

 <p><b>JAVNI GOSPODARSKI ZAVOD PROTOKOLARNE STORITVE REPUBLIKE SLOVENIJE</b></p>		<p><b>PRAVILNIK</b></p>	
<p><b>Pravilnik o varovanju zaupnih in osebnih podatkov, o dostopu do informacij javnega značaja in o načinu dajanja informacij za javnost</b></p>			
<p><b>Velja od:</b> 15. 05. 2004</p>	<p><b>Namesto:</b> -</p>	<p><b>Stran/strani:</b> 1/12</p>	<p><b>Številka:</b> 484-IV/04</p>

Na podlagi 30. člena Odloka o ustanovitvi Javnega gospodarskega zavoda Protokolarne storitve Republike Slovenije, 14. člena Zakona o varstvu osebnih podatkov (Ur. l. RS, št. 59/99, v nadaljevanju: ZVOP), tretjega odstavka 45. člena Zakona o medijih (Ur. l. RS št. 35/01, v nadaljevanju: ZMed) in Zakona o dostopu do informacij javnega značaja (Ur. l. RS št. 24/03, v nadaljevanju: ZDIJZ) ter po obravnavi na 15. seji Upravnega odbora Javnega gospodarskega zavoda Protokolarne storitve Republike Slovenije dne 16. 04. 2004 je direktor Javnega gospodarskega zavoda Protokolarne storitve Republike Slovenije dne 04. 05. 2004 sprejel naslednji

**PRAVILNIK  
O VAROVANJU ZAUPNIH IN OSEBNIH PODATKOV,  
O DOSTOPU DO INFORMACIJ JAVNEGA ZNAČAJA IN  
O NAČINU DAJANJA INFORMACIJ ZA JAVNOST**

**I. SPLOŠNE DOLOCBE**

1. člen

S tem pravilnikom se:

- določajo organizacijski ter tehnični postopki in ukrepi za varovanje zaupnih in osebnih podatkov v Javnem gospodarskem zavodu Protokolarne storitve Republike Slovenije (v nadaljevanju: zavod) z namenom, da se prepriča nepooblaščenim osebam dostop, obdelava, uporaba, uniceenje, spreminjanje in posredovanje zaupnih in osebnih podatkov,
- določa prost dostop do informacij javnega značaja na način in po postopku določenem z zakonom in
- določa način dajanja informacij za javnost.

2. člen

Izrazi, uporabljeni v tem pravilniku, imajo naslednji pomen:

**DRŽAVNA SKRIVNOST** in **VOJAŠKA SKRIVNOST** so podatki, ki so jih za take določili pristojni državni organi in posredovali zavodu ter so tako pomembni, da bi z njihovo izdajo nastale ali bi očitno nastale škodljive posledice za varnost države ali njene politične ali gospodarske koristi.

**URADNA SKRIVNOST** so podatki, ki so jih za take določili pristojni državni organi ali organi lokalnih skupnosti in posredovali zavodu ter so tako pomembni, da bi z njihovo izdajo nastala ali bi lahko nastale hujše škodljive posledice za njihovo delovanje.

**POSLOVNA SKRIVNOST** so podatki, ki so jih v dokumentih zavoda direktor zavoda, predsednik upravnega odbora ali vodje sektorjev s sklepom določili za poslovno skrivnost, ker so tako pomembni, da bi z njihovim razkritjem lahko nastale škodljive posledice za delovanje in poslovanje zavoda.

**ZAUPEN PODATEK** so podatki z delovnega področja zavoda, ki so bili na predpisan način določeni za poslovno skrivnost, ker so tako pomembni, da bi z njegovim razkritjem lahko nastale škodljive posledice za delovanje in poslovanje zavoda, podatki, ki so jih posredovale zavodu druge osebe kot skrivnost ter osebni podatki in zbirke podatkov o zaposlenih in o uporabnikih storitev zavoda zbrani v skladu z zakonom ali z njihovo privolitvijo.

