DRUŠTVO PARAPLEGIKOV SEVERNE PRIMORSKE
REJČEVA ULICA 5 – 5000 NOVA GORICA
TELEFON: 05 300 28 22 - GSM: 040 543-338
SPLET: www.paraplegiki-primorske.si
E-POŠTA: paraplegiki.primorske@gmail.com
TR: 04750-0001024080 Nova KBM d.d.
Davčna št.: 15717224

Na podlagi 12. člena Statuta Društva paraplegikov severne Primorske z dne 28. 3. 2015 je zbor članov tega društva dne 25.3.2024 sprejel sledeči

PRAVILNIK
o varstvu osebnih in zaupnih podatkov
Društva paraplegikov severne Primorske

I. SPLOŠNE DOLOČBE

1. člen
(predmet urejanja)

(1) Ta pravilnik ureja tehnične in organizacijske ukrepe za zavarovanje osebnih in zaupnih podatkov v Društvu paraplegikov severne Primorske; matična številka: 5189390 (v nadaljevanju društvo) z namenom, da se prepreči nepooblaščena obdelava osebnih ali zaupnih podatkov v društvu.

(2) Ta pravilnik določa tudi sprejem evidenc obdelav osebnih podatkov, način določitve oseb, ki so v društvu odgovorne za zagotavljanje varnosti osebnih in zaupnih podatkov in oseb, ki imajo zaradi narave dela pravico do obdelave osebnih podatkov.

2. člen
(osebni in zaupni podatki)

(1) Osebni podatki po tem pravilniku so osebni podatki, kot jih določajo predpisi, ki urejajo varstvo osebnih podatkov in ki društvo zavezujejo.

(2) Zaupni podatki po tem pravilniku so:

- podatki, ki so tako pomembni, da bi z njihovim razkritjem nepooblaščeni osebi, društvu nastala ali lahko nastala škoda ali bi bilo njihovo razkritje kako drugače v nasprotju z interesi društva,
- podatki, ki so poslovna skrivnost po zakonu, ki ureja poslovno skrivnost,
- predlogi projektov in programov, vključno z njihovo finančno konstrukcijo,
- podatki o donatorjih društva, v kolikor ti niso javno objavljeni in
- podatki, ki jih kot zaupne označi Predsednica oziroma Predsednik društva (v nadaljevanju Predsednik) ali Upravni odbor.

(3) S štampiljkami društva se ravna kot z zaupnimi podatki.

3. člen
(načela pri obdelavi osebnih podatkov)

(1) Društvo obdeluje osebne podatke, če za to obstaja ustrezna pravna podlaga (npr. privolitev posameznika, zakon, zakoniti interes društva).

(2) Društvo obdeluje osebne podatke zakonito, pravično in pregledno.

(3) Osebni podatki v društvu morajo biti točni in po obsegu omejeni na to, kar je potrebno za namene, za katere se obdelujejo, če predpis ne določa drugače.

4. člen
(odgovornost za izvajanje pravilnika)

(1) Za izvajanje tega pravilnika glede osebnih in zaupnih podatkov, ki se obdelujejo znotraj določenega programa ali projekta (v nadaljevanju program) je odgovoren vodja tega programa.

(2) Za izvajanje tega pravilnika glede osebnih in zaupnih podatkov, ki se obdelujejo znotraj programa, kjer vodja ni imenovana ali je dalj časa odsotna, in za obdelavo, ki se ne obdeluje znotraj posebnega programa (npr. osebni podatki, ki se obdelujejo za splošne potrebe delovanja društva) je odgovoren Predsednik ali od njega pooblaščena oseba.

(3) Nadzor nad izvajanjem tega pravilnika opravlja Nadzorni odbor.

II. UKREPI ZA VAROVANJE OSEBNIH IN ZAUPNIH PODATKOV

5. člen
(splošna obveznost delavca glede varovanja osebnih in zaupnih podatkov)

(1) Vsaka delavka oziroma delavec, ki opravlja delo za društvo na podlagi pogodbe o zaposlitvi, pogodbe civilnega prava, kot samozaposlena oseba ali prostovoljec društva in vsak član organa društva (v nadaljevanju delavec), izvaja predpisane ukrepe za zavarovanje osebnih in zaupnih podatkov po tem pravilniku in varuje osebne in zaupne podatke, s katerimi se seznani pri opravljanju dela za društvo. Obveza varovanja osebnih in zaupnih podatkov ne preneha s prenehanjem delovnega ali drugega pogodbenega razmerja z društvom ali s prenehanjem članstva v organu društva.

