

Na podlagi 28. člena Statuta Atletske zveze Slovenije in Zakona o varstvu osebnih podatkov, je Upravni odbor AZS na 27. dopisni seji dne 17. 6. 2019 sprejel

PRAVILNIK **o varstvu osebnih podatkov**

SPLOŠNE DOLOČBE

1. člen

S tem pravilnikom se določa namen obdelave osebnih podatkov, vrste osebnih podatkov, ki naj bi se obdelovale ter rok hrambe, arhiviranja ali izbrisa osebnih podatkov, s katerimi upravlja Atletska zveza Slovenije (v nadaljevanju: upravljavec).

V zadevah, ki jih ne ureja ta pravilnik, se neposredno uporabljajo določbe veljavnih predpisov.

2. člen

Izrazi, ki so uporabljeni v tem pravilniku, imajo v skladu z veljavnimi predpisi naslednji pomen:

1. »osebni podatki« pomeni katero koli informacijo v zvezi z določenim ali določljivim posameznikom (v nadaljnjem besedilu: 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;

2. »obdelava« pomeni 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;

3. »omejitev obdelave« pomeni označevanje shranjenih osebnih podatkov zaradi omejevanja njihove obdelave v prihodnosti;

5. »psevdonimizacija« pomeni obdelavo 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 pripisejo določenemu ali določljivemu posamezniku;

6. »zbirka« pomeni vsak strukturiran niz osebnih podatkov, ki so dostopni v skladu s posebnimi merili, niz pa je lahko centraliziran, decentraliziran ali razpršen na funkcionalni ali geografski podlagi;

7. »upravljavec« pomeni športno zvezo Atletska zveza Slovenije, ki samo ali skupaj z drugimi določa namene in sredstva obdelave; kadar namene in sredstva obdelave določa pravo Unije ali pravo države članice, se lahko upravljavec ali posebna merila za njegovo imenovanje določijo s pravom Unije ali pravom države članice;

8. »obdelovalec« pomeni fizično ali pravno osebo, javni organ, agencijo ali drugo telo, ki obdeluje osebne podatke v imenu upravljavca;

9. »uporabnik« pomeni fizično ali pravno osebo, javni organ, agencijo 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 Unije 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;

10. »atletičar« pomeni športniki in športnice, ki so registrirani pri Atletski zvezi Slovenije v skladu s pravilnikom, ki ureja registracijo.

11. »delavci« pomeni zaposlene pri Atletski zvezi Slovenije, ki so v rednem delovnem razmerju, ali pa pogodbene sodelavce, ki opravljajo določene naloge za Atletsko zvezo Slovenije na podlagi pogodbe o sodelovanju.

12. »druge fizične osebe« pomeni fizične osebe, ki podajo izrecno pisno izjavo upravljalcu, da lahko zbira njihove osebne podatke za potrebne obveščanja o aktivnostih upravljalca oziroma za druge namene, ki jih ta oseba izrecno označi na posebni izjavi.

13. »tretja oseba« pomeni fizično ali pravno osebo, javni organ, agencijo ali telo, ki ni posameznik, na katerega se nanašajo osebni podatki, upravljavec, obdelovalec in osebe, ki so pooblaščenice za obdelavo osebnih podatkov pod neposrednim vodstvom upravljavca ali obdelovalca;

14. »privolitev posameznika, na katerega se nanašajo osebni podatki« pomeni vsako prostovoljno, izrecno, informirano in nedvoumno izjavo 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;

15. »kršitev varstva osebnih podatkov« pomeni kršitev varnosti, ki povzroči nenamerno ali nezakonito uničenje, izgubo, spremembo, nepooblaščen razkritje ali dostop do osebnih podatkov, ki so poslani, shranjeni ali kako drugače obdelani;

16. »biometrični podatki« pomeni osebne podatke, ki so rezultat posebne tehnične obdelave v zvezi s fizičnimi, fiziološkimi ali vedenjskimi značilnostmi posameznika, ki omogočajo ali potrjujejo edinstveno identifikacijo tega posameznika, kot so podobe obraza ali daktiloskopski podatki;

17. »nadzorni organ« pomeni Informacijskega pooblaščenca, določenega s tem zakonom ter zakonom, ki ureja informacijskega pooblaščenca;

18. »čezmejna obdelava osebnih podatkov« pomeni bodisi: a) obdelavo osebnih podatkov, ki poteka v Uniji v okviru dejavnosti sedežev upravljavca ali obdelovalca v več kot eni državi članici, kadar ima upravljavec ali obdelovalec sedež v več kot eni državi članici, bodisi b) obdelavo osebnih podatkov, ki poteka v Uniji v okviru dejavnosti edinega sedeža upravljavca ali obdelovalca, vendar obdelava znatno vpliva ali bi lahko znatno vplivala na posameznike, na katere se nanašajo osebni podatki, v več kot eni državi članici;

19. »povezovanje zbirk« pomeni povezavo vsaj dveh zbirk, tako, da se omogoči, da se vsebina osebnih podatkov v različnih zbirkah samodejno posodablja na način, da so osebni podatki v zbirki osebnih podatkov posodobljeni ali da je avtomatično navedena oznaka, da je osebni podatek spremenjen.

20. »Varovani prostori«, kjer se nahajajo nosilci varovanih osebnih podatkov - vsak dokument, na katerem je zapisan osebni podatek in vsak drug računalniški ali elektronski nosilec podatka – in strojna ter programska oprema, morajo biti varovani z organizacijskimi ter fizičnimi in tehničnimi ukrepi, ki onemogočajo nepooblaščenim osebam dostop do podatkov.

