Na podlagi 29. člena Statuta Zveze društev upokojencev Slovenije je Upravni odbor Zveze društev upokojencev Slovenije na 29. redni seji dne 15. 5. 2019 sprejel naslednji

# Pravilnik
# o zavarovanju osebnih podatkov
# pri
# Zvezi društev upokojencev Slovenije

## I. SPLOŠNE DOLOČBE

1.člen

S tem pravilnikom se določajo organizacijski, tehnični in logistično-tehnični postopki in ukrepi za zavarovanje osebnih podatkov pri Zvezi društev upokojencev Slovenije; matična številka: 5147581000 (v nadaljevanju ZDUS) z namenom, da se prepreči slučajno ali namerno nepooblaščeno uničevanje podatkov, njihovo spremembo ali izgubo, kakor tudi nepooblaščen dostop, obdelava, uporaba ali posredovanje osebnih podatkov.

Zaposleni in zunanji sodelavci ZDUS, ki pri svojem delu obdelujejo in uporabljajo osebne podatke, morajo biti seznanjeni z predpisi s področja varstva osebnih podatkov in z vsebino tega pravilnika.

2. člen

V tem pravilniku uporabljeni izrazi imajo naslednji pomen:

1. **Osebni podatek** – je katerikoli podatek, ki se nanaša na določenega ali določljivega posameznika, ne glede na obliko, v kateri je izražen;
2. **Poseben osebni podatek** - je osebni podatek, ki se nanaša na rasno ali etično poreklo, politično mnenje, versko ali filozofsko prepričanje, podatki v zvezi z zdravjem ali spolno usmerjenostjo;
3. **Zbirka osebnih podatkov** – je vsak strukturiran niz 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;
4. **Obdelava osebnih podatkov** – pomeni kakršnokoli delovanje ali niz delovanj, ki se izvaja v zvezi z osebnimi podatki, ki so avtomatizirano obdelani ali ki so pri ročni obdelavi del zbirke osebnih podatkov, zlasti zbiranje, pridobivanje, vpis, urejanje, shranjevanje, prilaganje ali spreminjanje, priklicanje, vpogled, uporaba, razkritje s prenosom, sporočanje, širjenje ali drugo dajanje na razpolago, razvrstitev ali povezovanje, blokiranje, anonimiziranje, izbris ali uničenje; obdelava je lahko ročna ali avtomatizirana;
5. **Nosilec podatkov –** so vse vrste sredstev, na katerih so zapisani ali posneti osebni podatki (listine, akti, gradiva, spisi, računalniška oprema vključno s magnetnimi, optičnimi ali drugimi računalniškimi mediji, fotokopije, zvočno ali slikovno gradivo, mikrofilmi, naprave za prenos podatkov, ipd.);

## II. VAROVANJE PROSTOROV IN RAČUNALNIŠKE OPREME

4. člen

Prostori ZDUS, v katerih se nahajajo nosilci osebnih podatkov, strojna in programska oprema (v nadaljevanju varovani prostori), morajo biti varovani z organizacijskimi ter fizičnimi in tehničnimi ukrepi, ki onemogočajo nepooblaščenim osebam dostop do podatkov.

Dostop do varovanih prostorov je mogoč le v rednem delovnem času, izven tega časa pa samo na podlagi dovoljenja tajnika ali predsednika ZDUS.

Ključi varovanih prostorov se hranijo pri tajniku in se lahko dodelijo za posamezen varovan prostor (npr. pisarno) samo osebi, ki tam opravlja delo. Ključi se ne puščajo v ključavnici v vratih z zunanje strani.

Varovani prostori ne smejo ostajati nenadzorovani, oziroma se morajo zaklepati ob odsotnosti delavcev, ki jih nadzorujejo.

Izven delovnega časa morajo biti omare in pisalne mize z nosilci osebnih podatkov zaklenjene, računalniki in druga strojna oprema izklopljeni in fizično ali programsko zaklenjeni.

Zaposleni in druge delavci ZDUS ne smejo puščati nosilcev osebnih podatkov na mizah v prisotnosti oseb, ki nimajo pravice vpogleda vanje.

