

Na podlagi 14. člena Zakona o varstvu osebnih podatkov (Uradni list RS št. 59/99, 57/01 in 59/01-popr.) izdaja direktor Knjižnice Velenje

P R A V I L N I K

o zavarovanju osebnih podatkov

I. SPLOŠNE DOLOČBE

1. člen

S tem pravilnikom se določajo postopki in ukrepi za zavarovanje osebnih podatkov vodenih v zbirkah osebnih podatkov, s katerimi upravlja zavod.

Ta pravilnik določa ukrepe za zavarovanje pri zbiranju, obdelovanju, shranjevanju, posredovanju in uporabi osebnih podatkov v zavodu.

2. člen

Za varovane osebne podatke štejejo tisti podatki o fizični osebi, ki kažejo na lastnosti, stanja ali razmerja posameznika, ne glede na obliko, v kateri so izraženi.

V smislu določbe 1. odstavka tega člena štejejo za osebne podatke o fizični osebi zlasti:

- identifikacijski podatki o posamezniku,
- podatki, ki se nanašajo na rasno poreklo in pripadnost narodu ali narodnosti,
- podatki, ki se nanašajo na družinska razmerja,
- podatki, ki se nanašajo na stanovanjske in bivalne pogoje posameznika,
- podatki o zaposlitvi,
- podatki o socialnem in ekonomskem stanju posameznika,
- podatki o izobrazbi in pridobljenih znanjih,
- podatki o uporabi komunikacijskih sredstev,
- podatki o aktivnostih v prostem času,
- podatki o zdravstvenem stanju posameznika,
- podatki o ideoloških in verskih prepričanjih,
- podatki o posamezniku na področju notranjih zadev,
- podatki o navadah posameznika.

3. člen

Zavarovanje osebnih podatkov zajema pravne, organizacijske in ustrezne logistično-tehnične postopke in ukrepe, s katerimi se:

- varujejo prostori, aparatura in sistemska programska oprema;
- varuje aplikativna programska oprema, s katero se obdelujejo osebni podatki;
- zagotavlja varnost posredovanja in prenosa osebnih podatkov;
- onemogoča nepooblaščenim osebam dostop do naprav, na katerih se obdelujejo osebni podatki in do njihovih zbirk;
- omogoča naknadno ugotavljanje kdaj so bili posamezni podatki uporabljeni in vnešeni v zbirko podatkov in kdo je to storil, in sicer za obdobje, za katero se posamezni podatki shranjujejo.

II. VAROVANJE PROSTOROV IN RAČUNALNIŠKE OPREME

4. člen

Prostori, kjer se nahajajo nosilci varovanih osebnih podatkov - vsak dokument, na katerem je zapisan osebni podatek in vsak drug računalniški ali elektronski nosilec podatka - in strojna ter programska oprema (v nadaljevanju besedila: varovani prostori), morajo biti varovani z organizacijskimi ter fizičnimi in tehničnimi ukrepi, ki onemogočajo nepooblaščenim osebam dostop do podatkov.

Dostop v prostore iz prvega odstavka tega člena je mogoč in dopusten le v delovnem času, izven delovnega časa pa le na podlagi dovoljenja vodje (direktorja).

Nosilci osebnih podatkov, hranjeni izven aktivnih delovnih prostorov oziroma izven varovanih prostorov (hodniki, skupni prostori, aktivni arhivi ipd.), morajo biti stalno zaklenjeni v ognjevarni in protivlomno zaščiteni omari.

Ključni varovanih prostorov se uporabljajo in hranijo v skladu z navodilom (ali pravilnikom) o varovanju in uničevanju ključev, ki ga izda direktor.

5. člen

Izven delovnega časa morajo biti nosilci osebnih podatkov shranjeni v zaklenjenih ognjevarnih in protivlomno zaščitenih omarah v delovnih prostorih.

Računalniki ali druga strojna oprema, na kateri se obdelujejo ali hranijo osebni podatki, mora biti izven delovnega časa izklopljena in fizično ali programsko zaklenjena, dostop do osebnih podatkov hranjenih na disku računalnika pa kodiran.

