

Na podlagi 24. in 25. člena Zakona o varstvu osebnih podatkov (Uradni list RS, 94/2007 – UPB I) je Senat Fakultete za zdravstvene vede na 48. seji 30. 01. 2012 sprejel

PRAVILNIK o zavarovanju osebnih podatkov

I. SPLOŠNE DOLOČBE

1. člen

S tem pravilnikom se določajo organizacijski, tehnični in logično-tehnični postopki ter ukrepi za zavarovanje osebnih podatkov na Fakulteti za zdravstvene vede (v nadaljevanju: fakulteta) z namenom, da se prepreči slučajno ali namerno nepooblaščen uničevanje podatkov, njihovo spremembo ali izgubo kakor tudi nepooblaščen dostop, obdelavo, uporabo ali posredovanje osebnih podatkov.

Delavci fakultete in njeni zunanji sodelavci, ki pri svojem delu obdelujejo in uporabljajo osebne podatke, morajo biti seznanjeni z zakonom, ki ureja varstvo osebnih podatkov, zakonom, ki ureja visoko šolstvo, zakonom, ki ureja evidence na področju dela ter z vsebino tega pravilnika. Poznavanje omenjenih predpisov in zavezanost varovanju osebnih podatkov potrdijo z izjavo, ki jo vsebuje pogodba o zaposlitvi ali druga pogodba, ki ureja sodelovanje s fakulteto, pri katerem omenjene osebe obdelujejo in uporabljajo osebne podatke ali posebna izjava z isto vsebino, ki jo podpišejo.

2. člen

V tem pravilniku uporabljeni izrazi imajo pomen, kot ga opredeljuje zakon, ki ureja varstvo osebnih podatkov.

II. ZBIRKE OSEBNIH PODATKOV

3. člen

Fakulteta vzpostavlja zbirke osebnih podatkov, če za to obstaja podlaga v zakonu, ki ureja varstvo osebnih podatkov. Enako velja za vsebino osebnih podatkov posamezne zbirke in njihovo obdelavo.

Pod predhodno naštetimi pogoji zbirke osebnih podatkov na posameznem delovnem področju fakultete vzpostavijo in so zanje odgovorni (v nadaljevanju: oseba, odgovorna za zbirko osebnih podatkov):

- tajnik fakultete: za zbirko osebnih podatkov delavcev fakultete in njenih zunanjih sodelavcev;
- vodja referata za študentske zadeve: za zbirke osebnih podatkov oseb, prijavljenih za vpis v študijske programe, študentov fakultete in diplomantov fakultete;
- druga odgovorna oseba, ki jo določi direktor fakultete, za morebitne druge zbirke osebnih podatkov.

Če fakulteta nima tajnika ali vodje referata za študentske zadeve, osebo, odgovorno za zbirko osebnih podatkov, imenuje direktor izmed delavcev fakultete.

4. člen

Fakulteta vodi katalog zbirk osebnih podatkov. Za vodenje kataloga zbirk osebnih podatkov je odgovoren tajnik fakultete. Zaposleni, ki obdelujejo osebne podatke, morejo biti seznanjeni s katalogom zbirk osebnih podatkov, vpogled v katalog zbirk osebnih podatkov pa je potrebno omogočiti vsakomur, ki to zahteva.

III. VAROVANJE PROSTOROV IN RAČUNALNIŠKE OPREME

5. 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 onemogočajo nepooblaščenim osebam dostop do podatkov.

Dostop v prostore, v katerih se nahajajo nosilci osebnih podatkov, je mogoč le v rednem delovnem času, izven tega časa pa samo na podlagi dovoljenja osebe, odgovorne za posamezno zbirko osebnih podatkov in direktorja.

Ključni prostori, v katerih se nahajajo nosilci osebnih podatkov, se uporabljajo in hranijo v skladu s hišnim redom. Ključev ni dovoljeno puščati v ključavnici v vratih od zunanje strani.

Prostori, v katerih se nahajajo nosilci osebnih podatkov, 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 osebnih podatkov zaklenjene, računalniki in druga strojna oprema izklopljeni in fizično ali programsko zaklenjeni.

