

Na osnovi 24. in 25. člena Zakona o varstvu osebnih podatkov (Ur. l. RS, 86/04) in 271. člena Statuta Univerze v Mariboru (Statut UM-UPB2, Ur. l. RS, št. 75/06) je Upravni odbor Univerze v Mariboru na 12. seji dne 02.10.2006 sprejel

**PRAVILNIK O ZAVAROVANJU
OSEBNIH IN ZAUPNIH PODATKOV
Št.: A11/2006-524 JR**

1. SPLOŠNE DOLOČBE

1. člen

S tem pravilnikom se predpišejo organizacijski, tehnični in logično-tehnični postopki in ukrepi zavarovanja osebnih podatkov na Univerzi v Mariboru (v nadaljevanju: univerzi) z namenom, da se:

- prepreči slučajno ali namerno nepooblaščenno uničevanje podatkov, njihova sprememba ali izguba ter nepooblaščen obdelava osebnih podatkov.
- določijo osebe, ki so odgovorne za zbirke osebnih podatkov.
- določijo osebe, ki na podlagi delovnih zadolžitvev lahko obdelujejo določene osebne podatke na univerzi.

Ta pravilnik določa tudi postopke in ukrepe zavarovanja zaupnih podatkov.

V zadevah, ki jih ne ureja ta pravilnik, se neposredno uporabljajo določbe Zakona o varstvu osebnih podatkov.

2. člen

Osebne podatke se zavaruje z organizacijskimi, tehničnimi in logično-tehničnimi postopki in ukrepi, ki obsegajo:

- 1) varovanje prostorov, sistemske programske opreme in računalniške strojne opreme, vključno z vhodno-izhodnimi enotami;
- 2) varovanje aplikativne programske opreme, s katero se obdelujejo osebni podatki;
- 3) preprečevanje nepooblaščenega dostopa do osebnih podatkov ter njihovega prenosa, vključno s prenosom po telekomunikacijskih sredstvih in omrežjih;
- 4) zagotavljanje učinkovitega blokiranja, uničenja, izbrisa ali anonimiziranja osebnih podatkov;
- 5) omogočanje poznejšega ugotavljanja, kdaj so bili posamezni osebni podatki vneseni v zbirko osebnih podatkov, uporabljeni za zunanje institucije ali drugače obdelani in kdo je to storil, in sicer za obdobje, ko je mogoče zakonsko varstvo pravice posameznika zaradi nedopustnega posredovanja ali obdelave osebnih podatkov.

3. člen

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

2. ODGOVORNOST ZA IZVAJANJE UKREPOV ZAVAROVANJA OSEBNIH PODATKOV

4. člen

Za izvajanje postopkov in ukrepov za zavarovanje zbirk osebnih podatkov so na univerzi odgovorni: glavni tajnik, tajnik članice, pomočnik direktorja oziroma tajnik knjižnice (v nadaljevanju: odgovorna oseba).

5. člen

Vsak zaposleni, ki obdeluje osebne podatke, je dolžan izvajati predpisane postopke in ukrepe za zavarovanje podatkov in varovati podatke, za katere je izvedel oziroma bil z njimi seznanjen pri opravljanju svojega dela.

Pred nastopom dela na delovnem mestu, kjer se zbirajo in obdelujejo osebni podatki ali nosilci osebnih podatkov, mora zaposleni podpisati izjavo (priloga 1), ki ga zavezuje k varovanju osebnih podatkov in ga opozarja na posledice kršitve. Obveza varovanja osebnih podatkov, s katerimi se zaposleni seznanj pri svojem delu na univerzi, traja tudi po prenehanju delovnega razmerja na univerzi.

Odgovorne osebe ter rektor, dekan, direktor in ravnatelj so pooblaščen, da za potrebe svojega dela vpogledajo in uporabijo osebne podatke, vsebovane v vseh zbirkah osebnih podatkov vodenih na univerzi oziroma na članici.

Odgovorna oseba določi po funkciji oziroma delovnem mestu pooblaščen osebe za obdelavo osebnih podatkov v zbirki ali zbirkah osebnih podatkov tako, da izda pooblastilo za obdelavo osebnih podatkov v zbirki ali zbirkah osebnih podatkov (priloga 2), s katerim določi obseg pooblastila in vrsto zbirke ali zbirk za obdelavo za katere ali katerih je odgovoren oziroma pooblaščen delavec osebnih podatkov.