Nosilci osebnih podatkov, ki se nahajajo izven zavarovanih prostorov (hodniki, skupni prostori), morajo biti stalno zaklenjeni.

Posebni osebni podatki se ne smejo hraniti izven varovanih prostorov.

5. člen

V prostorih, ki so namenjeni poslovanju s strankami, morajo biti nosilci podatkov in računalniški prikazovalniki nameščeni tako, da stranke nimajo vpogleda vanje.

6. člen

Vzdrževanje in popravila strojne računalniške in druge opreme je dovoljeno samo z vednostjo tajnika ali od njega pooblaščene osebe, izvajajo pa ga lahko samo pooblaščeni servisi in vzdrževalci, ki imajo z ZDUS sklenjeno ustrezno pisno pogodbo, s katero so zavezani k varovanju osebnih podatkov, s katerimi se lahko seznanijo pri opravljanju svojega dela za ZDUS.

7. člen

Vzdrževalci prostorov, strojne in programske opreme, obiskovalci in poslovni partnerji se smejo gibati v zavarovanih prostorih samo z vednostjo tajnika ali od njega pooblaščene osebe. Čistilka, varnostniki idr., se lahko izven delovnega časa gibljejo samo v tistih varovanih prostorih, kjer je onemogočen vpogled v osebne podatke (nosilci podatkov so

shranjeni v zaklenjenih omarah in pisalnih mizah, računalniki in druga strojna oprema so izklopljeni ali kako drugače fizično ali programsko zaklenjeni).

## III. VAROVANJE SISTEMSKE IN APLIKATIVNO PROGRAMSKE RAČUNALNIŠKE OPREME TER PODATKOV, KI SE OBDELUJEJO Z RAČUNALNIŠKO OPREMO

8. člen

Dostop do programske opreme mora biti varovan tako, da dovoljuje dostop samo za to v naprej določenim zaposlenim ali pravnim ali fizičnim osebam, ki v skladu s pisno pogodbo za ZDUS opravljajo dogovorjene storitve in ki so zavezani k varovanju osebnih podatkov, s katerimi se lahko seznanijo pri opravljanju svojega dela za ZDUS.

9. člen

Popravljanje, spreminjanje in dopolnjevanje sistemske in aplikativne programske opreme je dovoljeno samo na podlagi odobritve tajnika ali od njega pooblaščene osebe, izvajajo pa ga lahko samo pooblaščeni servisi in organizacije in posamezniki, ki imajo z ZDUS sklenjeno ustrezno pisno pogodbo, s katero so zavezani k varovanju osebnih podatkov, s katerimi se lahko seznanijo pri opravljanju svojega dela za ZDUS. Izvajalci morajo spremembe in dopolnitve sistemske in aplikativne programske opreme ustrezno dokumentirati.

10. člen

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

11. člen

Vsebina diskov mrežnega strežnika in lokalnih delovnih postaj, kjer se nahajajo osebni podatki, se sprotno preverja glede na prisotnost računalniških virusov. Ob pojavu računalniškega virusa se tega čim prej odpravi s pomočjo ustrezne strokovne službe, obenem pa se ugotovi vzrok pojava virusa v računalniškem informacijskem sistemu.

Vsi osebni podatki in programska oprema, ki so namenjeni uporabi v računalniškem informacijskem sistemu, in prispejo na medijih za prenos računalniških podatkov ali preko telekomunikacijskih kanalov, morajo biti pred uporabo preverjeni glede prisotnosti računalniških virusov.

12. člen

Zaposleni in drugi delavci ZDUS ne smejo na računalniško opremo ZDUS inštalirati programske opreme brez vednosti osebe, zadolžene za delovanje računalniškega informacijskega sistema. Prav tako ne smejo odnašati programske opreme brez odobritve tajnika ali od njega pooblaščene osebe in vednosti osebe, zadolžene za delovanje računalniškega informacijskega sistema.