(2) Delavec pri opravljanju dela za društvo, ki zajema obdelavo osebnih ali zaupnih podatkov, te podatke lahko obdeluje samo v skladu z navodili društva kot delodajalca ali odredbodajalca in lastnika osebnih ali zaupnih podatkov, jih obdeluje v skladu z veljavnimi predpisi in sam ne določa namenov njihove obdelave.

(3) Predsednik ali vodja programa lahko izdata podrobnejša ustna ali pisna navodila za izvajanje tega pravilnika, ki so za delavca zavezujoča.

6. člen
(razvrščanje gradiva)

Delavec pri opravljanju dela za društvo hrani in razvršča dokumentarno gradivo, ki pri tem nastaja ali ki ga prejme (npr. dokumenti društva, dopisi, seznami, kopije listin, datoteke, slike), z logičnimi nazivi in po posameznih mapah, tako da jo lahko po potrebi v njegovi odsotnosti ali po prenehanju njegovega dela za društvo, enostavno najde drug delavec.

7. člen
(varovanje prostorov)

(1) Prostori, v katerih se nahajajo nosilci osebnih ali zaupnih podatkov v fizični ali elektronski obliki (v nadaljevanju varovani prostori), so dostopni samo delavcem in se ob njihovi odsotnosti zaklepajo. Delavec ključa za dostop do varovanih prostorov ali do posameznega dela varovanih prostorov (npr. do posamezne pisarne) ne hrani na mestu, kjer je lahko dostopen drugemu delavcu ali osebi, ki ni pooblaščena za obdelavo osebnih ali zaupnih podatkov (npr. ključa ne pušča v ključavnici ali na drugem dostopnem mestu).

(2) Delavec dostopa do varovanih prostorov samo v času, ki se šteje za njegov redni delovni čas, izven tega časa, pa samo na podlagi odredbe ali dovoljenja Predsednika ali vodje programa.

(3) Delavec prisotnost v varovanih prostorih izven rednega delovnega časa evidentira v okviru že obstoječih evidenc o opravljenem delu (npr. v evidenci o izrabi delovnega časa, v poročilu o delu).

(4) Delavec v času opravljanja dela v varovanih prostorih skrbi, da nepooblaščene osebe nimajo dostopa do nosilcev osebnih ali zaupnih podatkov.

(5) V varovanih prostorih je prepovedano kaditi, uporabljati odprt ogenj ali uporabljati začasno električno napeljavo brez nadzora. V takšnih prostorih se lahko hranijo gorljivi materiali samo v količinah, ki so nujno potrebni za delovanje društva.

8. člen
(varovanje nosilcev osebnih in zaupnih podatkov)

(1) Delavec nosilca osebnih ali zaupnih podatkov v fizični obliki (npr. listinska dokumentacija, mapa) v času, ko podatkov na njem ne obdeluje (npr. v času odmora, odhod domov) hrani v zaklenjeni omari znotraj varovanih prostorov. Delavec ključa od takšne omare ne hrani na mestu, kjer je lahko dostopen drugemu delavcu ali osebi, ki ni pooblaščena za obdelavo osebnih ali zaupnih podatkov (npr. ključa ne pušča v ključavnici ali na drugem dostopnem mestu).

(2) Delavec nosilca osebnih ali zaupnih podatkov v fizični obliki ne iznaša iz varovanih prostorov, razen če je to potrebno zaradi delovnega procesa ali če to vnaprej odredi ali odobri Predsednik ali vodja programa.

