

PRAVILNIK
O VAROVANJU ZAUPNIH IN OSEBNIH
PODATKOV

Lukavci, september 2001

Na podlagi 13. in 14. člena Zakona o varstvu osebnih podatkov (Uradni list RS št. 59/99) ter na podlagi 64. člena statuta zavoda (v nadaljevanju zavod) izdaja direktor-ica naslednji

PRAVILNIK O VAROVANJU ZAUPNIH IN OSEBNIH PODATKOV

I. SPLOŠNE DOLOČBE

1. člen

S tem pravilnikom se določajo organizacijski in logično tehnični postopki in ukrepi za zavarovanje zaupnih in osebnih podatkov v zavodu v skladu z 13. in 14. členom Zakona o varstvu osebnih podatkov z namenom, da se prepreči slučajno ali namerno nepooblaščen uničevanje podatkov, njihovo spremembo ali izgubo kakor tudi nepooblaščen dostop, obdelava, uporaba ali posredovanje zaupnih in osebnih podatkov.

Določbe tega pravilnika veljajo za vse klasično ali računalniško vodene zbirke podatkov.

Zaposleni in zunanji sodelavci, ki pri svojem delu uporabljajo osebne podatke, morajo biti seznanjeni z Zakonom o varstvu osebnih podatkov, s področno zakonodajo, ki ureja posamezno področje njihovega dela ter z vsebino tega pravilnika.

2. člen

1.1.1 V tem pravilniku uporabljeni izrazi imajo naslednji pomen:

1. 1. **zaupen podatek:** podatek, ki je razglašen za tajnost, ker je tako pomemben, da bi z njegovim razkritjem lahko nastale škodljive posledice za delovanje zavoda;
2. 2. **osebni podatek:** podatek, ki kaže lastnosti, stanja ali razmerja posameznika ne glede na obliko, v kateri je izražen;
3. 3. **zbirka podatkov:** zbirka, ki vsebuje zaupne ali osebne podatke (npr. evidenca, baza podatkov), ki se vodi s sredstvi za avtomatsko obdelavo podatkov ali s klasičnimi sredstvi in je namenjena izvajanju nalog zavoda;
4. 4. **obdelava podatkov:** postopki in procesi zbiranja, shranjevanja, spreminjanja, združevanja, uporabe, brisanja in posredovanja podatkov;
5. 5. **dokument:** vsi pisni, tiskani, risani in posneti podatki;
6. 6. **nosilec podatkov:** vse vrste sredstev, na katerih so zapisani ali posneti podatki;
7. 7. **varovani prostori:** vsi prostori, v katerih se nahajajo nosilci zaupnih ali osebnih podatkov ali prostori, v katerih je oprema, preko katere je mogoč dostop do teh podatkov;
8. 8. **pooblaščen oseba:** direktor zavoda ali vodje organizacijskih enot v skladu z izdanimi pooblastili ali delavec pooblaščen v skladu s tem pravilnikom ali s pisnim pooblastilom direktorja.

3. člen

Vrste tajnosti zaupnih podatkov v zavodu so:

1. 1. **uradna tajnost:** so podatki, ki so tako pomembni, da bi z njihovo izdajo nastale ali bi lahko nastale hujše škodljive posledice za delovanje služb v zavodu. Podatkom, ki so določeni za uradno tajnost, se glede na njihov pomen določi stopnja zaupnosti:

- **strogo zaupno,**
- **zaupno ali**
- **interno.**

- uradna tajnost – strogo zaupno in so:

- zapisniki o posvetovanju in glasovanju,
- uradna poročila,
- osnutki odločb,
- uradni zapisi,
- ostalo določi ustanovitelj, svet zavoda ali direktor

- uradna tajnost – zaupno in so:

- vsi osebni podatki zaposlenih,
- vsi osebni podatki uporabnikov in njihovih zakonitih zastopnikov,
- podatki in poročila o obravnava uporabnikov,
- podatki o prošnjah, zahtevah in pritožbah strank, uporabnikov ali zaposlenih,
- podatki v zvezi z javnimi naročili,
- pogodbe,
- prispela in arhivirana pošta ustanove,
- arhivirani dokumenti ustanove,
- poslovna poročila in evidence,
- drugo določi direktor ali pooblaščen oseba.

