

Na podlagi 20. in 21. člena Statuta Društva medicinskih sester, babic in zdravstvenih tehnikov Maribor in na podlagi 24. in 25. člena Zakona o varstvu osebnih podatkov (UL RS št. 94/ 2007) je Občni zbor Društva medicinskih sester, babic in zdravstvenih tehnikov Maribor, dne 31.03.2009 sprejel

PRAVILNIK O VAROVANJU OSEBNIH PODATKOV DRUŠTVA MEDICINSKIH SESTER, BABIC IN ZDRAVSTVENIH TEHNIKOV MARIBOR

(v nadaljevanju društvo)

I. SPLOŠNE DOLOČBE

1. člen

Pravilnik določa organizacijske, tehnične in logično- tehnične postopke in ukrepe za zagotavljanje varnosti osebnih podatkov v Društvu medicinskih sester, babic in zdravstvenih tehnikov Maribor (v nadaljevanju društvo), z namenom, preprečiti naključen ali nameren nepooblaščen dostop do podatkov, njihovo obdelavo, uporabo, posredovanje, spremembo, uničevanje ali izgubo.

Osebni podatki se obdelujejo zakonito in pošteno, biti morajo ustrezni in po obsegu primerni glede na namene, za katere se zbirajo in obdelujejo. Člani in funkcionarji društva in zunanji sodelavci, ki pri svojem delu uporabljajo osebne podatke, morajo biti seznanjeni z Zakonom o varstvu osebnih podatkov, s področno zakonodajo, ki ureja področje njihovega dela ter z vsebino Pravilnika o varovanju osebnih podatkov društva (v nadaljevanju pravilnik).

2. člen

Razlaga pojmov v pravilniku:

- **ZVOP-1:** Zakon o varstvu osebnih podatkov (UL RS, št. 86/04 in 113/05),
- **osebni podatek:** katerikoli podatek, ki se nanaša na posameznika, ne glede na obliko, v kateri je izražen,
- **posameznik:** določena ali določljiva fizična oseba, na katero se nanaša osebni podatek; fizična oseba je določljiva, če se lahko neposredno ali posredno identificira, predvsem s sklicevanjem na identifikacijsko številko ali na enega ali več dejavnikov, značilnih za njegovo fizično, fiziološko, duševno, ekonomsko, družbeno in kulturno identiteto, pri čemer način identifikacije ne povzroča velikih stroškov, nesorazmerno velikega napora ter ne zahteva veliko časa;
- **obdelava osebnih podatkov:** kakršnokoli delovanje ali niz delovanj, ki se izvaja- jo v zvezi z osebnimi podatki, ki so avtomatizirano obdelani ali so pri ročni obdelavi del zbirke osebnih podatkov ali so namenjeni vključitvi v zbirko osebnih podatkov, zlasti zbiranje, pridobivanje, vpis, urejanje, shranjevanje, prilagajanje ali spreminjanje, vpogled, uporaba, razkritje s prenosom, sporočanje, širjenje ali drugo razpolaganje, razvrstitev, povezovanje, blokiranje, anonimiziranje, izbris ali uničenje; obdelava je lahko ročna ali avtomatizirana (sredstva obdelave);
- **avtomatizirana obdelava:** obdelava osebnih podatkov s sredstvi informacijske tehnologije;
- **zbirka osebnih podatkov:** vsak strukturiran niz podatkov, ki vsebuje vsaj en osebni podatek, dostopen na podlagi meril, ki omogočajo uporabo ali združevanje podatkov, ne glede na to, ali je niz centraliziran, decentraliziran, razpršen na funkcionalni ali geografski podlagi;
- **strukturiran niz podatkov:** niz podatkov, organiziran na takšen način, da določi ali omogoči določljivost posameznika;
- **upravljavec osebnih podatkov:** fizična ali pravna oseba ali druga oseba javnega ali zasebnega sektorja, ki sama ali skupaj z drugimi določa namene in sredstva obdelave osebnih podatkov oziroma oseba, ki določena z zakonom določa tudi namene in sredstva obdelave;

