja objavlja Informacijski pooblaščenec na spletni strani <https://www.ip-rs.>

si/mnenja-zvop-2/ in so razvrščena v več kot 70 vsebinskih področij. Zbirka vseh objavljenih mnenj predstavlja **pomembno bazo znanja o različnih vidikih varstva osebnih podatkov**, ki je v pomoč tako zavezancem kakor tudi posameznikom s ciljem učinkovitega varstva podatkov in pravic posameznikov. Informacijski pooblaščenec vsak delovnik svetuje preko telefonskega dežurstva: dežurni državni nadzorniki za varstvo osebnih podatkov so **v letu 2025 po telefonu svetovali 1.446 posameznikom in organizacijam.**

Najpogostejše teme pri zaprosilih za pisna mnenja v letu 2025.



IZBOR MNENJ V OKVIRU SVETOVANJA POSAMEZNIKOM IN ORGANIZACIJAM

Obračunavanje omrežnine in obdelava podatkov

Obravnavali smo vprašanje zakonitosti obdelave osebnih podatkov pri obračunavanju omrežnine s strani elektrooperaterjev v zvezi z zagotavljanjem in delovanjem t. i. naprednih merilnih števecov. Področje ureja Zakon o oskrbi z električno energijo, zato ločena privolitvev posameznikov za obdelavo osebnih podatkov v tem delu ni potrebna. Zakonodajalec je namreč ocenil, da je uvajanje naprednih sistemov merjenja v javnem interesu; analogne števce bodo sčasoma zamenjali napredni, zato je pravno podlago za s tem povezano obdelavo osebnih podatkov uredil v zakonu.

Pridobitev podatkov s strani policije

Obravnavali smo vprašanje dostopa do konkretnega dokumenta policije in s tem povezanih osebnih podatkov. Posameznik lahko dostop do lastnih osebnih podatkov vedno zahteva na podlagi 15. člena Splošne uredbe ali 24. člena Zakona o varstvu osebnih podatkov na področju obravnavanja kaznivih dejanj, pri čemer lahko na ta način pridobi le podatke, ki se nanašajo nanj, če za to ni zakonskih omejitev. Na podlagi obrazložene in utemeljene pisne zahteve ter ob hkrati izkazanem pravnem interesu posameznika (npr. ob izkazani premoženjski in nepremoženjski škodi, telesni poškodbi, sumu storitve kaznivega dejanja ali prekrška in podobnih primerih) pa mora policija na podlagi 116. člena Zakona o nalogah in pooblastilih policije posamezniku posredovati tudi druge podatke, zbrane pri obravnavanju dogodka ali opravljanju policijskih nalog.

Posredovanje podatkov o absentizmu delodajalcu

Informacijski pooblaščenec je obravnaval vprašanje, ali lahko Zavod za zdravstveno zavarovanje Slovenije na prošnjo delodajalcev posreduje anonimizirane statistične podatke o odsotnosti zaposlenih, vključno s podatki o diagnozah. Takšno posredovanje je načeloma dopustno, če so podatki absolutno anonimizirani – če torej posameznik na podlagi le-teh ni določen ali določljiv. Vprašanje, kdaj je določen nabor statističnih podatkov dejansko anonimiziran ali zgolj psevdonimiziran, pa je odvisno od konkretnega primera in relevantnih okoliščin, kot so: raven specifičnosti diagnoz, obdobje, zajeto v statistiki, število odsotnosti po posameznih kazalnikih in

skupno število zaposlenih, vrste analiz in način prikaza podatkov, stopnja generalizacije ter posebne okoliščine, kot so redke bolezni.

Prepoznavna registrskih tablic na parkirišču trgovskega centra

Informacijski pooblaščenec je v mnenju poudaril, da se parkirišče trgovskega centra šteje za javno površino v smislu določb Zakona o urejanju prostora (ZUreP-3). V praksi se kot pravna podlaga za prepoznavo registrskih tablic v takem primeru najpogosteje uporablja podlaga zakonitih interesov iz točke f prvega odstavka 6. člena Splošne uredbe. Izvajalec take obdelave pa mora na podlagi izvedenega testa zakonitih interesov poskrbeti, da se obdelava izvaja zakonito in na način, ki najmanj posega v zasebnost posameznikov. O morebitni uporabi drugih pravnih temeljev opisane obdelave presoja izvajalec glede na vse okoliščine (npr. kdo dostopa do parkirišča, pod katerimi pogoji in komu je parkiranje dovoljeno).

Javnost registra plovil

Informacijski pooblaščenec je obravnaval vprašanje skladnosti Registra plovil v aplikaciji eUprava s predpisi o varstvu osebnih podatkov – konkretno, ali je zakonito, da so javno dostopni ime in priimek, naslov stalnega bivališča lastnika plovila ter podatki o plovilu. Informatiziran dostop do podatkov o plovilih v aplikaciji eUprava je zakonsko utemeljen na določbah Pomorskega zakonika, ki predvidevajo, da se omogoči javni dostop do podatkov iz glavne knjige ladijskega registra, vključno z vpisnikom čolnov.

Posredovanje podatkov o bolniškem režimu detektivu

Informacijski pooblaščenec je v mnenju poudaril, da lahko detektiv pridobiva informacije neposredno od osebe, na katero se podatki nanašajo, kot tudi od drugih oseb, ki s podatki razpolagajo, če so jih pripravljene prostovoljno posredovati. Ne glede na to pa ima detektiv v skladu z Zakonom o detektivski dejavnosti v okviru pooblastila naročnika tudi samostojen pravni temelj za pridobivanje določenih osebnih podatkov iz zbirk, ki so določene v zakonu. Tako ima za izvedbo nadzora zaradi suma zlorabe pravice do zadržanosti z dela zaradi bolezni ali poškodbe detektiv pravico pridobiti navodilo o ravnanju osebe pod nadzorom v času zadržanosti od dela, pri čemer se ne sme seznaniti z drugimi podatki iz zdravstvene dokumentacije. Zahtevi mora biti priložena tudi fotokopija pisnega pooblastila.

Dostop etažnih lastnikov do dokumentacije o upravljanju stavbe

Informacijski pooblaščenec je v mnenju izpostavil, da mora upravnik vsakemu etažnemu lastniku na njegovo zahtevo, vendar ne več kot enkrat mesečno, omogočiti vpogled v določeno dokumentacijo, ki se nanaša na upravljanje večstanovanjske stavbe. Etažni lastnik lahko pod določenimi pogoji za vpogled pooblasti tretjo osebo. Pooblastilo mora biti dano v pisni obliki, iz njega pa mora jasno izhajati zlasti, koga in za kakšen namen etažni lastnik pooblašča ter časovna veljavnost pooblastila.

Obdelava osebnih podatkov pri vpisu v osnovno šolo

Informacijski pooblaščenec je prejel več zaprosil za mnenje glede obdelave osebnih podatkov otroka pri vpisu v prvi razred osnovne šole. Šola, ki je otroka dolžna vpisati v prvi razred, na podlagi Zakona o osnovni šoli pridobi seznam otrok iz šolskega okoliša iz evidence šoloobveznih otrok, ki jo vodi ministrstvo, pristojno za šolstvo. Gre za podatke o otroku (ime in priimek, EMŠO, naslov prebivališča) in podatke o starših (ime in priimek, naslov prebivališča). Zakonodaja pošiljanja vabil na vpis posebej ne ureja, vendar bi bila taka obdelava lahko dopustna, če je to nujno potrebno za izvajanje zakonitih nalog šole in se s tem ne poseže v upravičen interes posameznika.

Videonadzor v gozdu

Informacijski pooblaščenec je v mnenju izpostavil, da bi bilo izvajanje videonadzora s strani lovskega inšpektorja lahko zakonito na podlagi Zakona o divjadi in lovstvu, in sicer za nadzor nad krmišči, solnicami, kalužami, lokacijami, na katerih člani upravljavca lovišča krmijo divjad v nasprotju z načrti lovsko upravljavskih območij, in mesti za prevzem divjadi v skladu s predpisi, ki urejajo veterinarstvo, ter pod pogojem, da se pri tem upoštevajo vse ostale določbe glede varstva podatkov. Lovski inšpektor lahko tak videonadzor izvaja v konkretnem primeru oz. posameznem postopku, ne pa za namen splošnega in stalnega izvajanja nadzora. Subjekti zasebnega sektorja bi za posamezne vnaprej določene namene (pridobivanje podatkov o divjadi za potrebe lova in upravljanja z divjadjo, znanstveno raziskovalno delo v zvezi z divjadjo ...) videonadzor lahko izvajali, če za to obstaja zakoniti interes in pod pogojem, da pri tem ne gre za opravljanje nalog v javnem interesu ali pri izvajanju javne oblasti ter da nad zakonitim interesom ne pretehtajo interesi ali te-

meljne pravice in svoboščine posameznika točka f prvega odstavka 6. člena Splošne uredbe.

Fotografiranje in objava fotografij otrok

Informacijski pooblaščenec v mnenju poudarja, da so fotografije osebni podatki, kadar omogočajo prepoznavnost posameznika, tudi če obraz ni razviden. Pri objavi fotografij je pravni temelj zanjo najpogostejše privolitev – ta mora biti prostovoljna, konkretna, informirana in nedvoumna. Pri otrocih privolitev običajno podajo starši ali drugi zakoniti zastopniki. Posebno previdnost je treba v teh primerih nameniti objavam v občutljivih okoliščinah (npr. fotografije v kopalkah, fotografije v situacijah in na način, ki je za otroka žaljiv ali do njega posmehljiv, fotografije v kriznih centrih, rejništvu), ki bi se jim morali izogibati. Vedno je namreč treba upoštevati največjo korist otroka in vse posledice vsake objave. Prav tako je treba spoštovati določbe Zakona o preprečevanju nasilja v družini, ki prepovedujejo razkrivanje identitete žrtve ali njene družine ter nalagajo zaščito otrok pred izpostavljanjem javnosti.

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, pri čemer posebno pozornost pri svetovanju namenja skrbi, da predlagatelji ustrezno upoštevajo določbe Ustave (zlasti 38. člena) ter ZVOP-2. Zlasti ministrstva redno zaprošajo za pomoč pri pripravi predpisov, ki pomembno vplivajo na varstvo osebnih podatkov. V javnem sektorju morajo namreč obdelavo načeloma urejati zakoni, ki določajo, kako, kdaj in v kakšnem obsegu bodo posegi v zasebnost posameznika dopustni. Zakoni morajo biti zato sorazmerni, učinkoviti, jezikovno jasni in razumljivi ter določati predvidljiva, jasna in ustavno skladna pravila obdelave osebnih podatkov. Informacijski pooblaščenec vsa mnenja na predpise objavlja na svoji spletni strani⁷.

Leta 2025 je Informacijski pooblaščenec pripravil **117 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 pravočasno vključevanje vseh deležnikov in strokovnjakov s področja informacijskih tehnologij v pripravo (npr. zlasti različnih ministrstev in drugih državnih organov, ki so upravljavci največjih zbirk osebnih podatkov) ter zavedanje o nujnosti temeljite predhodne analize in naslovitve tveganj, ki jih takšne obdelave prinašajo.

Mnenje na Predlog Evropske komisije o Digitalnem omnibusu

Informacijski pooblaščenec je Ministrstvo za digitalno preobrazbo v mnenju opozoril, da nekatere predlagane rešitve Digitalnega omnibusu, kot je sprememba opredelitve pojma osebnega podatka, lahko škodijo temeljni pravici do varstva osebnih podatkov. Med drugim je opozoril tudi na nevarnosti pomanjkljivo opredeljene širitve dopustnega obsega obdelav osebnih podatkov za znanstvenoraziskovalne namene tudi v zgolj komercialne namene ter na nevarnosti predlaganih določb glede izrecnega omogočanja treniranja, testiranja in delovanja sistemov umetne inteligence ali modelov na zbirkah posebnih vrst osebnih podatkov ter širitve dopustnega obsega obdelav vseh podatkov za te namene.