NAMEN OBDELAVE OSEBNIH PODATKOV IN ZBIRKE

3. člen

Upravljalec sam ali po pooblaščenem obdelovalcu obdeluje osebne podatke zaposlenih, atletov, atletskih delavcev in drugih fizičnih oseb, ki za to podajo izrecno soglasje, za potrebe izvajanja nalog Atletske zveze Slovenije.

Upravljalec za vsak strukturiran niz osebnih podatkov, ki je centraliziran, vzpostavi zbirko.

Upravljalec mora skrbeti za točnost in ažurnost vsebine zbirke.

Upravljalec vodi evidenco dejavnosti obdelovalcev osebnih podatkov.

4. člen

Upravljalec vodi predvsem naslednje osnovne zbirke:

- *evidence, ki so vezane na zaposlene pri upravljalcu,*
- *evidenco atletov,*
- *evidenco delavcev,*
- *evidenco drugih fizičnih oseb,*
- *lahko pa vzpostavi tudi druge zbirke za posebne namene obdelave.*

(1) Vsako zbirko osebnih podatkov na predlog direktorja AZS s sklepom vzpostavi Upravni odbor. V sklepu določi:

- *naziv zbirke;*
- *odgovorno osebo zbirke;*
- *pravno podlago za obdelavo;*
- *namen(e) obdelave;*
- *opis kategorij posameznikov, na katere se nanašajo osebni podatki*
- *vrste osebnih podatkov;*
- *kategorije uporabnikov, ki so jim bodo razkriti osebni podatki, vključno z uporabniki v tretjih državah ali mednarodnih organizacijah;*
- *kadar je mogoče, predvidene roke za izbris različnih vrst podatkov.*

(2) Sklep služi kot podlaga za prvi vpis zbirke v evidenco dejavnosti obdelave.

Za varovane osebne podatke štejejo tisti podatki, ki kažejo na lastnosti, stanja ali razmerja posameznika, ne glede na obliko, v kateri so izraženi.

V smislu prvega odstavka tega člena štejejo za osebne podatke zlasti:

- *identifikacijski podatki o posamezniku,*
- *podatki, ki se nanašajo na družinska razmerja,*
- *podatki o zaposlitvi,*
- *podatki o komunikacijskih sredstvih.*

Osební podatki se smejo v zvezi zbirati samo za namene, določene v zakonski podlagi, ali opredeljene v informacijski, posredovani posamezniku, na katerega se nanašajo obdelovani podatki, v okviru pridobivanja privolitve za obdelavo ali sklenitve pogodbe, na podlagi katere se izvaja obdelava.

Besedilo privolitve in besedilo pogodbe, ki določa pravno podlago obdelave podatkov, je določeno v prilogah tega pravilnika.

Upravljalca lahko osebne podatke zbira ali obdeluje za drug namen kot je prvotni namen njihovega zbiranja ali obdelave določen v prvem odstavku 4. člena tega pravilnika in sicer pod pogojem pisne presoje o združljivosti novega namena obdelave, ki vključuje naslednja merila:

- a) ali so izpolnjene zahteve glede zakonitosti, poštenosti in sorazmernosti prvotne obdelave;*
- b) oceno združljivosti načrtovanega namena s prvotnim namenom obdelave ali zbiranja;*
- c) oceno poštenosti in sorazmernosti načrtovane nadaljnje obdelave;*
- č) okoliščine, v katerih so bili osebni podatki zbrani, zlasti kar zadeva razmerje med posamezniki, na katere se nanašajo osebni podatki, in upravljavcem;*
- e) razumna pričakovanja posameznikov, na katere se nanašajo zadevni osebni podatki, še zlasti pa morebitne posledice načrtovane nadaljnje obdelave na njihove pravice in obveznosti, položaje ali osebna stanja,*
- f) obstoj ustreznih ukrepov varnosti glede obdelave osebnih podatkov (v nadaljnjem besedilu: zavarovanje osebnih podatkov), ki lahko vključujejo tudi psevdonimizacijo, anonimizacijo ali kriptiranje.*

Obdelava za drug namen od prvotnega se lahko brez zagotovitve posebne pravne podlage izvede le, če pisna presoja po prejšnjih odstavkih jasno pokaže, da je razširitev obdelave osebnih podatkov potrebna zaradi uresničevanja zakonitih interesov upravljavca in ti interesi očitno prevladujejo nad interesi posameznika, na katerega se nanašajo osebni podatki. Pisna presoja po tem odstavku je del dokumentacije, s katero upravljavec izkazuje skladnost njegove obdelave s pravili iz določb veljavnih predpisov.

Ob upoštevanju pravilnika, je obdelava osebnih podatkov za drug namen dovoljena le, če:

- a) je podana privolitev posameznika, na katerega se nanašajo osebni podatki,*
- b) obdelavo za drug namen določa zakon ali pravni akt ali odločitev Evropske unije, ki je enakovreden zakonu in se v Republiki Sloveniji uporablja neposredno,*
- c) je to potrebno za namene preprečevanja, preiskovanja, odkrivanja, pregona kaznivih dejanj ali prekrškov, izvrševanje kazenskih sankcij, varovanje pred grožnjami javni varnosti in njihovim preprečevanjem, varnosti države ali obrambe, ali*
- č) je to potrebno za uveljavljanje, izvajanje ali obrambo civilnopravnih zahtevkov, če ne prevladujejo interesi posameznika, na katerega se nanašajo osebni podatki, zlasti zaupnost pravnega razmerja, iz katerega izvira obdelava osebnih podatkov.*

5. člen

Posamezna zbirka je lahko sestavljena iz ene ali več fizičnih zbirk.

