

Na podlagi 8. člena Pravil Fundacije za financiranje invalidskih in humanitarnih organizacij v Republiki Sloveniji (Uradni list RS, št.: 9/99, 89/99 in 45/05) je Svet Fundacije za financiranje invalidskih in humanitarnih organizacij v Republiki Sloveniji na 30. seji dne 16.4.2007 sprejel

## **PRAVILNIK**

### **O VAROVANJU OSEBNIH IN TAJNIH PODATKOV V**

### **Fundaciji za financiranje invalidskih in humanitarnih organizacij v Republiki Sloveniji**

#### **I. Splošne določbe**

##### **1. člen**

S tem pravilnikom se urejajo organizacijski, tehnični in logično-tehnični postopki ter ukrepi, s katerimi se v Fundaciji za financiranje invalidskih in humanitarnih organizacij v Republiki Sloveniji (v nadaljevanju: fundacija) varujejo osebni in tajni podatki, preprečuje slučajno ali namerno nepooblaščen uničevanje podatkov, njihova sprememba ali izguba ter nepooblaščen obdelava teh podatkov.

##### **2. člen**

Funkcionarji, člani organov fundacije, zaposleni in zunanji sodelavci fundacije so dolžni ravnati po tem pravilniku.

#### **II. Osebni in tajni podatki**

##### **3. člen**

Osebni podatek po tem pravilniku je katerikoli podatek, ki se nanaša na posameznika, ne glede na obliko, v kateri je izražen.

Zbirka osebnih podatkov je vsak strukturiran niz podatkov, ki je organiziran na takšen način, da določi ali omogoči določljivost posameznika in je dostopen na podlagi meril, ki omogočajo uporabo ali združevanje podatkov, ne glede na to, ali je niz centraliziran, decentraliziran ali razpršen.

Za vsako zbirko osebnih podatkov se vzpostavi katalog zbirke osebnih podatkov s sestavinami, ki jih določa 26. člen Zakona o varstvu osebnih podatkov (ZVOP)

Direktor fundacije določi zaposleno osebo, ki je odgovorna za posamezno zbirko osebnih podatkov in katere osebe zaradi narave svojega dela lahko obdelujejo osebne podatke, ki se nanašajo na posamezno zbirko osebnih podatkov.

Zaposleni, ki obdelujejo osebne podatke, lahko pregledujejo posamezne kataloge zbirk osebnih podatkov. Vpogled v katalog zbirke osebnih podatkov je omogočen tudi posameznikom, na katere se ti osebni podatki nanašajo.

#### **4. člen**

Tajni podatek je podatek, ki je označen z oznako tajnosti, ker je tako pomemben, da bi z njegovim morebitnim razkritjem lahko nastale škodljive posledice za delovanje fundacije ali pa je kot tajen označen z odločitvijo organa oz. organizacije, od katere je fundacija podatek pridobila.

Vrsti tajnosti podatkov sta glede na vsebinsko naravo podatkov: uradna tajnost in poslovna tajnost.

Podatkom, ki so v fundaciji določeni kot uradna ali poslovna tajnost, se glede na njihov pomen in značilnosti – ob smiselni uporabi 13. člena Zakona o tajnih podatkih (Ur. l. RS št. 50/06) - določi ena od naslednjih stopenj tajnosti:

1. Strogo tajno, ki se določi za tajne podatke, katerih razkritje nepoklicani osebi bi lahko ogrozilo opravljanje osnovne dejavnosti fundacije;
2. Tajno, ki se določi za tajne podatke, katerih razkritje nepoklicani osebi bi lahko hudo škodovalo interesom fundacije;
3. Zaupno, ki se določi za tajne podatke, katerih razkritje nepoklicani osebi bi lahko povzročilo motnje v delovanju fundacije;
4. Interno, ki se določi za tajne podatke, katerih razkritje nepoklicani osebi bi lahko škodovalo opravljanju nalog posameznih organov fundacije.

Vrsto in stopnjo tajnosti podatkov določi in umakne direktor fundacije, v primeru njegove daljše odsotnosti ali nezmožnosti pa njegov pooblaščenec. Pri določanju tajnosti podatka se določi najnižja stopnja tajnosti, ki še zagotavlja potrebno varovanje podatka.

#### **5. člen**

Z osebnimi podatki se ravna kot s podatki z lastnostjo uradne tajnosti z določeno stopnjo tajnosti glede na njihovo vsebino. Zbirke osebnih podatkov, ki se obdelujejo v skladu z ZVOP, se varujejo s stopnjo tajnosti, ki je višja ali enaka kot »uradna tajnost – zaupno«.

Na enak način se ravna s podatki, ki jih na podlagi javnih razpisov za razporeditev sredstev fundacije posredujejo invalidske in humanitarne organizacije.

