Predsedstvo Zveze slovenskih častnikov (v nadaljevanju Predsedstvo) je na podlagi prve alineje 22. člena in v povezavi s 36. členom Statuta Zveze slovenskih častnikov (v nadaljevanju Statut) na svoji 7. seji, dne 12. 12. 2018 sprejelo

PRAVILNIK
o zavarovanju osebnih podatkov

I. SPLOŠNE DOLOČBE

1. člen

S Pravilnikom o zavarovanju osebnih podatkov (v nadaljevanju Pravilnik) se določajo organizacijski, tehnični in logično-tehnični postopki ter ukrepi za zavarovanje osebnih podatkov v Zvezi slovenskih častnikov (v nadaljevanju Zveza) 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.

2. člen

(1)V tem pravilniku uporabljeni izrazi imajo enake pomene, kot jih določa 4. člen Splošne uredbe EU o varstvu posameznikov pri obdelavi osebnih podatkov (v nadaljevanju Uredba).
(2) V Zvezi osebne podatke obdeluje generalni sekretar z osebnimi podatki (v nadaljevanju obdelovalec).

3. člen

(1) Opis zbirk osebnih podatkov, katerih upravljavec je Zveza, se vodi v posebni evidenci dejavnosti obdelave (opis zbirk osebnih podatkov), ki se vodi v skladu z določbami 30. člena Uredbe. Evidenca se dopolnjuje ob vsaki spremembi vrste osebnih podatkov v posamezni zbirki.
(2) Ravnalec z osebnimi podatki mora biti seznanjen z evidenco dejavnosti obdelave, vpogled vanjo pa je potrebno omogočiti tudi vsakomur, ki to zahteva.
(3) Generalni sekretar Zveze, je dolžan voditi ažuren seznam, iz katerega je za vsako zbirko osebnih podatkov jasno razvidno, katera oseba je odgovorna za posamezno zbirko osebnih podatkov ter katere osebe lahko zaradi narave svojega dela obdelujejo osebne podatke, ki se nanašajo na posamezno zbirko osebnih podatkov. V seznam se vpisujejo naslednji podatki: naziv zbirke osebnih podatkov, osebno ime in/ali delovno mesto osebe, ki je odgovorna za zbirko osebnih podatkov ter osebno ime in/ali delovno mesto oseb, ki lahko zaradi narave njihovega dela obdelujejo osebne podatke, ki se nanašajo na zbirko osebnih podatkov, po potrebi pa tudi omejitve dostopa.

II. VAROVANJE PROSTOROV IN RAČUNALNIŠKE OPREME

4. člen

(1) Prostor, v katerem se nahajajo nosilci osebnih podatkov, strojna in programska oprema mora biti varovan z ukrepi, ki onemogočajo nepooblaščenim osebam dostop do podatkov.
(2) Nosilcev osebnih podatkov ni dovoljeno iznašati iz prostorov Zveze brez dovoljenja odgovorne osebe.
(3) Posredovanje tretjim osebam je na podlagi ustrezne pravne podlage mogoče samo z dovoljenjem odgovorne osebe, o čemer se takšno posredovanje zabeleži v evidenco posredovanj osebnih podatkov.
(4) Nosilci osebnih podatkov morajo biti zaklenjeni v ognjevarni in protivlomni omari.
(5) Ta prostor ne sme ostajati nenadzorovan, oziroma se mora zaklepati ob odsotnosti ravnalca, ki ga nadzoruje.

(6) Izven delovnega časa morajo biti omare z nosilci osebnih podatkov zaklenjene, računalniki in druga strojna oprema izklopljeni in fizično ali programsko zaklenjeni.
(7)Ravnalec ne sme puščati nosilcev osebnih podatkov (vključujoč dokumente) na mizah v prisotnosti oseb, ki nimajo pravice vpogleda vanje (npr. stranke).
(8Vsakokrat, ko ravnalec zapusti svoje delovno mesto, mora zagotoviti, da se na mizi ali drugi delovni površini ne nahajajo osebni podatki (politika »čiste mize«), vključujoč nosilce zbirk osebnih podatkov.
(9) Dostop do prostora ima samo ravnalec in osebe, ki jih pooblasti predsednik. Osebe, ki niso pooblaščene, lahko v ta prostor vstopijo zgolj v spremstvu generalnega sekretarja. Ravnalec jih mora v tem času nadzorovati in po njihovem odhodu prostor zakleniti.