Fizična zbirka lahko obstaja v:

- papirni obliki (knjiga, register, datotečna omara, ipd.);*
- elektronski obliki (magnetni diski, tračne enote, CD-ROMi in drugi nosilci elektronskih zapisov).*

VODENJE EVIDENCE DEJAVNOSTI OBDELAVE

6. člen

Zveza za namen dokazovanja skladnosti z uredbo, ZVOP-1 in drugimi predpisi, ki urejajo obdelavo, hrani evidenco zapisov o dejavnostih obdelav, s katerimi upravlja. Podatki evidence so dostopni pooblaščenim osebam AZS in na njegovo zahtevo tudi nadzornemu organu.

Evidenca dejavnosti obdelave osebnih podatkov za posamezno zbirko obsega:

- a) naziv zbirke;*
- b) odgovorno osebo zbirke;*
- c) pravno podlago za obdelavo;*
- d) namene obdelave;*
- e) morebitno obdelavo za namene avtomatiziranega odločanja in profiliranja;*
- f) opis kategorij posameznikov, na katere se nanašajo osebni podatki, in vrst osebnih podatkov;*
- g) kategorije uporabnikov, ki jim bodo razkriti osebni podatki, vključno z uporabniki v tretjih državah ali mednarodnih organizacijah;*
- h) informacije o prenosih osebnih podatkov v tretjo državo ali mednarodno organizacijo, vključno z identifikacijo te tretje države ali mednarodne organizacije, v primeru prenosov v tretjo državo ali mednarodno organizacijo, za katero še ni bil izdan sklep o skladnosti pa tudi dokumentacijo o ustreznih zaščitnih ukrepih;*
- i) predvidene roke za izbris različnih vrst podatkov;*
- j) splošni opis tehničnih in organizacijskih varnostnih ukrepov.*

Odgovorna oseba evidence dejavnosti obdelave je pooblaščen oseb.

7. člen

Zavarovanje osebnih podatkov zajema pravne, organizacijske in ustrezne logistično-tehnične postopke in ukrepe, s katerimi se varujejo osebni podatki, preprečuje slučajno ali namerno nepooblaščen uničevanje podatkov, njihovo spremembo ali izgubo ter nepooblaščen obdelavo teh podatkov tako da se:

- varujejo prostori, aparatura in sistemska programska oprema, vključno z vhodnimi in izhodnimi enotami;*
- varuje aplikativna programska oprema, s katero se obdelujejo osebni podatki;*
- preprečuje nepooblaščen dostop do osebnih podatkov pri njihovem prenosu, vključno s prenosom po telekomunikacijskih sredstvih in omrežjih;*
- zagotavlja učinkovit način blokiranja, uničenja, izbrisa ali anonimiziranja osebnih podatkov;*
- onemogoča nepooblaščenim osebam dostop do naprav, na katerih se obdelujejo osebni podatki in do njihovih zbirk;*
- omogoča poznejše ugotavljanje, kdaj so bili posamezni osebni podatki vneseni v zbirko osebnih podatkov, uporabljeni ali drugače obdelani in kdo je to storil, in sicer za obdobje, za katero se posamezni podatki shranjujejo.*

Način vodenja, zavarovanja, posodabljanja in dostopa do podatkov posamezne evidence obdelave določa navodilo Postopki zaščite in varovanja osebnih podatkov v zbirki.

POOBLAŠČENE OSEBE ZA VARSTVO OSEBNIH PODATKOV

8. člen

Upravljalca na podlagi poklicnih odlik in zlasti strokovnega znanja o zakonodaji in praksi na področju varstva podatkov ter zmožnosti za izpolnjevanje nalog s področja varstva osebnih podatkov imenuje pooblaščen osebno za varstvo osebnih podatkov.

Upravljalca, ko imenuje pooblaščen osebno, mora v roku 8 dni od imenovanja vpisati njene kontaktne podatke v svoji evidenci dejavnosti obdelave, jih javno objaviti na primeren način ter jih sporočiti informacijskemu pooblaščenju.

S temi kontaktnimi podatki pooblaščen osebno upravljalca seznanjeni tudi posamezniki, na katere se nanašajo osebni podatki, ki jih pooblaščen osebno obdeluje.

9. člen

Pooblaščen osebno za varstvo osebnih podatkov (v nadaljevanju: pooblaščen osebno) je osebno z ustreznimi poklicnimi odlikami in zlasti strokovnim znanjem o zakonodaji in praksi na področju varstva osebnih podatkov, ki upravljavcu na neodvisen način pomaga pri zagotavljanju skladnosti obdelave osebnih podatkov s pravili Splošne uredbe ter določbami veljavnih predpisov, ki urejajo obdelavo in varstvo osebnih podatkov.

10. člen

Pooblaščen osebno za varstvo podatkov ima naslednje naloge:

- *obveščanje upravljalca in zaposlenih, ki izvajajo obdelavo, ter svetovanje navedenim o njihovih obveznostih;*
- *spremljanje skladnosti z veljavnimi predpisi in politikami upravljalca v zvezi z varstvom osebnih podatkov, vključno z dodeljevanjem nalog, ozaveščanjem in usposabljanjem osebja, vključenega v dejanja obdelave, ter s tem povezanimi revizijami;*
- *sodelovanje z nadzornim organom;*
- *delovanje kot kontaktna točka za nadzorni organ pri vprašanjih v zvezi z obdelavo.*

Pooblaščen osebno opravlja navedene naloge v zvezi z vsemi obdelavami osebnih podatkov, ki jih izvaja upravljavec, pri katerem je imenovana.