Mnenje na Predlog Zakona o nujnih ukrepih za zagotavljanje javne varnosti (t. i. Šutarjev zakon)

Informacijski pooblaščenec je v svojem mnenju zakonodajalca opozoril na neustreznost določb glede uporabe tehničnih sredstev za fotografiranje in video ter avdio snemanje ter glede avtomatske prepoznavne registrskih tablic vozil s samodejno obdelavo in primerjavo tako zbranih podatkov. Pri tem je posebej poudaril, da so tako nameni kot tudi načini uporabe tehničnih sredstev v predlogu zakona določeni preširoko, nesorazmerno in ne glede na konkretno stopnjo resnosti situacije na varnostno tveganem območju, saj npr. dopuščajo vse oblike uporabe tehničnih sredstev za fotografiranje ter video in avdio snemanje iz tako rekoč vseh lokacij in objektov, torej tudi povsem zasebnih. Snemanje posameznikov na javnih površinah iz vozila ima namreč povsem drugačen domet, kot pa snemanje zasebnih površin.

Mnenje na Predlog Zakona o digitalizaciji zdravstva

Informacijski pooblaščenec je v več mnenjih, naslovljenih na ministrstvo za zdravje in na zakonodajalca v zakonodajnem postopku, opozoril, da gre v primeru osrednje centralne zbirke z zdravstvenimi podatki – t. i. Centralni elektronski zdravstveni zapis – za zbirko podatkov, v kateri je zabeleženo vse o posamezniku in številni podatki o njegovih družinskih članih, zato bi morali biti v zakonu izjemno jasno in sorazmerno določeni vsi vidiki obdelave, ustrezno bi morale biti zagotovljene pravice posameznika do informacijske samoodločbe, omejeni bi morali biti nameni zbiranja in obdelave, roki hrambe podatkov ter drugi vidiki zagotavljanja omejitev posegov v posameznikovo

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

zasebnost. Informacijski pooblaščenec je posebej izpostavil nejasnosti glede vloge in nalog nove družbe, ki bo imela osrednjo vlogo pri procesih digitalizacije in obdelave podatkov in bo imela izredno veliko moč ter široka pooblastila. Čeprav je namreč predlog zakona družbo opredelil kot pogodbenega obdelovalca, naloge, ki ji jih je zakon podelil, kažejo na to, da bo ta družba dejansko upravljavec osrednje nacionalne zbirke zdravstvenih podatkov.

Mnenje na Predlog Zakona o centralnem kreditnem registru

Informacijski pooblaščenec je v mnenju predlagatelja opozoril na potencialno preobsežno zbiranje osebnih podatkov o zadolženosti posameznikov v osrednji nacionalni zbirki – centralni kreditni register – in vnovič predlagal dodaten razmislek o opredelitvi potrebnega višjega praga okoliščin »zadolžitve« oziroma okoliščin zamude, ki bi predstavljal predpogoj, da se osebni podatki fizične osebe beležijo v sistem. Prav tako je opozoril na nesorazmerno dolg rok hrambe vseh osebnih podatkov v centralnem kreditnem registru v psevdonimizirani obliki skupaj z davčno številko. Glede avtomatiziranega dostopa in povezovanja sistema izmenjave informacij – preko katerega banke in druge finančne institucije oz. dajalci kreditov dostopajo do podatkov v centralnem kreditnem registru – z zbirkami bank in drugih članov sistema je Informacijski pooblaščenec opozoril, da predlog zakona ne opredeljuje namena takega povezovanja, preširoko določa zbirke bank in drugih članov sistema, s katerimi se lahko sistem povezuje, in ne določa nobenih ukrepov za zaščito pravic in svoboščin ter zakonitih interesov posameznika v zvezi z uporabo in obdelavo tako pridobljenih osebnih podatkov, ki jih bodo banke in drugi člani sistema posledično kopirali v lastne zbirke.

Mnenje na Predlog sprememb Zakona o osnovni šoli

Informacijski pooblaščenec je v svojem mnenju izpostavil zlasti pomanjkljivo utemeljitev nujnosti, potrebnosti in sorazmernosti ter same izvedbe glede poseganja v pravice posameznikov – tako staršev kot otrok – z zbiranjem podatka o »pripadnosti romski skupnosti« za namen vzpodbujanja in zagotavljanja enakega obravnavanja, enakih možnosti ter zajamčenih osebnih pravic pripadnikov romske skupnosti. Predlagatelj je na podlagi mnenja v zakon dodal varovalko in pogoj, da se podatek o romski pripadnosti lahko zbira zgolj na podlagi soglasja staršev. Nejasnosti glede izvajanja v Državnem zboru potrjene določbe v praksi potrjujejo, da so bila opozorila Informacijskega pooblaščenca glede pomanjkljivosti sprejete ureditve utemeljena.

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 zaradi nesorazmerno dolgih zakonskih rokov hrambe osebnih podatkov v evidenci kaznivih dejanj, na kar sicer opozarja že vrsto let, v letu 2024 vložil zahtevo za oceno ustavnosti⁸ 129. člena Zakona o nalogah in pooblastilih policije (ZNPPol). Zahtevo je Informacijski pooblaščenec vložil v zvezi s pritožbenim postopkom zaradi pravice do izbrisa, saj se v tej policijski evidenci 30 let hrani obsežen nabor podatkov posameznikov, vključno s tistimi, ki so bili storitve kaznivega dejanja zgolj osumljeni, ne pa tudi pravnomočno obsojeni. Prav tako so v tej evidenci zajeti podatki drugih oseb, ki so s kaznivim dejanjem zgolj povezane, kot so prijavitelji, oškodovanci in prejemniki premoženjskih koristi.

Ustavno sodišče je v odločbi št. U-I-9/24 z dne 25. 9. 2025 odločilo, da je bila ureditev hrambe osebnih podatkov po 129. členu ZNPPol v delu, ki se nanaša na evidenco kaznivih dejanj, v neskladju z Ustavo⁹. Čeprav je Državni zbor v začetku leta 2025 sprejel novelo ZNPPol-C, s katero je delno spremenil ureditev rokov hrambe, je Ustavno sodišče ocenilo, da je presoja ustavnosti izpodbijanih določb še vedno potrebna, saj so se izpodbijane določbe uporabljale v konkretnem postopku.

Ustavno sodišče je ugotovilo, da je ZNPPol določal večfazno hrambo osebnih podatkov:

- osnovno fazo do ustavitve policijske preiskave ali izdaje sklepa o zavrženju kazenske ovadbe ali do pravnomočne zavrnilne ali oprostilne sodbe, če pa tega ni, do zastaranja kazenskega pregona,
- blokirano fazo, v kateri so se podatki hranili še 30 let, in
- anonimizirano fazo, v kateri (kljub morebitni drugačni praksi) ni šlo več za osebne podatke.

⁸ https://www.ip-rs.si/fileadmin/user_upload/Pdf/ocene_ustavnosti/Zahteva_za_oceno_ustavnosti_129_clen_ZNPPol_anon_za_splet.pdf

⁹ <https://www.us-rs.si/sl/zadeve-in-odlocitve/odlocitve/u-i-924>

Čprav so bili podatki v drugi fazi formalno blokirani, je imela policija do njih še vedno dostop, zato je Ustavno sodišče presodilo, da tudi takšna hramba pomeni obdelavo osebnih podatkov in s tem poseg v pravico do informacijske zasebnosti iz prvega odstavka 38. člena Ustave. Sodišče je ob tem opozorilo, da se lahko skupna hramba podatkov (osnovna in blokirana faza skupaj) v praksi giblje od približno 36 do 80 let, pri nekaterih kaznivih dejanjih pa celo brez časovne omejitve, kar pomeni poseg, ki se približuje trajni hrambi osebnih podatkov.

Po presoji Ustavnega sodišča je bila izpodbijana ureditev sicer skladna z načelom jasnosti in pomen-ske določljivosti iz 2. člena Ustave ter je sledila dopustnemu cilju odkrivanja storilcev kaznivih dejanj zaradi učinkovite zaščite pred kriminalno dejavnostjo, vendar pa se ni omejila na nujno potreben obseg za doseg tega cilja. Ni namreč omogočala:

1. zahteve za izbris podatkov, če njihova hramba ni več nujna, niti obdobjnega preverjanja nujnosti nadaljnje hrambe podatkov po uradni dolžnosti;
2. določitve roka hrambe glede na težo in naravo kaznivega dejanja, s čimer bi bila hramba omejena na obseg, nujen za doseganje njenega namena, ter
3. razlikovanja med različnimi kategorijami oseb (npr. osumljenci, obdolženci, obsojenci, žrtve kaznivega dejanja) ter upoštevanja posebnega položaja oseb, ki jim je zagotovljena domneva nedolžnosti iz 27. člena Ustave.

Glede na navedeno je Ustavno sodišče ugotovilo, da sta bila prvi odstavek 129. člena in prva alineja drugega odstavka istega člena ZNPPol, kolikor se nanašata na evidenco kaznivih dejanj, v neskladju z Ustavo. Zaradi njune vsebinske povezanosti je enako odločilo tudi glede tretjega in četrtega odstavka tega člena.

3.4.4. 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. Pomembno novost na področju ocen učinka je prinesla 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 obdelavo osebnih podatkov, za katero je treba izdelati oceno učinka, predlagatelj predpisa izvede zakonodajno oceno učinka in jo posreduje v predhodno posvetovanje Informacijskemu pooblaščenecu.

Informacijski pooblaščenec je na podlagi izkušenj iz obravnave prejetih ocen učinka izdal infografiko o učinkovitem obvladovanju tveganj na področju varstva osebnih podatkov. Neustrezno definiranje tveganj se namreč kaže kot glavna težava pri izdelavi ocen učinka na varstvo osebnih podatkov. Število izdanih mnenj na ocene učinka se je ustalilo: Informacijski pooblaščenec je v postopku predhodnega posvetovanja v letu 2025 izdal 30 mnenj.

V letu 2025 je s področja mnenj na t. i. projektne ocene učinka treba izpostaviti mnenje glede ocene učinka na varstvo osebnih podatkov v zvezi s projektom **Virtualni pomočnik Vrhovnega državnega tožilstva Republike Slovenije**. Šlo je za prvo mnenje na podlagi 49. člena ZVOPOKD, ocena učinka pa se dotika tudi področja umetne inteligence, saj obravnava tveganja glede razvoja, testiranja in produkcijske vzpostavitve informacijskega sistema, ki bo na osnovi tehnologije umetne inteligence pomagal državnim tožilcem in drugim zaposlenim na državnem tožilstvu pri izvrševanju pristojnosti državnih tožilstev. Ocena učinka je bila kakovostno pripravljena, Informacijski pooblaščenec pa je opozoril predvsem na podrobno analizo tveganj iz naslova morebitnega avtomatiziranega odločanja. Ker v času izdelave mnenja Informacijski pooblaščenec še ni imel pooblastil za ugotavljanje skladnosti z Aktom o umetni inteligenci, v tem delu ni mogel podati mnenja.

Dodana vrednost pravočasne izdelave ocene učinka se je izkazala tudi v primeru ocene učinka glede **evidence študentskega dela (EŠD)**, kjer je Informacijski pooblaščenec zavezanca opozoril, da bi obstoječi način dostopa do osebnih podatkov na spletni strani EŠD, kjer je dostop do osebnih podatkov posameznika možen zgolj z vnosom EMŠO in davčne številke posameznika, lahko predstavljal kršitev določb Splošne uredbe.

Podobno velja v primeru ocene učinka, ki se je nanašala na **genetski presejalni test, namenjen oceni dedne nagnjenosti k raku**. Predvideno obdelavo osebnih podatkov spremljajo visoka tveganja, saj gre za obdelavo posebnih vrst osebnih podatkov (genetskih podatkov), za prenos osebnih podatkov v tretje države (na Kitajsko, v Hongkong) ter za izrazita tveganja za posameznike iz naslova točnosti v primeru napačnih rezultatov. Zavezanec je v mnenju na oceno učinka prejel številne informacije, katera so relevantna tveganja in kako dopolniti oceno učinka s ciljem celovite in pravočasne obravnave tveganj.

Precejšnje število prejetih ocen učinka se je nanašalo na problematiko iz lokalnih okolij, npr. na uvajanje videonadzora na javnih površinah in zagotavljanje varnosti v šolah. Posebej zanimiva je bila ocena učinka glede **uvajanja pametnih senzorjev, ki so zmožni detekcije kajenja v različnih oblikah (vejping, kajenje, zloraba THC) na osnovni šoli**. Pametni senzori naj bi bili nameščeni v toaletnih prostorih, kjer se največkrat pojavljajo kršitve hišnega reda, povezane s kajenjem. Informacijski pooblaščenec je v mnenju na oceno učinka zavezanca opozoril, naj se posebej posveti tveganjem, postopkom in varovalkam v povezavi z identifikacijo in nadaljnjo obravnavo kršiteljev, saj so glede na način delovanja sistema tu tveganja najbolj izrazita.

