Na podlagi Uredbe (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 (v nadaljevanju: Uredba) in na podlagi 65. člena Statuta Zbornice za arhitekturo in prostor Slovenije (Uradni list RS, št. 81/18), je Zbornica za arhitekturo in prostor Slovenije na 56. seji Skupščine ZAPS dne 9. 12. 2020 sprejela naslednji

# SPLOŠNI AKT

## o varnosti obdelave osebnih podatkov pri ZAPS

I. SPLOŠNE DOLOČBE

### 1. člen
### (vsebina splošnega akta)

(1) ZAPS kot upravljavec osebnih podatkov posameznikov nastopa:
- pri izvajanju svojih nalog na področju arhitekturne dejavnosti na podlagi določb zakona, ki ureja arhitekturno in inženirsko dejavnost,
- pri izvajanju nalog v zvezi z zastopstvom stanovskih interesov članov ZAPS,
- zaradi namena poslovanja in
- v svojstvu delodajalca.

(2) S tem splošnim aktom se določajo pravni, organizacijski in tehnični postopki ter ukrepi za varovanje in zavarovanje osebnih podatkov, katerih upravljavec je ZAPS, z namenom, da se prepreči naključno ali namerno nepooblaščeno obdelavo, spremembo ali izgubo osebnih podatkov.

### 2. člen
### (pomen izrazov)

(1) Izrazi, uporabljeni v tem splošnem aktu in spremljajoči dokumentaciji, ki na njem temelji, imajo naslednji pomen:

- *osebni podatki* so katera koli informacija v zvezi z določenim ali določljivim posameznikom (v nadaljevanju: posameznik, na katerega se nanašajo osebni podatki); določljiv posameznik je tisti, ki ga je mogoče neposredno ali posredno določiti, zlasti z navedbo identifikatorja, kot je ime, identifikacijska številka, podatki o lokaciji, spletni identifikator, ali z navedbo enega ali več dejavnikov, ki so značilni za fizično, fiziološko, genetsko, duševno, gospodarsko, kulturno ali družbeno identiteto tega posameznika;
- *posebne vrste osebnih podatkov* so informacije v zvezi s posameznikovim rasnim ali etničnim poreklom, političnim prepričanjem, verskim ali podobnih prepričanjem, članstvom (ali nečlanstvom) v sindikatih, telesnim ali duševnim zdravjem ali stanjem, spolnim življenjem ali spolno usmerjenostjo, postopkih in obsodbah za kazniva dejanja ali prekrške, genetskimi in biometričnimi informacijami;
- *podatki o zdravstvenem stanju* so posebne vrste osebnih podatkov, ki se nanašajo na telesno ali duševno zdravje posameznika, vključno z zagotavljanjem zdravstvenih storitev, in razkrivajo informacije o njegovem zdravstvenem stanju;
- *nosilci osebnih podatkov* so vse vrste sredstev, na katerih so zapisani ali posneti osebni podatki v papirni ali elektronski obliki, slednji na kateremkoli elektronskem mediju ali napravi, ki omogoča obdelavo osebnih podatkov;
- *obdelava* je vsako dejanje ali niz dejanj, ki se izvaja v zvezi z osebnimi podatki ali nizi osebnih podatkov z avtomatiziranimi sredstvi ali brez njih, kot je zbiranje, beleženje, urejanje, strukturiranje, shranjevanje, prilagajanje ali spreminjanje, priklic, vpogled, uporaba, razkritje s posredovanjem, razširjanje ali drugačno omogočanje dostopa, prilagajanje ali kombiniranje, omejevanje, izbris ali uničenje;

- *avtomatizirana obdelava* je obdelava osebnih podatkov s sredstvi informacijske tehnologije;
- *omejitev obdelave* pomeni označevanje shranjenih osebnih podatkov zaradi omejevanja njihove obdelave v prihodnosti;
- *posredovanje osebnih podatkov* je posredovanje ali razkritje osebnih podatkov;
- *oblikovanje profilov* pomeni vsako obliko avtomatizirane obdelave osebnih podatkov, ki vključuje uporabo osebnih podatkov za ocenjevanje nekaterih osebnih vidikov v zvezi s posameznikom, zlasti za analizo ali predvidevanje uspešnosti pri delu, ekonomskega položaja, zdravja, osebnega okusa, interesov, zanesljivosti, vedenja, lokacije ali gibanja tega posameznika;
- *zbirka osebnih podatkov* je vsak strukturiran niz osebnih podatkov, ki vsebuje vsaj en osebni podatek, ki je dostopen na podlagi meril, ki omogočajo uporabo ali združevanje podatkov, ne glede na to, ali je niz centraliziran, decentraliziran ali razpršen na funkcionalni ali geografski podlagi;
- *psevdonimizacija* je obdelava osebnih podatkov na tak način, da osebnih podatkov brez dodatnih informacij ni več mogoče pripisati specifičnemu posamezniku, na katerega se nanašajo osebni podatki, če se take dodatne informacije hranijo ločeno ter zanje veljajo tehnični in organizacijski ukrepi za zagotavljanje, da se osebni podatki ne pripišejo določenemu ali določljivemu posamezniku;
- *anonimizacija* je obdelava osebnih podatkov na način, ki ne omogoča povratne identifikacije posameznika, na katerega se nanašajo osebni podatki, tako da ta ni več določen ali določljiv niti z uporabo drugih dodatnih informacij iz prejšnje alineje;
- *upravljavec podatkov* je fizična ali pravna oseba, javni organ, agencija ali drugo telo, ki samo ali skupaj z drugimi določa namene in sredstva obdelave;
- *obdelovalec podatkov* je fizična ali pravna oseba, javni organ, agencija ali drugo telo, ki obdeluje osebne podatke v imenu upravljavca;
- *osebe, ki so pooblaščene za obdelavo osebnih podatkov za ZAPS* so zaposleni, funkcionarji in pogodbeni sodelavci ZAPS, ki so v okviru zaposlitve, imenovanja ali pogodbeno danim jih pooblastil zadolženi za obdelavo osebnih podatkov iz posamezne zbirke osebnih podatkov pod neposrednim vodstvom ZAPS;
- *uporabnik podatkov* je fizična ali pravna oseba, javni organ, agencija ali drugo telo, ki so mu bili osebni podatki razkriti, ne glede na to, ali je tretja oseba ali ne. Vendar pa se javni organi, ki lahko prejmejo osebne podatke v okviru posamezne poizvedbe v skladu s pravom EU ali pravom države članice, ne štejejo za uporabnike; obdelava teh podatkov s strani teh javnih organov poteka v skladu z veljavnimi pravili o varstvu podatkov glede na namene obdelave;
- *tretja oseba* je fizična ali pravna oseba, javni organ, agencija ali drugo telo, ki ni posameznik, na katerega se nanašajo osebni podatki, upravljavec, obdelovalec in osebe, ki so pooblaščene za obdelavo osebnih podatkov pod neposrednim vodstvom upravljavca ali obdelovalca;
- *privolitev posameznika, na katerega se nanašajo osebni podatki*, je vsaka prostovoljna, izrecna, informirana in nedvoumna izjava volje posameznika, na katerega se nanašajo osebni podatki, s katero z izjavo ali jasnim pritrdilnim dejanjem izrazi soglasje z obdelavo osebnih podatkov, ki se nanašajo nanj in je preklicna;
- *kršitev varstva osebnih podatkov* je kršitev varnosti, ki povzroči nenamerno ali nezakonito uničenje, izgubo, spremembo, nepooblaščeno razkritje ali dostop do osebnih podatkov, ki so poslani, shranjeni ali kako drugače obdelani;
- *politike na področju varstva osebnih podatkov* so zavezujoča poslovna pravila, ki jih upravljavec ali obdelovalec spoštuje pri prenosih ali nizih prenosov osebnih podatkov upravljavcu ali obdelovalcu povezane družbe ali skupine podjetij, ki opravljajo skupno gospodarsko dejavnost, v eni ali več tretjih državah.