- **uporabnik osebnih podatkov:** fizična ali pravna oseba ali druga oseba javnega ali zasebnega sektorja, ki se ji posredujejo ali razkrijejo osebni podatki;
- **posredovanje osebnih podatkov:** posredovanje ali razkritje osebnih podatkov;
- **katalog zbirke osebnih podatkov:** opis zbirke osebnih podatkov;
- **osebna privolitev posameznika:** prostovoljna izjava volje posameznika, da se lahko njegovi osebni podatki obdelujejo za določen namen in je dana na podlagi informacij, ki mu jih mora zagotoviti upravljavec po zakonu ZVOP-1, lahko je pisna, ustna ali druga ustrezna privolitev posameznika;
- **pisna privolitev posameznika:** podpisana privolitev posameznika, ki ima obliko listine, določila v pogodbi, določila v naročilu, priloge k vlogi ali drugo obliko v skladu z zakonom; podpis je na podlagi zakona s podpisom izenačena oblika, podana s telekomunikacijskim sredstvom ter na podlagi zakona s podpisom izenačena oblika, ki jo poda posameznik, ki ne more pisati;
- **ustna ali druga ustrezna privolitev posameznika:** ustno ali s telekomunikacijskim ali drugim ustreznim sredstvom ali na drug ustrezen način dana privolitev, iz katere je mogoče nedvomno sklepati na posameznikovo privolitev;
- **občutljivi osebni podatki:** podatki o rasnem, narodnem ali narodnostnem poreklu, političnem, verskem, filozofskem prepričanju, članstvu v sindikatu, zdravstvenem stanju, spolnem življenju, vpisu ali izbrisu v ali iz kazenske ali prekrškovne evidence ter biometrične značilnosti posameznika;
- **nosilec podatkov:** vse vrste sredstev, na katerih so zapisani ali posneti podatki (listine, akti, gradiva, spisi, računalniška oprema, magnetni, optični ali drugi računalniški mediji, fotokopije, zvočno in slikovno gradivo, mikrofili, naprave za prenos podatkov ipd.).

3. člen

Opis zbirk osebnih podatkov, katerih upravljavec je društvo, se vodi v katalogu zbirk osebnih podatkov (opisi zbirk osebnih podatkov), ki se vodi v skladu z določbami 26. člena ZVOP-1.

Osebe, ki obdelujejo osebne podatke, morajo biti seznanjene s katalogom zbirk osebnih podatkov, vpogled v katalog zbirk je potrebno omogočiti vsakomur, ki to zahteva.

Društvo je kot upravljavec osebnih podatkov dolžno 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 osebe, ki je odgovorna za zbirko osebnih podatkov,
- osebno ime oseb, ki lahko zaradi narave njihovega dela obdelujejo osebne podatke, ki se nanašajo na zbirko osebnih podatkov;

II. VAROVANJE PROSTOROV IN RAČUNALNIŠKE OPREME

4. člen

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

Dostop do osebnih podatkov je mogoč v času uradnih ur, izven tega časa pa le na podlagi dovoljenja predsednika društva. Ključni varovanih prostorov se uporabljajo in hranijo v skladu s hišnim redom. Varovani prostori ne smejo ostajati nenadzorovani, v času odsotnosti morajo biti zaklenjeni.

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 ne smejo puščati nosilcev osebnih podatkov na mizah v prisotnosti oseb, ki nimajo pravice vpogleda vanje. Nosilci osebnih podatkov, ki se nahajajo izven varovanih prostorov (hodnik, skupni prostori), morajo biti stalno zaklenjeni.

Občutljivi osebni podatki se ne smejo hraniti izven varovanih prostorov.

5. člen

V prostorih, namenjenih za poslovanje s strankami morajo biti nosilci podatkov in računalniški prikazovalniki nameščeni tako, da stranke nimajo vpogleda vanje.

6. člen

Vzdrževanje in popravila strojne računalniške ter druge opreme je dovoljeno le z vednostjo pooblaščen osebe, izvajajo pa ga lahko le pooblašчени servisi in vzdrževalci, ki imajo z društvom sklenjeno ustrezno pogodbo.

7. člen

Vzdrževalci prostorov, strojne in programske opreme, obiskovalci in poslovni partnerji se smejo gibati v varovanih prostorih le z vednostjo pooblaščen osebe. Zaposleni (snažilke, varnostnik idr.) se izven delovnega časa lahko gibljejo le v tistih varovanih prostorih, kjer je onemogočen vpogled v osebne podatke (nosilci podatkov so hranjeni v zaklenjenih omarah in pisalnih mizah, računalniki in druga strojna oprema so izklopljeni ali drugače fizično ali programsko zaklenjeni).

III. VAROVANJE SISTEMSKÉ IN APLIKATIVNO PROGRAMSKÉ RAČUNALNIŠKE OPREME TER PODATKOV, KI SE OBDELUJEJO Z RAČUNALNIŠKO OPREMO

8. člen

Dostop do programske opreme mora biti varovan tako, da dovoljuje dostop le za to vnaprej določenim osebam društva, pravnim ali fizičnim osebam, ki v skladu s pogodbo opravljajo dogovorjene storitve.

9. člen

Popravljanje, spreminjanje in dopolnjevanje systemske in aplikativne programske opreme je dovoljeno le na podlagi odobritve pooblaščen osebe, izvajajo pa jih lahko le pooblašчени servisi in organizacije ter posamezniki, ki imajo z društvom sklenjeno ustrezno pogodbo. Izvajalci morajo spremembe in dopolnitve systemske in aplikativne programske opreme ustrezno dokumentirati.