Glede t. i. zakonodajnih ocen učinka se je precejšnje število prejetih ocen učinka nanašalo na predpise, ki določajo povezovanje zbirk osebnih podatkov, kot npr. na povezovanje registra dejanskih lastnikov in sistema MFERAC, informacijskega sistema elektronske Zemljiške knjige (eZK) in Slovenskega okoljskega javnega sklada (Eko sklad) ter Centralnega registra prebivalstva in Sistema za izmenjavo informacij o zadolženosti posameznikov (SISBON).

Glede povezovanja zbirk osebnih podatkov je bistveni del zakonodajne ocene učinka, da se preveri, ali so vsa predvidena povezovanja utemeljena in tudi ustrezno zapisana v samem besedilu zakona. V primeru povezovanja uradnih evidenc ali javnih knjig

je namreč glede na ustaljeno prakso v zakonu predvsem treba določiti:

- povezovalni znak,
- namen povezovanja,
- upravljavca (oz. upravljivce) povezanih evidenc ter
- katere podatke se iz povezane zbirke (oz. povezanih zbirk) pridobi.

Med najpomembnejšimi temami na področju zakonodajnih ocen učinka je v letu 2025 izstopalo sprejemanje Zakona o digitalizaciji zdravstva. Informacijski pooblaščenec je v letih 2023 in 2024 že izdal tri mnenja na osnutke predloga zakona, v letu 2025 pa je v mnenju na oceno učinka še vedno ugotavljal določene pomanjkljivosti, zlasti glede nezadostne primerjave z ureditvami v tujini, pomanjkljive opredeljenosti nabora podatkov, upravljavcev in uporabnikov, rokov hrambe ter nepopolnega obvladovanja tveganj za pravice in svobščine posameznika.

Kot tudi sicer je Informacijski pooblaščenec opozoril, da je pri pripravi predpisa treba opraviti premislek o možnih ukrepih za obvladovanje tveganj – identificirana tveganja se upravlja z ustreznimi varovalkami (kavtelami), kot so npr. kratki roki hrambe, anonimizacija, psevdonimizacija, minimizacijski postopki, sledljivost obdelave, logične in fizične kontrole pri vnosu podatkov, redni notranji nadzor ipd. Gre za ukrepe za obvladovanje tveganj, ki jih je treba in jih je primerno nasloviti že na ravni priprave predpisa (zakona), in ne za ukrepe, ki se jih lahko prepusti upravljavcu.

Mnenja na zakonodajne ocene učinkov glede varstva osebnih podatkov so objavljena na spletni strani Informacijskega pooblaščenca poleg mnenj na predloge predpisov¹⁰. Objava mnenj na zakonodajne ocene učinkov glede varstva osebnih podatkov prispeva k večji preglednosti in je v pomoč predlagateljem predpisov, ki lahko iz objavljenih mnenj razberejo, katerim točkam je pri pripravi ocen učinka treba posvetiti posebno pozornost.

¹⁰ <https://www.ip-rs.si/zakonodajja/priponbe-informacijskega-poobla%C5%A1%C4%8Denca-na-predloge-predpisov/>

3.5 SKLADNOST IN PREVENTIVA

3.5.1 AKTIVNOSTI ZA DOSEGANJE SKLADNOSTI IN PREVENTIVNA DEJAVNOST

Informacijski pooblaščenec uporablja širok nabor orodij za dviganje ozaveščenosti in doseganje skladnosti, med katera sodijo:

- spletne strani Informacijskega pooblaščenca (www.ip-rs.si, www.tiodlocas.si in www.upravljavec.si),
- smernice,
- vzorci in obrazci,
- infografike,
- brezplačna predavanja in izobraževanja,
- objave na družabnih omrežjih,
- preventivne aktivnosti za skladnost,
- pisna mnenja posameznikom,
- pisna mnenja na predloge predpisov,
- pisna mnenja na ocene učinkov glede varstva osebnih podatkov,
- telefonsko svetovanje,
- povezovanje s pooblaščenimi osebami za varstvo osebnih podatkov,
- spodbujanje aktivne udeležbe mladih,
- sodelovanje z drugimi organizacijami na nacionalni in mednarodni ravni pri pripravi vodnikov in drugih izobraževalnih vsebin,
- organizacija dneva varstva osebnih podatkov,
- priprava meril na področju certifikacije in akreditacije,
- priprava kriterijev in seznamov nadzornega organa glede obveznosti po Splošni uredbi ter
- sodelovanje na konferencah, strokovnih srečanjih, posvetih, okroglih mizah in drugih dogodkih.

Tudi v letu 2025 je Informacijski pooblaščenec izvajal preventivne aktivnosti za skladnost (angl. *privacy sweep*), in sicer izpostavljamo sodelovanji v **usklajeni akciji sodelovanja v okviru EDPB, t. i. CEF** (*Coordinated Enforcement Framework*) ter v okviru povezave **Global Privacy Enforcement Network (GPEN)**.

Tema usklajene akcije CEF 2025 je bila pravica do izbrisa. Na ravni Slovenije smo se osredotočali na izvrševanje pravice do izbrisa, ki jo zahtevajo potrošniki v sektorju deljene mobilnosti in javnega prevoza. Informacijski pooblaščenec je izvedel inšpekcijske nadzore pri treh upravljavcih na področju deljene mobilnosti in javnega prevoza. Rezultat akcije so ključne ugotovitve in priporočila za vse upravljivce, ki nudijo digitalne storitve.

Informacijski pooblaščenec je ugotovil nekaj ključnih pomanjkljivosti, ki so se pri upravljavcih osebnih podatkov pogosto pojavljale:

- Zavajajoča ali nepregledna uporaba funkcije »izbrisi račun«: posameznik želi izbris osebnih podatkov, vendar s funkcijo izbrisi račun doseže samo odstranitev aplikacije s svoje naprave ali omejitve obdelave osebnih podatkov do poteka roka hrambe, ne pa resničnega izbrisa osebnih podatkov. Posamezniki o takšnem načinu izbrisa svojih osebnih podatkov niso ustrezno obveščeni.
- O zavrnitvi pravice do izbrisa posamezniki niso ustrezno obveščeni: kadar je bila posameznikova zahteva za izbris zavrjena (ker jih upravljavec na primer potrebuje zaradi uveljavljanja ali obrambe pravnih zahtevkov), posamezniki pogosto niso prejeli jasne in pravočasne informacije o razlogih za zavrnitev ter o pravici do pritožbe.
- Pomanjkljiva dokumentacija in sledljivost zahtev: več upravljavcev ni imelo urejenih evidenc o prejetih zahtevah za izbris in sprejetih odločitvah, kar otežuje dokazovanje, da upravljavec deluje skladno s Splošno uredbo.
- Pazljivo pri anonimizaciji podatkov: izbris podatkov se v praksi pogosto izvaja z anonimizacijo podatkov, kar je sicer lahko dopustno, če podatkov po izvedenem postopku ni več mogoče povezati z določljivim posameznikom.

Na podlagi ugotovitev iz nadzorne akcije Informacijski pooblaščenec upravljavcem predlaga:

- če je možnost za izbris ponujena v aplikaciji, mora uporaba te možnosti s strani uporabnikov dejansko pomeniti tudi izbris osebnih podatkov, ne zgolj tehnične ali organizacijske omejitve obdelave, o čemer pa mora biti posameznik jasno obveščen;
- če upravljavec podatkov na podlagi zahteve ne izbrisi, mora posameznika jasno, razumljivo in pravočasno obvestiti o razlogih za zavrnitev ter o pravici do pritožbe;
- upravljivci morajo imeti jasno opredeljene notranje postopke, določene odgovornosti in ustrezno evidencirane obravnave posameznih zahtev za izbris;

- roki hrambe osebnih podatkov morajo biti utemeljeni, sorazmerni in pregledno navedeni v informacijah za posameznike;
- pri uporabi zunanjih ponudnikov IT-rešitev, odgovornost za zakonito in pregledno izvajanje pravice do izbrisa ostaja na strani upravljavca.

V usklajeni nadzorni akciji CEF je sodelovalo 32 nadzornih organov iz celotnega Evropskega gospodarskega prostora, zaključila pa se je s sprejemom skupnega poročila v februarju 2026¹¹.

Konec leta 2025 je 27 nadzornih organov za varstvo podatkov in zasebnost z vsega sveta v okviru združenja Global Privacy Enforcement Network (GPEN) izvedlo usklajen pregled, v katerem so pregledali skoraj 900 spletnih mest in aplikacij, ki jih uporabljajo otroci. Letošnji pregled so usklajevali nadzorni organi iz Kanade, Združenega kraljestva in Guernseyja, v njem pa so sodelovali tudi predstavniki Informacijskega pooblaščenca, ki so pregledali 17 spletnih mest in aplikacij, ki so priljubljene med otroki v Sloveniji.

Nadzorni organi so preverili mehanizme in prakse platform v zvezi z zbiranjem osebnih podatkov uporabnikov, v zvezi s preglednostjo, preverjanjem starosti in omejevanjem zbiranja podatkov. S ponovitvijo pregleda, ki so ga nadzorni organi izvedli leta 2015, so sodelujoči organi lahko primerjali, kako so spletne storitve ščitile otroke nekoč in danes.

Ugotovljene so bile določene dobre prakse za zaščito otrok in njihovih osebnih podatkov, kot so obvestila, ki otrokom svetujejo, naj ne uporabljajo svojih pravih imen, naj ne nalagajo slik ter da imajo privzeto onemogočeno skupno rabo lokacije. Kljub temu pa so nadzorni organi opazili tudi prakse, ki vzbujajo pomisleke glede varovanja zasebnosti otrok, in ugotavljajo, da so se nekatera tveganja v zadnjih 10 letih povečala. V primerjavi z letom 2015 namreč več spletnih storitev, ki jih uporabljajo otroci, zahteva, da uporabniki posredujejo svoje osebne podatke za dostop do polne funkcionalnosti platforme. Poleg tega več platform v svojih pravilnikih o zasebnosti navaja, da lahko delijo osebne podatke s tretjimi osebami.

Nadzorni organi so ocenjevali spletne strani in mobilne aplikacije na podlagi petih kazalnikov, ki so v veliki meri sledili kazalnikom iz pregleda leta 2015:

- Preverjanje starosti: pri 72 % pregledanih spletnih mest in mobilnih aplikacij se je možno izogniti ukrepom za preverjanje starosti, največkrat tam, kjer je uporabljena samoprijava.

- Zbiranje podatkov otrok: več kot polovica (59 %) spletnih strani in mobilnih aplikacij zahteva zbiranje naslovov elektronske pošte za dostop do polne funkcionalnosti platform, sledi 50 % spletnih strani in mobilnih aplikacij, ki zahtevajo geolokacijo. Na splošno so nadzorni organi opazili povečanje zbiranja določenih vrst podatkov v primerjavi z letom 2015.
- Zaščitni ukrepi: 71 % spletnih mest in mobilnih aplikacij ni imelo informacij o zaščitnih ukrepih in otrokom prilagojenih nastavitvah zasebnosti.
- Izbris računa: več kot tretjina (36 %) spletnih mest in mobilnih aplikacij ne nudi enostavno dostopnega načina za izbris računov.
- Neprimerna vsebina in visoko tvegani oblikovni elementi: samo 35 % spletnih mest in mobilnih aplikacij, za katere je bilo ugotovljeno, da nudijo otrokom neprimerno vsebino in uporabljajo visoko tvegane oblikovne elemente, ima informacije o zasebnosti, kot npr. pojavna okna, ki otroke usmerjajo, naj zaprosijo za dovoljenje staršev za nadaljnjo uporabo spletne strani ali aplikacije.

Skupno poročilo aktivnosti GPEN Privacy Sweep 2025 je bilo objavljeno konec marca 2026¹².