## II. OBDELAVA PODATKOV PRI ZAPS

### 3. člen
### (temeljna načela)

(1) ZAPS osebne podatke obdeluje zakonito, pravično in pregledno.

(2) ZAPS zbira osebne podatke le za določene, izrecne in zakonite namene in v obsegu, ki na teh podlagah opravičujejo namen njihove obdelave, ter jih nadalje ne obdeluje na način, ki s temi nameni ni združljiv.

(3) Osebni podatki, ki jih ZAPS obdeluje, so točni in, kadar je to potrebno, posodobljeni. Netočni osebni podatki se brez odlašanja izbrišejo ali popravijo ob upoštevanju namenov, za katere se obdelujejo.

(4) ZAPS osebne podatke hrani v obliki, ki dopušča identifikacijo posameznikov, na katere se nanašajo osebni podatki, le toliko časa, kolikor je to potrebno za namene, za katere se osebni podatki obdelujejo. Izjemoma se lahko osebni podatki shranjujejo za daljše obdobje, če bodo obdelani zgolj za namene arhiviranja v javnem interesu, za znanstveno-raziskovalne namene ali statistične namene, če to izhaja iz zakonskih obveznosti ZAPS.

(5) ZAPS osebne podatke obdeluje z ustreznimi tehničnimi ali organizacijskimi ukrepi izključno na način, ki zagotavlja ustrezno varnost osebnih podatkov, vključno z zaščito pred nedovoljeno ali nezakonito obdelavo ter pred nenamerno izgubo, uničenjem ali poškodbo.

## 4. člen
## (obdelava osebnih podatkov pri ZAPS)

(1) ZAPS v zakonitem obsegu in skladno s predpisi in načeli iz prejšnjega odstavka obdeluje:

- osebne podatke svojih članov, kandidatov za pridobitev poklicnega naziva in posameznikov, ki so začasno vpisani v imenik in so poklicno kvalifikacijo pridobili v drugi državi pogodbenici ter želijo v Republiki Sloveniji začasno ali občasno opravljati regulirani poklic, vse zaradi izvajanja svojih nalog na področju arhitekturne dejavnosti na podlagi določb zakona, ki ureja arhitekturno in inženirsko dejavnost in zaradi zagotavljanja strokovnosti in varovanja javnega interesa na področju urejanja prostora in graditve objektov ter varstva tretjih oseb, kar vključuje tudi z zakonom predvideno izvajanje javnih pooblastil z dejanji obdelave,
- osebne podatke svojih članov v zvezi z zastopstvom stanovskih interesov, kadar za to obstaja zakonita podlaga ali izrecna privolitev posameznika, na katerega se osebni podatki nanašajo,
- osebne podatke svojih zaposlenih, ki so nujno potrebni za izpolnjevanje pravic in obveznosti ZAPS in/ali delavca s področja delovnega prava ter prava socialne varnosti in kadar za to obstaja zakonita podlaga ali izrecna privolitev posameznika, na katerega se osebni podatki nanašajo,
- druge osebne podatke posameznikov, ki jih obdeluje zaradi namena poslovanja, kot so finančni, upravni, regulativni, pogodbeni, statistični, plačni in drugi kadrovski namen ter za namen razvoja poslovanja zaradi ciljev ustanovitve ZAPS skladno z določbami zakona, ki ureja arhitekturno in inženirsko dejavnost, kadar za to obstaja zakonita podlaga ali izrecna privolitev posameznika, na katerega se osebni podatki nanašajo.

(2) ZAPS obdeluje osebne podatke le, če za to obstaja zakonita (pravna) podlaga, in sicer, če je izpolnjen eden od naslednjih pogojev:

- posameznik, na katerega se nanašajo osebni podatki, je privolil v obdelavo njegovih osebnih podatkov v enega ali več določenih namenov;
- obdelava je potrebna za pripravo ali izvajanje pogodbe, katere pogodbena stranka je posameznik, na katerega se nanašajo osebni podatki, ali za izvajanje ukrepov na zahtevo takega posameznika pred sklenitvijo pogodbe;
- obdelava je potrebna za izpolnitev zakonskih obveznosti, ki jih ZAPS izvaja na podlagi zakona, ki ureja arhitekturno in inženirsko dejavnost, in drugih zakonov, ki veljajo za ZAPS po pravu Republike Slovenije ali pravu EU;
- obdelava je potrebna za zaščito življenjskih interesov posameznika, na katerega se nanašajo osebni podatki, ali druge fizične osebe;
- obdelava je potrebna za opravljanje nalog v javnem interesu, ki jih ZAPS izvaja na podlagi zakona, ki ureja arhitekturno in inženirsko dejavnost, in drugih zakonov, ki veljajo za ZAPS po pravu Republike Slovenije ali pravu EU;
- obdelava je potrebna zaradi zakonitih interesov, za katere si prizadeva upravljavec ali tretja oseba, razen kadar nad takimi interesi prevladajo interesi ali temeljne pravice in svoboščine posameznika, na katerega se nanašajo osebni podatki, ki zahtevajo varstvo osebnih podatkov, zlasti kadar je posameznik, na katerega se nanašajo osebni podatki, otrok.

