Študentska organizacija Slovenije
Dunajska cesta 51
1000 Ljubljana

Na podlagi določil Splošne uredbe o varstvu osebnih podatkov (Uredba (EU) 2016/679 Evropskega parlamenta in Sveta z dne 27. aprila 2016) in 33. člena Študentske ustave (ŠU-3-UPB, Uradni list Republike Slovenije, št. 14/18), po predhodni seznanitvi delavcev, dne 24. 5. 2018, sprejema Predsedstvo Študentske organizacije Slovenije na svoji 3. korespondenčni seji dne 24. 5. 2018 naslednji

PRAVILNIK O VARNOSTI OSEBNIH PODATKOV

1. člen
(splošne določbe)

(1) S tem pravilnikom se na Študentski organizaciji Slovenije (v nadaljevanju: ŠOS) določajo organizacijski, tehnični in logično-tehnični postopki in ukrepi za varnost osebnih podatkov na ŠOS z namenom, da se prepreči slučajno, namerno ali drugače nezakonito uničenje, spremembo, izgubo, nepooblaščeno razkritje, dostop ali drugo nepooblaščeno obdelavo osebnih podatkov.

(2) Določbe tega pravilnika se smiselno uporabljajo tudi za varnost podatkov, ki so v dokumentaciji tehničnega in poslovnega značaja s strani ŠOS in/ali zunanjih izvajalcev označeni kot poslovna skrivnost in/ali imajo oznako zaupno.

(3) Določbe tega pravilnika veljajo za zaposlene in funkcionarje na ŠOS ter zunanje izvajalce, ki pri svojem delu obdelujejo in uporabljajo osebne podatke. Za navedene osebe velja, da so seznanjene z vsakokrat veljavnimi predpisi s področja varstva osebnih podatkov, kot jih določa 4. člen tega pravilnika.

2. člen
(uporaba spola)

(1) V tem pravilniku uporabljeni izrazi, zapisani v moški spolni slovnični obliki, se uporabljajo kot nevtralen izraz za moške in ženske.

3. člen
(pomen izrazov)

(1) V tem pravilniku uporabljeni izrazi imajo naslednji pomen:
a) **Osebni podatek** – 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, gensko, duševno, gospodarsko, kulturno ali družbeno identiteto tega posameznika.

b) **Obdelava osebnih podatkov** – 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.

c) **Psevdonimizacija** – pomeni obdelavo osebnih podatkov na 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.

d) **Zbirka** – je 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.

e) **Upravljavec** – pomeni fizično ali pravno osebo, javni organ, agencijo ali drugo telo, 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.

f) **Obdelovalec** – pomeni fizično ali pravno osebo, javni organ, agencijo ali drugo telo, ki obdeluje osebne podatke v imenu upravljavca.

g) **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.

h) **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 pooblaščene za obdelavo osebnih podatkov pod neposrednim vodstvom upravljavca ali obdelovalca.

i) **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 za obdelavo osebnih podatkov, ki se nanašajo nanj.

j) **Kršitev varstva osebnih podatkov** – pomeni 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.

k) **Nadzorni organ** – pomeni neodvisen javni organ, Informacijskega pooblaščenca, določenega z vsakokrat veljavnim Zakonom o varstvu osebnih podatkov ter zakonom, ki ureja informacijskega pooblaščenca.
l) **Splošna uredba o varstvu osebnih podatkov** – Uredba (EU) 2016/679 Evropskega parlamenta in Sveta z dne 27. aprila 2016 o varstvu posameznikov pri obdelavi osebnih podatkov in o prostem pretoku takih podatkov ter o razveljavitvi Direktive 95/46/ES.
m) **Predpisi s področja varstva osebnih podatkov** – pomeni predpise, ki urejajo področje varnosti osebnih podatkov (primeroma: Splošna uredba, Zakon o varstvu osebnih podatkov, področna zakonodaja, ki se nanaša na varstvo osebnih podatkov, predmetni pravilnik ipd.).
n) **Nosilci osebnih podatkov** – pomeni vse vrste sredstev, na katerih so zapisani ali posneti podatki (listine, akti, gradiva, spisi, računalniška oprema, vključno z magnetnimi, optičnimi ali drugimi računalniškimi mediji, fotokopije, zvočno in slikovno gradivo, tračne enote, naprave za prenos podatkov ipd.).
o) **Varovani prostori** – pomeni prostore, v katerih se nahajajo nosilci podatkov, ki vsebujejo osebne podatke, poslovne skrivnosti in druge zaupne podatke, strojna in programska oprema.
p) **Poslovna skrivnost** – so podatki, ki so označeni z oznako zaupnosti v skladu z Zakonom o gospodarskih družbah in so podrobneje opredeljeni v Organizacijskem predpisu – 08: Klasifikacija in ravnanje z informacijami.