5. člen

V prostoru, ki je namenjen 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 pooblaščene osebe, izvajajo pa ga lahko samo pooblaščeni servisi in vzdrževalci, ki imajo z Zvezo sklenjeno ustrezno pogodbo.

7. člen

Vzdrževalci prostora, strojne in programske opreme, obiskovalci in poslovni partnerji se smejo gibati v tem prostoru samo z vednostjo pooblaščene osebe.

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

8. člen

Generalni sekretar zagotovi za informacijsko varnost naslednje:

a) določi stopnje zaupnosti podatkov za vse osebne podatke, ki jih obdeluje Zveza;
b) glede na naravo dela in potrebe, posameznemu ravnalcu, pogodbenemu obdelovalcu ali uporabniku dodeli ustrezne pravice samo v obsegu, ki je nujen za njegovo delo;
c) vodi uporabniško dokumentacijo z vsemi potrebnimi podatki o dodelitvi pravic, gesel in drugimi podatki, potrebnimi za zagotavljanje varnega delovanja računalniškega sistema;

9. člen

(1) Popravljanje, spreminjanje in dopolnjevanje sistemske in uporabniške programske opreme je dovoljeno samo na podlagi odobritve pooblaščene osebe, izvajajo pa ga lahko samo pooblaščeni servisi, organizacije ali posamezniki, ki imajo z Zvezo sklenjeno ustrezno pogodbo. Izvajalci morajo spremembe in dopolnitve sistemske in uporabniške programske opreme ustrezno dokumentirati.
(2)Ravnalec za vsak poseg naveden v prejšnjem odstavku, vodi evidenco, iz katere je razvidno naslednje:

a) datum in ura, kdaj je bilo opravilo izvedeno;
b) kdo je posegel v računalniški sistem;
c) kakšen je bil namen posega;
d) kaj je bilo narejeno med posegom.

10. člen

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

11. člen

(1) Vsebina diskov mrežnega strežnika, lokalnih delovnih postaj in drugih elektronskih naprav, na katerih se nahajajo osebni podatki, se sprotno preverja glede na prisotnost računalniških virusov. Ob pojavu računalniškega virusa se tega čim prej odpravi, obenem pa se ugotovi vzrok pojava virusa v računalniškem sistemu.

(2) Ob vsakem sumu vdora v računalniški sistem Zveze ali kakršenkoli drug varnostni incident, se mora začeti preiskovati takoj, ko se zanj izve. Generalni sekretar Zveze mora zagotoviti, da se vsak vdor v računalniški sistem takoj blokira, nato pa je treba incident preiskati, ugotoviti pomanjkljivosti v sistemu in v pisnem poročilu o incidentu navesti uveljavljene izboljšave.

(3) Ob zaznavi incidenta mora ravnalec ravnati v skladu s sedmim poglavjem tega Pravilnika.

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

12. člen

Samo ravnalec ali druga pooblaščena oseba sme namestiti programsko opremo in jo odnašati iz prostorov Zveze.

13. člen

(1) Pristop 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 so bili posamezni osebni podatki vneseni v zbirko podatkov, uporabljeni ali drugače obdelovani (kar vključuje tudi vpogled) ter kdo je to storil. V sistemih, kjer je to možno, mora biti zagotovljen tudi podatek o tem, za kakšen namen se je določeni osebni podatek obdeloval.

(2)Generalni sekretar Zveze določi režim dodeljevanja, hranjenja in spreminjanja gesel.

(3)Katerokoli geslo, ki je v uporabi v računalniškem sistemu Zveze, mora biti dolgo vsaj 8 znakov, nujno pa mora vsebovati vsaj eno malo in veliko črko, vsaj eno številko in vsaj en poseben znak (npr. #%&'()«). Geslo ne sme vsebovati imen, priimkov, znanih dejstev ali besed iz kateregakoli slovarja. Geslo je potrebno zamenjati vsaj enkrat na 6 mesecev. Novo geslo ne sme biti enako kot je bilo zadnjih pet gesel. Geslo se ne sme razkrivati nikomur, vključno ne svojim nadrejenim ali nadzornikom sistema.