(3) ZAPS posebne vrste osebnih podatkov obdeluje le ob izpolnitvi enega od naslednjih pogojev:

- kadar je dana izrecna privolitev posameznika, na katerega se nanašajo osebni podatki, v obdelavo navedenih osebnih podatkov za enega ali več določenih namenov, razen kadar pravo Unije ali pravo RS določa, da odstop od prepovedi obdelave s strani posameznika ni dopusten;
- kadar je to nujno potrebno za izpolnjevanje pravic in obveznosti ZAPS ali delavca s področja delovnega prava ter prava socialne varnosti in za to obstaja zakonita podlaga v pravnih predpisih Republike Slovenije ali EU, ki zagotavlja ustrezne zaščitne ukrepe za temeljne pravice in interese posameznika ali izrecna privolitev posameznika, na katerega se osebni podatki nanašajo;

- če gre za podatke, ki jih ZAPS obdeluje v okviru svojih zakonitih dejavnosti in nalog z ustreznimi zaščitnimi ukrepi in pod pogojem, da se obdelava nanaša samo na člane ZAPS, nekdanje člane ZAPS ali na osebe, ki so v rednem stiku z ZAPS v zvezi s cilji in nameni ustanovitve ZAPS, ter da osebni podatki niso posredovani izven ZAPS brez privolitve posameznikov, na katere se nanašajo osebni podatki;
- če je obdelava povezana z osebnimi podatki, ki jih posameznik, na katerega se nanašajo osebni podatki, sam objavi;
- kadar je obdelava potrebna za uveljavljanje, izvajanje ali obrambo pravnih zahtevkov ali kadar koli sodišča izvajajo svojo sodno pristojnost;
- če je obdelava je potrebna iz razlogov bistvenega javnega interesa na podlagi prava Unije ali prava RS, ki je sorazmerna z zastavljenim ciljem, spoštuje bistvo pravice do varstva podatkov ter zagotavlja ustrezne in posebne ukrepe za zaščito temeljnih pravic in interesov posameznika, na katerega se nanašajo osebni podatki;
- če je obdelava potrebna za namene arhiviranja v javnem interesu, za znanstveno, zgodovinsko raziskovalne ali statistične namene na podlagi prava Republike Slovenije ali EU, ki je sorazmerna z zastavljenim ciljem, spoštuje bistvo pravice do varstva podatkov ter zagotavlja ustrezne in posebne ukrepe za zaščito temeljnih pravic in interesov posameznika, na katerega se nanašajo osebni podatki;
- če so za to podani drugi zakoniti razlogi, določeni z Uredbo in področno zakonodajo, ki ureja varstvo osebnih podatkov.

(4) Pri presoji o tem, katera pravna podlaga se uporabi za posamezni namen obdelave, je treba izhajati iz tega, katera je najprimernejša za posamezni namen obdelave.

## 5. člen
## (pravice posameznika, na katerega se nanašajo osebni podatki)

(1) Posameznik, na katerega se nanašajo podatki, lahko dano privolitev kadar koli prekliče, pri tem pa preklic ne vpliva na zakonitost obdelave osebnih podatkov, ki je bila izvedena do preklica.

(2) V postopku obdelave osebnih podatkov ZAPS posamezniku, na katerega se nanašajo osebni podatki, na primeren način (pisno ali neposredno ustno) nudi vse informacije, povezane z obdelavo osebnih podatkov, zlasti o namenu obdelave podatkov, njihovi vrsti, o uporabnikih ali kategorijah uporabnikov, ki so jim bili ali jim bodo razkriti osebni podatki, o predvidenem obdobju hrambe osebnih podatkov oziroma o merilih, ki se uporabijo za določitev tega obdobja, kadar osebni podatki niso zbrani pri posamezniku, na katerega se ti nanašajo, vse razpoložljive informacije v zvezi z njihovim virom in o drugih pravicah posameznika, na katerega se nanašajo osebni podatki (npr. pravica do dostopa, popravljanja, izbrisa osebnih podatkov in pravica do omejitve obdelave, pravica do pritožbe pri Informacijskem pooblaščencu RS, obstoj avtomatiziranega sprejemanja odločitev, vključno z oblikovanjem profilov ter vsaj v takih primerih smiselne informacije o razlogih zanj, kot tudi pomen in predvidene posledice take obdelave za posameznika, na katerega se nanašajo osebni podatki).

(3) Posameznik, na katerega se nanašajo osebni podatki, ima pravico od ZAPS dobiti potrditev, ali se v zvezi z njim obdelujejo osebni podatki, in kadar je temu tako, dostop do osebnih podatkov, ki se nanj nanašajo.

(4) Posameznik, na katerega se nanašajo osebni podatki, ima pravico do dostopa z vpogledom in reprodukcijo njihove vsebine, če pri tem ne gre za očitno neutemeljene, pretirane ali ponavljajoče se zahteve. V takih primerih lahko ZAPS zaračuna razumno pristojbino skladno z aktom, ki ureja plačevanje članarine in drugih prispevkov ZAPS, pri čemer upošteva administrativne stroške posredovanja informacij, sporočila ali izvajanja zahtevanega ukrepa, ali pa zavrne ukrepanje v zvezi z zahtevo. Za dodatne kopije, ki jih zahteva posameznik, na katerega se nanašajo osebni podatki, lahko upravljavec zaračuna razumno pristojbino ob upoštevanju administrativnih stroškov.