4. člen
(evidenca dejavnosti obdelav in vzpostavitev zbirke osebnih podatkov)

(1) ŠOS vodi evidenco dejavnosti obdelav. Del evidence dejavnosti obdelav so posamezne zbirke osebnih podatkov, katerih upravljavec ali obdelovalec je ŠOS.

(2) Zbirko osebnih podatkov na posameznem delovnem področju ŠOS vzpostavi odgovorna oseba za določeno zbirko osebnih podatkov (v nadaljevanju: odgovorna oseba), ki jo določi generalni sekretar ŠOS.

(3) Zaposleni, ki obdelujejo osebne podatke (v nadaljevanju: pooblaščeni obdelovalci), morajo biti seznanjeni z evidenco dejavnosti obdelav, vpogled v evidenco dejavnosti obdelav osebnih podatkov pa je potrebno omogočiti vsakomur, ki to zahteva.

(4) Zbirka osebnih podatkov v evidenci dejavnosti obdelav se dopolnjuje ob vsaki spremembi vrste osebnih podatkov.

5. člen
(seznam zbirk osebnih podatkov)

(1) ŠOS je dolžna voditi ažuren seznam, iz katerega je za vsako zbirko osebnih podatkov jasno razvidno, kdo je odgovorna oseba za posamezno zbirko osebnih podatkov ter katere osebe so pooblaščeni obdelovalci. V seznam se vpisujejo sledeči podatki:

a) naziv zbirke osebnih podatkov,
b) osebno ime in delovno mesto odgovorne osebe ter
c) osebno ime in delovno mesto pooblaščenih obdelovalcev.

6. člen
(obdelava osebnih podatkov)

(1) V zbirki osebnih podatkov se lahko obdelujejo le tisti osebni podatki, ki imajo ustrezno pravno podlago, ki je določena v 6. členu Splošne uredbe (primer: zakon, privolitev posameznika, pogodba itd.).

(2) Osebni podatki se smejo zbirati samo za določene in zakonite namene ter se ne smejo nadalje obdelovati tako, da bi bila njihova obdelava v neskladju s temi nameni, razen če zakon določa drugače.

(3) Odgovorne osebe in pooblaščeni obdelovalci morajo biti pred obdelavo osebnih podatkov seznanjene z določbami predpisov s področja varstva osebnih podatkov.

(4) V primeru, da je pravna podlaga za obdelavo osebnih podatkov podana osebna privolitev posameznika, mora biti slednji obveščen o obdelavi osebnih podatkov na način kot določa 13. člen Splošne uredbe.

(5) Obdelava osebnih podatkov lahko poteka na način, da se osebni podatki posameznikov psevdonimizirajo.

7. člen
(posredovanje osebnih podatkov)

(1) Osebni podatki se na zahtevo uporabnika posredujejo samo tistim uporabnikom, ki se izkažejo z ustrezno zakonsko podlago ali s pisno privolitvijo posameznika, na katerega se podatki nanašajo.

(2) Osebni podatki se po uradni dolžnosti posredujejo samo tistim uporabnikom, ki imajo ustrezno zakonsko podlago.

(3) Uporabnik lahko posredovanje osebnih podatkov iz prvega odstavka tega člena zahteva s pisno vlogo. Ob vložitvi pisne vloge mora uporabnik jasno navesti določbo zakona, ki ga pooblašča za pridobitev osebnih podatkov, ali pa mora k vlogi priložiti pisno privolitev posameznika, na katerega se podatki nanašajo. Vlogo preuči generalni sekretar ŠOS v sodelovanju s pooblaščeno osebo za varstvo osebnih podatkov na ŠOS.

(4) Osebni podatki, ki se posredujejo uporabniku v fizični obliki, morajo biti posredovani v ovojnici, ki ne omogoča, da bi bila ob normalni svetlobi ali pri osvetlitvi ovojnice z običajno lučjo vidna vsebina ovojnice. Ovojnica mora tudi zagotoviti, da odprtja ovojnice in seznanitve z njeno vsebino ni mogoče opraviti brez vidne sledi odpiranja ovojnice.