6. člen

Za kršitev določil tega pravilnika so zaposleni na univerzi tudi disciplinsko odgovorni, ostali pa so odgovorni na podlagi pogodbenih določil oziroma študenti (za opravljanje dela preko študentskega servisa) na podlagi izjav.

3. VAROVANJE PROSTOROV IN RAČUNALNIŠKE OPREME

7. člen

Prostori, kjer se nahajajo nosilci varovanih osebnih podatkov, morajo biti zavarovani z organizacijskimi in tehničnimi ukrepi, ki onemogočajo dostop nepooblaščenim osebam (v nadaljevanju: varovani prostori).

8. člen

Nosilci osebnih podatkov, hranjeni izven varovanih prostorov (npr.: skupni prostori, hodniki, aktivni arhivi, ipd.), morajo biti stalno zaklenjeni v ognjevarni in proti vlomno zaščiteni omari.

Osebe, ki delajo z zbirkami osebnih podatkov, so dolžne ravnati z nosilci osebnih podatkov tako, da je onemogočen nepooblaščen vpogled vanje.

Pooblaščen oseb in drugi zaposleni, ki delajo v varovanih prostorih, morajo vestno in skrbno nadzorovati prostor in ob zapustitvi prostora zakleniti elektronsko in drugo strojno opremo, ustrezno zavarovati nosilce podatkov ter zavarovati prostor pred nepooblaščenim vstopom.

Ključni in gesla varovanih prostorov se uporabljajo in hranijo v skladu s pravilnikom univerze oziroma članice, ki določa varovanje in hrambo ključev. Varovani prostori ne smejo ostati nenadzorovani oziroma se morajo ob odsotnosti pooblaščen oseb zavarovati pred nepooblaščenim vstopom.

9. člen

Na računalnikih ali drugi strojni opremi, na kateri se obdelujejo ali hranijo osebni podatki, mora biti vzpostavljen sistem, ki onemogoča nepooblaščen dostop osebnih podatkov.

Zaposleni na univerzi, ki pri svojem delu uporablja osebne podatke ali jih kakorkoli obdeluje, ne sme med delovnim časom puščati nosilcev osebnih podatkov na pisalnih mizah ali jih kako drugače izpostavljati nevarnosti vpogleda vanje nepooblaščenim osebam.

10. člen

V prostorih, kjer imajo vstop stranke oziroma osebe, ki niso zaposlene na univerzi, morajo biti nosilci podatkov in računalniški prikazovalniki v času obdelave ali dela na njih postavljeni tako, da jim ni omogočen vpogled v vsebino.

Zunanji vzdrževalci strojne in programske opreme se lahko nahajajo v prostorih za obdelavo osebnih podatkov samo v prisotnosti pooblaščenih oseb.

11. člen

Prepovedano je kopiranje, razmnoževanje in odnašanje nosilcev varovanih osebnih podatkov izven prostorov univerze brez predhodnega dovoljenja odgovornih oseb.

4. ZAVAROVANJE SISTEMSKÉ IN APLIKATIVNE PROGRAMSKE RAČUNALNIŠKE OPREME TER PODATKOV, KI SE OBDELUJEJO Z RAČUNALNIŠKO OPREMO

12. člen

Za shranjevanje in varovanje nosilcev podatkov se uporabljajo določila tega pravilnika kot veljajo za osebne podatke.

13. člen

Dostop do računalniške programske in ostale opreme mora biti varovan na način, ki omogoča dostop samo pooblaščenim osebam in zunanjim izvajalcem, ki za univerzo po pogodbi opravljajo servisiranje računalniške in programske opreme.

14. člen

Popravljanje, spreminjanje, vzdrževanje in nadgradnja strojne in aplikativne programske opreme je dovoljeno samo na podlagi odobritve pooblaščenih oseb, izvajajo pa jo lahko samo zaposleni na univerzi ali zunanji izvajalci, ki imajo z univerzo sklenjeno ustrezno pogodbo, v kateri so opredeljena pooblastila in odgovornosti.

Vsak poseg v sistemsko ali aplikativno programsko opremo iz zgornjega odstavka je izvajalec dolžan ustrezno dokumentirati.

15. člen

Pooblaščen osebja mora biti v času servisiranja računalnika in programske opreme ves čas prisotna in mora nadzirati, da ne pride do nedopustnega ravnanja z osebnimi podatki.