**OSEBNI PODATEK** so podatki, ki kažejo na lastnost, stanja ali razmerja posameznikov ne glede na obliko, v kateri so izraženi.

**ZBIRKA PODATKOV** je zbirka, ki vsebuje zaupne ali osebne podatke (evidence, registri, baze podatkov ipd.), ki se vodi s sredstvi za avtomatsko obdelavo podatkov ali s klasičnimi sredstvi in je namenjena izvajanju nalog zavoda.

**OBDELAVA PODATKOV** so postopki in procesi zbiranja, shranjevanja, spreminjanja, združevanja, uporabe, brisanja in posredovanja podatkov.

**DOKUMENT** je vsak napisan, narisano, natisnjen, razmnožen, posnet, fotografiran, magneten, optičen ali kakšen drugaceni način zapisa zaupnega ali osebnega podatka.

**NOSILECI PODATKOV** so vse vrste sredstev, na katerih so zapisani ali posneti zaupni ali osebni podatki.

**VAROVAN PROSTOR** so vsi prostori, v katerih so nosilci zaupnih ali osebnih podatkov ali prostori, v katerih je oprema, s katero je mogoč dostop do teh podatkov.

### 3. člen

Varovanje zasebnosti zaposlenih in uporabnikov storitev zavoda izvaja zavod v skladu z zakonom, da se preprečujejo nezakoniti in neupravičeni posegi v zasebnost posameznika ter neupravičeni vpogledi ali posredovanje podatkov o posamezni osebi pri obdelavi, varovanju in uporabi le-teh.

Osebne podatke o zaposlenih in o uporabnikih storitev zavoda in njihovem poslovanju z zavodom so vsi zaposleni v zavodu zavezani varovati in jih brez njihovega dovoljenja ne smejo izdati ali sporočiti tretji osebi.

### 4. člen

V zavodu se lahko s privolitvijo posameznika obdelujejo samo tisti osebni podatki o zaposlenih in o uporabnikih storitev zavoda:

- za katere je tako določeno z zakonom in
- samo za namene določene v zakonu.

Obdelava osebnih podatkov pomeni zbiranje, shranjevanje ali združevanje podatkov v zbirke osebnih podatkov ročno ali s sredstvi informacijske tehnologije ter spreminjanje, uporabo ali sporočanje, vključno s prenosom, iskanjem, blokiranjem in brisanjem.

Osebni podatki o zaposlenih in o uporabnikih storitev ne smejo biti uporabljeni na način, ki ni združljiv z nameni določenimi v zakonu.

#### 5. člen

Podatki v dokumentih, ki so povezani s poslovanjem zavoda ter dejstva in okoliščine, ki so povezane s poslovnim odnosom zavoda in uporabnikov njegovih storitev, so zaupni podatki. Ti podatki predstavljajo poslovno skrivnost, kadar je tako določeno s sklepom predsednika upravnega odbora, direktorja ali vodje sektorja.

S tem sklepom morajo biti seznanjeni zaposleni, člani organov zavoda in druge osebe, ki so dolžne varovati poslovno skrivnost.

Ne glede na to, ali so določeni podatki opredeljeni kot poslovna skrivnost, pa se štejejo za poslovno skrivnost podatki, za katere je očitno, da bi nastala občutna škoda, ce bi zanje zvedela nepooblaščenca oseba.

Za razkritje poslovne skrivnosti odgovarjajo zaposleni, člani organov zavoda ter druge osebe, ce so vedeli ali bi morali vedeti za tak značaj podatkov.

#### 6. člen

Za poslovno skrivnost se ne morejo določiti podatki, ki so po zakonu javni in podatki o kršitvi zakona ali dobrih poslovnih običajev.

#### 7. člen

Zavod deluje in posluje javno, zato posameznikom in pravnim osebam v rokih in po postopku določenem v ZDIJZ omogoča prost dostop do informacij javnega značaja, s katerimi razpolaga.