11. člen

Upravljalca pooblaščen osebno zagotovi pogoje za učinkovito in neodvisno opravljanje njenih nalog po 10. členu tega pravilnika, zlasti:

- 1. je ustrezno in pravočasno vključena v vsa vprašanja in postopke, povezane z varstvom osebnih podatkov in ima možnost podati ustrezeni nasvet, mnenje ali predlog,*
- 2. ima dostop do vseh osebnih podatkov ter dejanj obdelave,*
- 3. ima na razpolago sredstva, potrebna za izvajanje njenih nalog in za ohranjanje njenega strokovnega znanja,*

4. lahko posamezniki, na katere se nanašajo osebni podatki, z njo v slovenščini ali v uradnem jeziku države prebivališča vstopijo v stik in se posvetujejo glede vseh vprašanj, povezanih z obdelavo njihovih osebnih podatkov in uresničevanje njihovih pravic po Splošni uredbi, ter

5. da ima neposredni dostop do vodstva upravljavca, če oceni, da je to zaradi določene obdelave osebnih podatkov nujno potrebno, zlasti kadar gre za tvegane obdelave, obdelave posebnih vrst osebnih podatkov, množične obdelave in vpliv na človekove pravice, temeljne svoboščine ali interese posameznikov, na katere se nanašajo osebni podatki ali za očitno neustreznost ukrepov zavarovanja osebnih podatkov.

Upravljavec zagotovi, da pooblaščen osebni pri izvajanju svojih nalog ne prejema nobenih navodil. Pooblaščen osebni o svojem izvedenem delu neposredno in neodvisno poroča vodstvu upravljavca.

Upravljavec pooblaščen osebni za varstvo podatkov zaradi izvajanja njenih nalog ne sme razrešiti, je kaznovati ali je zapostavljati.

Odpoved delovnega razmerja pooblaščen osebni ni dovoljena za čas njenega imenovanja in še eno leto po prenehanju imenovanja, razen v primeru redne odpovedi iz razloga nesposobnosti ali krivdnega razloga, izredne odpovedi, odpovedi v postopku prenehanja delodajalca, oziroma če v primeru poslovnega razloga odkloni ponujeno ustrezno zaposlitev pri delodajalcu. V primeru spremembe delodajalca, pooblaščen osebni ohrani svoj položaj pooblaščen osebni, če pri delodajalcu prevzemniku še naprej obstaja obveznost imenovanja v skladu s tem zakonom.

Pooblaščen osebni in v njenem imenu delujoče osebe so pri opravljanju nalog zavezani k varstvu zaupnosti obdelovanih osebnih podatkov. Pooblaščen osebni in v njenem imenu delujoče osebe smejo informacije, ki so jim bile dane na razpolago, uporabljati izključno za opravljanje nalog, in so tudi po zaključku dejavnosti zavezane k varovanju zaupnosti podatkov. To velja zlasti v zvezi z identiteto posameznika, na katerega se nanašajo osebni podatki, ki se je obrnil na pooblaščen osebni za varstvo podatkov.

Če ima pooblaščen osebni za varstvo podatkov pri svoji dejavnosti vpogled v podatke, v zvezi s katerimi ima osebni, ki je podvržena nadzoru pooblaščen osebni, pravico do molka, ta pravica velja tudi za pooblaščen osebni in za v njenem imenu delujoče osebe, in sicer do mere, v kateri je osebni, ki ima zakonsko pravico do molka, slednjo uveljavila.

VAROVANJE PROSTOROV IN RAČUNALNIŠKE OPREME

12. člen

Dostop v prostore kjer se nahajajo nosilci varovanih osebnih podatkov je mogoč in dopusten le v delovnem času, izven delovnega časa pa le na podlagi dovoljenja vodje (direktorja).

Ključni varovanih prostorov se uporabljajo in hranijo v prostorih upravljalca in se uporabljajo v skladu z navodilom o varovanju in uničevanju ključev.

Nosilci osebnih podatkov, hranjeni izven aktivnih delovnih prostorov oziroma izven varovanih prostorov (hodniki, skupni prostori, aktivni arhivi ipd.), morajo biti stalno shranjeni v zaklenjenem prostoru upravljalca.

13. člen

Izven delovnega časa morajo biti nosilci osebnih podatkov shranjeni v zaklenjenih omarah v delovnih prostorih.

Računalniki ali druga strojna oprema, na kateri se obdelujejo ali hranijo osebni podatki, mora biti izven delovnega časa izklopljena in fizično ali programsko zaklenjena, dostop do osebnih podatkov, hranjenih na disku računalnika pa kodiran.

14. člen

V varovane prostore osebe, z izjemo pooblaščenih osebe za varstvo osebnih podatkov, ki ne delajo v prostorih in ki niso zaposlene pri upravljalcu, ne smejo vstopati brez predhodne najave. Delavci, ki delajo v varovanih prostorih, morajo vestno in skrbno nadzorovati prostor in ob zapustitvi prostora zakleniti prostor.

Delavec, ki pri svojem delu uporablja osebne podatke ali jih kakorkoli obdeluje, ne sme med delovnim časom puščati nosilcev osebnih podatkov na pisalnih mizah ali jih kako drugače izpostavljati nevarnosti vpogleda vanje nepooblaščenim osebam oziroma delavcem.

V prostorih, kjer imajo vstop stranke oziroma osebe, ki niso zaposlene pri upravljalcu, morajo biti nosilci podatkov in računalniški prikazovalniki nameščeni v času obdelave ali delna na njih tako, da strankam ni omogočen vpogled vanje.