- uradna tajnost – interno so:

- strokovna navodila za opravljanje delovnih nalog in okrožnice,
- sezname zaposlenih,
- delovni materiali za zakonske in podzakonske predpise,
- analitična, statistična in druga gradiva o delu služb zavoda,
- interno informiranje in interni imeniki,
- informacije s strokovnih sestankov in koordinacij,
- plačila stanovalcem,
- prisotnost v zavodu,
- jubilejne nagrade,
- drugo določi direktor ali pooblaščen oseba.

4. 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,

Z osebnimi podatki se glede na njihovo vsebino, ravna kot s podatki »uradna tajnost – strogo zaupno«, »uradna tajnost – zaupno« ali »uradna tajnost – interno« (npr. interni telefonski imenik, seznam zaposlenih, ki so na dopustu). Stopnjo zaupnosti zbirk osebnih podatkov določi pooblaščen oseba. Zbirke osebnih podatkov, ki se obdelujejo v skladu z zakonom, se varujejo s stopnjo zaupnosti, ki je višja ali enaka kot **»uradna tajnost – zaupno«**.

5. člen

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

- varujejo prostori, strojna 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

6. člen

Prostori, kjer se nahajajo nosilci osebnih podatkov - vsak dokument, strojna in programska oprema (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 pooblaščenih oseb ali direktorja.

Za prostore, kjer se hranijo nosilci podatkov z oznako »uradna tajnost – strogo zaupno«, morajo varnostni ukrepi omogočiti popoln nadzor nad delom in gibanjem v teh prostorih.

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

Nosilci zaupnih ali osebnih podatkov, ki se hranijo izven aktivnih delovnih prostorov oziroma izven zavarovanih prostorov (hodniki, skupni prostori, aktivni arhivi, ipd.) morajo biti stalno zaklenjeni.

7.člen

Za prostore, kjer se hranijo nosilci podatkov z oznako »uradna tajnost – strogo zaupno in zaupno«, morajo varnostni ukrepi omogočiti popoln nadzor nad delom in gibanjem v teh prostorih.

To prostori so :

Na sedežu zavoda:

- **pisarna direktorja:** uradne ure po predhodni najavi dnevno med 8.00 in 9.00 uro, za delavce vsak dan med 8.00 in 10.00 uro oziroma po dogovoru.

Dostop do listin hranjenih v tem prostoru in izdajo posameznih listin za potrebe drugih delavcev ali strank ima direktor.

- **pisarna tajništva:** uradne ure dnevno med 8.30 in 12.30 uro, dodatno določena cona gibanja. Listine, ki se hranijo v tajništvu za potrebe dela ostalih zaposlenih ali strank izdaja izključno tajnica ali direktor. Do vpogleda v dnevno tekočo pošto in pooblastilo za obdelavo ima tajnica ali direktor. V primeru daljše odsotnosti tajnice pa delavec, ki ga pooblasti direktor. Tajnica ne odpre pošte le v primeru, da je na ovojnici zapisano:

- osebno pošiljatelju,
- strogo zaupno/zaupno ali
- prijava na razpis.

Kroženje listin znotraj ustanove se določi z dodatnimi navodili, ki je priloga temu pravilniku.