(5) Osebne podatke je dovoljeno posredovati z informacijskimi, komunikacijskimi in drugimi sredstvi le ob izvajanju postopkov in ukrepov, ki nepooblaščenim osebam preprečujejo prilaščanje ali uničenje podatkov ter neupravičeno seznanjanje z njihovo vsebino.

(6) Delavec, ki je zadolžen za sprejem in evidenco pošte, mora izročiti poštno pošiljko z osebnimi podatki direktno posamezniku, na katerega je pošiljka naslovljena.

(7) Delavec, ki je zadolžen za sprejem in evidenco pošte, odpira in pregleduje vse poštne pošiljke in pošiljke, ki na drug način prispejo na ŠOS - prinesejo jih stranke ali kurirji, razen pošiljk:
a) ki so naslovljene na drug organ ali organizacijo in so pomotoma dostavljena ali
b) kjer je na ovojnici navedeno, da se vročijo osebno naslovniku ali
c) na katerih je navedena ŠOS in poslovni naslov ter navedeno osebno ime delavca.

(8) Osebni podatki se pošiljajo priporočeno.

(9) ŠOS nikoli ne posreduje originalnih dokumentov, razen v primeru pisne odredbe sodišča.

8. člen
(evidenca posredovanj)

(1) Vsako posredovanje osebnih podatkov iz 2. člena se zaznamuje z navedbo naslednjih podatkov:
a) kateri osebni podatki so bili posredovani,
b) osebno ime/firmo in naslov/sedež osebe, ki so ji bili posredovani osebni podatki, oziroma navedba, da je bilo posredovanje opravljeno po uradni dolžnosti,
c) datum in ura posredovanja osebnih podatkov ter

d) pravna podlaga, na kateri so bili posredovani osebni podatki.
e) Uradni zaznamek iz prejšnjega odstavka je v pisni ali elektronski obliki kot del podatkov zadeve, o kateri se vodi postopek.

(2) Uradni zaznamek iz prvega odstavka tega člena naredi odgovorna oseba ali pooblaščeni obdelovalec, ki je podatke posredoval uporabniku.

(3) Določbe 2. in 3. člena se smiselno uporabljajo tudi za posredovanje osebnih podatkov zaposlenih znotraj ŠOS.

9. člen
(hramba osebnih podatkov)

(1) Osebni podatki se lahko shranjujejo le toliko časa, kot je razvidno iz posamezne zbirke osebnih podatkov. Za brisanje/uničenje podatkov se uporabljajo določbe področne zakonodaje.

(2) Po preteku roka hranjenja se osebni podatki zbrišejo, uničijo, blokirajo ali anonimizirajo, razen če zakon za posamezne vrste osebnih podatkov ne določa drugače.

(3) Za brisanje osebnih podatkov v elektronski obliki se uporabi takšna metoda brisanja, da je nemogoča restavracija vseh ali dela brisanih podatkov.

(4) Osebni podatki v fizični obliki se uničijo na način, s katerim se zagotovi, da postane osebni podatek nerazpoznaven in neobnovljiv (npr. rezalnik papirja). Prepovedano je odmetavati odpadne nosilce podatkov, ki vsebujejo osebne podatke, na način, ki omogoča obnovitev ali razpoznavnost osebnih podatkov (npr. v koš za smeti).

(5) Pri prenosu nosilcev osebnih podatkov na mesto uničenja je potrebno zagotoviti ustrezno zavarovanje tudi v času prenosa.

11.člen
(varovanje prostorov)

(1) ŠOS ima poslovne prostore na Dunajski cesti 51 v Ljubljani. Vhod v stavbo je varovan z varnostnikom in alarmnim sistemom, poslovni prostori pa z varnostnimi vrati.

(2) Nosilci osebnih podatkov se nahajajo v ustrezno varovanih prostorih/mestih, ki onemogočajo nepooblaščenim osebam dostop do podatkov. Nosilci osebnih podatkov se nahajajo v varovanih prostorih ŠOS.

(3) Varovani prostori morajo biti varovani s tehničnimi in organizacijskimi ukrepi, s katerimi se varujejo osebni podatki ter preprečuje njihovo slučajno, namerno ali drugače nezakonito uničenje, spremembo, izgubo, nepooblaščeno razkritje, dostop ali drugo nepooblaščeno obdelavo.

(4) Dostop v prostore je mogoč le v rednem delovnem času, izven tega časa pa samo po predhodni odobritvi generalnega sekretarja ŠOS. Izven delovnega časa je vklopljena alarmna naprava. Vstop je mogoč le ob vpisu pravilnega gesla.