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

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

Občutljivi osebni podatki se ne smejo hraniti izven varovanih prostorov.

6. člen

V prostorih, ki so namenjeni poslovanju s strankami, morajo biti nosilci podatkov in računalniški prikazovalniki nameščeni tako, da stranke nimajo vpogleda vanje.

7. člen

Vzdrževanje in popravila strojne računalniške in druge opreme je dovoljeno samo z dovoljenjem direktorja in v prisotnosti delavca fakultete - strokovnega sodelavca za vzdrževanje informacijskih sistemov.

8. člen

Obiskovalci fakultete, vzdrževalci njenih prostorov ipd. se v prostorih, v katerih se nahajajo nosilci osebnih podatkov, ne smejo gibati brez prisotnosti vsaj enega od delavcev fakultete. Delavci fakultete, kot so npr. čistilke in hišnik, se lahko izven delovnega časa gibljejo samo v tistih prostorih, v katerih se nahajajo nosilci osebnih podatkov, v katerih je onemogočen vpogled v osebne podatke (nosilci podatkov so shranjeni v zaklenjenih omarah in pisalnih mizah, računalniki in druga strojna oprema so izklopljeni ali kako drugače fizično ali programsko zaklenjeni).

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

9. člen

Dostop do programske opreme mora biti varovan tako, da dovoljuje dostop samo za to v naprej določenim delavcem fakultete ali, z dovoljenjem direktorja in v prisotnosti delavca fakultete - strokovnega sodelavca za vzdrževanje informacijskih sistemov, pravnim oz. fizičnim osebam, ki opravljajo storitve na njej.

10. člen

Popravljanje, spreminjanje in dopolnjevanje systemske in aplikativne programske opreme je dovoljeno samo z dovoljenjem direktorja in v prisotnosti delavca fakultete - strokovnega sodelavca za vzdrževanje informacijskih sistemov. Izvajalci morajo spremembe in dopolnitve systemske in aplikativne programske opreme ustrezno dokumentirati in takšen dokument, po opravljenem delu, izročiti delavcu fakultete - strokovnemu sodelavcu za vzdrževanje informacijskih sistemov

11. člen

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

12. člen

Vsebina diskov mrežnega strežnika in lokalnih delovnih postaj, kjer se nahajajo osebni podatki, delavec fakultete - strokovni sodelavec za vzdrževanje informacijskih sistemov, tekoče preverja glede na prisotnost računalniških virusov. V primeru ugotovljenega računalniškega virusa, je poleg njegovega odstranjevanja potrebno ugotoviti vzrok njegovega pojava.

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

13. člen

Zaposleni ne smejo inštalirati programske opreme brez vednosti delavca fakultete - strokovnega sodelavca za vzdrževanje informacijskih sistemov. Prav tako brez odobritve osebe, odgovorne za posamezno zbirko osebnih podatkov in vednosti delavca fakultete - strokovnega sodelavca za vzdrževanje informacijskih sistemov, iz pisarn ne smejo odnašati programske opreme.

14. člen

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 so bili posamezni osebni podatki vneseni v zbirko podatkov, uporabljeni ali drugače obdelovani ter kdo je to storil. Režim dodeljevanja, hranjenja in spreminjanja gesel določi direktor.

15. člen

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

16. člen

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.

Te kopije se hranijo v za ta namen določenih mestih, ki morajo biti ognjevarna, zavarovana proti poplavam in elektromagnetnim motnjam, v okviru predpisanih klimatskih pogojev ter zaklenjena.

17. člen

Papirni nosilci osebnih podatkov, ki služijo za vnos osebnih podatkov v računalniško vodeno zbirko podatkov, se morajo zaklepati v omare. Prav tako se morajo zaklepati tudi nosilci osebnih podatkov drugih oblik.

Nosilcev osebnih podatkov delavci brez izrecnega dovoljenja direktorja ne smejo odnašati iz fakultete.

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

18. 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 praviloma 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 pooblastil fakultete in podatkov ne smejo obdelovati ali drugače uporabljati za noben drug namen.