#### **6. člen**

Funkcionarji, člani organov fundacije, zaposleni in zunanji sodelavci fundacije ter druge osebe, ki se pri svojem delu v fundaciji seznanijo z osebnimi in tajnimi podatki, so dolžne varovati tajnost teh podatkov. Dolžnost varovanja tajnosti jih obvezuje tudi po prenehanju funkcije, zaposlitve oz. opravljanja dela v fundaciji.

### **III. Varovanje prostorov in sredstev, nosilcev osebnih in tajnih podatkov**

#### **7. člen**

Prostori, v katerih se nahajajo nosilci osebnih in tajnih podatkov (vse vrste sredstev, na katerih so zapisani ali posneti podatki – listine, akti, gradivo, spisi, računalniška oprema vključno z magnetnimi, optičnimi ali drugimi računalniškimi mediji, fotokopije, zvočno in slikovno gradivo, mikrofili, naprave za prenos podatkov, ipd. – v nadaljevanju: nosilci podatkov) so varovani z organizacijskimi ter fizičnimi in tehničnimi ukrepi, ki nepooblaščenim osebam onemogočajo dostop do teh podatkov.

Vstop v varovane prostore je mogoč le v rednem delovnem času, izven tega časa pa samo na podlagi dovoljenja direktorja fundacije ali od njega pooblaščene osebe.

V prostorih, kjer se nahajajo nosilci podatkov z oznako »uradna tajnost – strogo tajno« morajo varnostni ukrepi omogočiti popoln nadzor nad delom in gibanjem v teh prostorih.

Ključni varovanih prostorov se uporabljajo in hranijo v skladu s hišnim redom. Ključni se ne puščajo v ključavnici v vratih od 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 podatkov zaklenjene, računalniki in druga strojna oprema izklopljeni in fizično ali programsko zaklenjeni.

Zaposleni ne smejo puščati nosilcev podatkov na mizah v prisotnosti oseb, ki nimajo pravice vpogleda vanje.

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

Podatki, ki imajo značaj občutljivih osebnih podatkov po 19. točki 6. člena ZVOP, se ne smejo hraniti izven varovanih prostorov.

#### **8. člen**

S štipaljkami, papirjem z glavo fundacije, internimi obrazci in drugimi pripomočki, s katerimi bi bilo mogoče ponarediti dokumente, se ravna kot s tajnimi podatki.

#### **9. člen**

Nosilce podatkov z oznako »uradna tajnost – strogo tajno« zaposleni ne smejo odnašati izven prostorov fundacije, ostale nosilce podatkov, ki vsebujejo osebne in tajne podatke, pa samo z dovoljenjem direktorja fundacije ali od njega pooblaščene osebe.

#### **10. člen**

V prostorih, ki so namenjeni sestankom, sprejemanju obiskovalcev in drugih oseb ter delu z njimi, morajo biti nosilci podatkov in računalniški prikazovalniki nameščeni tako, da nepooblaščene osebe nimajo vpogleda vanje.

#### **11. člen**

Vzdrževanje in popravila strojne, računalniške in druge opreme se lahko opravlja le z dovoljenjem direktorja fundacije ali od njega pooblaščene osebe.

#### **12. člen**

Vzdrževalci prostorov, strojne in programske opreme, obiskovalci in druge osebe, se smejo nahajati v varovanih prostorih le z vednostjo pooblaščenih oseb.

Izven delovnega časa mora biti čistilkam, varnostnikom in drugim zunanjim delavcem pri opravljanju njihovega dela v varovanih prostorih onemogočen vpogled v nosilce podatkov.

### **IV. Varovanje systemske in aplikativno programske računalniške opreme ter podatkov, ki se obdelujejo z računalniško opremo**

#### **13. člen**

Dostop do programske opreme je dovoljen samo za to vnaprej določenim zaposlenim oziroma osebam, ki v skladu s pogodbo opravljajo dogovorjene storitve.

#### **14. člen**

Popravljanje, spreminjanje in dopolnjevanje systemske in aplikativne programske opreme je dovoljeno samo na podlagi odobritve pooblaščenih oseb. Izvajalci morajo spremembe in dopolnitve systemske in aplikativne programske opreme dokumentirati.

#### **15. člen**

Aplikativna programska oprema se hrani in varuje na enak način kot po tem pravilniku velja za nosilce podatkov.

#### **16. člen**

Vsebina diskov mrežnega strežnika in lokalnih delovnih postaj, kjer se nahajajo osebni oz. tajni podatki, se vsakodnevno preizkusi glede na prisotnost računalniških virusov. Če se ugotovi prisotnost računalniškega virusa, se tega nemudoma odpravi.

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

#### **17. člen**

Brez dovoljenja in vednosti osebe, odgovorne za delovanje računalniškega informacijskega sistema, zaposleni ne smejo nameščati programske opreme niti je ne smejo odnašati iz prostorov fundacije.

#### **18. člen**

Pristop do podatkov preko aplikativne programske opreme je zavarovan 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 to storil.

Oseba, pooblaščen za delovanje računalniškega informacijskega sistema, določi režim dodeljevanja, hranjenja in spreminjanja gesel.