(5) Varovani prostori ne smejo ostajati nenadzorovani, oziroma se morajo zaklepati ob odsotnosti oseb, ki so zadolžene za njihov nadzor.

(6) V času odsotnosti oseb, odgovornih za varnost osebnih podatkov, morajo biti omare, pisalne mize in druga nahajališča nosilcev osebnih podatkov zaklenjeni, računalniki in druga strojna oprema izklopljeni in kako drugače fizično ali programsko zaklenjeni. Ključe se hranijo v skladu s hišnim redom in se ne puščajo v ključavnici v vratih od zunanje strani.

(7) Delavci in zunanji izvajalci ne smejo puščati nosilcev osebnih podatkov na mizah in drugih nezavarovanih mestih v prisotnosti oseb, ki nimajo pravice vpogleda v te podatke, nosilci podatkov in računalniški prikazovalniki pa morajo biti nameščeni tako, da te osebe nimajo vpogleda vanje.

(8) Vzdrževanje in popravila strojne računalniške in druge opreme lahko izvajajo samo pooblaščeni servisi in vzdrževalci, ki imajo s ŠOS sklenjeno ustrezno pogodbo.

(9) Vzdrževalci prostorov, strojne in programske opreme, obiskovalci in poslovni partnerji se smejo gibati v varovanih prostorih samo z vednostjo zaposlenega, ki nadzoruje varovani prostor, kjer se oseba giba.

12. člen
(varovanje računalniške opreme)

(1) Dostop do programske opreme mora biti varovan tako, da je omogočen dostop samo zaposlenim, ki jih je določil odgovorna oseba (generalni sekretar ŠOS) in zunanjim izvajalcem,

ki v skladu s pogodbo opravljajo dogovorjene storitve. Odobritev dostopa do programske opreme za zunanje izvajalce odobri generalni sekretar ŠOS.

(2) Popravljanje, spreminjanje in dopolnjevanje sistemske in aplikativne programske opreme je dovoljeno samo na podlagi odobritve pooblaščene osebe, izvajajo pa ga lahko samo pooblaščeni servisi in organizacije, ki imajo s ŠOS sklenjeno ustrezno pogodbo. Izvajalci morajo spremembe in dopolnitve sistemske in aplikativne programske opreme ustrezno dokumentirati.

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

(4) Na diskih mrežnega strežnika in lokalnih delovnih postaj, kjer se nahajajo osebni podatki, se avtomatsko preverja prisotnost računalniških virusov (z antivirusnim programom). V primeru, da se pojavi računalniški virus, ga odgovorna oseba nemudoma odpravi, obenem pa ugotovi vzrok pojava virusa v računalniškem informacijskem sistemu ŠOS in sprejme ustrezne ukrepe.

(5) Vsi osebni podatki in programska oprema, ki so namenjeni uporabi v računalniškem informacijskem sistemu, in prispejo na ŠOS na medijih za prenos računalniških podatkov ali preko telekomunikacijskih kanalov, morajo biti pred uporabo preverjeni glede prisotnosti računalniških virusov. Preverjanje opravi oseba, pooblaščena s strani generalnega sekretarja.

(6) Zaposleni ne smejo nameščati programske opreme brez vednosti generalnega sekretarja ŠOS. Zaposleni prav tako ne smejo odnašati programske opreme iz ŠOS brez odobritve generalnega sekretarja.

(7) Dostop do podatkov preko aplikativne programske opreme se varuje s sistemom gesel za avtorizacijo in identifikacijo uporabnikov programov in podatkov, sistem gesel pa mora omogočati tudi možnost naknadnega ugotavljanja, kdaj je bil opravljen vnos posameznih osebnih podatkov v zbirko podatkov, kdaj so bili podatki uporabljeni ali drugače obdelovani ter kdo je to storil.

(8) 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. Računalniške kopije vsebin zbirk osebnih podatkov (backup) na medijih se hranijo v zavarovanih zaklenjenih prostorih in v predpisanih klimatskih razmerah. Za varnostno kopiranje in shranjevanje podatkov je odgovoren generalni sekretar ŠOS.

13. člen
(pogodbena obdelava osebnih podatkov)

(1) ŠOS za potrebe pogodbene obdelave osebnih podatkov z vsako zunanjo pravno ali fizično osebo, ki opravlja posamezna opravila v zvezi z obdelavo osebnih podatkov in je registrirana za opravljanje takšne dejavnosti (obdelovalec), sklene pisno pogodbo, kot je določeno v 28. členu Splošne uredbe.