Informacijski pooblaščenec je pripravil tudi dve novi infografiki, ki sta objavljeni na spletni strani: razlago psevdonimizacije ter infografiko o učinkovitem obvladovanju tveganj na področju varstva osebnih podatkov. Neustrezno definiranje tveganj je namreč glavna težava pri izdelavi ocen učinka na varstvo osebnih podatkov.

Zavezanec je Informacijski pooblaščenec opozoril na potek prehodnega obdobja za uskladitev dnevnikov obdelave osebnih podatkov, saj je s 26. 1. 2025 poteklo dvoletno prehodno obdobje, v katerem bi morali zavezanci uskladiti vodenje dnevnikov obdelav z zahtevami ZVOP-2. Zlasti pri velikih zbirkah osebnih podatkov, kot so državni registri, in pri zbirkah, kjer se obdelujejo večje količine posebnih vrst osebnih podatkov, kot so zdravstveni podatki, je bistveno, da se zabeleži, kdaj so bili izvedeni dostopi do podatkov, kdaj so bili podatki spremenjeni, uporabljeni ali drugače obdelani. Beleženje obdelave se izvaja v dnevnikih obdelave, ki se vodijo zaradi izkazovanja zakonitosti obdelave, za izvajanje notranjega in zunanjega nadzora, za zagotavljanje celovitosti in varnosti osebnih podatkov ter za odpravljanje napak pri obdelavi podatkov.

¹¹ https://www.ip-rs.si/go?u=external%3Awww.edpb.europa.eu%2Fnews%2Fnews%2F2026%2Ffedpb-identifies-challenges-hindering-full-implementation-right-erasure_en

¹² https://www.privacyenforcement.net/system/files/2026-03/GPEN_Sweep_Report_-_March_2026_-_EN.pdf

3.5.2 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. Pooblaščenca oseba 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 2025 je bilo Informacijskemu pooblaščenču sporočenih 3583 pooblaščenih oseb za varstvo podatkov (leto prej 3486). Podatke o pooblaščenih osebah za varstvo osebnih podatkov je možno enostavno sporočiti in popraviti s pomočjo spletnega obrazca, dostopnega na naslednji povezavi: <https://www.ip-rs.si/pooblascene-osebe>. Ocenjujemo, da je večina zavezancev izpolnila svojo dolžnost glede posredovanja podatkov o pooblaščenih osebah 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).

Pomembno je povezovanje z reprezentativnimi skupinami pooblaščenih oseb za varstvo podatkov, med katerimi so zlasti relevantne pooblaščenca osebe na ministrstvih, s katerimi se Informacijski pooblaščenec redno srečuje, saj so ministrstva predlagatelji predpisov in vodijo velike državne zbirke osebnih podatkov.

3.5.3 AKTIVNOSTI IZOBRAŽEVANJA IN OZAVEŠČANJA

Informacijski pooblaščenec posebno pozornost namenja izobraževanju in ozaveščanju splošne in strokovne javnosti o pomembnih temah na področju varstva osebnih podatkov in v ta namen organizira različne dogodke, pripravlja različne objave ter na druge načine skrbi za dvig ozaveščenosti.

Na dogodku ob evropskem dnevu varstva podatkov je Informacijski pooblaščenec podelil nagrado *ambasador zasebnosti* točki osveščanja o varni in odgovorni rabi interneta Safe.si. Rdeča nit dogodka so bili otroci in pomen ozaveščanja o varovanju zasebnosti v digitalnih okoljih, pri uporabi pametnih naprav. Podelitvi nagrad je sledila okrogla miza o stanju in izzivih varovanja zasebnosti in odgovorni

uporabi digitalnih storitev pri otrocih ter o vključevanju izobraževalnih vsebin na to temo v učne načrte. Dogodek se je zaključil s projekcijo filma *Lars je LOL*.



Podelitev nagrade ambasador zasebnosti za leto 2024, 28. januar 2025.

Informacijski pooblaščenec je aprila 2024 prijavil projekt *Become a PrivacyPRO(tector)* na razpis Evropske komisije za financiranje projektov, ki jih izvajajo nadzorni organi za varstvo osebnih podatkov za namen ozaveščanja širše javnosti o varstvu osebnih podatkov (CERV-2024-DATA). Projekt *Become a PrivacyPRO(tector)*, s krajšim nazivom *PrivacyPRO*, se je po oceni Evropske komisije uvrstil med najvišje ocenjene projekte ter je bil izbran za sofinanciranje v okviru programa Državljeni, enakost, pravice in vrednote 2021–2027.

Namen projekta *PrivacyPRO* je povečati ozaveščenost in razumevanje načel varstva osebnih podatkov med otroki, učitelji, starši in skrbniki ter tako prispevati h kulturi varstva zasebnosti in osebnih podatkov že od zgodnjega otroštva. Ciljno skupino projekta predstavljata dve starostni skupini otrok, in sicer otroci, stari od 6 do 10 let, in otroci, stari od 11 do 14 let, ter njihovi starši in skrbniki, učitelji, socialni delavci in ostali posamezniki, ki delajo z njimi.

Informacijski pooblaščenec je projekt *PrivacyPRO* začel izvajati v letu 2025. Aktivnosti projekta so bile primarno usmerjene v izdelavo izobraževalnih materialov za otroke, učitelje in starše. Izdelana je bila družabna namizna igra *Misija IP: postani varuh podatkov* in istoimenski stripi, ki bodo od decembra

2025 do junija 2026 vsak mesec izhajali v reviji Pil. Z igralcem Juretom Henigmanom smo posneli sedem kratkih video vsebin, v katerih otroke in mladostnike na zabaven način opozarja na pasti deljenja podatkov. Organizirali smo tudi dneve odprtih vrat, na katerih smo za osnovnošolce pripravili aktivnosti po modelu sobe pobegov in jih na ta način seznanjali z varstvom osebnih podatkov. Za lažje poučevanje varstva osebnih podatkov v šolah pa smo pripravili tudi učno uro in posebna predavanja za učitelje, ki bodo izvedena v letu 2026.

Izobraževalni materiali, ki so nastali v okviru projekta PrivacyPRO, so objavljeni na posebni strani:

<https://www.ip-rs.si/varstvo-osebnih-podatkov/projekti/privacypro/vsebine-za-otroke/>.

Pomemben del projekta je tudi dvig ozaveščenosti o izdelanih materialih, zato Informacijski pooblaščenec skrbi za obveščanje javnosti prek medijev: o rezultatih projekta so poročali v različnih tiskanih in spletnih medijih, v radijskih oddajah in v podkastih¹³.

Kot vsako leto so bila izvedena tudi številna *pro bono* predavanja na področju varstva osebnih podatkov, in sicer je bilo v letu 2025 izvedenih 59 predavanj. Predstavniki Informacijskega pooblaščenca so aktivno sodelovali na konferencah, seminarjih in drugih dogodkih.

Ministrstva morajo kot eni najpomembnejših upravljavcev osebnih podatkov ter predlagateljev zakonodaje dobro poznati zahteve Splošne uredbe, zato je Informacijski pooblaščenec v marcu in aprilu 2025 izvedel dve ponovitvi izobraževanja o zakonodajnih ocenah učinka in varstvu osebnih podatkov pri pripravi predpisov ter ločeno izobraževanje za predstavnike Ministrstva za notranje zadeve in policije. Izobraževanja so bila zelo dobro obiskana, saj se jih je skupaj udeležilo več kot 250 udeležencev.



Družabna igra Misija IP: Postani varuh podatkov.

¹³ Seznam medijskih objav o rezultatih projekta PrivacyPRO je dostopen na povezavi: <https://www.ip-rs.si/varstvo-osebnih-podatkov/projekti/privacypro/medijske-objave>

3.6. MEDNARODNO SODELOVANJE

3.6.1 SODELOVANJE V EVROPSKEM ODBORU ZA VARSTVO PODATKOV

SPLOŠNO O DELOVANJU EDPB

Evropski odbor za varstvo podatkov (EDPB) 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. EDPB sestavljajo predstavniki nacionalnih nadzornih organov iz vseh držav članic EU, vključno s Slovenijo, ter Islandije, Lihtenštajna in Norveške, ki so del Evropske gospodarske skupnosti (EGS). Odbor predseduje dr. Anu Talus, predstojnica finskega nadzornega organa za varstvo podatkov, ob pomoči dveh podpredsednikov. Konec leta 2025 je bila za podpredsednico izvoljena slovenska informacijska pooblaščenka, dr. Jelena Virant Burnik, in sicer za petletni mandat.

Delovanje in usmeritve EDPB opredeljuje Strategija za obdobje 2024–2027¹⁴, konkretizira pa jo dvoletni Delovni program.¹⁵

Ključni dokument iz leta 2025, ki bo usmerjal delo EDPB v prihodnje, je t. i. helsinška izjava¹⁶, s katero so se članice EDPB zavezale, da si bodo še bolj prizadevale pomagati organizacijam za lažje doseganje skladnosti s Splošno uredbo, da bodo okrepile skladnost svojih nadzornih praks in še intenzivneje vključevale deležnike v delo EDPB.

Temeljna struktura EDPB je razdeljena na dva glavna dela, in sicer na plenarno zasedanje in na ekspertne podskupine. Predstavniki Informacijskega pooblaščenca so v letu 2025 aktivno sodelovali na 12 rednih plenarnih zasedanjih, na enem izrednem ter na enem strateškem sestanku na najvišji ravni v Helsinkih na Finskem. Ekspertne podskupine so bile ustanovljene posebej za obravnavo pomembnih tem, povezanih z varstvom osebnih podatkov. Zaposleni so se v letu 2025 udeležili več kot 170 sestankov v okviru 20 podskupin in drugih delovnih teles.

"Izvolitev za podpredsednico mi je v veliko čast. Veseli me, da bom tako lahko še aktivneje prispevala h krepitvi vloge evropskega odbora kot osrednje institucije za varstvo podatkov v Evropski uniji.

Sodelovanje med organi za varstvo osebnih podatkov in njihova odprta izmenjava mnenj sta namreč ključna za enotno razumevanje in usklajeno izvajanje Splošne uredbe o varstvu podatkov v EU.

Krajina digitalne regulacije se hitro spreminja, zato je pomembno, da evropski odbor ohranja vlogo regulatorja, ki razume medsebojni preplet zakonodajnih aktov, in tako tvorno prispeva k razpravam o regulaciji na evropski ravni."