6. člen

V varovane prostore (tajništvo, pisarna kadrovnika, likvidatura plač, pasivni arhivi ipd.) nezaposlene osebe ne smejo vstopati brez spremstva ali prisotnosti zaposlenega delavca. Delavec, ki dela v varovanih prostorih, mora vestno in skrbno nadzorovati prostor in ob zapustitvi prostora zakleniti prostor.

Delavec, 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 oziroma delavcem.

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

7. člen

Nosilcev osebnih podatkov delavci zavoda ne smejo odnašati izven zavoda brez izrecnega dovoljenja direktorja.

Direktor lahko dovoli iznos nosilcev osebnih podatkov iz zavoda, ko predhodno delavec vpiše namen in razlog za iznos podatkov iz zavoda v **knjigo evidenc o manipulaciji z osebnimi podatki**.

Posredovanje osebnih podatkov pooblaščenim eksternim institucijam in drugim, ki izkažejo zakonsko podlago za pridobitev osebnih podatkov, dovoli direktor.

Posredovanje osebnih podatkov iz predhodnega odstavka tega člena se vpiše v **knjigo evidenc o manipulaciji z osebnimi podatki**.

8. člen

Vzdrževanje in popravilo strojne računalniške in druge opreme, s katero se obdelujejo osebni podatki, je dovoljeno samo z vednostjo in odobritvijo pooblaščenih oseb (ali direktorja), izvajajo pa ga lahko samo pooblaščenih servisi in njihovi vzdrževalci, ki imajo z zavodom sklenjeno pogodbo o servisiranju računalniške oziroma strojne opreme.

9. člen

Vzdrževalci prostorov in druge opreme v varovanih prostorih, poslovni partnerji in drugi obiskovalci, se smejo gibati v varovanih prostorih le ob prisotnosti delavca zavoda.

10. člen

Zaposleni tehnično vzdrževalni delavci in čistilke se lahko gibljejo v varovanih prostorih izven delovnega časa in brez prisotnosti odgovornega delavca le, če so nosilci podatkov shranjeni na način, ki ga določa ta pravilnik za čas izven delovnega časa.

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

11. člen

Dostop do računalniške programske opreme mora biti varovan, na način ki omogoča dostop samo določenim pooblaščenim delavcem in delavcem, ki za zavod po pogodbi opravljajo servisiranje računalniške in programske opreme.

12. člen

Popravljanje, spreminjanje in dopolnjevanje systemske in aplikativne programske opreme je dovoljeno samo na podlagi odobritve direktorja, izvajajo pa ga lahko samo pooblaščenih servis in organizacije oziroma njihovi delavci, ki imajo z zavodom sklenjeno ustrezno pogodbo.

Izvajalci morajo spremembe in dopolnitve systemske in aplikativne programske opreme ustrezno dokumentirati.

13. člen

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

Delavec, pooblaščen za obdelavo in manipulacijo z osebniimi podatki na računalniku, mora skrbeti, da se v primeru servisiranja, popravila, spreminjanja ali dopolnjevanja systemske ali aplikativne programske opreme ob morebitne kopiranje osebniimi podatkov, po prenehanju potrebe po kopiji, kopija uniči.

Delavec, pooblaščen za obdelavo in manipulacijo z osebniimi podatki na računalniku, mora biti v času servisiranja računalnika in programske opreme ves čas prisoten in mora nadzirati, da ne pride do nedopustnega ravnanja z osebniimi podatki.

V primeru izkazane potrebe po popravilu računalnika, na čigar disku se nahajajo osebni podatki, izven zavoda in brez kontrole pooblaščenega delavca zavoda, se morajo podatki iz diska računalnika izbrisati na način, ki onemogoča restavrancijo. Če tak izbris ni mogoč, se mora popravilo opraviti v poslovnih prostorih zavoda v prisotnosti pooblaščenega delavca.

14. člen

Vsebina diskov mrežnega strežnika in lokalnih delovnih postaj, kjer se nahajajo osebni podatki, se dnevno preverja glede na prisotnost računalniških virusov.

Ob pojavu računalniškega virusa je potrebno storiti vse, da se s pomočjo strokovnjakov virus odpravi in da se ugotovi vzrok pojava virusa.