15. člen

Nosilcev osebnih podatkov delavci upravljalca ne smejo odnašati izven prostorov upravljalca brez izrecnega dovoljenja vodje (direktorja).

Obdelovanje osebnih podatkov iz zbirk je dovoljeno le v prostorih upravljalca.

Posredovanje osebnih podatkov pooblaščenim zunanjim institucijam in drugim, ki izkažejo zakonsko ali pogodbeno podlago za pridobitev osebnih podatkov, dovoli vodja (direktor).

Delavec, ki s soglasjem direktorja posreduje osebne podatke zunanjim institucijam in drugim, ki izkažejo zakonsko ali pogodbeno podlago za pridobitev osebnih podatkov, mora dejstva o posredovanju osebnih podatkov vpisati v evidenco dejavnosti obdelave.

16. člen

Vzdrževanje in popravilo strojne računalniške in druge opreme, s katero se obdelujejo osebni podatki, je dovoljeno samo z vednostjo in odobritvijo pooblaščenih osebe (ali direktorja), izvajajo pa ga lahko samo pooblaščeni servisi in njihovi vzdrževalci, ki imajo z upravljalcem sklenjeno pogodbo o servisiranju računalniške oziroma strojne opreme.

17. člen

Vzdrževalci prostorov in druge opreme v varovanih prostorih, poslovni partnerji in drugi obiskovalci, se smejo gibati v varovanih prostorih le ob prisotnosti delavca.

ZAVAROVANJE SISTEMSKÉ IN APLIKATIVNE PROGRAMSKE RAČUNALNIŠKE OPREME TER PODATKOV, KI SE OBDELUJEJO Z RAČUNALNIŠKO OPREMO

18. člen

Dostop do računalniške programske opreme mora biti varovan na način, ki omogoča dostop samo določenim pooblaščenim delavcem in delavcem, ki za upravljalca po pogodbi opravljajo servisiranje računalniške in programske opreme.

19. člen

Za shranjevanje in varovanje aplikativne programske opreme veljajo enaka določila kot za ostale podatke iz tega pravilnika.

Delavec, pooblaščen za obdelavo in ravnanje z osebnimi podatki in računalniku, mora skrbeti, da se v primeru servisiranja, popravila, spreminjanja ali dopolnjevanja systemske ali aplikativne programske opreme, da se naredi varnostna kopija, ki se jo po zaključku navedene aktivnosti uniči.

Delavec, pooblaščen za obdelavo in ravnanje z osebnimi podatki in računalniku, mora biti v času servisiranja računalnika in programske opreme vse čas prisoten in mora nadzirati, da ne pride do nedopustnega ravnanja z osebnimi podatki.

20. člen

*Vsebina diskov mrežnega strežnika in lokalnih delovnih postaj, kjer se nahajajo osebni podatki, se dnevno preverja glede na prisotnost zlonamerne programske opreme
Ob pojavi zlonamerne programske opreme je potrebno storiti vse, da se s pomočjo strokovnjakov virus odpravi in da se ugotovi vzrok pojava virusa.*

21. člen

Zaposleni delavci ne smejo brez izrecnega dovoljenja direktorja inštalirati programske opreme in odnašati programske opreme iz prostora upravljalca.

DOSTOPNOST

22. člen

Upravljevec mora zagotoviti dostopnost obdelovanih podatkov.

Pristop do podatkov prek aplikativne programske opreme mora biti varovan s sistemom gesel za avtorizacijo in identifikacijo uporabnikov programov in podatkov.

Direktor določi režim dodeljevanja, hranjenja in spreminjanja gesel.

23. člen

Vsa gesla in postopki, ki se uporabljajo za vstop in za administriranje v mreži osebnih računalnikov, administriranje z elektronsko pošto in administriranje prek aplikativnih programov, se hranijo v zaprtih ovojnica v prostorih upravljalca.

Varovana gesla, hranjena v zaprtih ovojnica, se smejo uporabiti v izjemnih in nujnih primerih. Vsaka uporaba vsebine zaprtih ovojnic se dokumentira.

Po uporabi zaprtih gesel iz ovojnic direktor določi nova gesla.

24. člen

Za potrebe restavriranja osebnih podatkov oziroma računalniškega sistema po okvarah ali izgubi podatkov iz drugih razlog, mora upravljalca redno izdelovati kopije vsebine osebnih podatkov, ki jih vodi.

Vse izdelane kopije vsebin zbirk osebnih podatkov se morajo vpisati v knjigo evidenc dejavnosti obdelave.

Računalniške kopije vsebin zbirk osebnih podatkov se hranijo na zunanjih pomnilniških medijih in v zavarovanih zaklenjenih omarah.

RAVNANJE Z OSEBNIMI PODATKI IN ZBIRKAMI

25. člen

Pisemske pošiljke, ki vsebujejo osebne podatke, se pošiljajo naslovniku priporočeno s povratnico.

Prenašanje osebnih podatkov prek telekomunikacijskih sredstev, elektronske pošte ali drugih računalniških medijev izven prostorov upravljalca mora biti zavarovano s postopki in ukrepi na način, ki nepooblaščenim preprečuje prilaščanje, uničevanje ali nedovoljeno seznanjanje z njihovo vsebino.

Prenos osebnih podatkov po elektronski pošti mora biti zavarovan z geslom za identifikacijo.

ZAUPNOST PODATKOV

26. člen

Upravljalca mora zagotoviti zaupnost obdelovanih podatkov.