10. člen

Za shranjevanje in varovanje aplikativne programske opreme veljajo enaka določila, kot za ostale 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 le tega se ga čim prej odpravi s pomočjo ustrezne službe, potrebno je ugotoviti vzrok in izvor pojava virusa v računalniškem informacijskem sistemu.

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

12. člen

Zaposlenim ni dovoljeno nameščati programske opreme brez vednosti osebe, zadolžene za delovanje računalniškega informacijskega sistema. Prav tako ne smejo odnašati programske opreme iz društva brez odobritve predsednika društva in vednosti osebe, zadolžene za delovanje računalniškega informacijskega sistema.

13. člen

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 ter kdo je obdeloval podatke.

Predsednik društva določi postopek dodeljevanja, hranjenja in spreminjanja gesel.

14. člen

Vsa gesla in postopki, ki se uporabljajo za vstop in administriranje mreže osebnih računalnikov (nadzorna gesla), administriranje elektronske pošte in aplikativnih programov, se hranijo v zapečatenih ovojnica in se jih varuje pred dostopom nepooblaščenih oseb. Uporabi se jih le v izrednih okoliščinah oziroma ob nujnih primerih.

Vsaka uporaba vsebine zapečatenih ovojnic se dokumentira. Po takšni uporabi se določi nova vsebina gesel.

15. člen

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

Te kopije se hranijo na določenih mestih, ki morajo biti zavarovana pred požarom, 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 opravlja posamezna opravila v zvezi z zbiranjem, obdelovanjem, shranjevanjem ali posredovanjem osebnih podatkov in je registrirana za opravljanje takšne dejavnosti (pogodbeni obdelovalec), se sklene pisna pogodba, predvidena v drugem odstavku 11. člena ZVOP-1. V tovrstni pogodbi morajo biti obvezno predpisani pogoji in ukrepi za zagotovitev

varstva osebnih podatkov in njihovega zavarovanja. 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 le storitve obdelave osebnih podatkov v okviru naročnikovih pooblastil in podatkov ne smejo obdelovati ali drugače uporabljati za drug namen.

Pooblaščenca pravna ali fizična oseba, ki za društvo opravlja dogovorjene storitve izven prostorov upravljavca, mora imeti vsaj enako strog način varovanja osebnih podatkov, kot ga predvideva ta pravilnik.

V. SPREJEM IN POSREDOVANJE OSEBNIH PODATKOV

17. člen

Poslovni tajnik društva, zadolžen za sprejem in evidenco pošte, mora izročiti poštno pošiljko z osebnimi podatki neposredno posamezniku ali organu, na katerega je pošiljka naslovljena. Odpira in pregleduje vse poštno pošiljke ter pošiljke, ki prispejo na društvo drugače (prinesejo stranke ali kurirji, razen pošiljk iz tretjega in četrtega odstavka tega člena).

Ne odpira tistih pošiljk, ki so naslovljene na drug organ ali organizacijo in so pomotoma dostavljene ter pošiljk, ki so označene kot osebni podatki ali za katere iz označb na ovojnici izhaja, da se nanašajo na razpis ali natečaj.

Poslovni tajnik društva, ki je zadolžen za sprejem in evidenco pošte, ne sme odpirati pošiljk, naslovljenih na delavca in je na ovojnici navedeno, da se vročijo naslovniku osebno ter pošiljk, na katerih je najprej navedeno osebno ime delavca brez označbe njegovega uradnega položaja in šele nato naslov društva.

18. člen

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.

Občutljivi osebni podatki se pošiljajo naslovníkom v zaprtih ovojnicah proti podpisu v dostavni knjigi ali z vročilnico.

Osebni podatki se pošiljajo priporočeno.

Ovojnica, v kateri se posredujejo osebni podatki mora biti izbrana tako, da pri normalni svetlobi ali pri osvetlitvi z običajno lučjo ne omogoča berljivosti vsebine. Prav tako mora ovojnica zagotoviti, da odprtje in seznanitev z njeno vsebino ni mogoče brez vidne sledi odpiranja.

19. člen

Obdelava morebitnih občutljivih osebnih podatkov mora biti posebej označena in zavarovana.

Podatki iz prejšnjega odstavka se smejo posredovati preko telekomunikacijskih omrežij le, če so posebej zavarovani s kriptografskimi metodami in elektronskim podpisom tako, da je zagotovljena nečitljivost podatkov med njihovim prenosom.

20. člen

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

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

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 (22. člen ZVOP-1).

Ne posredujejo se 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 zbršejo, uničijo, blokirajo ali anonimizirajo, razen če zakon ali drug akt ne določi drugače.

Roki, po katerih se osebni podatki izbrišejo iz zbirke podatkov so razvidni iz 7. točke kataloga zbirke osebnih podatkov (rok hrambe osebnih podatkov).