(3) Računalnik ali podobna elektronska naprava (v nadaljevanju računalnik), na kateri se obdelujejo osebni ali zaupni podatki društva ali s katero se dostopa do takšnih podatkov, ima sledeče nastavitve oziroma lastnosti:

- zagon računalnika ali dostop do osebnih ali zaupnih podatkov na njem je mogoč z vnosom uporabniškega imena in močnega gesla, ki se zamenja, ko pride do nepooblaščenega dostopa ali do suma, da bi do tega lahko prišlo (npr. poskus vdora, razkritje gesla),
- vsak delavec, ki uporablja računalnik, ima svoje geslo, ki ga lahko spremeni sam,
- če se na računalniku obdeluje več zbirk osebnih podatkov ali več sklopov zaupnih podatkov, do katerih zaradi narave dela nimajo dostopa vsi delavci, ki uporabljajo računalnik, je dostop do zbirk oziroma sklopov podatkov urejen tako, da ima dostop do posamezne zbirke ali do sklopov podatkov samo delavec, ki ima pravico do njihove obdelave (npr. z dodatnim geslom za dostop do mape, kjer so osebni ali zaupni podatki, ali s programskimi omejitvami dostopa do posamezne mape s podatki),

- računalnik ima vključeno beleženje, kdaj je bil določen uporabnik (delavec) prijavljen v operacijski sistem računalnika,
- operacijski sistem računalnika je nastavljen tako, da se samodejno posodablja,
- računalnik ima požarni zid, ki varuje pred poskusi vdora iz svetovnega spleta,
- računalnik ima nameščen program za odkrivanje nezaželene programske opreme, ki je nastavljen tako, da se samodejno posodablja, da redno pregleduje računalnik in da ob priključitvi zunanje podatkovne enote na računalnik (npr. USB ključa, prenosnega diska), le-to preveri za prisotnost nezaželene programske opreme in
- operacijski sistem se v primeru neaktivnosti zaklene in za nadaljevanje dela zahteva vnos gesla.

(4) Delavec računalnik, na katerem obdeluje osebne ali zaupne podatke, v času svoje odsotnosti iz prostora, kjer se takšen računalnik nahaja (npr. odmor, odhod domov), ugasne ali programsko zaklene.

(5) Popravljanje, spreminjanje, vzdrževalna dela ali nameščanje programske opreme na računalniku, na katerem se obdelujejo osebni ali zaupni podatki, je dovoljeno samo, če to vnaprej ustno ali pisno odredi ali odobri Predsednik ali vodje programa.

(6) Delavec uporablja računalnik in drugo elektronsko opremo, ki je v lasti društva, samo za opravljanje delovnih nalog, ki jih ima do društva.

(7) Nosilec osebnih ali zaupnih podatkov v elektronski obliki (npr. USB ključ, prenosni disk) se varuje in hrani na enak način kot nosilec osebnih ali zaupnih podatkov v fizični obliki.

9. člen
(varovanje osebnih in zaupnih podatkov pri delu z uporabniki in obiskovalci)

(1) Delavec zagotovi, da se obiskovalec varovanih prostorov (npr. vzdrževalec, serviser, poslovni partner, član, uporabnik), ki ga je sprejel ali ki je prišel k njem, giba v varovanih prostorih samo z njegovo vednostjo in pod njegovim nadzorom. Delavec pri tem pazi, da ne pride do neupravičenih dostopov ali obdelave osebnih ali zaupnih podatkov.

(2) Delavec pri delu z obiskovalcem ne pušča nosilca osebnih ali zaupnih podatkov na mizi ali kje drugje v njegovi prisotnosti.

(3) V prostoru društva, ki je namenjen poslovanju z obiskovalci, so nosilci podatkov in računalniški zasloni nameščeni tako, da obiskovalec nima vpogleda vanje.

10. člen
(način brisanja osebnih podatkov)

(1) Po poteku roka hrambe osebnih podatkov se osebne podatke izbriše ali anonimizira, kar se dokumentira.

(2) Ne glede na prejšnji odstavek se osebne podatke po poteku roka hrambe lahko arhivira v skladu s predpisi o arhiviranju, če gre za osebne podatke, ki se nanašajo na delovanje društva v javnem interesu in če tako odloči pristojni arhiv.