#### **19. 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 ovojnica, ki so varovane pred dostopom nepooblaščenih oseb. Uporabi se jih samo v izjemnih okoliščinah oziroma ob nujnih primerih. Vsaka uporaba vsebine zapečatenih ovojnic se dokumentira. Po vsaki takšni uporabi se določi nova vsebina gesel.

#### **20. člen**

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

Te kopije se hranijo v zato določenih posebnih omarah, ki so varne pred ognjem, pred poplavami in elektromagnetnimi motnjami, v okviru predpisanih klimatskih pogojev ter zaklenjene.

### **V. Storitve, ki jih opravljajo zunanje pravne ali fizične osebe**

#### **21. 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. V takšni pogodbi morajo biti obvezno predpisani tudi 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 storitve obdelave osebnih podatkov samo v okviru naročnikovih pooblastil in podatkov ne smejo obdelovati ali drugače uporabljati za noben drug namen.

Pooblaščen pravna ali fizična oseba, ki za fundacijo opravlja dogovorjene storitve izven njenih prostorov, mora imeti vsaj enako strog način varovanja osebnih podatkov, kakor ga predvideva ta pravilnik.

### **V. Sprejemanje in posredovanje osebnih in tajnih podatkov**

#### **22. člen**

Delavec fundacije, ki je določen in pooblaščen za sprejem in evidenco pošte, odpira in pregleduje vse poštno pošiljke in pošiljke, ki na drug način prispejo v fundacijo. S pošto, ki nosi oznako tajnosti, pooblaščen delavec ravna na način, ki je glede posebnega shranjevanja in varovanja določen v tem pravilniku.

### **23. člen**

Osebne in tajne 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.

Osebni in tajni podatki se pošiljajo priporočeno.

Ovojnica, v kateri se pošiljajo osebni ali tajni podatki, mora biti izdelana na takšen način, da ovojnica 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.

### **24. člen**

Obdelava občutljivih osebnih podatkov mora biti posebej označena in zavarovana.

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

### **25. člen**

Osebni in tajni podatki se posredujejo samo tistim zunanjim uporabnikom, ki v pisni vlogi izkažejo ustrezno zakonsko podlago ali vlogi priložijo pisno zahtevo oziroma privolitev posameznika, na katerega se podatki nanašajo.

Vsako posredovanje osebnih in tajnih podatkov se zabeleži v evidenci posredovanj, iz katere mora biti razvidno, kateri podatki so bili posredovani, komu, kdaj, na kakšni podlagi in na kakšen način.

Nikoli se ne posredujejo originali dokumentov, razen če to zaradi sodnega postopka pisno zahteva pristojno sodišče. Originalni dokument se mora v času odsotnosti nadomestiti s kopijo.

## **VI. Ureditev podatkov po preteku roka hranjenja**

### **26. člen**

Po preteku splošnega roka hranjenja se osebni in tajni podatki zbršejo, uničijo, blokirajo ali anonimizirajo, razen če zakon ali drug akt ne določa drugače.

### **27. 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 čitanje vseh ali dela uničenih podatkov.

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

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

Pri prenosu nosilcev osebnih in tajnih podatkov na mesto uničenja je potrebno zagotoviti ustrezno zavarovanje tudi v času prenosa.

Prenos nosilcev podatkov na mesto uničenja ter njihovo uničevanje nadzoruje posebna komisija, ki o uničenju sestavi tudi ustrezen zapisnik. Sestavo komisije določi direktor fundacije.

## **VII. Ukrepanje ob sumu nepooblaščenega dostopa**

### **28. člen**

Zaposleni so dolžni o aktivnostih, ki so povezane z nepooblaščenim odkrivanjem ali uničenjem osebnih in tajnih podatkov, o njihovi zlonamerni ali nepooblaščeni uporabi, prilaščanju, spreminjanju ali poškodovanju, takoj obvestiti pooblaščeno osebo ali direktorja fundacije, sami pa storiti vse, kar je v njihovi moči, da taka ravnanja preprečijo.

## **VIII. Odgovornost za izvajanje varnostnih ukrepov in postopkov**

### **29. člen**

Za izvajanje postopkov in ukrepov za varovanje osebnih in tajnih podatkov po tem pravilniku je odgovoren direktor fundacije oz. od njega pooblaščen oseba.

### **30. člen**

Vsak, ki obdeluje osebne ali tajne 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 razmerja.

Pred nastopom dela na delovno mesto, kjer se obdelujejo osebni ali tajni podatki, mora zaposleni podpisati posebno izjavo, s katero se zavezuje k njihovem varovanju.

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

### **31. člen**

Za kršitev določil tega pravilnika so zaposleni odgovorni disciplinsko, ostali pa na temelju prevzetih pogodbenih obveznosti.

## **IX. Končna določba:**

### **32. člen**

Ta pravilnik prične veljati naslednji dan po objavi v Uradnem listu RS.

Predsednik sveta FIHO  
Janko KUŠAR