(5) ZAPS bo na Uredbi ali zakonu, ki ureja varstvo osebnih podatkov, temelječi upravičeni zahtevi posameznika, na katerega se nanašajo osebni podatki, ali zaradi izpolnitve svoje pravne obveznosti:
- popravila oziroma dopolnila netočne ali nepopolne osebne podatke posameznika, ki se nanašajo nanj,
- izbrisala osebne podatke kadar niso več potrebni za namene, za katere so bili zbrani ali kako drugače obdelani ali v primeru njihove nezakonite obdelani, oziroma na podlagi preklica privolitve, na podlagi katere poteka obdelava, če za obdelavo ni druge pravne podlage,
- upoštevala ugovor glede obdelave osebnih podatkov posameznika, poveznih z njegovim posebnim položajem, razen če je njihova obdelava potrebna za opravljanje nalog, ki jih ZAPS izvaja po javnem

pooblastilu na podlagi zakona, ki ureja arhitekturno in inženirsko dejavnost zaradi varovanja javnega interesa, ki prevlada nad interesi in temeljnimi pravicami in svoboščinami posameznika, na katerega se nanašajo osebni podatki,

- omejila obdelavo osebnih podatkov za čas preveritve točnosti osebnih podatkov, če posameznik oporeka njihovi točnosti, če je obdelava nezakonita in posameznik, na katerega se nanašajo osebni podatki, nasprotuje izbrisu osebnih podatkov ter namesto tega zahteva omejitev njihove uporabe, če je ZAPS ne potrebuje več za namene obdelave, temveč jih posameznik, na katerega se nanašajo osebni podatki, potrebuje za uveljavljanje, izvajanje ali obrambo pravnih zahtevkov.

(6) Zahteva ali ugovor iz prejšnjega odstavka se zavrne, če niso izpolnjeni osnovni pogoji za seznanitev ker npr. ne gre za osebne podatke ali so ti posamezniku že na voljo, ali je zahteva očitno neutemeljena ali pretirana, zlasti v primeru ponavljajočih se zahtev, ali če so v ustavi, mednarodnih aktih ali področnih zakonih določene posebne izjeme. Kadar ZAPS obdeluje veliko količino informacij v zvezi s posameznikom, na katerega se nanašajo osebni podatki, mora posameznik ob uveljavljanju pravic iz prejšnjega odstavka podrobno opredeliti, na katere informacije ali dejavnosti obdelave se zahteva nanaša.

(7) Rok za sprejem odločitve iz prejšnjega odstavka je en mesec od prejema zahteve. Rok se konča s pretekom tistega dneva v naslednjem mesecu glede na mesec vložitve popolne zahteve, ki se po svoji številki ujema z dnem, ko je bila vložena popolna zahteva. Če naslednji mesec nima ustreznega števila dni, se rok izteče zadnji dan v naslednjem mesecu. Ta rok se lahko po potrebi podaljša za največ dva dodatna meseca ob upoštevanju kompleksnosti in števila zahtev. ZAPS obvesti posameznika, na katerega se nanašajo osebni podatki, o vsakem takem podaljšanju v enem mesecu po prejemu zahteve skupaj z razlogi za zamudo.

(8) Posameznik, na katerega se nanašajo osebni podatki, ki meni, da mu je kršena katera od pravic, ki mu jo zagotavljajo predpisi s področja varstva osebnih podatkov, ima pravico do vložitve pritožbe pri Informacijskem pooblaščencu Republike Slovenije.

## 6. člen
## (obdelava osebnih podatkov za ZAPS)

(1) Obdelovalci osebnih podatkov in osebe, ki so pooblaščene za obdelavo osebnih podatkov za ZAPS, morajo biti seznanjeni z Uredbo, področno zakonodajo, ki ureja varstvo osebnih podatkov, ter z vsebino tega splošnega akta.

(2) Obdelovalci osebnih podatkov in osebe, ki pri svojem delu, pri opravljanju svoje funkcije ali pri izpolnjevanju pogodbenih obveznosti obdelujejo osebne podatke za ZAPS, so sami odgovorni za skladnost svojega ravnanja s tem splošnim aktom in za to, da pri varovanju osebnih podatkov v celoti izvajajo vse ustrezne tehnične in organizacijske ukrepe za njihovo zaščito in vse ukrepe za zagotavljanje vgrajenega in privzetega varovanja osebnih podatkov in zasebnosti, vključno z načeli najmanjšega obsega podatkov obdelave, preglednostjo, psevdonimizacijo, anonimizacijo, dovoljenjem posameznikov, da spremljajo proces in drugimi načeli, ki zagotavljajo ustrezno varnost pri obdelavi podatkov.

(3) Vsak obdelovalec osebnih podatkov in vsak, ki pri svojem delu ali opravljanju svoje funkcije obdeluje osebne podatke za ZAPS, ima v zvezi z varstvom osebnih podatkov, do katerih ima dostop pri svojem delu ali se pri tem z njimi seznani, naslednje obveznosti:

- sme obdelovati samo tiste osebne podatke, ki sodijo v okvir njegovih delovnih ali pogodbenih obveznosti ali v okvir njegovega imenovanja v funkcijo, vse pa le v okviru ciljev in namena ustanovitve ZAPS ali poslovnih namenov ZAPS,
- mora vedno ugotavljati obstoj pravne podlage za obdelavo osebnih podatkov,
- sme osebne podatke obdelovati le za namen, za katerega so bili pridobljeni in jih ne sme obdelovati za kakršen koli drug nepovezan namen, razen če je posameznik, na katerega se nanašajo podatki, v to privoli,
- ne sme dostopati do osebnih podatkov, ki jih ne potrebuje pri opravljanju svojih delovnih ali pogodbenih obveznosti ali v okviru svoje funkcije niti v primeru, če mu dostop do teh podatkov ni omejen,
- mora skrbeti za to, da so postopki pridobivanja privolitev posameznikov zakoniti,
- mora skrbeti, da so osebni podatki, ki jih obdeluje, točni in kadar je to potrebno posodobljeni,
- mora skrbeti, da so vse aktivnosti obdelave podatkov, ki jih izvaja, skladne s tem splošnim aktom in upravičene,
- ne sme z osebnimi podatki ravnati malomarno,

- mora ohraniti zaupnost vseh osebnih podatkov in informacij, s katerimi je seznanjen pri opravljanju svojih delovnih ali poverjenih mu nalog in obveznosti,
- mora brez odlašanja obvestiti predsednika ZAPS ali imenovano pooblaščeno osebo za varstvo podatkov ZAPS o kakršnihkoli zaznanih kršitvah varnosti ali o zaznavi česarkoli sumljivega v zvezi z osebnimi podatki,
- mora, če v okviru svojih nalog in obveznosti obdeluje osebne podatke za ZAPS, striktno ravnati po določbah tega splošnega akta, veljavni zakonodaji Republike Slovenije in EU.