- **pisarne računovodstva:** uradne ure od ponedeljka do petka med 12.00 in 14.00 uro oziroma po dogovoru. Pooblastila za dostop do listin hranjenih v tem prostoru imajo le delavci računovodstva in direktor, za izdajanje posameznih listin za potrebe ostalih zaposlenih ali strank so prav tako pooblaščen delavci računovodstva in direktor.
- **prostor strokovnega vodje:** po predhodni najavi oz po dogovoru. Za izdajo listin iz tega prostora je pooblaščen strokovni vodja.
- **prostor arhiva:** za dostop listin so pooblaščen direktor ali tajnica, za posamezne listine vezane na finančno poslovanje pa tudi delavci računovodstva. Nepooblaščenim delavcem ali strankam je vstop prepovedan. Listine opredeljene kot zaupno ali strogo zaupno morajo biti vsebinsko ločene v različnih zaklenjenih omarah, v kolikor se nahajajo v istem prostoru. Začasni iznos listin iz arhiva se vodi v zvezku z datumom in podpisom ter nazivom, številko listine. Nepooblaščenim osebam je vstop prepovedan.
V ločenih omarah se arhivira tudi soc. zdrav. dokumentacija, do katere ima dostop strokovni vodja.

8. člen

Izven delovnega časa morajo biti nosilci osebnih podatkov shranjeni v zaklenjenih ognje varnih omarah v delovnih prostorih.

Računalniki in 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.

9. člen

V varovane prostore nezaposlene osebe ne smejo vstopati brez spremstva ali prisotnosti zaposlenega delavca. Delavec, ki dela v varovanih prostorih, mora vestno in skrbno nadzorovati prostor, ob zapustitvi prostora, pa prostor ustrezno zavarovati in zakleniti.

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 nevarnostim vpogleda vanje nepooblaščenim osebam oziroma delavcem.

V prostorih, kamor imajo vstop stranke oziroma osebe, ki niso zaposlene v zavodu, morajo biti nosilci podatkov in računalniški prikazovalniki nameščeni tako, da v času obdelave ali dela na njih, stranke nimajo vpogleda v zaupne in osebne podatke drugih oseb. Prav tako mora biti onemogočen pogled skozi okno prostorov.

10. člen

Nosilcev podatkov z oznako »uradna tajnost – strogo zaupno« zaposleni ne smejo odnašati izven prostorov zavoda, ostale nosilce podatkov, ki vsebujejo zaupne ali osebne podatke, pa samo z dovoljenjem direktorja.

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

Pooblaščen oseba oziroma direktor lahko dovoli iznos nosilcev zaupnih ali 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 tretjega in četrtega odstavka tega člena se vpiše v **knjigo evidenc o manipulaciji z osebnimi podatki**.

11. člen

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

12. člen

Vzdrževalci prostorov, strojne in programske opreme, poslovni partnerji in drugi obiskovalci se smejo gibati v varovanih prostorih samo z vednostjo pooblaščen osebe oziroma ob prisotnosti delavca zavoda.

13. člen

Zaposleni tehnično vzdrževalni delavci in čistilke se lahko gibljejo v varovanih prostorih izven delovnega časa in brez prisotnosti odgovornega delavca le, če je onemogočen pogled v podatke (nosilci podatkov so 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

14. 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, tako, da dovoljuje dostop samo za to v naprej določenim zaposlenim ali pravnim ali fizičnim osebam, ki v skladu s 7. členom ZVOP-a opravljajo dogovorjene storitve.

15. člen

Popravljanje, spreminjanje ali dopolnjevanje systemske in aplikativne programske opreme je dovoljeno samo na podlagi odobritve direktorja, izvajajo pa ga lahko samo pooblašteni 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.

16. 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 osebnimi podatki na računalniku mora skrbeti, da se v primeru servisiranja, popravila, spreminjanja ali dopolnjevanja systemske in aplikativne programske opreme ob morebitnem kopiranju osebnih podatkov po prenehanju potrebe po kopijah kopija uniči.

Delavec, pooblaščen za obdelavo in manipulacijo z osebnimi 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 osebnimi podatki.

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

17. 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.

Popravljanje, spreminjanje ali dopolnjevanje systemske in aplikativne programske opreme je dovoljeno samo na podlagi odobritve direktorja, izvajajo pa ga lahko samo pooblašteni 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.