#### 8. člen

Informacije javnega značaja so informacije, ki izhajajo iz delovanja in poslovanja zavoda, nahajajo pa se v obliki dokumenta, zadeve, dosjeja, registra, evidence ali dokumentarnega gradiva, ki ga je izdelal zavod sam, v sodelovanju z drugimi, ali pridobil od drugih oseb.

#### 9. člen

Zavod mora dajati resnicne, popolne in pravčasne informacije urednikom, novinarjem in drugim avtorjem programskih prispevkov o vprašanih s svojega delovnega področja za objavo prek medijev.

#### 10. člen

Z informacijami s svojega delovnega področja seznanja zavod javnost na naslednje načine:

- z objavljanjem informacij na svoji spletni strani;
- s samoiniciativnim posredovanjem informacij medijem;
- s posredovanjem informacij urednikom, novinarjem in drugim avtorjem programskih prispevkov, kadar prejme njihovo zahtevo;
- z omogočanjem vpogleda osebam iz prejšnje alineje v javno dokumentacijo zavoda.

#### 11. člen

Dostop urednikov, novinarjev in drugih avtorjev programskih prispevkov ter drugih upravičencev do javnih informacij je prost, razen v primerih, ki jih določa četrti odstavek 45. člena ZMed in razen za izjeme, ki se nanašajo na podatke opredeljene v 6. členu ZDIJZ.

Ce je možno informacijo iz prejšnjega odstavka izlociti iz dokumenta, ne da bi to ogrozilo njegovo zaupnost, direktor tako informacijo izloci ter seznanil prosilca z vsebino preostalega dela dokumenta.

#### 12. člen

Informacija javnega znacaja niso:

- osebni podatki o zaposlenih in o uporabnikih storitev zavoda, ce bi to pomenilo kršitev zaupnosti osebnih podatkov v skladu z zakonom, razen ce se z njihovo objavo lahko prepreci hujše kaznivo dejanje ali nevarnost za življenje ljudi in njihovo premoženje,
- podatki, ki so bili v zavodu na predpisan način določeni kot poslovna skrivnost in
- podatki, ki so bili zavodu dostavljeni kot državna, vojaška ali uradna skrivnost s strani drugih oseb.

#### 13. člen

V skladu s predpisi o posredovanju informacij javnega znacaja zavod pripravi, vzdržuje in v svetovnem spletu objavi katalog informacij javnega znacaja.

V svetovni splet zavod posreduje tudi besedilo ustanovitvenega akta, splošnih aktov, informacije v zvezi z javnimi razpisi, programe dela in poročila ter druge informacije, kar predstavlja informativni delovni pripomoček, glede katerega zavod ne jamči odškodninsko ali kako drugače.

#### 14. člen

Javnost dela zavoda zagotavlja direktor, ki je tudi odgovorna oseba, ki skrbi za resničnost in popolnost posredovanih informacij posameznikom in pravnim osebam ter javnosti.

#### 15. člen

Način in organizacija varovanja prostorov in podatkov na osebnih računalnikih, delovnih postajah in strežnikih zavoda se na predlog organizatorja informacijskih sistemov podrobneje določita z organizacijskim predpisom na osnovi določb tega pravilnika in drugih predpisov.

## **II. OBJAVLJANJE INFORMACIJ NA SPLETNI STRANI ZAVODA, SAMOINICIATIVNO POSREDOVANJE INFORMACIJ ZAVODA MEDIJEM, POSREDOVANJE INFORMACIJ NA ZAHTEVO UPRAVICENCEV IN OMOGOCANJE VPOGLEDA V DOKUMENTACIJO ZAVODA**

#### 16. člen

Zavod objavlja na svoji spletni strani naslednje vrste informacij:

- ustanovitveni akt in veljavne splošne akte
- informacije o komercialnih in protokolarnih dejavnostih;
- informacije in gradiva v zvezi z javnimi razpisi zavoda;
- programe dela in poročila o opravljenih nalogah;
- redna letna poročila o poslovanju;
- druge informacije, po nalogu direktorja, ter informacije, katerih objavo predlagajo delavci zavoda, ce se s tako objavo strinja direktor.