(4) Vse delovne postaje, ki jih ravnalec uporablja pri svojem delu, morajo biti kriptirane.

14. člen

Vsa gesla in postopki, ki se uporabljajo za vstop in administriranje mreže osebnih računalnikov (supervizorska oz. nadzorna gesla), administriranje elektronske pošte in administriranje aplikativnih programov se hranijo v zapečatenih ovojnicah in se jih skrbno varuje pred dostopom nepooblaščenih oseb. Uporabi se jih samo v izrednih okoliščinah oziroma ob resnično nujnih primerih. Vsaka uporaba vsebine zapečatenih ovojnic se dokumentira. Po vsaki takšni uporabi se določi nova vsebina gesel.

15. člen

(1) 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.

(2) Kopije iz prejšnjega odstavka se hranijo v zato določenih mestih, ki morajo biti ognjevarna, zavarovana proti poplavam in elektromagnetnim motnjam, v okviru predpisanih klimatskih pogojev ter zaklenjena.

(3) Za potrebe evidentiranja in nadzora nad varnostnimi kopijami je zadolžen generalni sekretar.

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

16. člen

(1) Z vsako zunanjo pravno ali fizično osebo, ki opravlja posamezna opravila v zvezi z zbiranjem, obdelovanjem, shranjevanjem ali posredovanjem osebnih podatkov (obdelovalec), se sklene pisna pogodba, predvidena v tretjem odstavku 28. člena Uredbe. Omenjeno velja tudi za zunanje osebe, ki vzdržujejo strojno in programsko opremo ter izdelujejo in nameščajo novo strojno ali programsko opremo, če imajo te dostop do osebnih podatkov.

(2) Zunanje pravne ali fizične osebe smejo opravljati storitve obdelave osebnih podatkov samo v okviru naročnikovih pooblastil in določenega obsega vrste osebnih podatkov ter teh ne smejo obdelovati ali drugače uporabljati za noben drug namen.

(3) Pravna ali fizična oseba, ki za Zvezo opravlja dogovorjene storitve izven prostorov upravljavca, mora imeti vsaj enako strog način varovanja osebnih podatkov, kakor ga predvideva ta Pravilnik.

(4) Generalni sekretar Zveze vodi ažurno evidenco vseh sklenjenih pogodb o pogodbeni obdelavi osebnih podatkov.

V. SPREJEM IN POSREDOVANJE OSEBNIH PODATKOV

17. člen

(1) Oseba, ki je zadolžena za sprejem in evidenco pošte, mora izročiti poštno pošiljko z osebnimi podatki neposredno posamezniku na katerega je ta pošiljka naslovljena.

(2) Oseba, ki je zadolžena za sprejem in evidenco pošte, odpira in pregleduje vse poštne pošiljke in pošiljke, ki na drug način prispejo v Zvezo–(prinesejo jih stranke ali kurirji), razen pošiljk iz tretjega in četrtega odstavka tega člena.

(3) Oseba, ki je zadolžena za sprejem in evidenco pošte, ne odpira tistih pošiljk, ki so naslovljene na drugo osebo ali organizacijo in so pomotoma dostavljena ter pošiljk, ki so označene kot osebni podatki.

(4) Oseba, ki je zadolžena za sprejem in evidenco pošte, ne sme odpirati pošiljk, naslovljenih na osebo, če je na ovojnici navedeno, da se vročijo osebno naslovniku, ter pošiljk, na katerih je najprej navedeno osebno ime osebe brez označbe njenega položaja in šele nato naslov Zveze.

18. člen

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

(2) Osebni podatki se pošiljajo po pošti priporočeno.

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

19. člen

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

(2) Za vsako posredovanje osebnih podatkov mora upravičenec vložiti pisno vlogo, v kateri mora biti jasno navedena določba zakona ali Uredbe, ki uporabnika pooblašča za pridobitev osebnih podatkov, ali pa mora biti k vlogi priložena pisna zahteva oziroma privolitev posameznika, na katerega se podatki nanašajo.

(3) 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.

(4) 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

20. člen

(1) Po preteku roka hrambe ali namena obdelave se osebni podatki zbrišejo, uničijo, blokirajo ali anonimizirajo, razen če zakon ali drug akt ne določa drugače.
(2) Roki, po katerih se osebni podatki izbrišejo iz zbirke podatkov, so razvidni iz evidence dejavnosti obdelave.