(2) Obdelovalec sme opravljati storitve obdelave osebnih podatkov samo v okviru pooblastil ŠOS kot upravljavca in podatkov ne sme obdelovati ali drugače uporabljati za noben drug namen.

(3) Obdelovalec, ki za ŠOS opravlja dogovorjene storitve izven prostorov upravljavca, mora imeti vsaj enako strog način varovanja osebnih podatkov, kakor ga predvideva ta pravilnik.

(4) Navedeno v 5. členu velja tudi za pogodbene obdelovalce, ki vzdržujejo obstoječo strojno in programsko opremo ter izdelujejo in nameščajo novo strojno ali programsko opremo.

(5) ŠOS vodi seznam zunanjih izvajalcev, ki vsebuje:
a) naziv in sedež zunanjega izvajalca,
b) ime in priimek oseb, ki izvajajo zunanje storitve ter kontaktne podatke teh oseb (naslov e-pošte in telefonska številka).

(6) Določbe tega pravilnika se smiselno uporabljajo tudi v primerih, ko je ŠOS obdelovalec osebnih podatkov.

(7) ŠOS lahko za vsak primer pogodbene obdelave poda pisno privolitev, da se obdelava osebnih podatkov podeli v obdelavo drugemu obdelovalcu (podobdelava).

14. člen
(ukrepanje ob sumu nepooblaščenega dostopa in obveščanje o kršitvah varnosti)

(1) ŠOS redno načrtuje, izvaja in upravlja procese, ki so potrebni za izpolnjevanje zahtev informacijske varnosti. V kolikor, kljub skrbnemu načrtovanju, izvajanju in upravljanju varnostnih procesov, pride do kršitve varstva osebnih podatkov, mora ŠOS reagirati na način in v rokih kot jih določa predmetni pravilnik.

(2) Zaposleni in funkcionarji so dolžni o aktivnostih, ki so povezane z odkrivanjem ali nepooblaščenim uničenjem zaupnih podatkov, nevestnim ravnanjem, zlonamerni ali nepooblaščeni uporabi, prilaščanju, spreminjanju ali ogrožanju celovitosti sistemov/strežnikov, odpovedovanje dostopnosti storitev (npr. denial of service – DOS/DDOS), spreminjanju ali okvari spletnih strani ali strežnikov, vdoru ali poizkusu vdora v sistem, prevari ipd. (v nadaljevanju: varnostni incident), nemudoma po zaznanem varnostnem incidentu obvestiti generalnega sekretarja ŠOS, sami pa poskušajo takšno aktivnost preprečiti. Prijava varnostnega incidenta se poda preko različnih kanalov (telefonski klic, elektronska pošta).V primeru, da se pri pregledu varnosti odkrije zlorabo pooblastil, mora biti o tem obveščen generalni sekretar ŠOS.

(3) V kolikor se pri pregledu varnosti odkrije, da je za varnostni incident odgovoren zaposleni ali funkcionar na ŠOS, mora biti o tem obveščen generalni sekretar ŠOS.

(4) Z nastankom varnostnega incidenta začne generalni sekretar ŠOS voditi ažuren, natančen in verodostojen zapis incidentov (v nadaljevanju: dnevnik aktivnosti), ki vsebuje vse informacije in akcije, povezane z varnostnim incidentom. Za vsak vnos v dnevnik je potrebno dodati datum, čas in vir informacije.

(5) Po končani aktivnosti osebe iz prejšnjega odstavka tega člena potrdijo odpravo incidenta. Vsi varnostni incidenti se beležijo v dokument »Varnostni incidenti«, ki je na strežniku ŠOS dostopen osebam, ki opravljajo preiskave incidentov. Ni dovoljeno razkrivati podatkov o preiskavi, njenega namena, podrobnosti ali rezultatov nikomur, razen tistim, za katere generalni sekretar ŠOS odloči, da se jim lahko razkrije.

(6) V kolikor je ŠOS upravljavec osebnih podatkov mora v primeru varnostnega incidenta, na podlagi 33. člena Splošne uredbe, obvestiti nadzorni organ najpozneje v 72 urah. V primeru, da je ŠOS obdelovalec osebnih podatkov, mora po seznanitvi z varnostnim incidentom brez nepotrebnega odlašanja uradno obvestiti upravljavca.

15. člen
(odgovornost za izvajanje varnostnih ukrepov in postopkov)

(1) Vsak, ki obdeluje osebne podatke (zaposleni, funkcionarji in zunanji izvajalci), je dolžan izvajati predpisane postopke in ukrepe za varnost osebnih podatkov v skladu s predpisi s področja varstva osebnih podatkov in varovati osebne podatke, za katere je zvedel oziroma bil z njimi seznanjen pri opravljanju svojega dela.