18. člen

Zaposleni ne smejo inštalirati programske opreme brez odobritve direktorja in vednosti osebe, zadolžene za delovanje računalniškega informacijskega sistema. Prav tako ne smejo odnašati programske opreme iz zavoda brez odobritve direktorja in vednosti osebe, zadolžene za delovanje računalniškega informacijskega sistema.

19. 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.

20. 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 se jih varuje kot »uradna tajnost – strogo zaupno«.

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

Po uporabi zapečatenih gesel iz ovojnic direktor določi novo vsebino gesel.

21. člen

Za potrebe restavriranja osebnih podatkov oziroma računalniškega sistema ob okvarah in ob drugih izjemnih situacijah se zagotavlja redna izdelava kopij vsebine mrežnega strežnika in lokalnih postaj (če se podatki nahajajo tam).

Vse izdelane kopije vsebine 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 elektromagnetskim motnjam in v predpisanih klimatskih razmerah.

IV. SPREJEM IN POSREDOVANJE ZAUPNIH IN SEBNIH PODATKOV

22. člen

Zaupne in 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.

23. člen

Komunikacijski kanali med zavarovanimi prostori, ki so prostorsko oddaljeni, morajo biti zavarovani pred nepooblaščenim pristopom. Vse povezave morajo biti opisane v načrtu komunikacijskih mrež.

24. člen

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

Zaposleni, ki je zadolžen za sprejem in evidenco pošte, mora izročiti poštno pošiljko z osebni podatki direktno posamezniku, ali službi, na katero je ta pošiljka naslovljena.

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, uničevanje ali nedovoljeno seznanjanje z njihovo vsebino.

25. 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.

26. 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 7 dni od dneva, ko je bila sestavljena 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 15 dni od dneva prejema pisne zahteve. Stroške izpisa nosi oseba, ki izpis zahteva.

27. 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, ko so vsebovani v zbirki podatkov zavoda in se nanašajo nanj.

Storitve, ki jih opravljajo zunanje pravne ali fizične osebe

28. člen

Z vsako zunanjo pravno ali fizično osebo, ki opravlja posamezna opravila v zvezi z zbiranjem, obdelovanjem, shranjevanjem in posredovanjem osebnih podatkov, se sklene pisna pogodba, predvidena v drugem odstavku 7. člena ZVOP-a, ki mora vsebovati tudi pogoje in ukrepe za zagotovitev varstva osebnih podatkov in njihovega zavarovanja. Omenjeno velja tudi za zunanje osebe, ki vzdržujejo strojno in programsko opremo, izdelujejo in instalirajo novo strojno ali programsko opremo.

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

V. BRISANJE PODATKOV OZIROMA UNIČENJE NOSILCEV OSEBNIH PODATKOV

29. 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 izbrišejo oziroma uničijo nosilci podatkov.

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

30. člen

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

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

31. 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.

Prepovedano je odmetavati odpadne nosilce podatkov z zaupno vsebino v koše za smeti. Uničevanje osebnih podatkov na nosilcih iz predhodnega odstavka se mora izvajati tekoče in ažurno.

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

32. 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 pravilnik.

Zaposleni, ki izvejo ali opazijo, 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, morajo 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, sami pa poskušajo takšno aktivnost preprečiti.

33. 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 ali namenom zlorabiti osebne podatke ali jih uporabiti v nasprotju z nameni, za katere so bili 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.

VIII. ODGOVORNOST ZA IZVAJANJE UKREPOV ZAVAROVANJA OSEBNIH PODATKOV

34. člen

Za izvajanje postopkov in ukrepov za varovanje zaupnih in osebnih podatkov so odgovorni vodje organizacijskih enot in pooblašcene osebe, ki jih imenuje svet zavoda, nadzor nad izvajanjem postopkov in ukrepov, določenih s tem pravilnikom, pa opravlja direktor in strokovni vodja zavoda.