Organizacijsko, se zaupnost podatkov lahko zagotavlja v aktu o sistematizaciji delovnih mest, kjer se za vsako delovno mesto opredelijo pravice in pooblastila na posamezni zbirki. Če to v

sistemizaciji delovni mest ni podrobneje opredeljeno, omenjene pravice in pooblastila izhajajo iz operacijskega predpisa, ki je sprejet na podlagi tega pravilnika. Za vsako delovno mesto se v notranjih aktih upravljalca lahko opredeli tudi dolžnost varovanja zaupnosti osebnih podatkov.

Zaupnost podatkov se zagotavlja tudi s fizičnim varovanjem prostorov, sistemske in aplikativne programske opreme ter podatkovnih nosilcev.

POSREDOVANJE

27. člen

Upravljavec osebnih podatkov mora proti plačilu stroškov posredovanja, če zakon ne določa drugače, posredovati osebne podatke uporabnikom osebnih podatkov.

28. člen

Upravljavec mora za vsak prenos osebnih podatkov zagotoviti, da je mogoče pozneje ugotoviti, kateri osebni podatki so bili posredovani, komu, kdaj in po kateri pravni podlagi, in sicer za obdobje, ko je mogoče zakonsko varstvo pravic posameznika, na katerega se nanašajo osebni podatki, zaradi nedopustnega posredovanja osebnih podatkov.

Osebni podatki naročnikov se zbirajo v ustrezni programski opremi, ki je zaščitena z vstopnimi kodami. Namen zbiranja in obdelave podatkov je vzdrževanje aktivne evidence naročnikov storitev.

ROK HRAMBE OSEBNIH PODATKOV

29. člen

Upravljavalec v skladu z načelom sorazmernosti in namenom obdelave osebne podatke iz 4. člena pravilnika, hrani najkrajše mogoče obdobje.

BRISANJE

30. člen

Po prenehanju potrebe po vodenju osebnih podatkov, ki je zapisana na posebnih izjavi, ki jo stranka ali zaposleni podpišejo, se podatki zбриšejo oziroma uničijo nosilci podatkov, če to ni v nasprotju z veljavnimi splošnimi pravili, aktualnim pogodbenim razmerjem ali naravo delovnega razmerja.

31. člen

Brisanje osebnih podatkov na računalniških medijih se opravi na način, ki onemogoča restavriranje brisanih podatkov.

Osebni podatki, vsebovani na klasičnih nosilcih (listine, kartoteke, register, seznam) se brišejo z uničenjem nosilcev. Nosilci se fizično uničijo (zažgejo, razrežejo) v prostorih upravljalca, pod nadzorom pooblaščenega delavca upravljalca pa lahko tudi pri drugi organizaciji, ki se ukvarja z uničevanjem zaupne dokumentacije.

32. člen

Z vestnostjo in skrbnostjo določeno s tem pravilnikom za uničevanje osebnih podatkov, vodenih v zbirkah oziroma na posameznih nosilcih podatkov, se mora brisati in uničevati tudi pomožna dokumentacija ali računalniški produkti oziroma predloge, ki vsebujejo posamezne osebne podatke.

Uničevanje osebnih podatkov na nosilcih iz predhodnega odstavka se mora izvajati tekoče in ažurno.

UKREPANJE OB UGOTOVITVI O ZLORABI OSEBNIH PODATKOV ALI VDORU V ZBIRKE OSEBNIH PODATKOV

33. člen

Delavec, ki izve ali opazi, da je prišlo do zlorabe osebnih podatkov (odkrivanje osebnih podatkov, nepooblaščen uničevanje, nepooblaščen spreminjanje, poškodovanje zbirke, prilaščanje osebnih podatkov) ali do vdora v zbirko, mora o tem takoj obvestiti direktorja in pooblaščenega delavca, ki vodi in ureja zbirko, ki je bila zlorabljena ali v katero se je vdrl.

34. člen

Upravljalca mora o kršitvah varstva osebnih podatkov v 72 urah od seznanitve s kršitvijo, poslati uradno obvestilo informacijskemu pooblaščenцу, razen če ni verjetno, da bi bile s kršitvijo varstva osebnih podatkov ogrožene pravice in svoboščine posameznikov.

Obdelovalec po seznanitvi s kršitvijo varstva osebnih podatkov brez nepotrebnega odlašanja uradno obvesti upravljalca.

Kadar je verjetno, da kršitev varstva osebnih podatkov povzroči veliko tveganje za pravice in svoboščine posameznikov, upravljalca brez nepotrebnega odlašanja sporoči posamezniku, na katerega se nanašajo osebni podatki, da je prišlo do kršitve varstva osebnih podatkov.

Direktor mora zoper tistega, ki je zlorabil osebne podatke ali nepooblaščen vdrl v zbirko, ustrezno ukrepati.

Če obstaja sum pri vdoru v zbirko, da je ta storjen z naklepom in namenom zlorabiti osebne podatke ali jih uporabiti v nasprotju z nameni, za katere so zbrani ali če je do zlorabe osebnih podatkov že prišlo, mora direktor poleg uvedbe disciplinskega postopka zoper storilca ali izreka opomina pred redno odpovedjo pogodbe o zaposlitvi ali poleg redne odpovedi pogodbe o zaposlitvi iz krivdnih razlogov ali poleg izredne odpovedi pogodbe o zaposlitvi, če je ta delavec, vdor ali zlorabo oziroma poskus zlorabe prijaviti organom pregona.