Dr. Jelena Virant Burnik
Informacijska pooblaščenka

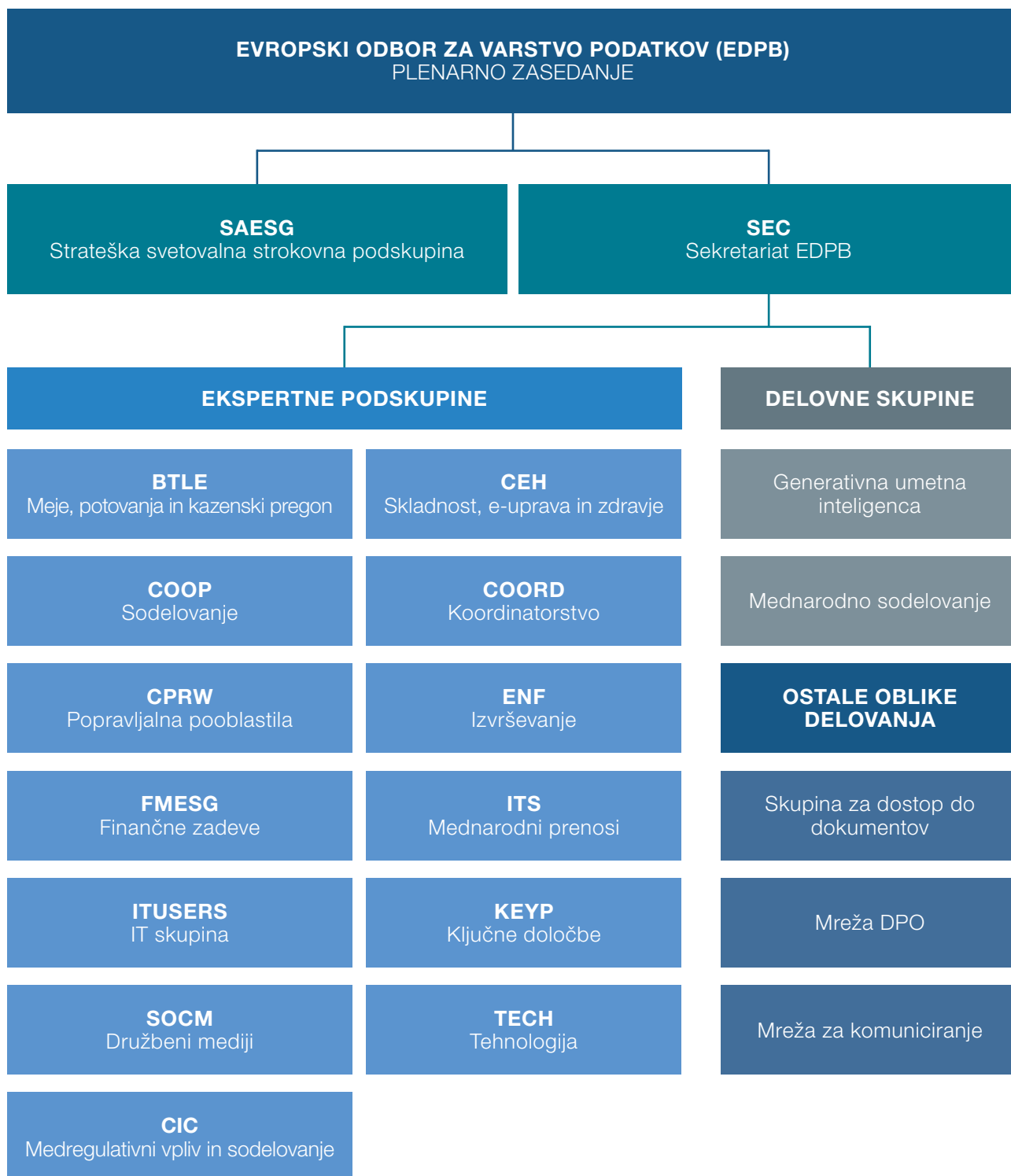


¹⁴ https://www.edpb.europa.eu/our-work-tools/our-documents/strategy-work-programme/edpb-strategy-2024-2027_sl

¹⁵ https://www.edpb.europa.eu/our-work-tools/our-documents/strategy-work-programme/edpb-work-programme-2024-2025_en

¹⁶ https://www.edpb.europa.eu/our-work-tools/our-documents/statements/helsinki-statement-enhanced-clarity-support-and-engagement_en

Struktura Evropskega odbora za varstvo podatkov.



Podskupine EDPB na strokovni ravni razpravljajo o različnih temah in pripravljajo osnutke gradiv za plenarno zasedanje, na katerem vodje nadzornih organov sprejmejo končne dokumente EDPB, predvsem:

- **smernice, priporočila, dobre prakse** in druge dokumente, ki predstavljajo splošne usmeritve za delo nadzornih organov in upravljavcev ter razlagajo pravice posameznikov,
- **obvezna mnenja,**
- **mnenja na predloge evropske zakonodaje,**
- **zavezujoče odločitve.**

EDPB izvaja tudi druge aktivnosti in nudi podporo nadzornim organom v drugih oblikah sodelovanja. Kot eno od zavez za podporo nadzornim organom in okrepljeno sodelovanje je EDPB vzpostavil **program podporne skupine strokovnjakov**¹⁷ za podporo pri razreševanju posebej zahtevnih pravnih in tehnoloških vprašanj ter za operativno podporo. V letu 2025 so bile v okviru programa zaključene in objavljene študije o digitalnem evru, o zavarovanju podatkov v okviru umetno-inteligenčnih sistemov, o tveganjih in ukrepih za zmanjševanje tveganj za varstvo zasebnosti v kontekstu velikih jezikovnih modelov, o nadzoru nad kompleksnimi umetno-inteligenčnimi algoritmi ter študija o čezmejnih primerih na področju dostopa do osebnih podatkov po 15. členu Splošne uredbe.

EDPB strategijo okrepljenega sodelovanja in spodbujanja skladnosti udejanja tudi z **usklajenimi skupnimi akcijami nadzora**, katerih glavni cilj je povečati ozaveščenost vseh deležnikov s skupnimi ukrepi in delovanjem na področju, ki ga EDPB za tisto leto izbere kot prednostno. Tema usklajenega skupnega nadzora za leto 2025 je bilo **izvajanje pravice do izbrisa osebnih podatkov po 17. členu Splošne uredbe**. V usklajeni nadzorni akciji je sodelovalo 32 nadzornih organov iz EU in EGP, med njimi aktivno tudi Informacijski pooblaščenec, ki se je leta 2025 osredotočil na izvrševanje pravice do izbrisa, ki jo zahtevajo potrošniki v sektorju deljene mobilnosti in javnega prevoza. V skupnem poročilu za leto 2025¹⁸ je EDPB opozoril na nekaj ključnih pomanjkljivosti, kot so odsotnost internih pravil in postopkov za obravnavo zahtev za izbris, pomanjkljivo usposabljanje zaposlenih, neustrezni in slabo obrazloženi razlogi za zavrnitev zahtev za izbris, težave z anonimizacijo idr.

SMERNICE, PRIPOROČILA, DOBRE PRAKSE

Smernice o psevdonimizaciji

V smernicah št. 01/2025¹⁹ je EDPB pojasnil, da je lahko psevdonimizacija učinkovit ukrep za varnost podatkov. Pogosto namreč za doseganje zastavljenih ciljev ni treba uporabiti surovih osebnih podatkov, saj zadostujejo predrugačeni, psevdonimizirani podatki. Slednjih pa ne smemo enačiti z anonimiziranimi podatki, saj gre še vedno za osebne podatke, pri katerih pa je za dostop do dejanske identitete posameznika potreben dodaten korak. Smernice EDPB poudarjajo vlogo psevdonimizacije pri zmanjševanju tveganj za kršitve varnosti podatkov ter pri izpolnjevanju načela vgrajenega in privzetega varstva osebnih podatkov, obravnavajo razliko med anonimizacijo in psevdonimizacijo opisujejo tehnične ukrepe proti nepooblaščenim (ponovni) določljivosti posameznikov ter vključujejo praktične primere uporabe tehnik psevdonimizacije za krepitev varstva osebnih podatkov v vsakodnevni praksi.

Smernice glede obdelave osebnih podatkov pri uporabi tehnologij za veriženje blokov

Smernice št. 02/2025²⁰ glede obdelave osebnih podatkov pri uporabi tehnologij za veriženje blokov (ang. *blockchain*) opisujejo nekatere ključne vidike skladnosti s Splošno uredbo za načrtovane dejavnosti obdelave. Vsebujejo pregled temeljnih načel te tehnologije in oceno različnih možnih arhitektur in njihovih posledic za obdelavo osebnih podatkov. Poleg tega pojasnjujejo, da je treba vloge in odgovornosti različnih akterjev, ki so udeleženi v obdelavi, povezani z verižnimi bloki, oceniti že med načrtovanjem obdelave in katere elemente je treba pri tem upoštevati.

Smernice glede prepleta Akta o digitalnih storitvah in Splošne uredbe

Smernice št. 3/2025²¹ glede prepleta Akta o digitalnih storitvah (DSA) in Splošne uredbe podrobno pojasnjujejo, da morajo ponudniki spletnih platform pri izvajanju vseh obveznosti iz DSA dosledno spoštovati temeljna načela varstva osebnih podatkov in zasebnosti. Sistemi za prijavo nezakonitih vsebin ne smejo zahtevati prekomerne identifikacije prijaviteljev, pri zaščiti mladoletnikov

¹⁷ https://www.edpb.europa.eu/support-pool-experts-spe-programme_en.

¹⁸ https://www.edpb.europa.eu/news/news/2026/edpb-identifies-challenges-hindering-full-implementation-right-erasure_en.

¹⁹ https://www.edpb.europa.eu/our-work-tools/documents/public-consultations/2025/guidelines-012025-pseudonymisation_en.

²⁰ https://www.edpb.europa.eu/our-work-tools/documents/public-consultations/2025/guidelines-022025-processing-personal-data_en.

²¹ https://www.edpb.europa.eu/our-work-tools/documents/public-consultations/2025/guidelines-32025-interplay-between-dsa-and-gdpr_en.

pa smernice izrecno prepovedujejo ciljno oglaševanje na podlagi profiliranja. Namesto invazivnega preverjanja starosti z osebnimi dokumenti EDPB spodbuja napredne metode ocenjevanja starosti, ki sledijo načelu najmanjšega obsega podatkov in preprečujejo neupravičeno sledenje. Smernice govorijo tudi uvedbi alternativnih priporočilnih sistemov brez profiliranja, ki omogočajo uporabo storitev brez sistematičnega sledenja vedenju uporabnikov. Dodatno je izpostavljena stroga prepoved oglasov na podlagi občutljivih podatkov, kot so zdravstveno stanje ter verska ali politična prepričanja.

Skupne smernice glede prepleta Akta o digitalnih trgih in Splošne uredbe

V skupnih smernicah EDPB in Evropske komisije glede prepleta Akta o digitalnih trgih (DMA) in Splošne uredbe²², prvih take vrste, instituciji ugotavljata različne namene in stične točke obravnavanih aktov. Medtem ko Splošna uredba varuje osebne podatke in zasebnost posameznikov, želi DMA urediti digitalni trg ter zagotoviti pošteno konkurenco velikih platform, medsebojno pa se dopolnjujeta glede ciljev in zaščite, ki jo zagotavljata posameznikom. Smernice se osredotočajo predvsem na določbe DMA, ki se v znatni meri prekrivajo s pravili Splošne uredbe, tako da med drugim naslavljajo določbe glede soglasja, prenosljivosti in dostopa do podatkov, anonimizacije, interoperabilnosti ter skladnosti. Smernice poudarjajo tudi pomen usklajenega sodelovanja med Evropsko komisijo kot edinim organom, pristojnim za izvrševanje DMA, ter pristojnimi nadzornimi organi za varstvo podatkov, pristojnimi za izvrševanje Splošne uredbe.

Priporočilo glede obveznega ustvarjanja uporabniških računov

Priporočilo št. 2/2025²³ podaja nasvete upravljavcem, pod kakšnimi pogoji lahko od uporabnikov spletnih mest za elektronsko trgovanje zahtevajo, da si ustvarijo uporabniški račun, preden lahko dostopajo do ponudb ali nakupujejo. Obvezni uporabniški račun je mogoče utemeljiti le za zelo omejen nabor namenov, npr. za naročniška razmerja ali dostop do ekskluzivnih ponudb. Najprimernejše je, da imajo uporabniki možnost bodisi prostovoljno ustvariti uporabniški račun bodisi nadaljevati nakup brez njega.

SVETOVANJE EVROPSKI KOMISIJI GLEDE ZAKONODAJNIH PREDLOGOV

Skupno mnenje o predlogu spremembe Splošne uredbe

Skupno mnenje EDPB in EDPS št. 01/2025²⁴ o predlogu uredbe o spremembi Splošne uredbe uvaja poenostavitve za nekatera podjetja (za mala in srednje velika podjetja ter za mala podjetja s srednje veliko tržno kapitalizacijo). Po predlogu bi omenjena podjetja z manj kot 750 zaposlenimi uživala olajšavo pri obveznosti vodenja evidenc dejavnosti obdelave, razen pri visokotveganih obdelavah. EDPB je poudaril, da so olajšave lahko koristne, vendar je zakonodajalca pozval k ponovnemu razmisleku o pragu zaposlenih in poudaril, da mora vodenje evidenc ostati obvezno za obdelavo posebnih vrst osebnih podatkov ter visokotvegane obdelave.

Mnenja o osnutkih sklepov Komisije o ustreznosti ravni varstva osebnih podatkov

EDPB je v letu 2025 izdal nekaj mnenj, v katerih se je opredelil do osnutkov sklepov Komisije glede ustreznosti ravni varstva osebnih podatkov, in sicer glede odločitve o podaljšanju sklepa o ustreznosti za Združeno kraljestvo in Brazilijo ter za prvi sklep o ustreznosti mednarodne organizacije – Evropske patentne organizacije.