#### 17. člen

Informacije, ki jih zavod samoiniciativno posreduje medijem, lahko v objavo pošlje le direktor, razen v primerih iz 22. člena tega pravilnika.

Pobude za objavo informacije v medijih lahko dajo vsi zaposleni v zavodu.

#### 18. člen

Kadar urednik, novinar ali drug avtor programskega prispevka zahteva javno informacijo z delovnega področja zavoda, mu jo mora direktor zagotoviti najpozneje do konca naslednjega delovnega dne po prejemu zahteve.

Ce direktor ne zagotovi zahtevane javne informacije, mora pisno obrazložiti razloge za zavrnitev zahteve, ce to zahteva odgovorni urednik medija, in sicer najpozneje do konca naslednjega dne po prejemu zahteve odgovornega urednika.

Ce je popolna zagotovitev informacije mogoča le s posredovanjem prepisa iz dokumentacijskega gradiva zavoda, direktor zagotovi takšen prepis, od upravicenca pa v tem primeru lahko zahteva nadomestilo dejanskih stroškov za prepis zahtevanih informacij.

#### 19. člen

Kadar urednik, novinar, drug avtor programskega prispevka ali drugi upravicenec zahteva od zavoda obširno javno informacijo, ki jo zajema več enot dokumentacijskega gradiva, mu direktor lahko zagotovi takšno informacijo v skrajšani oziroma v opisni obliki.

Upravicenec, ki mu je bila zagotovljena informacija v skrajšani ali opisni obliki, lahko zahteva tudi neposreden vpogled v dokumentacijsko gradivo zavoda, iz katerega bi bila lahko razvidna zahtevana javna informacija.

Ce direktor ne zagotovi pravočasno javne informacije iz prvega odstavka tega člena, ali pa ne zagotovi pravočasno vpogleda v dokumentacijsko gradivo iz prejšnjega odstavka, mora na zahtevo odgovornega urednika pisno obrazložiti razloge za neizpolnitev zahteve najpozneje do konca naslednjega dne po prejemu zahteve odgovornega urednika.

#### 20. člen

Kadar direktor v zvezi z nameravano objavo informacije v medijih ali z zagotovitvijo informacije na zahtevo upravicenca potrebuje delovno gradivo, dodatno strokovno utemeljitev ali manjkajoče podatke, mora delavec, ki je zadolžen za izvajanje nalog v zvezi s predmetom informacije, in razpolaga s potrebnimi podatki in gradivom, to zagotoviti pred koncem naslednjega delovnega dne. Direktor lahko delavcu v enakem roku raloži tudi pripravo osnutka oziroma predloga informacije.

Ce delavec ne bi mogel zagotoviti delovnega gradiva, strokovnih utemeljitev, manjkajočih podatkov, ali pa osnutka oziroma predloga informacije, ali jih ne more zagotoviti v roku, mora še isti dan direktorju posredovati o tem pisno izjavo s potrebnimi pojasnili.

#### 21. člen

Direktor lahko zahteva od delavca zavoda, ki je zadolžen za izvajanje nalog v zvezi s predmetom zahtevane informacije, da omogoči uredniku, novinarju ali drugemu avtorju programskega prispevka ali drugemu upravicencu vpogled v dokumentacijsko gradivo na delovnem mestu.

Ce delavec zavoda v primeru iz prejšnjega odstavka ne more izpolniti svoje obveznosti, mora še pred koncem naslednjega dne po prejemu zahteve posredovati direktorju pisno izjavo s potrebnimi pojasnili.

#### 22. clen

Direktor lahko za zagotavljanje informacij z določenega področja pisno pooblasti tudi druge delavce zavoda.

Za resničnost in točnost informacij, ki jih posredujejo javnosti, delavci iz prejšnjega odstavka odgovarjajo neposredno direktorju.