(4) Katerakoli kršitev obveznosti iz prejšnjega odstavka s strani zaposlenega pomeni kršitev obveznosti iz delovnega razmerja, s strani sopogodbenika kršitev pogodbenih obveznosti, s strani funkcionarja ZAPS pa kršitev opravljanja obveznosti iz naslova imenovanja na funkcijo.

(5) Obveza varovanja osebnih podatkov velja trajno, tudi po prenehanju delovnega razmerja, funkcije ali pogodbenega sodelovanja.

(6) Pred začetkom zaposlitve, ob nastopu funkcije ali ob začetku drugačnega sodelovanja z ZAPS mora biti delavec, funkcionar ZAPS ali sopogodbenik seznanjen s tem splošnim aktom, kar potrdi s podpisom posebne izjave. Tudi v primeru odklonitve podpisa takšne izjave se glede na način sprejema in zaradi javne objave tega splošnega akta šteje, da so zaposleni, funkcionarji ZAPS, člani ZAPS in sopogodbeniki seznanjeni z vsebino tega splošnega akta.

## III. POOBLAŠČENA OSEBA ZA VARSTVO OSEBNIH PODATKOV

### 7. člen
### (imenovanje in razrešitev)

(1) Upravni odbor ZAPS imenuje in razrešuje Pooblaščeno osebo za varstvo podatkov ZAPS (v nadaljevanju: DPO).

(2) Za DPO je lahko imenovana oseba, ki izpolnjuje pogoje iz Uredbe in zakona, ki ureja varstvo osebnih podatkov, zlasti pa mora imeti izkušnje na področju varstva osebnih podatkov.

(3) ZA DPO je lahko imenovana oseba, zaposlena pri ZAPS, ali zunanja fizična ali pravna oseba, ki naloge opravlja na podlagi pogodbe o storitvah in če izpolnjuje pogoje iz prejšnjega odstavka.

(4) DPO ne sme biti razrešen ali kaznovan zaradi opravljanja svojih nalog.

### 8. člen
### (naloge DPO)

(1) DPO za ZAPS ob upoštevanju tveganj, povezanih z dejanji obdelave, izvaja naloge, kot jih določata Uredba in zakon, ki ureja varstvo osebnih podatkov, zlasti:
- predstavlja stik s posamezniki, na katere se nanašajo osebni podatki, pri reševanju vseh vprašanj, povezanih z obdelavo njihovih osebnih podatkov, in uresničevanjem njihovih pravic na podlagi Uredbe in zakona, ki ureja varstvo osebnih podatkov,
- s področja svojih nalog svetuje, obvešča in ozavešča vse, ki za ZAPS izvajajo dejanja obdelave, o njihovih obveznostih na področju varstva osebnih podatkov ter spremlja skladnost njihovih ravnanj v skladu z Uredbo, zakonom, ki ureja varstvo osebnih podatkov in tem splošnim aktom,
- upravnemu odboru ZAPS letno poroča o svojem delu in ga obvešča o morebitnih kršitvah,
- se udeležuje sej upravnega odbora ZAPS, na katerih se obravnavajo vprašanja s področja varstva osebnih podatkov,
- sodeluje z Informacijskim pooblaščencem Republike Slovenije in deluje kot kontaktna točka zanj pri vprašanjih v zvezi z obdelavo, kar vključuje posvetovanje skladno z Uredbo in zakonom, ki ureja varstvo osebnih podatkov.

(2) DPO mora biti zagotovljeno neodvisno opravljanje nalog in dostop do osebnih podatkov in dejanj obdelave. Za vsak dostop se ob izpolnitvi pogojev glede namena obdelave podeli pooblastilo za vpogled.

(3) DPO je zavezan k varovanju poklicne skrivnosti in k načelu zaupnosti.

### 9. člen
### (kontaktni podatki DPO ZAPS)

(1) Predsednik ZAPS Informacijskemu pooblaščencu Republike Slovenije sporoči podatke o DPO, ki jih zahtevata Uredba in zakon, ki ureja varstvo osebnih podatkov.

(2) ZAPS na spletni strani objavi kontaktne podatke DPO s podatki o poštnem naslovu, namensko telefonsko številko in namenskim e-poštnim naslovom.

## IV. VAROVANJE OPREME IN PROSTOROV OBDELAVE

### 10. člen
### (varovanje prostorov ZAPS in drugih prostorov obdelave)

(1) Prostori ZAPS, kjer se nahajajo nosilci osebnih podatkov v papirni ali elektronski obliki, strojna ter programska oprema, morajo biti varovani z organizacijskimi, fizičnimi in tehničnimi ukrepi, ki nepooblaščenim osebam onemogočajo dostop do osebnih podatkov, nenamerno izgubo ali uničenje, nepooblaščeno razkritje ali dostop do osebnih podatkov, njihovo nedopustno spremembo, nedopustno objavo in vsako drugo zlorabo.

(2) Dostop do prostorov ZAPS mora biti nadzorovan in vstop vanje ali gibanje po njih vzdrževalcem prostorov, obiskovalcem in pogodbenim sodelavcem, ki niso osebe, pooblaščene za obdelavo osebnih podatkov za ZAPS, ni dovoljen brez spremstva ali prisotnosti pooblaščenih oseb (zaposlenega delavca ali pooblaščenega funkcionarja ZAPS). Pooblaščene osebe, ki za ZAPS opravljajo delo v prostorih ZAPS, morajo vestno in skrbno nadzorovati prostor in ga ob odhodu zakleniti.

(3) Osebje čistilnega servisa se lahko giblje v prostorih ZAPS izven delovnega časa in brez prisotnosti zaposlenega delavca ali pooblaščenega funkcionarja ZAPS le, če so nosilci osebnih podatkov v papirni obliki varno shranjeni v zaklenjenih omarah, nosilci v elektronski obliki pa varovani na način, ki organizacijsko, fizično in programsko-tehnično onemogočajo dostop do podatkov na njih.