MEHANIZMI SKLADNOSTI (ZAVEZUJOČA MNENJA IN ODLOČITVE)

Zavezujoča mnenja po 64. členu

Nadzorni organi v EU in EGS lahko zahtevajo zavezujoče mnenje EDPB glede potrditve seznama dejanj obdelave, za katere je potrebna ocena učinkovitosti, kodeksov ravnanja, meril za akreditacijo certifikacijskega organa, meril certificiranja, zavezujočih poslovnih pravil ter standardnih pogodbenih določil. V letu 2025 je EDPB skladno s prvim odstavkom 64. člena Splošne uredbe sprejel 29 mnenj.

V skladu z drugim odstavkom 64. člena, ki vsakemu nadzornemu odboru, predsedniku odbora ali Komisiji omogoča postaviti vprašanje o kateri koli zadevi splošne uporabe ali kateri koli zadevi z učinkom v več kot eni državi članici, odbor v letu 2025 ni izdal nobenega mnenja.

²² https://www.edpb.europa.eu/system/files/2025-10/joint_com-edpb_gls_interplay_dma_gdpr_for_public_consultation_en.pdf.

²³ https://www.edpb.europa.eu/our-work-tools/documents/public-consultations/2025/recommendations-2025-legal-basis-requiring_en.

²⁴ https://www.edpb.europa.eu/our-work-tools/our-documents/edpb-edps-joint-opinion/edpb-edps-joint-opinion-012025-proposal_en.

Postopki spora po 65. členu in nujni postopki po 66. členu

EDPB sprejema tudi zavezujoče odločitve v sporih 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 v primeru nespoštovanja mnenja odbora s strani posameznega nadzornega organa. EDPB pa lahko sprejme tudi odločitve o začasnih ukrepih v nujnih postopkih (po 66. členu Splošne uredbe), kadar je ukrepanje potrebno zaradi varstva pravic in svobod ščin posameznikov.

V letu 2025 tako kot leto prej ni bila sprejeta nobena odločitev, ki bi bila rezultat postopka spora pred EDPB po 65. členu ali nujnega postopka po 66. členu Splošne uredbe.

KLJUČNE SODBE SODIŠČA EU

Najodmevnejša sodba Sodišča EU v letu 2025 na področju varstva osebnih podatkov je bila izdana v zadevi *SRB proti EDPS* (C-413/23 P). Sodišče EU je presodilo, da psevdonimizirani podatki ne predstavljajo nujno v vseh primerih osebnih podatkov. Če so podatki psevdonimizirani na način, ki drugim (razen upravljavcu) dejansko preprečuje identifikacijo posameznika, na katerega se podatki nanašajo, tako da ta zanje ni več določljiv, takšni podatki morda (in v kontekstu obravnavanega primera) niso osebni podatki. Sodišče je opozorilo, da je treba pri ugotavljanju, ali je posameznik določljiv, upoštevati vse ukrepe, za katere je razumno verjetno, da bi jih bilo mogoče uporabiti za njegovo neposredno ali posredno identifikacijo. Glede zahtev po preglednosti je sodišče odločilo, da mora upravljavec tudi v primerih, ko psevdonimizirani podatki niso osebni podatki, v svoji politiki zasebnosti vseeno zagotoviti informacije o razkritju takšnih psevdonimiziranih podatkov tretjim osebam.

Sklicujoč se na to sodbo je Evropska komisija novembra 2025 predstavila predlog sprememb Splošne uredbe o varstvu osebnih podatkov v zakonodajnem paketu z nazivom Digitalni omnibus. Predlog je nemudoma začel obravnavati Evropski odbor za varstvo podatkov, delo na zakonodajni spremembi pa se je nadaljevalo v letu 2026.

3.6.2 SODELOVANJE V DRUGIH NADZORNIH TELESIH EVROPSKE UNIJE

Informacijski pooblaščenec je leta 2025 na ravni EU aktivno sodeloval v treh delovnih telesih, ki se ukvarjajo z nadzorom nad izvajanjem varstva osebnih podatkov v okviru velikih informacijskih sistemov EU, in sicer:

- na koordinacijskih sestankih Odbora za usklajeni nadzor (*Coordinated Supervision Committee – CSC*),
- na koordinacijskih sestankih EDPS in nacionalnih organov za varstvo osebnih podatkov za nadzor nad CIS,
- na koordinacijskih sestankih EDPS in nacionalnih organov za varstvo osebnih podatkov za nadzor nad Eurodac.

V letu 2025 je bil v okviru Odbora za usklajeni nadzor sprejet vodič o preverjanju dnevnikov obdelav v Schengenskem informacijskem sistemu (SIS) ter poročilo o SIS statističnih podatkih v zvezi z uresničevanjem pravic posameznikov, na katere se nanašajo osebni podatki. V okviru nadzora nad obdelavo osebnih podatkov v CIS je bila sprejeta posodobitev splošnega dela vodiča za izvrševanje pravice posameznikov do dostopa do osebnih podatkov.

Predstavnik Informacijskega pooblaščenca je februarja 2025 sodeloval pri evalvaciji izvajanja schengenskega pravnega reda na področju varstva podatkov v Romuniji.

V marcu 2025 je bila v Republiki Sloveniji uspešno izvedena evalvacija izvajanja schengenskega pravnega reda, katere sestavni del je tudi področje varstva osebnih podatkov. Predstavnik Informacijskega pooblaščenca je opravljal vlogo nacionalnega koordinatorja za to področje.

3.6.3 SODELOVANJE V DRUGIH MEDNARODNIH TELESIH

POSVETOVALNI ODBOR T-PD

V letu 2025 je predstavnik Informacijskega pooblaščenca sodeloval v Posvetovalnem odboru Sveta Evrope, ustanovljenem na podlagi Konvencije Sveta Evrope o varstvu posameznikov glede na avtomatsko obdelavo osebnih podatkov (Konvencija št. 108), znanem kot Odbor T-PD. Odbor se je junija in novembra sestal na plenarnih zasedanjih, na katerih je obravnaval stanje glede pristopanja držav h konvenciji ter postopek sprejema Protokola

o spremembi te konvencije (t. i. Konvencija 108+). Kot vsako leto je Odbor obravnaval poročila o mednarodnem in globalnem sodelovanju Sveta Evrope na področju varstva osebnih podatkov ter poročila nadzornih organov držav članic Sveta Evrope o novostih in dosežkih na tem področju.

Posebna pozornost je bila namenjena aktualnim temam, kot so varstvo podatkov v kontekstu velikih jezikovnih modelov ter čezmejnih prenosov osebnih podatkov, vključno z uporabo vzorčnih pogodbenih klavzul. Odbor je sprejel program dela za obdobje 2026–2029.

Pomemben dosežek v letu 2025 je bil sprejem smernic o splošnih načelih iz 11. člena posodobljene konvencije. Odbor je nadaljeval s pripravo smernic o varstvu podatkov v nevroznanosti ter podelil nagrado Stefano Rodotà za izjemne prispevke na področju varstva podatkov.

SVETOVNA SKUPŠČINA ZA ZASEBNOST

Svetovna skupščina za zasebnost (ang. *Global Privacy Assembly – GPA*²⁵), ki povezuje prizadevanja več kot 130 nadzornih organov za varstvo zasebnosti in osebnih podatkov z vsega sveta, se je v letu 2025 posvečala zlasti izzivom, ki jih prinaša umetna inteligenca, s psevdonimizacijo in sintetičnimi podatki ter z izzivi sodelovanja nadzornih organov pri čezmejnih prenosih osebnih podatkov. Delo konference vodi izvršni odbor, kateremu predseduje predstavnik kanadskega nadzornega organa. Podporo delovanju skupščine in njenih delovnih skupin zagotavlja sekretariat, ki ga zagotavlja filipinski nadzorni organ, od leta 2022 pa morajo skladno s sprejeto resolucijo skupščine članice plačevati letno članarino.

Med pomembnejšimi resolucijami, sprejetimi na zadnji konferenci leta 2025, ki je potekala v Koreji, so resolucija o zbiranju, uporabi in razkrievanju osebnih podatkov za treniranje modelov umetne inteligence, resolucija o človeškem nadzoru nad odločitvami sistemov umetne inteligence ter resolucija o digitalnem izobraževanju za vključujoče digitalno državljanstvo.

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*²⁶; t. i. *Berlin group*) je ena najdlje delujočih mednarodnih skupin na področju varstva osebnih podatkov, ki že od leta 1983 združuje predstavnike informacijskih pooblaščenec ter organov za varstvo osebnih podatkov in zasebnosti z vsega sveta. Sprejeta mnenja skupine predstavljajo pomemben prispevek k mednarodni konferenci informacijskih pooblaščenec, usmerjajo delo nadzornih organov in regulatorjev ter veljajo za pomembna priporočila razvijalcem, ponudnikom in uporabnikom različnih tehnoloških rešitev ter regulatorjem in zakonodajalcem.

V letu 2025 je delovna skupina IWGDPT sprejela delovni dokument o globalnih preferenčnih signalih in sorodnih tehnologijah, delovni dokument o zaupanja vrednem računalništvu v oblaku (ang. *Confidential Cloud Computing*) ter delovni dokument o nevrotehnologijah.

Delovni dokument o globalnih preferenčnih signalih in sorodnih tehnologijah se nanaša na tehnične vidike sporočanja upravljavcem spletnih strani, da posameznik ne želi deljenja ali prodaje svojih podatkov. Delovni dokument o zaupanja vrednem računalništvu v oblaku pa se ukvarja z izzivi varovanja podatkov med samo uporabo storitev računalništva v oblaku, kar je precej težje dosegljivo in na nižji stopnji razvoja kot varnost podatkov med hrambo ali med prenosom.

Delovni dokument o nevrotehnologijah²⁷ predstavi značilnosti in načine delovanja sodobnih nevrotehnologij, tveganja, ki jih slednje predstavljajo za varovanje naše zasebnosti, ter podaja priporočila za njihove razvijalce, regulatorje in uporabnike. Zasebnost tradicionalno pojmuje z občutkom nadzora nad svojim prostorom, komunikacijo in podatki, medtem ko je zasebnost naših misli in kognitivnih procesov nekaj, kar dojemamo kot varno pred zaznavo in posegi iz zunanjega okolja. Napredek na področju nevroznanosti in nevrotehnologij pa počasi omogoča večjo dostopnost do naših kognitivnih podatkov ter s tem dobesedno

²⁵ <https://globalprivacyassembly.com>.

²⁶ Spletna stran IWGDPT: <https://www.bfdi.bund.de/EN/Fachthemen/Gremienarbeit/Berlin-Group/Berlin-Group-node.html>.

²⁷ <https://www.ip-rs.si/go?u=external%3Awww.bfdi.bund.de%2FSharedDocs%2FDownloads%2FEN%2FBerlin-Group%2F20250515-WP-Neurotechnologien.html%3Fnn%3D251944>.

pod vprašaj postavlja zasebnost naših misli in spomina. Nevrotehnologije odpirajo številna pravna in etična vprašanja ter se že začenejo uporabljati na primer na področju nadzora nad delavci v varnostno kritičnih situacijah, pri uporabi nosljivih naprav, kot so pametna očala in sistemi za navidezno resničnost, ter na področju komunikacije s pacienti.

3.6.4. DRUGO MEDNARODNO SODELOVANJE

INITIATIVE 20i7

Septembra 2025 so se nadzorni organi za varstvo osebnih podatkov iz Hrvaške, Severne Makedonije, Črne gore, Kosova in Slovenije srečali na Ptujju na sedmem 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 teh držav EU.

Na zasedanju so izmenjali izkušnje glede harmonizacije nacionalnih predpisov z evropskim okvirom varstva osebnih podatkov, implementacije nacionalnih strategij za varstvo podatkov, identifikacije kršitev varnosti podatkov z modernimi platformami, uporabe biometrijskih kamer na javnih površinah, povezovanja področij varstva podatkov in umetne inteligence ter soočanja z novimi tehnologijami. Nadzorni organi so na zasedanju sprejeli skupno izjavo²⁸, v kateri so poudarili pomen finančno, politično in strokovno neodvisnih nadzornih organov za varstvo osebnih podatkov pri varovanju temeljnih pravic in svoboščin.

Predstojniki nadzornih organov bodo nadaljevali tako z letnimi srečanji kakor tudi z bilateralnimi sodelovanji in sodelovanjem, ko se pojavi potreba po skupnem ukrepanju glede ozaveščanja javnosti in drugih deležnikov ali potreba po izvajanju nadzornih ukrepov. Informacijski pooblaščenec je v maju 2025 na študijskem obisku gostil predstavnike nadzornega organa za varstvo osebnih podatkov s Kosova in jim predstavil izkušnje na področju izvajanja nadzornih postopkov.