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

VI. SPREJEM IN POSREDOVANJE OSEBNIH PODATKOV

19. člen

Delavec, ki je zadolžen za sprejem in evidenco pošte, mora izročiti poštno pošiljko z osebnimi podatki direktno osebi, odgovorni za posamezno zbirko osebnih podatkov (3. člen tega pravilnika).

Delavec, ki je zadolžen za sprejem in evidenco pošte, odpira in pregleduje vse poštno pošiljke in pošiljke, ki na drug način prispejo na fakulteto, razen pošiljk iz tretjega in četrtega odstavka tega člena.

Delavec, ki je zadolžen za sprejem in evidenco pošte, ne odpira tistih pošiljk, ki so naslovljene na drugega naslovnika in so fakulteti pomotoma dostavljene ter pošiljk, ki so označene kot osebni podatki.

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

20. 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 naslovnikom v zaprtih ovojnicah proti podpisu v dostavni knjigi ali z vročilnico (osebna vročitev).

Drugi osebni podatki se pošiljajo priporočeno.

Ovojnica, v kateri se posredujejo osebni 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.

21. 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.

22. 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 upravičenec 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 osebni podatki nanašajo. O vlogi odloča oseba, odgovorna za posamezno zbirko osebnih podatkov.

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.

Nikoli se ne posredujejo originali dokumentov, razen v primeru pisne odredbe sodišča.

Originalni dokument se mora v času odsotnosti nadomestiti s kopijo.

VII. BRISANJE PODATKOV

23. člen

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

Roki, po katerih se osebni podatki izbrišejo iz zbirke podatkov, so razvidni iz kataloga zbirke osebnih podatkov.

24. 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 branje 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 podatki v koše za smeti.

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

Prenos nosilcev podatkov na mesto uničenja ter uničevanje nosilcev osebnih podatkov nadzoruje posebna komisija, ki jo imenuje direktor in ki o uničenju sestavi tudi ustrezen zapisnik.

VIII. UKREPANJE OB SUMU NEPOOBLAŠČENEGA DOSTOPA

25. člen

Delavci so dolžni o aktivnostih, ki so povezane z odkrivanjem ali nepooblaščenim uničenjem osebnih podatkov, zlonamerno ali nepooblaščeno uporabo, prilaščanjem, poškodovanjem ali spreminjanjem osebnih podatkov takoj obvestiti osebo, odgovorno za posamezno zbirko osebnih podatkov in direktorja, sami pa poskušajo takšno aktivnost preprečiti.

IX. ODGOVORNOST ZA IZVAJANJE VARNOSTNIH UKREPOV IN POSTOPKOV

26. člen

Za izvajanje postopkov in ukrepov za zavarovanje osebnih podatkov so zadolžene osebe, odgovorne za posamezno zbirko osebnih podatkov, vodje organizacijskih enot in delavec fakultete - strokovni sodelavec za vzdrževanje informacijskih sistemov.

Nadzor nad izvajanjem postopkov in ukrepov, določenih s tem pravilnikom, opravlja direktor.

27. člen

Vsak, ki obdeluje osebne podatke, je dolžan izvajati s tem pravilnikom predpisane postopke in ukrepe za zavarovanje podatkov in varovati podatke, za katere je izvedel oziroma bil z njimi seznanjen pri opravljanju svojega dela. Obveza varovanja podatkov ne preneha s prenehanjem delovnega razmerja.

28. člen

Za kršitev določil iz prejšnjega člena so delavci disciplinsko odgovorni, ostali pa na temelju pravil o odškodninski odgovornosti.

X. KONČNE DOLOČBE:

29. člen

Z dnem, ko prične veljati ta pravilnik, prenehajo veljati določbe o varstvu osebnih podatkov iz pravilnika o varovanju zaupnih podatkov in osebnih podatkov ter o varstvu dokumentarnega gradiva.

30. člen

Ta pravilnik prične veljati naslednji dan po sprejemu. Objavi se na spletni strani fakultete.

Datum: 30. 1. 2012



Dekanica:
doc. dr. Nevenka Kregar Velikonja