(3) Osebne podatke, shranjene na nosilcu v fizični obliki, se izbriše z nepovratnim uničenjem nosilca (npr. rezanje, sežig, predaja pooblaščeni službi v uničenje). Nosilca z osebnimi ali zaupnimi podatki ni dovoljeno brez uničenja odvreči v koš za smeti.

(4) Osebne podatke, shranjene v elektronski obliki, se izbriše z uporabo metode, ki onemogoča obnovitev podatkov.

11. člen
(ukrepanje v primeru kršitve varnosti osebnih ali zaupnih podatkov)

(1) Delavec v primeru ugotovljene aktivnosti, povezane s kršitvijo varnosti osebnih ali zaupnih podatkov (npr. poskus odtujitve podatkov, razkritje nepooblaščeni osebi, izguba nosilca osebnih ali zaupnih podatkov), stori vse potrebno, da kršitev preneha in o aktivnosti nemudoma obvesti Predsednika ali vodjo programa.

(2) Predsednik ali vodja programa ob prejemu obvestila iz prejšnjega odstavka preveri, kako je do kršitve prišlo in glede na okoliščine primera ustrezno ukrepa, da kršitev preneha in da do takšne kršitve v prihodnje ne pride.

12. člen
(ukrepi v primeru suma vdora v računalniško opremo društva)

(1) Delavec ob pojavu računalniškega virusa ali druge nezaželene programske opreme ali v primeru suma nepooblaščenega dostopa do podatkov na računalniku ali v primeru suma razkritja gesla za dostop do računalniške opreme društva, o tem nemudoma obvesti Predsednika ali vodjo programa in osebo, pooblaščeno za vzdrževanje računalniške opreme društva.

(2) Delavec iz prejšnjega odstavka nato izvede sledeče ukrepe, če s strani osebe, pooblaščene za vzdrževanje računalniške opreme društva, ne dobi drugačnih navodil:

- ugasnejo se vsi službeni računalniki, ki so povezani z računalnikom, kjer naj bi prišlo do vdora,
- oseba, pooblaščena za vzdrževanje računalniške opreme društva, opravi varnostni pregled z namenom ugotovitve, ali je prišlo do okužbe z virusom ali drugo nezaželeno programsko opremo in na kakšen način, ali je prišlo do nepooblaščenega dostopa in na kakšen način oziroma ali je prišlo do razkritja gesel in na kakšen način,
- oseba, pooblaščena za vzdrževanje računalniške opreme društva, preveri stanje varnostnih kopij,
- oseba, pooblaščena za vzdrževanje računalniške opreme društva, izvede vse potrebno, da se računalniška oprema društva zaščiti in da se ranljivosti odpravijo,
- službeni računalniki se po opravljenem varnostnem pregledu in odstranitvi nevarnosti, posamezno in pod nadzorom osebe, pooblaščene za vzdrževanje računalniške opreme društva, prižigajo nazaj,
- oseba, pooblaščena za vzdrževanje računalniške opreme društva, pripravi pisno poročilo o varnostnem incidentu.

(3) Delavci aktivno sodelujejo pri izvajanju ukrepov iz prejšnjega odstavka.

13. člen
(varovanje posebnih osebnih podatkov)

Posebne osebne podatke (npr. osebne podatke o zdravstvenem stanju članov) se varuje z dodatnimi oziroma strožjimi ukrepi kot ostale osebne podatke in sicer se izvaja še sledeče ukrepe:

- nosilec posebnih osebnih podatkov v fizični obliki je posebej označen (npr. z oznako »zaupno«) ali pa je tako označena omara ali fascikel, v katerem je takšen nosilec,
- dostop do zbirke osebnih podatkov, ki vsebuje posebne osebne podatke in ki se obdeluje na računalniku, je zaščiten z dodatnim močnim geslom, ki ga imajo samo delavci, ki dostop potrebujejo zaradi narave svojega dela,
- obdelava zbirke osebnih podatkov v fizični ali elektronski obliki, ki vsebuje posebne osebne podatke, je organizirana tako, da je možno za nazaj ugotoviti, kateri delavec je dostopal in obdeloval določene posebne osebne podatke in kdaj (npr. da se beleži vpoglede in spremembe podatkov),
- posebni osebni podatki v elektronski obliki se na nosilcu, ki ni računalnik (npr. USB ključ, prenosni disk), hranijo zaščiteni z enkripcijo,
- posebne osebne podatke se posreduje po navadni pošti priporočeno s povratnico in
- posebne osebne podatke se posreduje preko spleta zaščitene z enkripcijo in geslom, pri čemer se geslo za odklep ne posreduje v istem sporočilu.