(4) Osebni podatki se hranijo na strežniku ZAPS, na drugih napravah, s katerimi se obdelujejo osebni podatki, pa le, če je to nujno potrebno za opravljanje dela.

(5) Osebni podatki se lahko hranijo izven strežnika ZAPS le v primeru, če se ob tem zagotavlja vsaj enake ukrepe varnosti obdelave, kot jih določa ta splošni akt in če je za takšno hrambo z ZAPS sklenjena ustrezna pogodba ali obstaja druga pravna podlaga zanjo.

(6) Pri iznosu osebnih podatkov izven prostorov ZAPS in obdelavi osebnih podatkov zunaj prostorov ZAPS mora biti s strani zaposlenih, funkcionarjev ZAPS in pogodbenih sodelavcev, ki pri svojem delu ali opravljanju svoje funkcije obdelujejo osebne podatke za ZAPS, zagotovljena varnost osebnih podatkov v skladu s tem splošnim aktom.

### 11. člen
### (varovanje strojne in računalniške programske opreme)

(1) Dostop do strojne in računalniške (sistemske in uporabniške) programske opreme ter druge opreme in naprav, s katerimi se obdelujejo osebni podatki, mora biti varovan tako, da dovoljuje dostop samo za to vnaprej določenim zaposlenim ali funkcionarjem ZAPS ali pravnim ali fizičnim osebam, ki za ZAPS po pogodbi o obdelavi osebnih podatkov opravljajo servisiranje računalniške ali programske opreme.

(2) Popravljanje, vzdrževanje, spreminjanje in dopolnjevanje opreme iz prejšnjega ostavka je dovoljeno samo na podlagi splošne ali individualne odobritve predsednika ZAPS ali generalnega sekretarja ZAPS oziroma od njiju pooblaščene osebe, upoštevajoč vse varnostne kriterije, določene s tem splošnim aktom, izvajajo pa ga lahko le pooblaščeni izvajalci oziroma njihovi delavci, ki imajo z ZAPS sklenjeno pogodbo o obdelavi osebnih podatkov.

(3) Vsako popravljanje, vzdrževanje, spreminjanje in dopolnjevanje opreme iz prvega odstavka mora biti ustrezno dokumentirano, upoštevaje sorazmernost med obsegom posegov in tveganjem za varnost osebnih podatkov.

(4) Osebe, ki so pooblaščene za obdelavo osebnih podatkov za ZAPS, ne smejo brez izrecnega dovoljenja predsednika ZAPS ali generalnega sekretarja ZAPS nameščati programske opreme ali je spreminjati izven običajne dopustne rabe.

## 12.člen
## (varovanje osebnih podatkov na elektronskih nosilcih)

(1) Naprave, na kateri se obdelujejo osebni podatki v elektronski obliki, morajo biti izven delovnega časa izklopljene ter fizično in programsko-tehnično zaklenjene oziroma kodirane.

(2) Če mora biti naprava, na kateri se obdelujejo osebni podatki v elektronski obliki ali druga strojna oprema zaradi zagotovitve stalnega dostopa priklopljena ves čas, se varovanje osebnih podatkov organizacijsko, fizično in programsko-tehnično zagotavlja na način, ki nepooblaščenim osebam onemogoča dostop do osebnih podatkov.

(3) Pri ravnanju z nosilci osebnih podatkov ob prisotnosti oseb, ki nimajo pravice do vpogleda vanje, in ob vsakokratni zapustitvi delovnega mesta, morata biti zagotovljeni prazna miza ter stanje praznega računalniškega zaslona. Računalniški zasloni ne smejo biti nameščeni na način, ki bi v času obdelave ali dela na njih omogočali vpogled nanje s strani oseb, ki nimajo pravice do vpogleda v osebne podatke v obdelavi.

(5) Nosilci posebnih vrst osebnih podatkov morajo biti posebej označeni in zavarovani.

(6) Dostop do podatkov prek programske opreme mora biti varovan s sistemom gesel za avtorizacijo in identifikacijo oseb, ki so pooblaščene za obdelavo osebnih podatkov za ZAPS ali pod neposrednim vodstvom drugega upravljavca ali obdelovalca programov in podatkov, in sicer na način, ki omogoča avtentično sledljivost in naknadno preverbo glede časa obdelave in identifikacije uporabnika in, če je to mogoče, tudi glede načina oziroma namena obdelave.

(7) Geslo mora biti dolgo vsaj 8 znakov in mora vsebovati vsaj eno malo in eno veliko črko, vsaj eno številko in vsaj en poseben znak in ne sme vsebovati imen, priimkov, znanih dejstev ali besed ali enakih gesel, ki jih oseba, ki so pooblaščene za obdelavo osebnih podatkov pod neposrednim vodstvom upravljavca, uporablja zunaj sistema ZAPS. Gesla se, razen ob prepoznanih tveganjih, menja periodično vsaj vsake dva meseca. Geslo si določi vsak sam in ga ne sme razkriti nikomur.

(8) Supervizorska in nadzorna gesla ter protokol postopkov za dostop in kakršnokoli administriranje (v mreži, z elektronsko pošto, prek uporabniških programov ipd.) se varno hranijo in se jih varuje pred dostopom nepooblaščenih oseb. Vsaka uporaba v izrednih in nujnih primerih se dokumentira, po vsaki takšni uporabi pa se določijo nova gesla za ta namen.

(9) Vsebina programske opreme in nosilcev osebnih podatkov se sprotno preverja glede na prisotnost računalniških virusov ter zlonamerne programske opreme. Ob njihovem pojavu se tega čimprej odpravi s pomočjo strokovnjakov in obenem ugotovi vzrok pojava virusa. Vsi podatki in programska oprema na medijih za prenos računalniških podatkov ali prejeta prek telekomunikacijskih kanalov mora biti pred uporabo preverjena glede prisotnosti računalniških virusov ter zlonamerne programske opreme.

(10) Razvojna in tesna okolja ne smejo vsebovati osebnih podatkov. Prehod iz testnega okolja v produkcijsko okolje mora biti pri vključitvi osebnih podatkov skrbno nadzorovan in primerno sledljivo dokumentiran. Osebni podatki ne smejo ostati nenadzorovani in se jih ne sme obdelovati, dokler produkcijsko okolje ne zagotavlja vseh varnostnih zahtev, določenih s tem splošnim aktom.