V primeru izkazane potrebe po popravilu opreme, ki vsebuje nosilce podatkov, izven univerze in brez kontrole pooblaščenih oseb, se morajo podatki izbrisati na način, ki onemogoča restavracijo. Če tak izbris ni mogoč, se mora popravilo opraviti v prostorih univerze v prisotnosti pooblaščenih oseb.

16. člen

Na nosilcih podatkov je potrebna vgradnja in redno posodabljanje protivirusnih programov za odkrivanje in odpravljanje virusov, ki naj rutinsko pregledujejo računalnik in nosilce podatkov.

Pred uporabo se mora preveriti prisotnost zlonamerne programske opreme v vseh pripetih in prenesenih datotekah, ki so prinesene prek elektronske pošte ali drugih nosilcev podatkov.

Odgovorne osebe morajo zagotoviti ukrepe, da se onemogoči ali vsaj zmanjša posledica napadov zlonamerne programske opreme tako, da se izdelujejo varnostne kopije podatkov in namešča varnostno programsko opremo ter izdelava postopke za obnovitev stanja opreme in podatkov.

17. člen

Zaposleni delavci ne smejo brez izrecnega dovoljenja odgovorne osebe nameščati programske opreme za obdelavo osebnih podatkov ali je odnašati iz univerze.

18. člen

Pristop do podatkov preko programske opreme mora biti varovan s sistemom gesel za avtorizacijo in identifikacijo uporabnikov programov in podatkov.

Odgovorna oseba določi režim dodeljevanja, hranjenja in spreminjanja gesel.

19. člen

Varovana gesla in postopki, ki se uporabljajo za vstop in za administriranje aplikativne in strojne opreme, se hranijo v zapečatenih ovojnica in varujejo v tajništvu univerze oziroma tajništvih članic.

Varovana gesla, hranjena v zapečatenih ovojnica, se smejo uporabiti v izjemnih in nujnih primerih. Vsaka uporaba vsebine zapečatenih ovojnic se dokumentira.

Po uporabi zapečatenih gesel iz ovojnic odgovorna oseba sproži postopek za dodelitev novih gesel.

20. člen

Vse izdelane kopije vsebin zbirk osebnih podatkov se morajo vpisati v evidenco posredovanj osebnih podatkov.

Varnostne kopije zbirk osebnih podatkov morajo biti zaščitene v skladu s standardi, ki veljajo za njihove originale, na osrednjem mestu in med prenosom. Skupaj z dokumentiranimi postopki za njihovo obnovo, naj bi bile shranjene na ločenem mestu, ki je dovolj oddaljeno, da ga ne dosežejo posledice nezgod na osrednjem mestu.

5. POSREDOVANJE OSEBNIH PODATKOV IZ ZBIRK OSEBNIH PODATKOV

21. člen

Pisemske pošiljke, ki vsebujejo dele ali celotne zbirke osebnih podatkov, se pošiljajo naslovniku priporočeno s povratnico.

Prenašanje osebnih podatkov preko telekomunikacijskih sredstev ali drugih računalniških medijev izven univerze mora biti zavarovano s postopki in ukrepi na način, ki nepooblaščenim osebam preprečuje prilaščanje, uničenje ali nedovoljeno seznanjanje z njihovo vsebino.

22. člen

Vsebina zbirke ali zbirk podatkov, ki se prenašajo po komunikacijskih kanalih ali fizično na računalniških medijih izven univerze, morajo biti med prenosom zaščitene pred nepooblaščenim dostopom.

23. člen

Zbirajo in obdelujejo se lahko samo tisti osebni podatki v zbirkah osebnih podatkov, za katere obstaja pravna podlaga.

Opisi zbirk osebnih podatkov, ki jih univerza vodi, so skladno z določili Zakona o varstvu osebnih podatkov opredeljeni v Katalogu zbirk osebnih podatkov univerze.

24. člen

Posameznik lahko pisno ali ustno vloži zahtevo za seznanitev z osebnimi podatki, ki se vodijo v zbirkah osebnih podatkov in se nanašajo nanj.

Zahteva se obravnava na podlagi določil Zakona o varstvu osebnih podatkov.

25. člen

Vsako posredovanje osebnih podatkov iz zbirk osebnih podatkov univerze, se vpiše v evidenco posredovanj in obdelave osebnih podatkov univerze oziroma članic.