Zasedanje Initiative 20i7, Ptuj, 8.–10. september 2025.

²⁸ <https://www.ip-rs.si/go?u=external%3Awww.bfdi.bund.de%2FSharedDocs%2FDownloads%2FEN%2FBerlin-Group%2F20250515-WP-Neurotechnologien.html%3Fnn%3D251944>



Drugo srečanje srednjeevropskih organov za varstvo osebnih podatkov, Budimpešta, 15.–17. september 2025.

POBUDA O SODELOVANJU SREDNJEEVROPSKIH NADZORNIH ORGANOV ZA VARSTVO OSEBNIH PODATKOV

Od 15. do 17. septembra 2025 je v Budimpešti potekalo drugo srečanje srednjeevropskih organov za varstvo osebnih podatkov iz Slovenije, Avstrije, Madžarske, Češke in Slovaške. Namen te pobude je vzpostaviti tesnejše sodelovanje med sodelujočimi organi ter izmenjava dobrih praks pri obravnavi sorodnih tem s področja varstva osebnih podatkov. Na delovnem srečanju so si predstavniki izmenjali informacije o novih načinih in mehanizmih (so)delovanja in izvrševanja nadzora v luči naraščajočih pristojnosti v hitro spreminjajoči se digitalni krajini, izrekanju glob po Splošni uredbi o varstvu podatkov in drugih izzivih pri delovanju nadzornih organov za varstvo podatkov. Informacijska pooblaščenka je drugi dan srečanja sodelovala na mednarodni konferenci ob 30. obletnici delovanja madžarskega nadzornega organa za varstvo osebnih podatkov, in sicer s prispevkom o gradnji mostov med varstvom osebnih podatkov, dostopom do informacij javnega značaja in nadzorom trga umetne inteligence.

3.6.5 IZVAJANJE PRISTOJNOSTI PO DRUGIH AKTIVIH DIGITALNE ZAKONODAJE

Evropska unija je v prizadevanju za varnejše in bolj konkurenčno digitalno okolje sprejela tudi paket digitalne zakonodaje, ki Informacijskemu pooblaščenцу podeljuje nove pristojnosti oz. povečuje obseg izvajanja obstoječih pristojnosti. Republika Slovenija je do konca leta 2025 v svoj pravni red prenesla izvajanje Akta o digitalnih storitvah (zakon o njegovem izvajanju v Sloveniji velja od 13. 4. 2024) in Akta o upravljanju podatkov (zakon o njegovem izvajanju velja od 18. 12. 2024). Na implementacijo v sklopu digitalne zakonodaje EU, kjer je to potrebno, čakajo še Akt o podatkih, Direktiva o platformnem delu in Uredba o transparentnosti in ciljanju v političnem oglaševanju. Pri prenosu vseh navedenih aktov v slovenski pravni red ima Informacijski pooblaščenec posvetovalno vlogo.

V povezavi z Aktom o digitalnih storitvah Informacijski pooblaščenec v letu 2025 ni vodil nobenega nadzornega ali prekrškovnega postopka, je pa izvedel številne aktivnosti, ki so se osredotočale na svetovanje, preventivo, promocijo in oblikovanje po-

litik. Informacijski pooblaščenec je opravil pregled spletne platforme, za katero v Sloveniji veljajo poglobljene zahteve Akta o digitalnih storitvah, saj med drugim cilja tudi na mladoletnike. Sodelovali smo tudi v usklajenem pregledu združenja Global Privacy Enforcement Network (GPEN), v okviru katerega smo z vidika Splošne uredbe o varstvu podatkov in 28. člena DSA pregledali 17 spletnih mest in aplikacij, ki so priljubljene med otroki v Sloveniji. Glede zaščite mladoletnikov in na splošno varne uporabe digitalnih storitev je Informacijski pooblaščenec v okviru svoje posvetovalne dejavnosti izdal številna mnenja, pripravil je izobraževalne materiale v okviru projekta PrivacyPRO (več o tem v poglavju 3.5.4) ter obveščal javnost o mednarodnih novostih, kot je sprejem izjave EDPB o preverjanju starosti in smernic Evropske komisije za zaščito mladoletnikov. Informacijski pooblaščenec je aktivno sodeloval pri pripravi smernic EDPB o medsebojnem vplivanju Akta o digitalnih storitvah in Splošne uredbe o varstvu podatkov ter prevzel koordiniranje podskupine EDPB o družbenih omrežjih, v okviru katere se obravnavajo vprašanja, povezana tudi z Aktom o digitalnih storitvah.

Informacijski pooblaščenec je bil intenzivno vpet tudi v posvetovalne aktivnosti glede priprave osnutkov zakonov o izvajanju aktov digitalne zakonodaje; v letu 2025 je bilo posebej veliko aktivnosti na področju implementacije Uredbe o transparentnosti političnega oglaševanja. Na nacionalni ravni se je Informacijski pooblaščenec udeležil več usklajevalnih in strokovnih sestankov z nekaterimi soredulatorji (Agencijo za komunikacijska omrežja in storitve ter Tržnim inšpektoratom) ter resornim Ministrstvom za digitalno preobrazbo.

Zaposleni pri Informacijskem pooblaščenecu razvoj področja digitalne zakonodaje spremljajo tudi v okviru EDPB, ki je v letu 2025 ustanovil posebno podskupino za medregulativni vpliv in sodelovanje, ki predstavlja tudi platformo za izmenjavo strokovnega znanja in informacij, ter je namenjena spodbujanju dobrih praks na področju medregulativnega upravljanja in sodelovanja. V okviru podskupine za skladnost, e-upravo in zdravje so zaposleni sodelovali pri pripravi na sestanke Evropskega odbora za inovacije (ki obravnava zakonodajo, kot je Akt o podatkih, področje podatkovnih prostorov itd.) ter v razpravi o prihodnosti digitalne zakonodaje in podatkovne ekonomije.

Posebno pozornost smo posvetili tudi izobraževanju zaposlenih na temo digitalne zakonodaje v okviru izmenjav znanja in dodatnega izobraževanja s strani zunanjih ponudnikov; posebna pozornost je bila posvečena Aktu o upravljanju podatkov in Aktu o digitalnih storitvah.



4 UMETNA INTELIGENCA

ZA NAPREDEK Z ODGOVORNO RABO UMETNE INTELIGENCE

4.1 REGULATORNI OKVIR NADZORA NAD SISTEMI UI V SKLADU Z AKTOM O UMETNI INTELIGENCI IN ZIUHPUI

Junija 2024 je EU s sprejemom Akta o umetni inteligenci dobila prvi celovit pravni okvir o umetni inteligenci na svetu. Namen Akta o umetni inteligenci je izboljšati delovanje notranjega trga z določljivijo enotnega pravnega okvira za razvoj, dajanje na trg, dajanje v uporabo ter uporabo sistemov UI, zagotoviti visoko raven varovanja zdravja, varnosti in temeljnih pravic ter podpirati inovacije. Akt o umetni inteligenci temelji na kategorizaciji sistemov UI glede na tveganja, ki jih predstavljajo za temeljne pravice, zdravje in varnost, ter določitev obveznosti za posamezne kategorije sistemov UI. Najbolj tvegani sistemi UI so prepovedani, sistemi UI, ki predstavljajo visoko stopnjo tveganja, so podvrženi številnim zahtevam, za določene sisteme UI veljajo obveznosti glede preglednosti, opredeljene pa so tudi obveznosti ponudnikov modelov UI za splošne namene. Poleg tega Akt ureja ukrepe za spremljanje in nadzor trga ter ukrepe za podporo inovacijam s posebnim poudarkom na malih in srednje velikih podjetjih.

Akt o umetni inteligenci na nacionalni ravni dopolnjuje ZIUHPUI, ki ga je Državni zbor sprejel 23. 10. 2025 in je začel veljati 21. 11. 2025. ZIUHPUI v prvi vrsti ureja pristojne nacionalne organe za izvajanje in nadzor nad obveznostmi Akta o umetni inteligenci ter določa kazni za kršitve Akta.

V skladu s 6. členom ZIUHPUI v Sloveniji nadzor nad določbami Akta o umetni inteligenci izvaja pet organov za nadzor trga, poleg Informacijskega pooblaščenca še Banka Slovenije, Agencija za zavarovalni nadzor, Tržni inšpektorat (TIRS) in Agencija za komunikacijska omrežja in storitve (AKOS); slednja bo delovala tudi kot enotna kontaktna točka. Informacijski pooblaščenec izvaja nadzor na področjih, ki so tesno povezana s tveganji za temeljne pravice in svoboščine. Pristojen je za nadzor nad:

1. prepovedanimi praksami UI;
2. visoko tveganimi sistemi iz Priloge III, in sicer iz:
 - 1. točke (biometrija),
 - 3. točke (izobraževanje in poklicno usposabljanje),
 - 6. točke (preprečevanje, odkrivanje in preiskovanje kaznivih dejanj),
 - 7. točke (migracije, azil in meje) in
 - 8. točke (pravosodje in demokratični procesi).

4.2 NADZOR V LETU 2025

ZIUHPUI, ki je Informacijskega pooblaščenca določil kot enega izmed organov za nadzor trga na področju UI, je začel veljati 21. 11. 2025. S tem dnem je Informacijski pooblaščenec dobil pooblastila za nadzor nad delom obveznosti iz Akta o umetni inteligenci, in sicer nad prepovedanimi praksami UI. Obveznosti za operaterje visoko tveganih sistemov UI se v letu 2025 še niso uporabljale, zato tudi ni bila podana pristojnost za nadzor s strani Informacijskega pooblaščenca. Zaradi kratkega obdobja veljavnosti nacionalnega zakona v letu 2025 in nadzora zgolj nad najbolj tveganimi praksami UI, ki morajo kumulativno izpolnjevati številne pogoje in so posledično relativno redke, Informacijski pooblaščenec v letu 2025 ni uvedel nobenega postopka inšpekcijskega nadzora nad prepovedanimi praksami UI niti nobenega prekrškovnega postopka.

4.3 MNENJA NA ZAKONODAJO

V letu 2025 je Informacijski pooblaščenec na področju umetne inteligence pripravil 9 mnenj ali stališč, ki so se nanašala na predlog Zakona o izvajanju Uredbe (EU) o določitvi harmoniziranih pravil o umetni inteligenci (UI) in predlog Uredbe Evropskega parlamenta in o spremembi uredb (EU) 2024/1689 in (EU) 2018/1139 glede poenostavitve izvajanja harmoniziranih pravil o umetni inteligenci (v nadaljevanju: Digitalni omnibus za UI), ki ga je z namenom poenostavitve Akta o umetni inteligenci 19. 11. 2025 predstavila Evropska Komisija.

Šest mnenj Informacijskega pooblaščenca se je nanašalo na predlog ZIUODHPUI. Informacijski pooblaščenec se je med drugim zavzel za to, da prevzame nadzor nad nekaterimi visoko tveganimi sistemi UI na področjih, ki so tesno povezana s tveganji za temeljne pravice posameznikov, predvsem v šolstvu, opozoril je na nekatere nejasnosti glede ureditve sankcioniranja ob sočasni uporabi določb ZIUODHPUI in Zakona o prekrških ter se zavzel za jasnejšo razdelitev vlog organov za nadzor trga pri vzpostavitvi in delovanju regulativnega peskovnika. Izpostavil je potrebo po okrepljenem sodelovanju in usklajevanju med organi za nadzor trga, tudi v obliki periodičnih sestankov, na katerih bi se vseh pet organov za nadzor trga posvetovalo z namenom usklajenega delovanja na nacionalni ravni ter na ravni EU (predvsem v okviru delovanja v podskupinah Evropskega odbora za umetno inteligenco). Zavzel se je za ohranitev visoke ravni varstva osebnih podatkov, med drugim tudi z nenaklonjenostjo uvedbi nacionalne izjeme, ki bi dopuščala uporabo sistemov UI za biometrično identifikacijo fizičnih oseb na daljavo v realnem času v javno dostopnih prostorih za namene preprečevanja, odkrivanja in preiskovanja kaznivih dejanj. Tovrstni sistemi UI posebej hudo posegajo v pravice in svoboščine posameznikov, vplivajo lahko na zasebno življenje velikega dela prebivalstva, vzbujajo občutek stalnega nadzora ter posredno odvrčajo od uresničevanja drugih temeljnih pravic in svoboščin, na primer svobode zbiranja. Poleg tega je Informacijski pooblaščenec večkrat poudaril nujnost čimprejše ureditve ustreznega financiranja organov za nadzor trga, predvsem zato, da bi bilo možno pridobivanje in zadržanje kadra z ustreznimi znanji na tem področju.