22. člen

Za brisanje podatkov iz računalniških medijev se uporabi metoda, ki onemogoča restavracijo 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 (izračuni, grafični izpisi, poskusne, neuspele izpise ipd.).

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

Pri prenosu nosilcev osebnih podatkov na mesto uničenja je potrebno zagotoviti ustrezno zavarovanje tudi v času prenosa. Prenos nosilce podatkov na mesto uničenja ter uničenje nosilcev osebnih podatkov nadzoruje posebna komisija, ki o uničenju izdela ustrezen zapisnik.

VII. UKREPANJE OB SUMU NEPOOBLAŠČENEGA DOSTOPA

23. člen

Člani in funkcionarji društva so dolžni o aktivnostih, povezanih z odkrivanjem ali nepooblaščenim uničenjem zaupnih podatkov, zlonamerni ali nepooblaščenim uporabi, prilaščanju, spreminjanju ali poškodovanju takoj obvestiti predsednika društva, sami pa poskušati takšno aktivnost preprečiti.

VIII. ODGOVORNOST ZA IZVAJANJE VARNOSTNIH UKREPOV IN POSTOPKOV

24. člen

Za izvajanje postopkov in ukrepov za zavarovanje osebnih podatkov je odgovoren predsednik društva in pooblašcene osebe, ki jih imenuje. Nadzor nad izvajanjem postopkov in ukrepov, določenih s tem pravilnikom, opravlja predsednik društva.

25. člen

Vsak, ki obdeluje osebne podatke, je dolžan izvajati predpisane postopke in ukrepe za zavarovanje podatkov in varovati podatke, s katerimi je bil seznanjen pri opravljanju svojega dela. Obveza varovanja podatkov ne preneha s prenehanjem delovanja ali funkcije.

Pred nastopom dela ali funkcije, kjer se obdelujejo osebni podatki, mora tisti, ki dela ali funkcionar podpisati posebno izjavo, ki ga zavezuje k varovanju osebnih podatkov. Iz podpisane izjave mora biti razvidno, da je podpisnik seznanjen z določbami tega pravilnika ter določbami ZVOP-1, izjava pa mora vsebovati tudi pouk o posledicah kršitve.

26. člen

V primeru kršitev določil iz prejšnjega člena so podpisniki disciplinsko odgovorni oziroma odgovarjajo na temelju pogodbenih obveznosti.

IX. KONČNE DOLOČBE

27. člen

Pravilnik prične veljati šestdeseti dan po sprejemu na Upravnem odboru društva. Pravilnik je objavljen na spletni strani društva.



Predsednica društva

Ksenija Pirš, dipl. m. s.



Priloga:

- Sklep o vzpostavitvi, vodenju in obdelovanju zbirk osebnih podatkov,
- Izjava o varovanju osebnih podatkov.

SKLEP O VZPOSTAVITVI, VODENJU IN OBDELOVANJU ZBIRK OSEBNIH PODATKOV ČLANOV DRUŠTVA

Na podlagi 20. in 21. člena Statuta in 3. členom Pravilnika o varovanju osebnih podatkov Društva medicinskih sester, babic in zdravstvenih tehnikov Maribor Občni zbor društva, dne 31.03.2009 sprejema

SKLEP

Društvo medicinskih sester, babic in zdravstvenih tehnikov Maribor vzpostavi, vodi in obdeluje zbirko osebnih podatkov:

- članov regijskega strokovnega Društva medicinskih sester, babic in zdravstvenih tehnikov Maribor: študentje, aktivni (člani, razvrščeni glede na zaposlitev v zavodih ali zasebnikih širše mariborske regije), upokojeni,
- članov Upravnega odbora,
- članov Izvršnega odbora,
- članov v drugih organih društva (komisije, odbori, sekcije, aktivni);

Pravno podlago za obdelavo podatkov predstavlja Zakon in osebna privolitev posameznikov ob včlanitvi v društvo ter ob prevzemanju funkcije v organih društva. Namen obdelave zbirk podatkov je doseganje namena in ciljev društva, kot jih določa Statut društva.

Kategorije podatkov, ki se obdelujejo so: ime in priimek, naslov, telefon, pošta, elektronska pošta, (EMŠO, davčna številka, v primeru odobrene kotizacije članu za strokovno izpopolnjevanje ter številka TR v primeru izplačila nagrade članu za opravljeno delo).

Sodelavci, ki v okviru svojih delovnih obveznosti lahko dostopajo ali obdelujejo te podatke so:

- predsednik društva,
- podpredsednik društva,
- poslovni tajnik društva.

Za varovanje zbirke osebnih podatkov je odgovoren zakonit zastopnik, predsednik društva oziroma v času njegove odsotnosti po pooblastilu podpredsednik društva.

Predsednica društva

Ksenija Pirš, dipl. m. s.