Za zlorabo osebnih podatkov šteje vsaka uporaba osebnih podatkov v namene, ki niso v skladu z nameni zbiranja, določenimi v veljavnih predpisih, na podlagi katerih se zbirajo ali nameni, določenimi v zbirkah. Za poskus zlorabe šteje poskus uporabe osebnih podatkov v nedovoljene namene.

PRAVICE POSAMEZNIKOV, NA KATERE SE NANAŠAJO OSEBNI PODATKI

35. člen

Posameznik, na katerega se nanašajo osebni podatki, ima pravico od upravljavca dobiti potrditev, ali se v zvezi z njim obdelujejo osebni podatki, in kadar je temu tako, dostop do osebnih podatkov in naslednje informacije:

- (a) namene obdelave;*
- (b) vrste zadevnih osebnih podatkov;*
- (c) uporabnike ali kategorije uporabnika, ki so jim bili ali jim bodo razkriti osebni podatki, zlasti uporabnike v tretjih državah ali mednarodnih organizacijah;*
- (d) kadar je mogoče, predvideno obdobje hrambe osebnih podatkov ali, če to ni mogoče, merila, ki se uporabijo za določitev tega obdobja;*
- (e) obstoj pravice, da se od upravljavca zahteva popravek ali izbris osebnih podatkov ali omejitev obdelave osebnih podatkov v zvezi s posameznikom, na katerega se nanašajo osebni podatki, ali obstoj pravice do ugovora taki obdelavi;*
- (f) pravico do vložitve pritožbe pri nadzornem organu;*
- (g) kadar osebni podatki niso zbrani pri posamezniku, na katerega se ti nanašajo, vse razpoložljive informacije v zvezi z njihovim virom.*

Posameznik pred predajo osebnih podatkov podpiše posebno izjavo, na kateri označi osebne podatke, ki jih želi predati, ter določi namen, za katerega dovoljuje uporabo osebnih podatkov (izjava posameznika PRILOGA 1).

Upravljavec zagotovi kopijo osebnih podatkov, ki se obdelujejo. Za dodatne kopije, ki jih zahteva posameznik, na katerega se nanašajo osebni podatki, lahko upravljavec zaračuna razumno pristojbino ob upoštevanju upravnih stroškov.

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

Posameznik, na katerega se nanašajo osebni podatki, ima pravico doseči, da upravljavec brez nepotrebnega odlašanja izbriše osebne podatke v zvezi z njim, upravljavec pa ima obveznost

osebne podatke brez nepotrebnega odlašanja izbrisati, kadar velja eden od naslednjih razlogov:

(a) osebni podatki niso več potrebni v namene, za katere so bili zbrani ali kako drugače obdelani;

(b) posameznik, na katerega se nanašajo osebni podatki, prekliče privolitev, na podlagi katere poteka obdelava in kadar za obdelavo ne obstaja nobena druga pravna podlaga;

Kadar upravljavec objavi osebne podatke in je v skladu z odstavkom 4 osebne podatke obvezan izbrisati, ob upoštevanju razpoložljive tehnologije in stroškov izvajanja sprejme razumne ukrepe, vključno s tehničnimi, da upravljavce, ki obdelujejo osebne podatke, obvesti, da posameznik, na katerega se nanašajo osebni podatki, od njih zahteva, naj izbrišejo morebitne povezave do teh osebnih podatkov ali njihove kopije.

36. člen

Pred nastopom dela delavca na delovnem mestu (seznam pooblaščenih oseb PRILOGA 3), kjer se zbirajo, urejajo, obdelujejo, spreminjajo, shranjujejo, posredujejo ali uporabljajo osebni podatki ali nosilci osebnih podatkov, mora delavec podpisati izjavo (izjava delavca PRILOGA 2), ki ga zavezuje k varovanju osebnih podatkov kot poklicne skrivnosti in ki ga opozarja na posledice kršitve zaveze.

Obveza varovanja osebnih podatkov, s katerimi se delavec seznanil pri svojem delu pri upravljalcu traja tudi po prenehanju delovnega ali poslovnega razmerja pri upravljalcu.

37. člen

Delavec stori lažjo kršitev delovne dolžnosti:

- če opusti vestno in skrbno nadzorovanje varovanih prostorov (prva točka 6. člena tega pravilnika);
- če opusti ravnanja za preprečitev vpogleda v ali na nosilce osebnih podatkov (5. točka prvega odstavka 6. člena tega pravilnika);
- če ne uniči kopije osebnih podatkov v primerih iz 2. odstavka 14. člena tega pravilnika;
- če ni ves čas servisiranja računalnika in programske opreme prisoten (3. odstavek 19. tega pravilnika);
- če ne izvaja preventive v zvezi z računalniškimi virusi (20. člen tega pravilnika);
- če ne vodi evidence kopij vsebin zbirk osebnih podatkov v knjigi evidenc o ravnanju z osebniimi podatki (1. odstavek 24. člena tega pravilnika) in
- če ne obvesti direktorja ali pooblaščenega delavca v primeru zlorabe osebnih podatkov ali vdora v zbirko osebnih podatkov (33. člena tega pravilnika).