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

26. člen

Z vsakim zunanjim izvajalcem (pravno ali fizično osebo), ki opravlja posamezna opravila v zvezi z zbiranjem, obdelovanjem, shranjevanjem ali posredovanjem osebnih podatkov ali vzdržuje strojno in programsko opremo, izdeluje in instalira novo strojno ali programsko opremo, se sklene pisna pogodba, ki mora vsebovati tudi pogoje in ukrepe za zagotovitev varstva osebnih podatkov in njihovega zavarovanja.

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

7. BRISANJE OSEBNIH PODATKOV IZ ZBIRKE OSEBNIH PODATKOV

27. člen

Osebni podatki se lahko shranjujejo v zbirki osebnih podatkov le toliko časa, kolikor je potrebno, da se doseže namen, za katerega se zbirajo ali nadalje obdelujejo.

Po izpolnitvi namena obdelave osebnih podatkov, se osebni podatki zbršejo, uničijo, blokirajo ali anonimizirajo.

Brisanje osebnih podatkov na računalniških medijih se opravi na način, po postopku in metodi, ki onemogoča restavriranje vseh ali dela brisanih podatkov. Podatki, vsebovani na klasičnih nosilcih (listine, kartoteke, register, seznam, ipd.) se brišejo s fizičnim uničenjem nosilcev, ki onemogoča branje vseh ali dela brisanih podatkov.

Komisija o uničenju oziroma brisanju podatkov sestavi zapisnik, ki se hrani najmanj 10 let. Komisijo imenuje rektor oz. na članici dekan.

Določila tega člena se ne uporabljajo v primerih, ko zakon, na podlagi katerega se podatki zbirajo, predvideva trajno hrambo zbirk osebnih podatkov.

28. člen

Z vestnostjo in skrbnostjo določeno s tem pravilnikom za uničevanje osebnih podatkov vodenih v zbirkah oziroma na posameznih nosilcih podatkov, se mora brisati in uničevati tudi pomožna dokumentacija ali računalniški produkti oziroma predloge, ki vsebujejo posamezne osebne podatke.

Uničevanje osebnih podatkov na nosilcih iz prvega odstavka tega člena se mora izvajati tekoče in ažurno.

8. UKREPANJE OB SUMU NEPOOBLAŠČENEGA DOSTOPA V ZBIRKE OSEBNIH PODATKOV

29. člen

Delavec, ki ugotovi, izve ali sumi, da prihaja do nepooblaščenega dostopa do podatkov, uničenja ali spreminjanja podatkov ali poškodovanja zbirke, mora storiti vse, kar je v njegovi moči, da prepreči nadaljnjo škodo ter nemudoma o tem obvesti pooblaščen osebo, ki vodi in ureja zbirko osebnih in odgovorno osebo.

9. ZAUPNI PODATKI IN VAROVANJE DOKUMENTOV, KI VSEBUJEJO ZAUPNE PODATKE

30. člen

Zaupni podatek je podatek, ki je tako pomemben, da bi z njegovim razkritjem nastale ali lahko nastale škodljive posledice za delovanje univerze.

31. člen

Dokumentom v fizični ali elektronski obliki, ki vsebujejo zaupne podatke, se glede na njihov pomen določi stopnja zaupnosti:

1. »STROGO ZAUPNO« - dokumenti, ki vsebujejo strogo zaupne podatke, katerih razkritje nepooblaščenim osebam bi lahko škodovalo delovanju univerze;
2. »ZAUPNO« - dokumenti, ki vsebujejo zaupne podatke, katerih razkritje nepooblaščenim osebam bi lahko škodovalo delovanju univerze;
3. »INTERNO« - dokumenti, ki so namenjeni korespondenci med službami uprave ali korespondenci med službami članice (dokumenti s strokovnimi navodili za opravljanje delovnih nalog, delovni materiali za interne predpise, analitična, statistična in druga gradiva o delu, interno informiranje in interni imeniki ipd.);

32. člen

Stopnjo zaupnosti »STROGO ZAUPNO« lahko določi rektor, predsednik upravnega odbora, glavni tajnik, dekan, direktor oziroma ravnatelj druge članice univerze.