(2) Obveznost varstva osebnih podatkov ne preneha s prenehanjem delovnega razmerja, funkcije ali s prenehanjem veljavnosti pogodbe, ki je podlaga za obdelavo osebnih podatkov.

(3) Za izvajanje postopkov in ukrepov za varnost osebnih podatkov so odgovorne določene odgovorne osebe za posamezno delovno področje in pooblaščeni obdelovalci osebnih podatkov.

(4) Nadzor nad izvajanjem postopkov in ukrepov, določenih s tem pravilnikom, opravlja generalni sekretar ŠOS.

(5) Osebe, ki obdelujejo osebne podatke morajo podpisati posebno izjavo, ki jih veže k varovanju zaupnih podatkov in ravnanju z njimi.

(6) Iz podpisane izjave mora biti najmanj razvidno, da je podpisnik seznanjen z določbami predpisov s področja varstva osebnih podatkov in da izjava vsebuje tudi pouk o posledicah kršitev teh predpisov.

(7) Kršitev določil tega pravilnika s strani zaposlenih in funkcionarjev na ŠOS pomeni hujšo kršitev pogodbenih obveznosti iz delovnega razmerja, zunanji izvajalci pa za kršitve odgovarjajo na temelju pogodbenih obveznosti.

(8) Odgovornost iz prejšnjega odstavka ne izključuje kazenske in/ali odškodninske odgovornosti.

16. člen
(pooblaščena oseba za varstvo osebnih podatkov)

(1) Pooblaščeno osebo za varstvo osebnih podatkov s sklepom imenuje generalni sekreatr ŠOS.

(2) Med naloge pooblaščene osebe za varstvo osebnih podatkov spadajo zlasti:
a) obveščanja upravljavca ali obdelovalca in zaposlenih ter funkcionarjev, ki izvajajo obdelavo, ter svetovanje navedenim o njihovih obveznostih glede Splošne uredbe in drugimi določbami prava EU ali prava države članice EU,
b) spremljanje skladnosti s Splošno uredbo, drugimi določbami prava EU ali prava države članice EU o varstvu osebnih podatkov, vključno z dodeljevanjem nalog, ozaveščanjem in usposabljanjem osebja, vključenega v dejanja obdelave, ter s tem povezanimi revizijami,

c) svetovanje, kadar je to zahtevano, glede ocene učinka v zvezi z varstvom osebnih podatkov in spremljanje njenega izvajanja,
d) sodelovanje z nadzornim organom,
e) delovanje kot kontaktna točka za nadzorni organ pri vprašanjih v zvezi z obdelavo, vključno s predhodnim posvetovanjem, in, kjer je ustrezno, posvetovanje glede katerekoli druge zadeve.

(3) Pooblaščena oseba za varstvo osebnih podatkov po navodilu generalnega sekretarja ŠOS pripravi in skrbi za seznam odgovornih oseb in pooblaščenih obdelovalcev, ki pri svojem delu obdelujejo osebne podatke in ki morajo biti seznanjene s predpisi s področja varstva osebnih podatkov.

(4) Oseba, pooblaščena za varstvo osebnih podatkov na ŠOS, skrbi za proaktivnost pri obdelavi osebnih podatkov. Najmanj enkrat letno za zaposlene, funkcionarje in po potrebi tudi za zunanje izvajalce pripravi izobraževanje na temo varnosti osebnih podatkov in tveganj, ki jim je ŠOS izpostavljena zaradi neizvajanja predmetnega pravilnika.

(5) Varnostna politika na ŠOS, veljavnost predmetnega pravilnika in njihovega izvajanja v praksi, se morajo redno (najmanj enkrat letno) preverjati in dokumentirati.

KONČNE DOLOČBE

17. člen

(1) Pravilnik stopi v veljavo s 25. 5. 2018 in bo za zaposlene dostopen na strežniku ŠOS, zunanjim izvajalcem pa je na vpogled na sedežu ŠOS.

(2) S tem preneha veljati Pravilnik o postopkih in ukrepih za zavarovanje zaupnih in osebnih podatkov z dne 20. 8. 2016.

(3) Spremembe in dopolnitve pravilnika se sprejemajo po enakem postopku, kot je bil sprejet.

Ljubljana, 24. 5. 2018

Jaka Trilar
predsednik ŠOS