#### 23. clen

Zaposleni praviloma ne dajejo izjav in javnosti ne posredujejo podatkov o delu in poslovanju zavoda.

Informacije, ki jih mediji objavijo na podlagi izjav in podatkov o delu in poslovanju zavoda, ki so jih posredovali zaposleni v zavodu, nimajo značaja uradne informacije zavoda, ce jih za javnost niso sporočili predsednik upravnega odbora ali direktor oziroma njegov pooblaščenec.

### **III. VRSTE SKRIVNOSTI IN STOPNJE ZAUPNOSTI PODATKOV V ZAVODU, PRAVILA OZNACEVANJA IN RAZMNOŽEVANJA TER ARHIVIRANJE, HRANJENJE IN NACIN PRENOSA ZAUPNIH IN OSEBNIH PODATKOV**

#### 24. clen

V zavodu se hranijo, obdelujejo in uporabljajo tudi zaupni podatki, ki so lahko opredeljeni kot državna, vojaška, uradna ali poslovna skrivnost ter osebni podatki in zbirke podatkov. Podatkom, ki so na predpisan način določeni za poslovno skrivnost, osebnim podatkom in zbirkam podatkov se glede na njihov pomen določi stopnja zaupnosti.

#### 25. clen

Posamezne stopnje zaupnosti podatkov lahko določijo naslednje pooblašcene osebe:

- »STROGO ZAUPNO« (ali »SZ«) ali »ZAUPNO« (ali »Z«) direktor in predsednik upravnega odbora s sklepom za podatke v dokumentih, o katerih odločata direktor in upravni odbor v okviru svojih pristojnosti
- »INTERNO« (ali »I«) direktor in vodje sektorjev (organizacijski predpisi in navodila, strokovna navodila za opravljanje delovnih nalog, delovni materiali za interne akte, analitična, statistična in druga gradiva o delu in poslovanju zavoda ipd.)

Stopnjo zaupnosti osebnih podatkov in zbirk osebnih podatkov, ki se obdelujejo v skladu z zakonom, določi pristojni vodja sektorja.

#### 26. clen

Vrsta skrivnosti in stopnja zaupnosti se na pisnih dokumentih na prvi strani označujeta v desnem zgornjem kotu tako, da se v posamezne vrstice od prve dalje vpiše naslednje podatke:

- vrsta skrivnosti (»POSLOVNA SKRIVNOST« ali »OSEBNI PODATKI«),
- stopnja zaupnosti (»STROGO ZAUPNO«, »ZAUPNO« ali »INTERNO«),
- datum določitve zaupnosti,
- ime in priimek pooblašcene osebe, ki je določila vrsto skrivnosti in stopnjo zaupnosti.

V peti vrstici sledi v levem zgornjem kotu glava zavoda, potem pa datum, številka in zadeva. Pred običajno številko dokumenta se vpišeta veliki crki »SZ« za strogo zaupno, »Z« za zaupno in »I« za interno.

Podatki o vrsti skrivnosti in stopnji zaupnosti morajo biti na prvi strani zapisani z velikimi poudarjenimi crkami velikosti 14.

Vsaka naslednja stran dokumenta ima v nogi dokumenta poleg številke strani na sredini desno z velikimi nepoudarjenimi crkami velikosti 12 izpisano tudi stopnjo zaupnosti (»STROGO ZAUPNO«, »ZAUPNO« ali »INTERNO«).

Drugi mediji kot so diskete, kompaktni diski, kasete imajo na nalepki enake podatke o vrsti skrivnosti in stopnji zaupnosti kot pisni dokumenti.

Osebni računalniki in vse datoteke z zaupnimi podatki morajo biti varovani z geslom.

#### 27. člen

Pri določanju stopnje zaupnosti se določi najnižja stopnja zaupnosti nosilca podatkov, ki še zagotavlja varovanje podatka.