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

15. člen

Zaposleni delavci ne smejo brez izrecnega dovoljenja vodje organizacijske enote oziroma direktorja inštalirati programske opreme.

Zaposleni delavci ne smejo odnašati programske opreme iz zavoda brez izrecnega dovoljenja vodje organizacijske enote oziroma direktorja.

16. člen

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

Direktor določi režim dodeljevanja, hranjenja in spreminjanja gesel.

17. člen

Vsa gesla in postopki, ki se uporabljajo za vstop in za administriranje v mreži osebnih računalnikov, administriranje z elektronsko pošto in administriranje prek aplikativnih programov, se hranijo v zapečatenih ovojnica in varujejo v blagajni zavoda.

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 direktor določi nova gesla.

18. člen

Za potrebe restavriranja osebnih podatkov oziroma računalniškega sistema po okvarah ali izgubi podatkov iz drugih razlogov mora delavec, ki vodi zbirke osebnih podatkov redno izdelovati kopije vsebine osebnih podatkov, ki jih vodi.

Vse izdelane kopije vsebin zbirk osebnih podatkov se morajo vpisati v **knjigo evidenc o manipulaciji z osebnimi podatki**.

Računalniške kopije vsebin zbirk osebnih podatkov na disketah ali drugih medijih se hranijo v zavarovanih zaklenjenih omarah odpornih proti ognju, poplavam in elektromagnetnim motnjam in v predpisanih klimatskih razmerah.

IV. MANIPULACIJA Z OSEBNIMI PODATKI IN ZBIRKAMI OSEBNIH PODATKOV

19. člen

Pisemske pošiljke, ki vsebujejo osebne podatke se pošiljajo naslovniku priporočeno s povratnico.

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

20. člen

Vsebina zbirke ali zbirk podatkov, ki se prenašajo po komunikacijskih kanalih ali fizično na računalniških medijih izven zavoda, se mora med prenosom napraviti nečitljiva z ustreznimi standardnimi kriptografskimi metodami.

21. člen

Zavod vodi osebne podatke v zbirkah osebnih podatkov, ki jih ustanovi na podlagi zakona in osebne podatke, ki jih vodi v okviru zakonsko določenih zbirk na podlagi soglasja osebe, na katero se podatki nanašajo.

Vrste zbirk osebnih podatkov, ki jih zavod vodi, so določene s **Katalogom zbirk osebnih podatkov**, ki ga določi direktor v 60 dneh od dneva izdaje tega pravilnika je priloga pravilnika.

Zavod mora 15 dni pred vzpostavitvijo zbirke osebnih podatkov posredovati republiškem upravnemu organu, ki v skladu z zakonom vodi katalog podatkov (Ministrstvo za pravosodje) zajetih v posamezni zbirki, podatke o zbirki, ki jo namerava vzpostaviti, v roku 7 dni od dneva sprememb pa mora zavod republiškem upravnemu organu posredovati tudi spremembe podatkov iz ustanovljene zbirke podatkov.

22. člen

Delavec oziroma oseba o kateri se vodijo osebni podatki oziroma pooblaščenec delavca ali osebe ali zakoniti zastopnik osebe o kateri se v zbirki osebnih podatkov vodijo njegovi osebni podatki lahko vpogleda v osebne podatke vodene o njem oziroma o zastopancu in jih ima pravico prepisati. Vpogled in prepis osebnih podatkov mora biti osebi omogočen v roku 15 dni od dneva, ko je bila stavljen pisna zahteva na zavod.

Osebe iz 1. odstavka tega člena imajo pravico zahtevati, da jim zavod posreduje izpis osebnih podatkov iz zbirke osebnih podatkov, ki se nanašajo nanj. Izpis je potrebno osebi zagotoviti v roku 30 dni od dneva prejema pisne zahteve. Stroške izpisa nosi oseba, ki izpis zahteva.

23. člen

Osebni podatki, vodeni v zbirki osebnih podatkov zavoda se lahko posredujejo drugim uporabnikom samo, če so za njihovo pridobitev in uporabo pooblaščen z zakonom ali na podlagi pisne zahteve ali privolitve osebe, na katero se osebni podatki nanašajo.