(11) Za potrebe restavriranja računalniškega sistema, ob okvarah in izjemnih situacijah se s sledljivostjo zagotavlja redna izdelava kopij vsebine mrežnega strežnika oziroma naprav, na katerih se obdelujejo osebni podatki.

Te kopije se hranijo na v za to določenih mestih, ki so ognjevarna, zavarovana proti poplavam in elektromagnetnim motnjam, v okviru predpisanih klimatskih pogojih in zaklenjena.

(12) V času servisiranja naprav ali med popravljanjem, vzdrževanjem, spreminjanjem ali dopolnjevanjem programske opreme mora biti zagotovljen nadzor, ki onemogoča nedopustno ravnanje z osebnimi podatki. Če to ni mogoče, se pred takšnimi posegi izdela kopija osebnih podatkov, podatki na nosilcu, na katerem se opravljajo takšni posegi, pa izbrišejo na način, ki ne omogoča restavriranja. Po prenehanju potrebe se izdelana kopija podatkov varno uniči.

## V. STORITVE, KI JIH OPRAVLJAJO ZUNANJE PRAVNE ALI FIZIČNE OSEBE

### 13. člen
### (pogodba o obdelavi osebnih podatkov)

(1) Z vsako zunanjo pravno ali fizično osebo, ki ni zaposlena v ZAPS, in ki opravlja posamezna opravila v zvezi z obdelavo osebnih podatkov in ima vsaj možnost dostopa do osebnih podatkov, se sklene pisna pogodba o obdelavi osebnih podatkov.

(2) Pogodba iz prejšnjega odstavka predpisuje pogoje in ukrepe za zagotovitev varnosti obdelave osebnih podatkov ali pa se obdelovalca zaveže k spoštovanju tega pravilnika. S pogodbo se obseg obdelave osebnih podatkov omeji izključno na vsebino danega pooblastila ali naročila, ki določa obseg in namen naročene obdelave osebnih podatkov; obdelava podatkov izven danega pooblastila ali naročila ni dopustna.

## VI. SPREJEM IN POSREDOVANJE OSEBNIH PODATKOV

### 14. člen
### (sprejem osebnih podatkov)

(1) Delavec, ki je zadolžen za sprejem in evidenco pošte, mora izročiti poštno pošiljko z osebnimi podatki neposredno posamezniku ali službi, na katero je ta pošiljka naslovljena.

(2) Delavec, ki je zadolžen za sprejem in evidenco pošte, ne sme odpirati pošiljk:
- ki so naslovljene na drug organ ali organizacijo in so pomotoma dostavljene,
- pošiljk z označbo, da vsebina pošiljke vsebuje osebne podatke, če delavec ob tem ni zadolžen tudi za njihovo obdelavo,
- pošiljk z zaznamkom, da se vročijo osebno naslovniku ali so nanj osebno tudi naslovljene,
- pošiljk, za katere iz označb na ovojnici izhaja, da se nanašajo na natečaj ali razpis.

### 15. člen
### (prenos osebnih podatkov)

(1) Osebne podatke je dovoljeno prenašati z informacijskimi, telekomunikacijskimi in drugimi sredstvi le ob izvajanju postopkov in ukrepov, ki preprečujejo nepooblaščeno obdelavo.

(2) Osebne podatke v fizični obliki se pošiljajo priporočeno in v ovojnici, ki v normalnih pogojih (dnevna svetloba, običajna luč) ne omogoča ogleda vsebine pošiljke.

(3) Posebne vrste osebnih podatkov se v fizični obliki pošiljajo naslovnikom v zaprtih ovojnicah in se vročajo osebno v prostorih ZAPS ali po pošti z vročilnico, v elektronki obliki preko telekomunikacijskih omrežij pa le kriptografirano na način, da je zagotovljena nečitljivost podatkov med njihovim prenosom.

## 16. člen
## (posredovanje osebnih podatkov tretjim osebam)

(1) Osebni podatki se lahko posredujejo tretjim osebam samo, če imajo za to ustrezno pravno podlago: če so za njihovo pridobitev in uporabo pooblaščeni z zakonom, na podlagi pisne zahteve ali privolitve posameznika, na katerega se osebni podatki nanašajo, ali če za to obstaja zakoniti interes.

(2) Iz vloge za posredovanje osebnih mora biti jasno razvidna identifikacija vlagatelja ter pravna podlaga za posredovanje osebnih podatkov.

(3) Vsako posredovanje osebnih podatkov tretjim osebam se beleži v evidenci posredovanj osebnih podatkov, ki vsebuje podatek o tem, kateri osebi so bili podatki posredovani, komu, kdaj, na kakšni podlagi in za kakšen namen.

(4) Izvirniki listin se po izdelavi kopije posredujejo le v primeru pisne odredbe sodišča in v nobenem drugem primeru.

(5) Pregledovanje in reproduciranje upravnih spisov in dajanje obvestil o poteku postopka se opravlja v skladu z določbami zakona, ki ureja splošni upravni postopek.

# VII. BRISANJE PODATKOV

## 17.člen
## (sprejem osebnih podatkov)

(1) Po preteku roka hrambe ali namena, za katerega so bili obdelovani, se osebni podatki v papirni obliki ali na elektronskih nosilcih zapisniško nepovratno uničijo, in sicer ali v prostorih ZAPS ali pod nadzorom pooblaščene osebe ZAPS pri organizaciji, ki se v okviru poklicne dejavnosti ukvarja z uničevanjem zaupne dokumentacije.

(2) Ob uničenju osebnih podatkov v prostorih ZAPS se zagotovi prisotnost treh oseb, imenovanih s strani predsednika ZAPS ali generalnega sekretarja ZAPS oziroma od njiju pooblaščene osebe. Ob uničenju pri organizaciji, ki se v okviru poklicne dejavnosti ukvarja z uničevanjem zaupne dokumentacije, pooblaščeno osebo ZAPS, ki sodeluje pri nadzoru uničenja, imenuje predsednik ZAPS ali generalni sekretar ZAPS.