13. člen

Pristop do osebnih podatkov preko aplikativne programske opreme se varuje s sistemom gesel za avtorizacijo in identifikacijo uporabnikov programov in podatkov. Gesla za dostop morajo biti močna, potrebno jih je zamenjati najmanj enkrat letno in se smejo hraniti v bližini računalniške opreme ZDUS v vidni ali prepoznavni obliki.

14. člen

Vsa gesla, ki jih zaposleni ali drugi delavci ZDUS uporabljajo za dostop do programske opreme (npr. gesla za zagon sistema) se hranijo v zapečatenih ovojnicah in se jih varuje pred dostopom nepooblaščenih oseb. Tako varovana gesla se sme uporabiti samo v izjemnih primerih, če to odobri predsednik. Predsednik odobri razkritje in uporabo gesla, če je dostop do programske opreme s takšnim geslom nujen za potrebe delovnega procesa ZDUS in če to prevlada nad posegom v zasebnost delavca.

Vsaka takšna uporaba gesel in razloge za uporabo se dokumentira. Po vsaki takšni uporabi se o tem obvesti delavca, katerega geslo je bilo uporabljeno in delavec določi novo geslo.

15. člen

Za potrebe restavriranja računalniškega sistema ob okvarah in ob drugih izjemnih situacijah se zagotavlja redna izdelava kopij vsebine mrežnega strežnika in lokalnih postaj, če se podatki tam nahajajo.

Te kopije se hranijo v zato določenih mestih, ki morajo biti ognjevarna, zavarovana proti poplavam in elektromagnetnim motnjam, v okviru predpisanih klimatskih pogojev ter zaklenjena.

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

16. člen

Z vsako zunanjo pravno ali fizično osebo, ki v imenu ZDUS opravlja posamezna opravila v zvezi z zbiranjem, obdelovanjem, shranjevanjem ali posredovanjem osebnih podatkov, se sklene pisna pogodba, predvidena v predpisih s področja varstva osebnih podatkov. V takšni pogodbi morajo biti obvezno predpisani tudi pogoji in ukrepi za zagotovitev varstva osebnih podatkov in njihovega zavarovanja ter pravice in obveznosti ZDUS ter izvajalca. Omenjeno velja tudi za zunanje osebe, ki vzdržujejo strojno in programsko opremo ter izdelujejo in instalirajo novo strojno ali programsko opremo.

Zunanje pravne ali fizične osebe smejo opravljati samo storitve obdelave osebnih podatkov v okviru navodil ZDUS in podatkov ne smejo obdelovati ali drugače uporabljati za noben drug namen.

## V. SPREJEM IN POSREDOVANJE OSEBNIH PODATKOV

17. člen

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

Delavec, ki je zadolžen za sprejem in evidenco pošte, odpira in pregleduje vse poštne pošiljke in pošiljke, ki na drug način prispejo na ZDUS – prinesejo jih stranke ali kurirji, razen pošiljk iz tretjega in četrtega odstavka tega člena.

Delavec, ki je zadolžen za sprejem in evidenco pošte, ne odpira tistih pošiljk, ki so naslovljene na drug organ ali organizacijo in so pomotoma dostavljene.

Delavec, ki je zadolžen za sprejem in evidenco pošte, ne sme odpirati pošiljk, naslovljenih na delavca, na katerih je na ovojnici navedeno, da se vročijo osebno naslovniku, ter pošiljk, na katerih je najprej navedeno osebno ime delavca brez označbe njegovega uradnega položaja in šele nato naslov ZDUS, razen, če to ni drugače urejeno s posebnim pooblastilom.

Osebnih podatkov iz zbirk ZDUS ni dovoljeno odtujevati v komercialne, trženjske in druge pridobitne namene.

18. člen

Osebne podatke je dovoljeno prenašati z informacijskimi, telekomunikacijskimi in drugimi sredstvi le ob izvajanju postopkov in ukrepov, ki nepooblaščenim preprečuje prilaščanje ali uničevanje podatkov ter neupravičeno seznanjanje z njihovo vsebino.

Osebni podatki se v primeru pošiljanja po navadni pošti, pošiljajo priporočeno.