Kratko pisno obrazložitev določenih zaupnih podatkov, ki se hrani z originalom, izdelava izdelovalec nosilca podatkov, podpiše pa jo direktor ali pristojni vodja sektorja.

#### 28. člen

Zaupnost lahko spremeni ali odpravi samo oseba, ki jo je določila, za kar izdelava tudi pisno obrazložitev, ki se hrani poleg nosilca podatkov.

#### 29. člen

Nosilcev podatkov z oznako zaupnosti prejemniki ne smejo razmnoževati, prepisovati ali kopirati.

Izjemoma se samo v tajništvu vodstva zavoda lahko razmnoži, prepíše ali kopira zaupen podatek z oznako »POSLOVNA SKRIVNOST - ZAUPNO« in »INTERNO«, ce to izrecno odobri direktor ali pristojni vodja sektorja.

Kopijo tajništvo vodstva zavoda oznaci in evidentira ter opremi z žigom registrirana kopija, datumom in podpisom izdelovalca kopije.

#### 30. člen

Arhivski izvod dokumenta z zaupnimi podatki je praviloma prvi (originalni) izvod, ki se hrani v tajništvu vodstva zavoda.

Poleg arhivskega izvoda dokumenta se hrani še kratka pisna obrazložitev, na podlagi katere je bila določena stopnja zaupnosti, seznam oseb, ki so dokument prejele, seznam oseb, ki so vpogledale arhivski izvod dokumenta in morebitna dovoljenja za razmnoževanje ali kopiranje.

### 31. clen

Zaupne in osebne podatke je dovoljeno prenašati z informacijskimi, telekomunikacijskimi in drugimi sredstvi le ob izvajanju postopkov in ukrepov, ki nepooblaščenim preprečujejo prilaščanje ali uniceenje podatkov ter neupravičeno seznanjanje z njihovo vsebino.

Pisni dokumenti z zaupnimi podatki se prenašajo v zaprtih ovojnica iz trdega in neprosojnega materiala.

### 32. clen

Zaupni podatki označeni s stopnjo zaupnosti »STROGO ZAUPNO« in »ZAUPNO« se prenašajo s kurirjem, zaupni podatki označeni s stopnjo »INTERNO« pa se lahko pošiljajo po pošti ali po elektronskih medijih.

Ovojnica z zaupnimi podatki mora imeti v zgornjem levem kotu glavo zavoda, številko in datum dokumenta, v desnem kotu pa oznako vrste skrivnosti in stopnje zaupnosti. Naslovnik je izpisan na sredini ovojnice, pod naslovom pa je poudarjeno z navednicami izpisano »ODPIRA SAMO NASLOVNIK«.

Pravila za prenos zaupnih podatkov določena prejšnjem in v tem clenu veljajo tudi za prenose med organizacijskimi enotami zavoda.

### 33. clen

Osebni podatki se lahko posredujejo samo tistim uporabnikom, ki se izkažejo z ustrezno zakonsko osnovo ali pisno privolitvijo posameznika, na katerega se podatki nanašajo.

Za vsako posredovanje osebnih podatkov mora upravičenec vložiti pisno vlogo, na kateri mora biti navedena zakonska osnova za pridobitev osebnih podatkov, ali predložiti pisno privolitev posameznika, na katerega se podatki nanašajo.

Vsako posredovanje osebnih podatkov se zabeleži v evidenco posredovanj, ki mora vsebovati pregled zahtevkov, kateri podatki so bili posredovani, komu so bili posredovani in kdaj.

## **IV. VAROVANJE PROSTOROV IN NOSILCEV PODATKOV TER SISTEMSKÉ IN APLIKATIVNO PROGRAMSKE RACUNALNIŠKE OPREME IN PODATKOV**

### 34. clen

Prostori, v katerih so nosilci zaupnih ali osebnih podatkov ter strojna in programska oprema ter arhivske omare, morajo biti varovani z organizacijskimi ter fizicnimi ali tehničnimi ukrepi tako, da onemogočajo nepooblaščenim osebam dostop do podatkov.