# VIII. KRŠITVE VARNOSTI

## 18. člen
## (obveznosti)

(1) Osebe, ki so pooblaščene za obdelavo osebnih podatkov za ZAPS, so dolžne ob zaznavi okoliščin, ki bi lahko privedle do kršitve zaupnosti (npr. nepooblaščeno razkritje podatkov, nepooblaščen dostop do podatkov idr.), kršitve celovitosti (npr. sprememba podatkov ipd.) ali kršitve dostopnosti (npr. izguba ali uničenje podatkov ipd.) osebnih podatkov, incident nemudoma javiti DPO in osebi, ki za ZAPS skrbi za raziskavo in odpravo posledic takšnega incidenta, ter tudi sami storiti vse, da se prepreči ali zmanjša nastanek škode.

(2) V primeru, da je do kršitve varnosti osebnih podatkov prišlo pri drugem pogodbenem obdelovalcu, je ta dolžan o incidentu ZAPS obvestiti najkasneje v roku 24 ur.

(3) Oseba, ki za ZAPS raziskuje oziroma odpravlja morebitne posledice incidenta, mora dokumentirati vsako zaznano kršitev varnosti osebnih podatkov, vključno z ugotovljenimi dejstvi v zvezi s tem, nastalimi posledicami in sprejetimi ukrepi ter dokumentacijo ZAPS na njeno zahtevo tudi predložiti, saj je ZAPS to dokumentacijo dolžna razkriti Informacijskemu pooblaščencu RS.

## 19. člen
## (obveščanje Informacijskega pooblaščenca)

(1) V primeru kršitve varnosti osebnih podatkov mora predsednik ZAPS najpozneje v 72. urah po seznanitvi s kršitvijo o njej obvestiti Informacijskega pooblaščenca RS, razen če ni verjetno, da bi bile s kršitvijo varstva osebnih podatkov ogrožene pravice in svoboščine posameznikov.

(2) Za obveščanje iz prejšnjega odstavka se uporabi zadnji objavljeni obrazec Informacijskega pooblaščenca RS za prijavo kršitve varnosti.

## 20. člen
## (obveščanje posameznika)

(1) Če DPO oceni, da je verjetno, da bi kršitev varnosti osebnih podatkov povzročila veliko tveganje za pravice in svoboščine posameznikov, mora predsednik ZAPS ali oseba po njegovem pooblastilu najkasneje v roku 24 ur posamezniku sporočiti, da je prišlo do kršitve varstva osebnih podatkov.

(2) Obvestilo posamezniku iz prejšnjega odstavka mora vsebovati informacijo o kontaktnih podatkih DPO, opis verjetnih posledic kršitve varnosti osebnih podatkov z opisom ukrepov za obravnavo teh kršitev varnosti in ukrepov za ublažitev morebiti nastalih škodljivih posledic, kadar in kolikor jih je mogoče izvesti.

(3) Obvestilo iz prejšnjih dveh odstavkov ni potrebno, če so bili v zvezi z osebnimi podatki zaradi kršitev varnosti izvedeni ustrezni ukrepi, ki preprečujejo obdelavo (npr. šifriranje), če so bili sprejeti naknadni ukrepi za zagotovitev, da se veliko tveganje iz prvega odstavka ne bo več ponovilo, ali v primerih, ko bi obveščanje posameznikov zahtevalo nesorazmeren napor. V slednjem primeru se namesto obvestila posamezniku objavi javno sporočilo na spletni strani ZAPS ali izvede podoben ukrep, ki posameznikom zagotovi pravico do obveščenosti.

# IX. VODENJE EVIDENC

## 21.člen
## (evidenca dejavnosti obdelave)

(1) Opis zbirk osebnih podatkov, ki jih vodi ZAPS kot upravljavec, se vodi v evidenci dejavnosti obdelave osebnih podatkov.

(2) Evidenca dejavnosti obdelave osebnih podatkov se zagotovi za vsako zbirko osebnih podatkov ob vzpostavitvi zbirke in se dopolnjuje ob vsaki spremembi vrste osebnih podatkov v posamezni zbirki oziroma drugi spremembi informacij, ki jih evidenca dejavnosti obdelave vsebuje.

(3) ZAPS za vsako posamezno zbirko podatkov v evidenci dejavnosti obdelave opredeli vsaj v naslednjem obsegu:

- naziv zbirke,
- namen obdelave,
- osebe, pooblaščene za obdelavo osebnih podatkov za ZAPS,

- opis kategorij posameznikov, na katere se nanašajo osebni podatki v zbirki,
- vrste osebnih podatkov v zbirki,
- kategorije uporabnikov, ki so jim bili ali jim bodo razkriti osebni podatki,
- morebitne informacije o prenosih osebnih podatkov v tretjo državo ali mednarodno organizacijo,
- kadar je to mogoče, rok hrambe osebnih podatkov,
- splošen opis varovanja zbirke osebnih podatkov,
- pravna podlaga za obdelavo osebnih podatkov.

(4) Za vzpostavitev, vodenje, ažuriranje in ravnanje z evidencami dejavnosti obdelave osebnih podatkov so za posamezno evidenco odgovorne osebe, pooblaščene za obdelavo osebnih podatkov za ZAPS za to evidenco, ki jim pomaga DPO.

(5) ZAPS ima vzpostavljen sistem rednega letnega pregledovanja in ustreznosti evidenc dejavnosti obdelave osebnih podatkov.

## X. PREHODNE IN KONČNE DOLOČBE

### 22. člen
### (prenehanje veljavnosti in uporabe drugih splošnih aktov ZAPS)

(1) Z dnem začetka veljavnosti tega splošnega akta preneha veljati:
- Pravilnik o ukrepih in postopkih za zavarovanje osebnih podatkov, sprejet s strani Upravnega odbora ZAPS dne 3.7.2007 ter
- 5., 6. in 7. člen Pravilnika o organizaciji in delu službe za evidence in strokovne izpite in drugih služb ZAPS, sprejet s strani Skupščine ZAPS dne 29.6.2004.

### 23. člen
### (začetek veljavnosti)

(1) Ta splošni akt prične veljati, ko ga sprejme skupščina ZAPS, uporablja pa se ga od dneva objave na spletnih straneh ZAPS.

Tomaž Krištof, univ. dipl. inž. arh.

Predsednik Zbornice za arhitekturo in prostor Slovenije