35. člen

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

36. člen

Pred nastopom dala na delovno mesto, kjer se obdelujejo podatki s stopnjo zaupnosti, ki je višja ali enaka od »uradna tajnost – zaupno«, mora zaposleni podpisati posebno izjavo, ki ga zavezuje k varovanju poklicne skrivnosti in vsebuje pouk o posledicah kršitve. Obveza varovanja osebnih podatkov, s katerimi se delavec seznanil pri svojem delu v zavodu traja tudi po prenehanju delovnega razmerja v zavodu.

37. člen

Zunanji sodelavci smejo opravljati samo storitve obdelave zaupnih in osebnih podatkov v okviru naročnikovih pooblastil in jih ne smejo obdelovati ali drugače uporabljati za noben drug namen. Medsebojne pravice in obveznosti se uredijo s pogodbo, ki mora vsebovati tudi pogoje in ukrepe za zagotovitev varstva zaupnih ali osebnih podatkov.

38. člen

Delavec stori lažjo kršitev delovne dolžnosti:

- če opusti vestno in skrbno nadzorovanje varovanih prostorov (1. odst. 5. člena),
- če opusti ravnanje 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)

39. 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 vsebine zbirk osebnih podatkov v zavarovanih zaklenjenih omarah (3. odst. 18. člena).

40. člen

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

IX. PREHODNE IN KONČNE DOLOČBE

41. 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 90 dni od dneva sprejema tega pravilnika.

42. 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.

43. 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.

44. člen

Ta pravilnik začne veljati osmi dan od dneva sprejema in objave na oglasni deski Doma Lukavci.

Datum: 18.09.2001
Številka: 225/2001

V.d.direktorice:
Stanka Vozlič, dipl.med.sestra

V tem pravilniku uporabljeni izrazi in okrajšave imajo naslednji pomen:

- 1. ZVOP-** Zakon o varstvu osebnih podatkov (Uradni list RS št. 59/99);
- 2. Osebni podatek** je podatek, ki kaže na lastnosti, stanja ali razmerja posameznika, ne glede na obliko, v kateri je izražen;
- 3. Zaupni podatek** je podatek, ki je razglašen za tajnost, ker je tako pomemben da bi z njegovim razkritjem lahko nastale škodljive posledice za delovanje;
- 4. Posameznik** je določen ali določljiva fizična oseba, na katero se nanaša osebni podatek; fizična oseba je določljiva, če se lahko identificira na način, ki ne povzroča velikih stroškov ali ne zahteva veliko časa;
- 5. Zbirka osebnih podatkov** je vsak niz podatkov, ki vsebujejo vsaj en osebni podatek ne glede na to, ali je centraliziran ali organiziran na podlagi meril, ki omogočajo uporabo ali združevanje podatkov in ne glede na to, ali se obdelujejo s sredstvi informacijske tehnologije ali ne;
- 6. Obdelava osebnih podatkov** pomeni zbiranje, shranjevanje ali združevanje podatkov v zbirkah osebnih podatkov, spreminjanje, uporabo ali sporočanje, vključno s prenosom, iskanjem, blokiranjem ali brisanjem; obdelava je lahko ročna ali s sredstvi informacijske tehnologije;
- 7. Upravljavac zbirke** je pravna ali fizična oseba (npr. podjetje, zavod, organizacija), ki je z zakonom ali pisno privolitvijo posameznika pooblaščen, da vzpostavi, vodi, vzdržuje, nadzoruje in uporablja zbirko osebnih podatkov;
- 8. Uporabnik podatkov** je fizična ali pravna oseba, ki je za pridobivanje osebnih podatkov pooblaščen z zakonom, pisno zahtevo ali privolitvijo posameznika, na katerega se podatki nanašajo;
- 9. Nosilec podatkov** so vse vrste sredstev, na katerih so zapisani ali posneti podatki (listine, akti, gradiva, spisi, računalniška oprema vključno s magnetni, optični ali drugi računalniški mediji, fotokopije, zvočno in slikovno gradivo, mikrofilmi, naprave za prenos podatkov, ipd);
- 10. Strojna oprema** je oprema za vnos, obdelavo, prikaz, shranjevanje in posredovanje podatkov: računalniška strojna oprema, oprema za prenos podatkov, oprema za kriptografijo, oprema za zvočno in

slikovno gradivo, merilni inštrumenti, mikrofilmska oprema, itd.;