21. člen

(1) Za brisanje podatkov iz računalniških medijev se uporabi takšna metoda brisanja, da je nemogoča restavracija vseh ali zgolj dela brisanih podatkov.
(2) Podatki na klasičnih medijih (listine, kartoteke, register, seznam ...) se uničijo na način, ki onemogoča branje vseh ali dela uničenih podatkov (sežig, razrez ...).
(3) Na enak način se uničuje pomožno gradivo (npr. matrice, izračune in grafikone, skice, poskusne oziroma neuspešne izpise ipd.).
(4) Prepovedano je odmetavati odpadne nosilce podatkov z osebnimi podatki v koše za smeti.
(5) Pri prenosu nosilcev osebnih podatkov na mesto uničenja je potrebno zagotoviti ustrezno zavarovanje tudi v času prenosa.
(6) Prenos nosilcev podatkov na mesto uničenja ter uničevanje nosilcev osebnih podatkov nadzoruje generalni sekretar, ki po uničenju sestavi kratek zapisnik o načinu in temeljitosti uničenja.

VII. UKREPANJE OB SUMU NEPOOBLAŠČENEGA DOSTOPA IN OBVEŠČANJE

22. člen

Ravnalec je dolžan o aktivnostih, ki so povezane z odkrivanjem ali nepooblaščeno obdelavo osebnih podatkov, zlonamerni ali nepooblaščeni uporabi, prilaščanju, spreminjanju ali poškodovanju takoj obvestiti predsednika, sam pa poskuša takšno aktivnost preprečiti.

23 člen

(1) V primeru kršitve varstva osebnih podatkov mora generalni sekretar najpozneje v 72 urah po seznanitvi s kršitvijo, o njej uradno obvestiti Informacijskega pooblaščenca Republike Slovenje, razen če ni verjetno, da bi bile s kršitvijo varstva osebnih podatkov ogrožene pravice in svoboščine posameznikov.
(2) Obvestilo iz prejšnjega odstavka mora vsebovati:

a) opis vrste kršitve varstva osebnih podatkov, kategorije in približno število zadevnih posameznikov, na katere se nanašajo osebni podatki, ter vrste in približno število zadevnih evidenc osebnih podatkov;
b) sporočilo o imenu in kontaktnih podatkih pooblaščene osebe za varstvo podatkov ali druge kontaktne točke, pri kateri je mogoče pridobiti več informacij;
c) opis verjetnih posledic kršitve varstva osebnih podatkov;
d) opis ukrepov, ki jih Zveza sprejme ali katerih sprejetje predlaga za obravnavanje kršitve varstva osebnih podatkov, pa tudi ukrepov za ublažitev morebitnih škodljivih učinkov kršitve, če je to ustrezno.

(3) V primeru, ko informacij iz prejšnjega odstavka ni mogoče sporočiti v celoti, se te sporočajo postopoma, in sicer v najkrajšem možnem času, ko se zanje izve.

(4)V primeru, da je do kršitve varstva osebnih podatkov prišlo pri obdelovalcu, je ta dolžan takoj obvestiti upravljavca. Takšno določilo mora biti zapisano v vsaki pogodbi o pogodbeni obdelavi, ki jo Zveza sklene z obdelovalcem.
(5) Pooblaščena oseba, ki raziskuje incident oz. odpravlja morebitne posledice incidenta mora dokumentirati vsako kršitev varstva osebnih podatkov, vključno z dejstvi v zvezi s kršitvijo varstva osebnih podatkov, njene učinke in sprejete popravne ukrepe. To dokumentacijo je služba dolžna razkriti Informacijskemu pooblaščencu, če ta tako zahteva.
(6) Ravnalec ali oseba, ki dela na raziskavi incidenta ali je kakorkoli povezan/a z odpravljanjem posledic incidenta, mora pooblaščeno osebo obveščati v najkrajšem možnem času, o vseh informacijah, povezanih z incidentom.