Ovojnica, v kateri se posredujejo posebni podatki, mora biti izdelana na takšen način, da ne omogoča, da bi bila ob normalni svetlobi ali pri osvetlitvi ovojnic z običajno lučjo vidna vsebina ovojnice. Prav tako mora ovojnica zagotoviti, da odprtja ovojnice in seznanitve z njeno vsebino ni mogoče opraviti brez vidne sledi odpiranja ovojnice.

Posebni osebni podatki se v primeru pošiljanja po navadni pošti pošiljajo naslovnikom v zaprtih ovojnicah proti podpisu v dostavni knjigi ali z vročilnico.

Posebni osebni podatki se v primeru pošiljanja po elektronski pošti pošiljajo v šifrirani obliki.

19. člen

Obdelava posebnih osebnih podatkov mora biti posebej označena in zavarovana (npr. z označbo na fasciklu).

20. člen

Osebni podatki se posredujejo samo tistim zunanjim osebam (uporabnikom), ki se izkažejo z ustrezno zakonsko podlago ali s pisno zahtevo oziroma privolitvijo posameznika, na katerega se podatki nanašajo ali če ima ZDUS sam ustrezno podlago za takšno posredovanje.

Za vsako posredovanje osebnih podatkov, ki se izvede na prošnjo ali zahtevo zunanje osebe (uporabnika) mora takšna oseba vložiti pisno vlogo, v kateri mora biti jasno navedena pravna podlaga za posredovanje osebnih podatkov. Če je pravna podlaga privolitev posameznika, mora biti ta priložena vlogi.

Vsako posredovanje osebnih podatkov se beleži v evidenco posredovanj, iz katere mora biti razvidno, kateri osebni podatki so bili posredovani, komu, kdaj in na kakšni podlagi.

Nikoli se ne posredujejo originali dokumentov, razen v primeru pisne odredbe sodišča. Originalni dokument se mora v času odsotnosti nadomestiti s kopijo.

## VI. BRISANJE PODATKOV

21. člen

Po preteku roka hranjenja se osebni podatki arhivirajo v skladu s predpisi o arhiviranju dokumentarnega gradiva, zbrišejo oz. uničijo, razen če zakon ali drug akt ne določa drugače.

Osebne mape zaposlenih pri ZDUS se ob prenehanju delovnega razmerja pregledajo in se iz njih izbriše osebne podatke, za katere v zakonu ni podlage za trajno hrambo. Pregled se opravi tudi preden gre mapa v trajno arhiviranje.

22. člen

Za brisanje podatkov iz računalniških medijev se uporabi takšna metoda brisanja, da je nemogoča restavracija vseh ali dela brisanih podatkov.

Podatki na klasičnih medijih (listine, kartoteke, register, seznam,…) se uničijo na način, ki onemogoča branje vseh ali dela uničenih podatkov.

Na enak način se uničuje pomožno gradivo (npr. matrice, izračune in grafikone, skice, poskusne oziroma neuspešne izpise itd.).

Prepovedano je odmetavati odpadne nosilce podatkov z osebnimi podatki v koše za smeti.

Pri prenosu nosilcev osebnih podatkov na mesto uničevanja je potrebno zagotoviti ustrezno varovanje tudi v času prenosa.

Prenos nosilcev podatkov na mesto uničenja ter uničevanje nosilcev osebnih podatkov nadzoruje posebna komisija, ki o uničevanju sestavi tudi ustrezen zapisnik.

## VII. UKREPANJE OB SUMU NEPOOBLAŠČENEGA DOSTOPA

23. člen

Zaposleni in drugi delavci ZDUS so dolžni o aktivnostih, ki so povezane z odkrivanjem ali nepooblaščenim uničevanjem zaupnih podatkov, zlonamerni ali nepooblaščeni uporabi, prilaščanju, spreminjanju ali poškodovanju osebnih podatkov takoj obvestiti tajnika ali predsednika, sami pa storiti vse potrebno, da se takšno aktivnost prepreči in da se zavaruje osebne podatke.