Informacijski pooblaščenec je pripravil tudi tri mnenja glede predloga Digitalnega omnibusa za UI. Predvsem se je zavzel za bolj predvidljiv rok za začetek uporabe obveznosti operaterjev visoko tveganih sistemov UI in za ohranitev visoke ravni varstva temeljnih pravic in svoboščin posameznikov, vključno z varstvom osebnih podatkov. Glede slednjih je izpostavil problematiko širjenja pravnih podlag za obdelavo osebnih podatkov in občutljivih podatkov v kontekstu sistemov UI. Obdelava občutljivih podatkov je sicer dopustna le izjemoma, zato Informacijski pooblaščenec vztraja pri uveljavitvi strogih omejitev in dopustitvi obdelave občutljivih podatkov zgolj v primeru, ko je to nujno za odpravljanje pristranskosti v sistemih UI.

4.4 PREVENTIVNE AKTIVNOSTI

Regulacija UI na podlagi Akta o umetni inteligenci in ZIUODHPUI predstavlja novo področje delovanja Informacijskega pooblaščenca, ki se po eni strani tesno prepleta v obstoječima področjema njegovega delovanja, predvsem z varstvom osebnih podatkov, po drugi strani pa gre za popolnoma drugačen pravni režim, ki združuje elemente urejanja varnosti proizvodov in varstva temeljnih pravic. Ker gre za popolnoma nov in izredno kompleksen pravni okvir, zavezanci čim prej potrebujejo vsaj osnovne usmeritve glede zagotavljanja skladnosti z Aktom o umetni inteligenci. V ta namen smo v letu 2025 skupaj z Agencijo za komunikacijska omrežja Republike Slovenije pripravili odgovore na najpogostejša vprašanja glede Akta o umetni inteligenci in ZIUODHPUI. Odgovori so bili v začetku leta 2026 objavljeni na spletnih straneh obeh organov za nadzor trga, vsebujejo pa tudi povezave na smernice in druga gradiva, ki jih pripravlja Urad za UI. Zavezanci lahko tako na enem mestu najdejo napotke za prve korake k zagotavljanju skladnosti z Aktom o umetni inteligenci, natančnejše usmeritve glede posameznih vprašanj pa so dostopne na dodanih povezavah.

V letu 2025 smo tudi prenovili in posodobili spletno stran Informacijskega pooblaščenca, da odseva novo strukturo področij njegovega delovanja: podstranema, namenjenima varstvu osebnih podatkov in dostopu do informacij javnega značaja, smo dodali podstran, namenjeno umetni inteligenci, na kateri javnost lahko najde odgovore na najpogostejša vprašanja, koristne povezave na drugo gradivo in osnovne informacije o prijavi kršitev, objavljena pa so tudi mnenja in smernice.

Informacijski pooblaščenec bo, tako kot na drugih dveh področjih svojega delovanja, tudi na področju umetne inteligence nudil podporo zavezancem preko telefonskega svetovanja in z mnenji, ki jih izda na posamezna vprašanja, ki so mu posredovana pisno. Vsa mnenja bodo sproti objavljena na spletni strani – konec leta 2025 je Informacijski pooblaščenec prejel prvo zaprosilo za mnenje na področju Akta o umetni inteligenci in mnenje je že objavljeno.

4.5 MEDNARODNO SODELOVANJE

4.5.1 EVROPSKI ODBOR ZA UMETNO INTELIGENCO

Na podlagi Akta o umetni inteligenci je bil leta 2024 ustanovljen Evropski odbor za umetno inteligenco (*European Artificial Intelligence Board*, v nadaljevanju *AIB*). V AIB sodeluje po en predstavnik vsake države članice, ki v odboru sodeluje največ tri leta z možnostjo enkratnega podaljšanja. Republiko Slovenijo v Evropskem odboru za umetno inteligenco od ustanovitve zastopa državna sekretarka na Ministrstvu za digitalno preobrazbo, dr. Aida Kamišalić Latifć. V letu 2025 se je AIB sestal štirikrat.

Naloga AIB je, da svetuje in pomaga Komisiji in državam članicam pri zagotavljanju dosledne in učinkovite uporabe Akta o umetni inteligenci, med drugim prispeva k usklajevanju med pristojnimi nacionalnimi organi, zbira in izmenjuje tehnično in regulativno strokovno znanje in najboljše prakse, svetuje, izdaja priporočila in pisna mnenja, prispeva k pripravi smernic na področju Akta o umetni inteligenci ter spodbuja oblikovanje skupnih meril in skupnega razumevanja ustreznih konceptov Akta o umetni inteligenci.

V okviru AIB sta ustanovljeni dve stalni podskupini, ki zagotavljata platformo za sodelovanje in izmenjavo med organi za nadzor trga, lahko pa AIB ustanovi tudi druge bodisi stalne bodisi začasne podskupine za proučitev posebnih vprašanj. V letu 2025 je delovalo 12 podskupin AIB:

- Usmerjevalna skupina za umetno inteligenco za splošne namene,
- Delovna skupina za medsebojno delovanje Akta o umetni inteligenci z drugo zakonodajo Unije,
- Delovna skupina za umetno inteligenco v finančnih storitvah,
- Delovna skupina za ekosistem inovacij na področju umetne inteligence,
- Delovna skupina za regulativne peskovnike za umetno inteligenco,
- Delovna skupina za visoko tvegane sisteme UI iz Priloge III,
- Delovna skupina za preprečevanje, preiskovanje, odkrivanje in pregon kaznivih dejanj ter varnost,
- Delovna skupina za prepovedi,
- Delovna skupina za pregled poslovnika,
- Delovna skupina za standarde,

- Delovna skupina za medsebojno delovanje Akta o umetni inteligenci in MDR/IVDR,
- Stalna podskupina za nadzor trga (ADCO).

Glede na pristojnosti Informacijskega pooblaščenca na podlagi ZIUODHPUI so bili predstavniki Informacijskega pooblaščenca vključeni v šest podskupin AIB: v Usmerjevalno skupino za umetno inteligenco za splošne namene, Delovno skupino za medsebojno delovanje Akta o umetni inteligenci z drugo zakonodajo Unije, Delovno skupino za regulativne peskovnike za umetno inteligenco, Delovno skupino za visoko tvegane sisteme UI iz Priloge III, Delovno skupino za preprečevanje, preiskovanje, odkrivanje in pregon kaznivih dejanj ter varnost in Delovno skupino za prepovedi. Delovne skupine so se sestajale na rednih virtualnih sestankih ter na dodatnih delavnicah, ki so bile organizirane za usmerjeno razpravo o določenih vprašanjih oz. področjih. Predstavniki Informacijskega pooblaščenca so se udeležili 44 sestankov in delavnic podskupin AIB in delovnih skupin za pripravo kodeksov prakse.

O delu v podskupinah, napredku glede posameznih dokumentov in časovnici za njihov sprejem ter o stališčih ostalih držav članic so predstavniki Informacijskega pooblaščenca četrtletno obveščali predstavnico Slovenije v AIB. Ker predstavniki Informacijskega pooblaščenca niso edini predstavniki Slovenije v navedenih skupinah, so pred sestanki, predvsem pa pred posredovanjem pisnih komentarjev na dokumente, sodelovali in se usklajevali z ostalimi predstavniki v navedenih podskupinah z namenom enotnega predstavljanja države članice na ravni EU.

Komisija je v letu 2025 sprejela naslednje smernice, v postopku sprejemanja katerih se je posvetovala tudi z Evropskim odborom za umetno inteligenco:

- *Smernice Komisije o prepovedanih praksah umetne inteligence*: v smernicah je Komisija podrobneje pojasnila, kateri pogoji morajo biti izpolnjeni, da gre za prepovedano prakso v skladu s 5. členom Akta o umetni inteligenci; podala je tudi usmeritve glede nekaterih splošnih vprašanj o uporabi in izvajanju Akta, na primer na katerih področjih se Akta o umetni inteligenci ne uporablja in na kakšen način medsebojno vpliva na drugo zakonodajo EU.
- *Smernice Komisije o definiciji umetne inteligence*: podrobneje opredeljujejo posamezne elemente definicije pojma sistema umetne inteligence kot temeljnega pojma Akta o umetni inteligenci.

- *Smernice Komisije o obsegu obveznosti ponudnikov modelov UI za splošne namene*: podrobneje opredeljujejo, kdaj model šteje kot model UI za splošne namene, kdaj gre za ponudnika takšnega modela in pod katerimi pogoji so ponudniki izvzeti iz spoštovanja določenih obveznosti, ter pojasnjujejo nadzorna pooblastila Urada za umetno inteligenco in opredeljujejo posledice pristopa k potrjenim kodeksom ravnanja.

Poleg tega je bil 10. julija 2025 objavljen *Kodeks prakse za umetno inteligenco za splošne namene (General Purpose AI Code of Practice)*, prostovoljno orodje za pomoč pri zagotavljanju skladnosti ponudnikov modelov UI za splošne namene. V postopek sprejemanja Kodeksa prakse je bilo vključenih več kot 1000 deležnikov, vodili pa so ga neodvisni strokovnjaki. Tako Komisija kot AIB sta potrdila ustreznost Kodeksa prakse za umetno inteligenco za splošne namene.

4.5.2 NEFORMALNA SKUPINA PRISTOJNIH ORGANOV ZA NADZOR NAD SISTEMI UI (CA@AI)

Predstavniki Informacijskega pooblaščenca so v letu 2025 sodelovali tudi v neformalnem združenju pristojnih organov za nadzor nad sistemi UI. Gre za neformalno združenje, nastalo na pobudo nizozemskega organa za digitalno infrastrukturo, ki združuje različne evropske organe, ki so bodisi že pristojni za nadzor nad sistemi umetne inteligence (na primer organi za nadzor trga in organi za varstvo osebnih podatkov) bodisi bodo to postali na podlagi Akta o umetni inteligenci. Skupina se srečuje na rednih mesečnih sestankih, na katerih so obravnavane splošne teme, povezane z nadzorom sistemov UI, ter v okviru podskupin, ki so namenjene obravnavi specifičnih vprašanj, na primer prepovedanih praks, regulativnih peskovnikov in resnih incidentov. Večina sestankov je organiziranih virtualno, v letu 2025 pa sta bila organizirana tudi dva tridnevna fizična sestanka, ki se ju je udeležila tudi predstavnica Informacijskega pooblaščenca.



ODGOVORNA UREDNICA:

dr. Jelena Virant Burnik, informacijska pooblaščenka

AVTORJI BESEDIL:

dr. Urban Brulc, samostojni svetovalec pooblaščenca

Jasna Duralija, svetovalka pooblaščenca I

Tina Ivanc, svetovalka pooblaščenca za varstvo osebnih podatkov

Alenka Jerše, namestnica informacijske pooblaščenke

mag. Eva Kalan Logar, namestnica informacijske pooblaščenke

Nina Kelhar, študentka

mag. Kristina Kotnik Šumah, namestnica informacijske pooblaščenke

mag. Polona Merc, vodja mednarodnega sodelovanja

Blaž Pavšič, strokovni vodja nadzora

Manja Resman, svetovalka pooblaščenca I

Matej Sironič, svetovalec pooblaščenca za varstvo osebnih podatkov

dr. Pika Šarf, vodja področja umetne inteligence

mag. Andrej Tomšič, namestnik informacijske pooblaščenke

Barbara Repovš, svetovalka pooblaščenca za odnose z javnostmi

Lidija Perčič, svetovalka pooblaščenca za mednarodne odnose

OBLIKOVANJE:

Matjaž Hančič

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 2026



Informacijski pooblaščenec Republike Slovenije

Dunajska cesta 22, 1000 Ljubljana

www.ip-rs.si, gp.ip@ip-rs.si, Ljubljana, maj 2026