24 člen

(1) Če pooblaščena oseba oceni, da je verjetno, da je kršitev varstva osebnih podatkov povzročila veliko tveganje za pravice in svoboščine posameznikov, mora najkasneje v roku 24 ur sporočiti posamezniku, na katerega se nanašajo osebni podatki, da je prišlo do kršitve varstva osebnih podatkov.
(2) Sporočilo iz prejšnjega odstavka mora biti napisano v jasnem in preprostem jeziku in mora vsebovati naslednje informacije:

a) sporočilo o imenu in kontaktnih podatkih pooblaščene osebe za varstvo podatkov ali druge kontaktne točke, pri kateri je mogoče pridobiti več informacij;
b) opis verjetnih posledic kršitve varstva osebnih podatkov;
c) opis ukrepov, ki jih Zveza sprejme ali katerih sprejetje predlaga za obravnavanje kršitve varstva osebnih podatkov, pa tudi ukrepov za ublažitev morebitnih škodljivih učinkov kršitve, če je to ustrezno.

(3) Sporočilo posamezniku iz prvega odstavka ni potrebno v naslednjih primerih:

a) pristojna služba Zveze je izvedla ustrezne tehnične in organizacijske zaščitne ukrepe in so bili ti ukrepi uporabljeni za osebne podatke, v zvezi s katerimi je bila storjena kršitev varstva, zlasti ukrepe, na podlagi katerih postanejo osebni podatki nerazumljivi vsem, ki niso pooblaščeni za dostop do njih, kot je šifriranje;
b) pristojna služba Zveze je sprejela naknadne ukrepe za zagotovitev, da se veliko tveganje za pravice in svoboščine posameznikov, na katere se nanašajo osebni podatki, iz prvega odstavka verjetno ne bo več udejanjilo;
c) v primerih, ko bi takšno obveščanje zahtevalo nesorazmeren napor. V takšnem primeru se namesto tega objavi javno sporočilo ali izvede podoben ukrep, s katerim so posamezniki, na katere se nanašajo osebni podatki, enako učinkovito obveščeni.

VIII. POOBLAŠČENA OSEBA

26. člen

Pooblaščena oseba je generalni sekretar Zveze.

IX. ODGOVORNOST ZA IZVAJANJE VARNOSTNIH UKREPOV IN POSTOPKOV

27. člen

Za izvajanje vseh postopkov in ukrepov za zavarovanje osebnih podatkov je odgovoren generalni sekretar Zveze.

28. člen

(1) Vsak, ki 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 funkcije ali pooblastila.

(2) Pred nastopom funkcije ali prejema pooblastila iz prejšnjega odstavka tega člena, mora podpisati posebno izjavo, ki ga zavezuje k varovanju osebnih podatkov. Vzorec izjave je Priloga 1 tega Pravilnika.
(3) Enako izjavo morajo podpisati tudi uporabniki in pogodbeni obdelovalci ter vzdrževalci iz 6. člena tega Pravilnika.

29. člen

Oseba, ki obdeluje osebne podatke je odgovorna za kršitev določil tega Pravilnika.

X. KONČNA DOLOČBA

30. člen

Ta Pravilnik prične veljati z dnem sprejema.

Št. 13/71-2018
Datum: 20. 12. 2018

Generalmajor
dr. Alojz Šteiner
predsednik

Priloga 1

IZJAVA

o seznanjenosti z varstvom osebnih podatkov, s Pravilnikom o zavarovanju osebnih podatkov Zveze slovenskih častnikov in z morebitnimi posledicami nespoštovanja

Spodaj podpisani _____ potrjujem, da sem seznanjen s Pravilnikom o zavarovanju osebnih podatkov Zveze slovenskih častnikov, ga razumem in se zavezujem k njegovemu izrecnemu uveljavljanju ves čas mojega opravljanja funkcije in trajanja danega pooblastila v Zvezi slovenskih častnikov, kakor tudi po prenehanju opravljanja funkcije in preklica pooblastila oziroma sodelovanja z Zvezo slovenskih častnikov.

Prav tako potrjujem, da sem seznanjen z določbami Zakona, ki ureja področje varstva osebnih podatkov in Uredbo ter s posledicami morebitnega neupoštevanja Pravilnika, Zakona ali Uredbe.

Seznanjen sem tudi, da sem odškodninsko odgovoren v primeru, da bo Zvezi slovenskih častnikov zaradi mojega nezakonitega delovanja ali delovanja v nasprotju s Pravilnikom o zavarovanju osebnih podatkov Zveze slovenskih častnikov, nastala škoda.

Datum in kraj: _____ Podpis: _____