## VIII. ODGOVORNOST ZA IZVAJANJE VARNOSTNIH UKREPOV IN POSTOPKOV

24. člen

Za izvajanje postopkov in ukrepov za zavarovanje osebnih podatkov po tem pravilniku je odgovoren tajnik. Predsednik ali Upravni odbor ZDUS lahko v okviru svojih pristojnosti na lastno pobudo ali na predlog tajnika izdata dodatna navodila glede izvajanja tega pravilnika.

Nadzor nad izvajanjem postopkov in ukrepov, določenih s tem pravilnikom, opravlja Nadzorni odbor ZDUS.

25. člen

Vsak zaposlen ali drug delavec ZDUS, ki pri opravljanju svojega dela za ZDUS obdeluje osebne podatke, je dolžan izvajati predpisane postopke in ukrepe za zavarovanje podatkov in varovati podatke, za katere je zvedel oziroma bil z njimi seznanjen pri opravljanju svojega dela. Obveza varovanja podatkov ne preneha s prenehanjem delovnega ali drugega pogodbenega razmera.

Pred nastopom dela na delovno mesto, kjer se obdelujejo osebni podatki, mora zaposleni podpisati posebno izjavo, ki ga zavezuje k varovanju osebnih podatkov.

Iz podpisane izjave mora biti razvidno, da je podpisnik seznanjen z določbami tega pravilnika, izjava pa mora vsebovati tudi pouk o posledicah kršitve.

26. člen

Za kršitev določil iz prejšnjega člena so zaposleni disciplinsko odgovorni, ostali pa na temelju pogodbenih obveznosti.

## IX. EVIDENCE OBDELAV OSEBNIH PODATKOV

27. člen

Upravni odbor za vsako zbirko osebnih podatkov v ZDUS sprejme v skladu s predpisi evidenco dejavnosti obdelave osebnih podatkov v zbirki, če ZDUS te podatke obdeluje redno, če zbirka vsebuje posebne osebne podatke ali če obdelava osebnih podatkov v zbirki pomeni

predstavlja tveganje za pravice in svoboščine posameznikov, na katere se nanašajo osebni podatki.

Evidenco dejavnosti obdelave osebnih podatkov vsebuje najmanj namen obdelave, opis kategorij posameznikov, na katere se nanašajo osebni podatki, vrste osebnih podatkov, uporabniki, ki so jim bili ali jim bodo razkriti osebni podatki, rok hrambe osebnih podatkov ter opis tehničnih in organizacijskih varnostnih ukrepov za zavarovanje osebnih podatkov.

## X. DOLOČITEV OSEB, ODGOVORNIH ZA DOLOČENO ZBIRKO OSEBNIH PODATKOV, OSEB, KI SO ZAVEZANE K POROČANJU O KRŠITVAH IN OSEB, KI LAHKO OBDELUJEJO OSEBNE PODATKE

28. člen

Upravni odbor ZDUS za vsako zbirko osebnih podatkov v ZDUS, s sklepom določi osebo ali osebe:
- ki je odgovorna, da se osebni podatki v zbirki obdelujejo v skladu s tem pravilnikom in predpisi ter, da se prepreči razkritje osebnih podatkov iz zbirke nepooblaščenim osebam,
- ki imajo za potrebe izvajanja svojih nalog za ZDUS pravico do dostopa do zbirke in do obdelave osebnih podatkov v njej,
- ki je odgovorna za zagotavljanje pravic posameznikov, katerih osebni podatki so v zbirki in
- ki je odgovorna za obveščanje nadzornih organov in posameznikov v primeru kršitev varnosti osebnih podatkov v zbirki.

## IX. KONČNE DOLOČBE

29. člen

Ta pravilnik spreminja ali dopolnjuje Upravni odbor ZDUS.

28. člen

Ta pravilnik prične veljati naslednji dan, ko ga sprejme Upravni odbor ZDUS.

Z dnem veljavnosti tega pravilnika preneha veljati Pravilnik o zavarovanju osebnih podatkov z dne 19. 6. 2008.

V Ljubljani, dne 15. 5. 2019

Janez Sušnik,
predsednik ZDUS in predsednik Upravnega odbora ZDUS