Stopnjo zaupnosti »ZAUPNO« poleg oseb navedenih v 1. odstavku tega člena, lahko stopnjo zaupnosti določijo prorektor, prodekan, pomočnik glavnega tajnika, vodja kabineta rektorja, predstojnik organizacijske enote, ki ima po Statutu UM pooblastilo v pravnem prometu, pomočnik direktorja, pomočnik ravnatelja, tajnik članice ali druge članice.

Stopnjo zaupnosti »INTERNO« poleg oseb navedenih v 1. in 2. odstavku tega člena, lahko stopnjo zaupnosti določijo pomočnik tajnika fakultete, predstojnik oz. upravnik organizacijske enote, ki nima pooblastila v pravnem prometu po Statutu UM, vodje služb.

33. člen

Za zavarovanje zaupnih podatkov se smiselno uporabljajo določila tega pravilnika, ki urejajo varovanje osebnih podatkov.

Z pečati univerze, suhim žigom, papirjem za diplome in priloge k diplomi, papirjem z glavo univerze ali njenih članic ali organizacijskih enot ter drugimi pripomočki, s katerimi bi bilo mogoče ponarediti dokumente, je potrebno ravnati kot zaupnimi podatki.

10. PREHODNE IN KONČNE DOLOČBE

34. člen

Interni seznam katalogov zbirk in zbirke osebnih podatkov, univerza mora uskladiti z Zakonom o varstvu osebnih podatkov in določbami tega pravilnika v roku 60 dni od dneva sprejema tega pravilnika.

35. člen

Z določili tega pravilnika morajo biti seznanjeni vsi delavci univerze.

Ta pravilnik prejmejo službe oziroma delavci v čigar delovne obveznosti sodi zbiranje, urejanje, obdelava, spreminjanje, shranjevanje, posredovanje ali uporaba osebnih podatkov ali nosilcev osebnih podatkov.

36. člen

Odgovorna oseba je dolžna predložiti v podpis Izjave (priloga 1) in izdati pooblastila (priloga 2) iz 5. člena tega pravilnika v roku šestdeset dni od dneva sprejema tega pravilnika.

37. člen

Spremembe in dopolnitve tega pravilnika se sprejemajo po postopku in na način kot je predpisan za njegov sprejem.

38. člen

Ta pravilnik stopi v veljavo osmi dan po objavi v Obvestilih Univerze v Mariboru.

Z dnem uveljavitve tega pravilnika prenehajo veljati vsi do sedaj veljavni akti Univerze v Mariboru ter interni akti članic/drugih članic Univerze v Mariboru, ki opredeljujejo varovanje zaupnih in osebnih podatkov.

Predsednik Upravnega odbora
Univerze v Mariboru

Izred. prof. dr. Zmago Turk l.r.

Univerza v Mariboru
naziv članice
naslov

Podpisani(a) roj., stanujoč seznanjen(a) o naravi osebnih podatkov, ki jih bom kot delavec(ka) na delovnem mestu zbiral(a), urejal(a), obdeloval(a), spreminjal(a), shranjeval(a), posredoval(a) oziroma uporabljal(a) pri svojem delu

IZJAVLJAM

da bom kot poklicno in poslovno skrivnost varoval(a) vse osebne podatke, s katerimi se bom pri svojem delu seznanil(a).

Podpisani(a) sem seznanjen(a) in se zavedam, da je razkrivanje osebnih podatkov nepooblaščenim osebam ali zloraba (raba v namene za katere niso zbrani) sankcionirano kot hujša kršitev delovnih obveznosti in kot kaznivo dejanje.

V dne

Delavec(ka)

.....

Dostaviti:

- kadrovske službi,
- delavcu(ki).

Univerza v Mariboru
naziv članice
naslov

..... (odgovorna oseba iz 4. člena tega pravilnika)

Na podlagi 4. odstavka 5. člena Pravilnika o zavarovanju osebnih in zaupnih podatkov št.:

POOBLAŠČAM

Delavca(ko)....., roj., stanujoč(o) zaposlenega(o) na delovnem mestu da obdeluje osebne podatke (študentov, zaposlenih,.....) vodene v naslednji(h) zbirki(ah) osebnih podatkov:

1.
2.
3.

Pooblastilo se izdaja do preklica.

žig Podpis
(odgovorna oseba iz 4. člena tega pravilnika)

.....

Dostaviti:

- kadrovske službi
- pooblaščenemu,
- arhiv evidence pooblaščenih oseb za vodenje osebnih podatkov