14. člen
(varnostna kopija)

Društvo izdeluje varnostno kopijo osebnih in zaupnih podatkov, ki se hranijo na računalniku, najmanj enkrat tedensko. Varnostna kopija se hrani na drugem računalniku kot je računalnik, kjer se osebni oziroma zaupni podatki izvirno hranijo ali na prenosnem nosilcu (npr. na USB ključu, prenosnem disku). Za varnostno kopijo velja enak način varovanja kot za izvirne nosilce osebnih podatkov.

15. člen
(ravnanje s prejeto pošto)

(1) Delavec, zadolžen za sprejem in dodelitev pošte, pregleda vso prejeto pošto samo z namenom ugotovitve, za katerega delavca je, in jo izroči neposredno temu delavcu.

(2) Ne glede na prejšnji odstavek delavec, zadolžen za sprejem in dodelitev pošte, pošte ne odpre, če je na njej navedeno, da se vroči osebno drugemu delavcu, če je naslovljena na delavca brez označbe delovnega mest ali če je šele pod njegovim imenom ime ali naslov društva ali če je pošta naslovljena na drugo organizacijo ali če gre za razpis ali natečaj.

16. člen
(posredovanje osebnih podatkov tretjim osebam)

(1) Osebne podatke se pošilja tretjim osebam samo na podlagi prošnje in če izkažejo za to ustrezno pravno podlago (npr. privolitev posameznika, na katerega se podatki nanašajo, konkretno zakonsko podlago). O takšnem pošiljanju odloči Predsednik ali vodja programa.

(2) Tretjim osebam se ne posreduje izvirnika nosilca z osebnimi podatki, razen če je društvo k temu zavezano na podlagi zakona.

(3) Osebne podatke se posreduje po navadni pošti priporočeno in z uporabo kuverte, ki onemogoča, da bi bila ob osvetlitvi vidna vsebina pošiljke.

(4) Osebne podatke se posreduje po elektronski pošti samo preko zavarovane povezave s poštnim strežnikom, ki tretjim osebam preprečuje, da se ob pošiljanju pošte seznanijo z vsebino sporočila (npr. preko protokola https).

(5) V primeru posredovanja osebnih podatkov tretjim osebam po tem členu društvo zagotavlja podatek o tem, kateri osebni podatki so bili posredovani, komu in kdaj. Te podatke se lahko zagotavlja v okviru drugih evidenc (npr. v knjigi izhodne pošte ali v zbirki poslane el. pošte).

17. člen
(urejanje razmerji z obdelovalci osebnih podatkov)

Druga oseba lahko v imenu društva obdeluje osebne podatke društva (npr. računovodski servis, vzdrževalci računalniške opreme), če ima z društvom sklenjeno pisno pogodbo, v kateri so v skladu s predpisi urejene pravice in obveznosti takšne osebe glede varovanja osebnih podatkov.

18. člen
(dostop do osebnih podatkov na službenem računalniku in v elektronski pošti delavca)

(1) Delavcu geslo za dostop do računalnika, na katerem obdeluje osebne ali zaupne podatke, in geslo za dostop do službene el. pošte, posreduje oseba, pooblaščena za vzdrževanje računalniške opreme društva. Geslo za dostop do službenega računalnika ali el. pošte delavca se ne hrani v berljivi obliki ter se v primeru pozabljenega gesla nastavi na novo.