Dejstva o posredovanih osebnih podatkih iz zbirke osebnih podatkov vodene v zavodu, se morajo v roku 3 dni od dneva posredovanja, sporočiti osebi o kateri so bili posredovani osebni podatki.

Posredovanje osebnih podatkov iz zbirk osebnih podatkov, ki jih vodi zavod, drugim upravičencem se vpiše v **knjigo evidenc o manipulaciji z osebnimi podatki**. Na zahtevo osebe, o kateri so bili posredovani osebni podatki, mora delavec, ki je osebne podatke posredoval, izročiti osebi seznam subjektov, katerim so bili v določenem obdobju posredovani podatki, ki so vsebovani v zbirki podatkov zavoda in se nanašajo nanj.

V. BRISANJE PODATKOV OZIROMA UNIČENJE NOSILCEV OSEBNIH PODATKOV

24. člen

Osebni podatki se lahko vodijo v zbirki osebnih podatkov le toliko časa, kolikor je potrebno, da se doseže namen, za katerega se zbirajo in vodijo.

Po prenehanju potrebe po vodenju osebnih podatkov, se podatki zbršejo oziroma uničijo nosilci podatkov.

25. člen

Brisanje osebnih podatkov na računalniških medijih se opravi na način, po postopku in metodi, ki onemogoča restavriranje brisanih podatkov.

Osebnih podatki vsebovani na klasičnih nosilcih (listine, kartoteke, register, seznam) se brišejo z uničenjem nosilcev. Nosilci se fizično uničijo (pokurijo, razrežejo) v prostorih zavoda ali pod nadzorom pooblaščenega delavca zavoda pri organizaciji, ki se ukvarja z uničevanjem zaupne dokumentacije.

26. 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 predhodnega odstavka se mora izvajati tekoče in ažurno.

VI. UKREPANJE OB UGOTOVITVI ZLORABE OSEBNIH PODATKOV ALI VDORU V ZBIRKE OSEBNIH PODATKOV

27. člen

Delavci zavoda so dolžni izvajati ukrepe za preprečevanje zlorabe osebnih podatkov in morajo z osebnimi podatki, s katerimi se seznanijo pri svojem delu ravnati vestno in skrbno na način in po postopkih, ki jih določa ta pravilnik.

Delavec, ki izve ali opazi, da je prišlo do zlorabe osebnih podatkov (odkrivanje osebnih podatkov, nepooblaščen uničenje, nepooblaščen spreminjanje, poškodovanje zbirke, prilaščanje osebnih podatkov) ali do vdora v zbirko osebnih podatkov, mora takoj o tem obvestiti direktorja in pooblaščenega delavca, ki vodi in ureja zbirko osebnih podatkov, ki so bili zlorabljeni ali v katero se je vdrl.

28. člen

Direktor mora zoper tistega, ki je zlorabil osebne podatke ali je nepooblaščen vdrl v zbirko osebnih podatkov ustrezno ukrepati.

Če obstaja sum pri vdoru v zbirko osebnih podatkov, da je ta storjen z naklepom in namenom zlorabiti osebne podatke ali jih uporabiti v nasprotju z nameni, za katere so zbrani, ali če je do zlorabe osebnih podatkov že prišlo, mora direktor poleg uvedbe disciplinskega postopka zoper storilca, če je ta delavec zavoda, vdor ali zlorabo prijaviti organom pregona.

Za zlorabo osebnih podatkov šteje vsaka uporaba osebnih podatkov v namene, ki niso v skladu z nameni zbiranja določenimi v zakonu, na podlagi katerega se zbirajo ali nameni, določenimi v katalogu zbirk osebnih podatkov.

VII. ODGOVORNOST ZA IZVAJANJE UKREPOV ZAVAROVANJA OSEBNIH PODATKOV

29. člen

Pred nastopom dela delavca na delovnem mestu, kjer se zbirajo, urejajo, obdelujejo, spreminjajo, shranjujejo, posredujejo ali uporabljajo osebni podatki ali nosilci osebnih podatkov, mora delavec

podpisati izjavo, ki ga zavezuje k varovanju osebnih podatkov kot poklicne skrivnosti in ki ga opozarja na posledice kršitve zaveze.