11. Sistemska programska oprema

so programi, ki jih računalnik uporablja za krmiljenje svoje strojne opreme in za komuniciranje z okoljem (operacijski sistem) in druga programska orodja, ki jih dobimo z operacijskim sistemom in so namenjena vzdrževalcem in uporabnikom računalnika;

12. Aplikativna programska oprema

so programi, s katerimi se izvaja obdelava podatkov;

13. Zavarovani prostori

so prostori, kjer se nahajajo nosilci osebnih podatkov, strojna, programska računalniška in druga oprema, preko katere je mogoč dostop do zbirk podatkov in drugi prostori za obdelavo osebnih podatkov s klasičnimi sredstvi;

14. Pooblaščen delavec

je s strani odgovorne osebe imenovan delavec in skrbi za izvajanje postopkov in ukrepov za izvajanje zavarovanja osebnih podatkov.

Vrste tajnosti zaupnih podatkov v zavodu so:

1. Uradna tajnost

so podatki, ki so z zakonom, z drugim predpisom, splošnim aktom ali s sklepom pristojnega organa, izdani na podlagi zakona in so tako pomembni, da bi z njihovo izdajo nastale ali bi lahko nastale hujše škodljive posledice za delovanje Podatkom, ki so določeni za uradno tajnost se glede na njihov pomen določi stopnja zaupnosti: **strogo zaupno, zaupno ali interno**.

1.1. uradna tajnost – strogo zaupno, določiin so:

-

1.2. uradna tajnost – zaupno, določi pooblaščen oseba in so:

-

1.3. uradna tajnost - interno so: strokovna navodila za opravljanje delovnih nalog, delovni materiali za zakonske in podzakonske predpise, analitična, statistična in druga navodila o delu služb, interno informiranje in interni imeniki.

2. Poslovna tajnost so listine in podatki, ki so zakonom, statutom pravili ali drugim splošnim aktom ali odredbo pristojnega organa ali druge upravičene osebe razglašeni za industrijsko, bančno ali drugo poslovno tajnost in so tako pomembni, da bi z njihovo izdajo očitno nastale ali bi lahko nastale hujše škodljive posledice za delovanje.....
Podatkom, ki so določeni za poslovno tajnost, se glede na njihov pomen določi stopnjo zaupnosti: **strogo zaupno, zaupno** ali **interno**.

2.1. poslovna tajnost – strogo zaupno določi in so :

-

2.2. poslovna tajnost – zaupno določi pooblaščenca oseba in so:

-

2.3. poslovna tajnost – interno so: strokovna navodila za opravljanje delovnih nalog, delovnih nalogov, delovni materiali za zakonske in podzakonske predpise, analitična, statistična in druga gradiva o delu služb, interni informiranje in interni imeniki.

3. Osebni podatki se lahko obdelujejo samo v skladu z zakonom ali na podlagi pisne privolitve posameznika. Z osebnimi podatki se, glede na njihovo vsebino, ravna, kot s podatki »uradna tajnost – strogo zaupno«, »uradna tajnost – zaupno« ali »uradna tajnost – interno« (npr. interni telefonski imenik, seznam zaposlenih, ki so na dopustu). Stopnjo zaupnosti zbirk osebnih podatkov določi pooblaščenca oseba. Zbirke osebnih podatkov, ki se obdelujejo v skladu z zakonom, se varujejo s stopnjo zaupnosti, ki je višja ali enaka kot »uradna tajnost – zaupno«.