(2) Društvo lahko od osebe, pooblaščene za vzdrževanje računalniške opreme, zahteva, da se geslo delavca nastavi na novo in ga sporoči društvu, če je dostop do službenega računalnika delavca ali do njegove elektronske pošte nujen zaradi varovanja interesov društva, ki jih ni mogoče doseči drugače, kot npr. zaradi grozeče poslovne škode, zaradi nenadne ali daljše odsotnosti delavca, ugotavljanja kršitev ali v drugih izjemnih situacijah. O takšni ponastavitvi gesla in vpogledu v podatke na računalniku ali v el. pošti odloči Predsednik ali vodja programa, ki je nadrejen delavcu. Odločitev se dokumentira in obrazloži. Geslo se lahko ponastavi in vpogleda v podatke na računalniku ali v el. pošti delavca tudi če delavec s tem soglaša.

(3) Vpogled društva v osebne podatke na računalniku ali v el. pošti delavca je omejen na razloge, ki so bili podlaga za ponastavitev gesla in vpogled. Pri vpogledu ali obdelavi osebnih podatkov na računalniku ali v elektronski pošti delavca sta prisotna Predsednik ali vodja programa in vsaj še ena oseba. O vpogledu se izdela zapisnik in se o tem obvesti delavca, katerega geslo se je ponastavilo.

(4) Ob prenehanju delovnega ali drugega pogodbenega razmerja delavca z društvom se njegov službeni elektronski naslov izbriše.

III. EVIDENCE OBDELAV OSEBNIH PODATKOV

19. člen
(sprejetje in vsebine evidence obdelave osebnih podatkov)

(1) Predsednik za vsako zbirko osebnih podatkov sprejme v skladu s predpisi evidenco dejavnosti obdelave osebnih podatkov, če društvo te podatke obdeluje redno, če zbirka vsebuje posebne osebne podatke ali če obdelava osebnih podatkov v zbirki predstavlja tveganje za pravice in svoboščine posameznikov, na katere se nanašajo osebni podatki.

(2) Evidenca dejavnosti obdelave osebnih podatkov vsebuje najmanj namen obdelave, opis kategorij posameznikov, na katere se nanašajo osebni podatki, vrste osebnih podatkov, uporabnike, 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.

(3) Če obdelava osebnih podatkov temelji na zakonitem interesu, se v evidenci obdelave osebnih podatkov dokumentira tudi test tehtanja zakonitega interesa društva.

IV. DOLOČITEV OSEB, ODGOVORNIH ZA DOLOČENO ZBIRKO OSEBNIH PODATKOV IN OSEB, KI LAHKO OBDELUJEJO OSEBNE PODATKE V ZBIRKI

20. člen
(določitev odgovornih oseb za zbirko osebnih podatkov)

(1) Predsednik za vsako zbirko osebnih podatkov iz prvega odstavka prejšnjega člena s sklepom določi:

- osebo, ki je odgovorna, da se osebni podatki v zbirki obdelujejo v skladu s tem pravilnikom in predpisi ter, da se prepreči nepooblaščeno razkritje ali druga nezakonita obdelava osebnih podatkov v zbirki in
- osebo ali osebe, ki lahko zaradi narave svojega dela, obdelujejo osebne podatke v zbirki, pri čemer se v sklepu posebej opredeli, ali lahko pri tem obdeluje tudi posebne osebne podatke, če jih zbirka vključuje.

(2) Oseba iz prve alineje prejšnjega odstavka je v zvezi z zbirko, za katero je odgovorna, odgovorna tudi za:

- informiranje posameznikov o obdelavi njihovih osebnih podatkov v zbirki,
- reševanje zahtevka posameznika, ki se nanaša na njegove pravice glede osebnih podatkov (npr. na pravico do vpogleda, popravka) in
- obveščanje nadzornih organov in posameznikov v primeru kršitev varnosti osebnih podatkov v tej zbirki v skladu s predpisi.

V. KONČNA DOLOČBA

21. člen
(veljavnost pravilnika)

(1) Ta pravilnik prične veljati in se uporabljati naslednji dan po sprejemu.

(2) Ta pravilnik se posreduje vsem delavcem in jim je tudi kasneje na voljo v prostorih na sedežu društva ali se delavcu pošlje kopija na njegovo zahtevo.

(3) Spremembe in dopolnitve tega pravilnika lahko sprejme Upravni odbor, dokler zbor članov ne odloči drugače.

Nova Gorica, 8.3.2024

Sebastjan Frefolja
predsednik

_____