Obveza varovanja osebnih podatkov, s katerimi se delavec seznanja pri svojem delu v zavodu traja tudi po prenehanju delovnega razmerja v zavodu.

30. člen

Delavec stori lažjo kršitev delovne dolžnosti:

- če opusti vestno in skrbno nadzorovanje varovanih prostorov (1. odst. 5. člena),
- če opusti ravnanja za preprečitev vpogleda v ali na nosilce osebnih podatkov (3. odst. 5. člena),
- če ne uniči kopije osebnih podatkov v primerih iz 2. odst. 13. člena,
- če ni ves čas servisiranja računalnika in programske opreme prisoten (3. odst. 13. člena),
- če ne izvaja preventive v zvezi z računalniškimi virusi (14. člen),
- če ne vodi evidence kopij vsebin zbirk osebnih podatkov v knjigi evidenc o manipulaciji z osebnimi podatki (2. odst. 18. člena) in
- če ne obvesti direktorja ali pooblaščenega delavca v primeru zlorabe osebnih podatkov ali vdora v zbirko osebnih podatkov (3. odst. 27. člena).

31. člen

Delavec stori hujšo kršitev delovne dolžnosti:

- če sporoča osebne podatke, s katerimi se je seznanil pri svojem delu, sodelavcem ali drugim osebam,
- če opusti skrb in nadzor nad nosilci osebnih podatkov med delovnim časom in tako dopusti možnost vpogleda vanje nepooblaščenim osebam (2. odst. 5. člena),
- če brez izrecnega dovoljenja odnaša iz zavoda nosilce osebnih podatkov (1. odst. 6. člena),
- če posreduje osebne podatke, pooblaščenim eksternim institucijam brez dovoljenja direktorja (3. odst. 6. člena),
- če ne vpiše v knjigo evidenc o manipulaciji z osebnimi podatki dejstva o posredovanju osebnih podatkov eksternim institucijam (4. odst. 6. člena),
- če popravlja, spreminja ali dopolnjuje sistemsko ali aplikativno programsko opremo (1. odst. 13. člena),
- če inštalira ali odnese programsko opremo iz zavoda brez izrecnega dovoljenja direktorja (15. člen),
- če ne izdeluje redno kopije vsebine osebnih podatkov (1. odst. 18. člena) in
- če ne hrani računalniških kopij vsebin zbirk osebnih podatkov v zavarovanih zaklenjenih omarah (3. odst. 18. člena).

32. člen

O zlorabi ali sumu o zlorabi osebnih podatkov vodenih v zbirkah osebnih podatkov zavoda oseb, ki niso delavci zavoda se obvesti organe pooblaščen za pregon.

VIII. PREHODNE IN KONČNE DOLOČBE

33. člen

Katalog zbirk in zbirke osebnih podatkov, organizacija zavarovanja osebnih podatkov in ureditev drugih zadev določenih s tem pravilnikom se mora uskladiti z Zakonom o varstvu osebnih podatkov in določbami tega pravilnika v roku 60 dni od dneva sprejema tega pravilnika.

34. člen

Ta pravilnik sprejme direktor.

Spremembe in dopolnitve tega pravilnika sprejme direktor po postopku in na način kot velja za sprejem pravilnika.

35. člen

Z določbami tega pravilnika morajo biti seznanjeni vsi delavci zavoda.

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

Delavci, ki delajo na delovnih mestih, kjer se zbirajo, urejajo, obdelujejo, spreminjajo, shranjujejo, posredujejo ali uporabljajo osebni podatki ali nosilci osebnih podatkov, morajo podpisati izjavo iz 29. člena tega pravilnika v roku 30 dni od dneva sprejema tega pravilnika.

37. člen

Ta pravilnik se vodi v evidenci aktov zavoda pod zaporedno številko 10/2004.

38. člen

Ta pravilnik začne veljati osmi dan po dnevu sprejema.

v.d. direktor:

Vlado Vrbič

Datum sprejema: 25. 10. 2004