38. člen

Delavec stori hujšo kršitev delovne dolžnosti:

- če sporoča osebne podatke, s katerimi se je seznanil pri svojem delu, sodelavcem ali drugim osebam;
- če opusti skrb in nadzor nad nosilci osebnih podatkov med delovnim časom in tako dopusti možnost vpogleda vanje nepooblaščenim osebam (2. odstavek 14. člena tega pravilnika);

- če brez izrecnega dovoljenja odnaša iz prostorov upravljalca nosilce osebnih podatkov (15. člen tega pravilnika);
- če posreduje osebne podatke pooblaščenim eksternim institucijam brez dovoljenja direktorja (3. odstavek 15. člena tega pravilnika);
- če ne vpiše v evidenco dejavnosti obdelave dejstva o posredovanju osebnih podatkov eksternim institucijam (4. odstavek 15. člena tega pravilnika);
- če popravlja, spreminja ali dopolnjuje sistemsko ali aplikativno programsko opremo (19. člen tega pravilnika);
- če inštalira ali odnese programsko opremo iz prostorov upravljalca brez izrecnega dovoljenja direktorja (20. člen tega pravilnika);
- če ne hrani računalniških kopij vsebin zbirk osebnih podatkov v zaklenjenih omarah (3. odstavek 24. člena tega pravilnika).

POSEBNE UREDITVE ZA ZBIRKE OSEBNIH PODATKOV VODENIH PRI UPRAVLJALCU

1. Odgovorni delavci

39. člen

Za vzpostavitev, vodenje, ažuriranje in ravnanje z zbirkami osebnih podatkov in osebnimi podatki vodenimi pri upravljalcu so odgovorne osebe iz PRILOGE 2.

40. člen

Zbirke osebnih podatkov delavcev se vzpostavijo ob sklenitvi delovnega razmerja z delavcem oziroma ažurirajo ob vsaki spremembi, ki jo javi delavec. Osebne podatke v zbirki osebnih podatkov delavcev vzpostavi oziroma ažurira kadrovski delavec oziroma vodja računovodstva.

Zbirke osebnih podatkov kupcev se vzpostavijo ob povpraševanju in nakupu in se ažurirajo ob vsaki spremembi, ki jo javi kupec.

41. člen

Za hrambo zbirk osebnih podatkov so odgovorni delavci, ki so pooblaščeni za obdelovanje zbirk osebnih podatkov.

PREHODNE IN KONČNE DOLOČBE

42. člen

Zbirke, organizacija zavarovanja osebnih podatkov in ureditev drugih zadev določenih s tem pravilnikom se mora uskladiti z veljavnimi predpisi in določbami tega pravilnika v roku 60 dni od dneva sprejema tega pravilnika.

43. člen

Spremembe in dopolnitve tega pravilnika se sprejmejo po postopku in na način kot velja za sprejem pravilnika.

44. člen

Ta pravilnik prejmejo delavci, kjer se zbirajo, urejajo, obdelujejo, spreminjajo, shranjujejo, posredujejo ali uporabljajo osebni podatki ali nosilci osebnih podatkov. Pravilnik mora biti prosto dostopen v prostorih upravljalca, kot tudi objavljen na spletni strani upravljalca.

POGODBENA OBDELAVA

45. člen

Za obdelavo, ki jo zveza zaupa zunanjemu izvajalcu (obdelovalcu), zveza z obdelovalcem sklene pisno pogodbo o obdelavi, s katero določi kontaktne podatke in pooblaščen osebe pogodbenih strank, vrsto in način izvajanja obdelave ter navodila podjetja obdelovalcu glede obdelave osebnih podatkov, morebitne prenose obdelovanih podatkov v tretje države, opis tehničnih in organizacijskih varnostnih ukrepov, ki se morajo izvajati v zvezi z obdelavo, ter druge obveznosti in pravice obeh strank.

Pogodba zlasti določa, da obdelovalec:

- a) obdeluje le tiste osebne podatke in le za namen kot je določeno v pogodbi ter osebne podatke obdeluje samo po dokumentiranih navodilih zveze, vključno glede prenosov osebnih podatkov v tretjo državo ali mednarodno organizacijo, razen če to od njega zahteva veljavna zakonodaja;*
- b) zagotovi, da so osebe, ki bodo izvajale obdelavo, zavezane k varovanju zaupnosti;*
- c) sprejme vse ukrepe za varnost obdelave, predvidene v uredbi, ZVOP in tem pravilniku;*
- d) morebitnega drugega (pod)obdelovalca zaposli samo na podlagi predhodnega dovoljenja podjetja;*
- e) ob upoštevanju narave obdelave z ustreznimi tehničnimi in organizacijskimi ukrepi zvezi pomaga pri izpolnjevanju njegovih obveznosti, da odgovori na zahteve za uresničevanje pravic posameznika, na katerega se nanašajo osebni podatki;*
- f) zvezi pomaga pri izpolnjevanju obveznosti glede zagotavljanja varnosti obdelave, ki je predmet pogodbe, ter mu na zahtevo nemudoma posreduje vse podatke, ki se nanašajo na obdelavo;*
- g) na zahtevo zveze po zaključku storitve obdelave izbriše ali zvezi vrne vse podatke ter uniči morebitne kopije, če veljavni predpisi ne določajo drugače;*
- h) da zvezi, revizorju, ki ga pooblasti zveza, ali pristojnemu državnemu organu, ki izvaja nadzor nad varstvom osebnih podatkov, na voljo vse informacije, potrebne za dokazovanje skladnosti obdelave s predpisanimi zahtevami, in pri dokazovanju sodeluje.*

V kolikor pride do varnostnega incidenta, ki se nanaša na obdelavo po pogodbi, je obdelovalec dolžan nemudoma, najpozneje pa v roku 48 ur, o incidentu pisno obvestiti zvezo.

46. člen

Ta pravilnik začne veljati osmi dan po dnevu sprejema.

Datum sprejema: 17. 6. 2019



*Predsednik AZS
Roman Dobnikar*

A handwritten signature in blue ink, appearing to read "R. Dobnikar", is written over the printed name.