### 35. clen

Zaposleni lahko vstopajo in se zadržujejo v prostorih, v katerih se hranijo nosilci zaupnih ali osebnih podatkov ter strojna in programska oprema ter arhivske omare samo v rednem delovnem času, izven tega casa pa samo na podlagi dovoljenja direktorja ali vodje sektorja.

Ključce prostorov hranijo in izdajajo varnostniki - receptorji, ključce arhivskih omar pa hranijo delavci, ki so zadolženi za zbiranje, hranjenje, urejanje, obdelovanje in varovanje osebnih ali zaupnih podatkov.

#### 36. clen

Prostori, v katerih se hranijo nosilci zaupnih in osebni podatkov, strojna in programska oprema in arhivske omare ne smejo ostajati nenadzorovani in morajo biti zaklenjeni, če v njih ni oseb pristojnih za njihov nadzor.

Izven delovnega časa morajo biti arhivske omare in pisalne mize v prostorih z nosilci podatkov zaklenjene, računalniki in druga strojna oprema pa izklopljeni in fizično ali programsko zaklenjeni.

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

#### 37. clen

S štipilkami, suhimi žigi, papirjem z glavo zavoda in drugimi pripomočki, s katerimi bi bilo mogoče ponarediti dokumente, je potrebno ravnati kot z zaupnimi podatki.

#### 38. clen

Nosilci podatkov vrste skrivnosti uradna in državna skrivnost se ne glede na stopnjo zaupnosti hranijo izključno le v prostorih tajništva vodstva zavoda.

Dostop do zaupnih podatkov s stopnjo zaupnosti »STROGO ZAUPNO« in »ZAUPNO« imajo samo osebe, ki imajo dovoljenje za dostop.

Osebe, ki nimajo ustreznega dovoljenja ne morejo prenašati, rokovati ali se seznanjati s temi podatki.

Nosilcev podatkov s stopnjo zaupnosti »STROGO ZAUPNO« se ne sme odnašati izven prostorov zavoda, ostale nosilce podatkov, ki vsebujejo zaupne podatke nižje stopnje zaupnosti, pa samo z dovoljenjem direktorja oziroma od njega pooblaščenega osebe.

#### 39. clen

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

#### 40. clen

Vzdrževanja in popravila strojne in programske računalniške opreme so dovoljena samo z vednostjo pristojnega vodje sektorja, izvajajo pa jih lahko samo organizator informacijskih sistemov ali delavci pooblaščenega servisa, s katerimi ima zavod sklenjeno ustrezno pogodbo.

#### 41. clen

Vzdrževalci strojne in programske računalniške opreme, vzdrževalci druge opreme, prostorov in naprav, obiskovalci in poslovni partnerji se smejo gibati v prostorih, v katerih se nahajajo in hranijo nosilci zaupnih ali osebni podatkov samo v delovnem času ob prisotnosti delavca zavoda, ki je skrbnik podatkov.

Zaposleni, kot so čistilke, vzdrževalci idr. se lahko izven delovnega časa gibljejo samo v tistih prostorih, kjer je fizično onemogočen vpogled v zaupne in osebne podatke.

Nosilci podatkov morajo biti izven delovnega časa shranjeni v zaklenjenih omarah in pisalnih mizah, računalniki in druga strojna oprema pa morajo biti izklopljeni ali kako drugače fizično ali programsko zaklenjeni.

#### 42. člen

Dostop do medijev za namestitve programske opreme mora biti varovan tako, da dovoljuje dostop samo organizatorju informacijskih sistemov ali osebam, ki v skladu s sklenjeno pogodbo opravljajo dogovorjene storitve.

#### 43. člen

Nadgradnja ter dopolnjevanje systemske in aplikativne programske opreme sta dovoljeni samo na podlagi odobritve pristojnega vodje sektorja, izvajajo pa ga lahko samo pooblaščenih servisi in organizacije ali posamezniki, ki imajo z zavodom sklenjeno ustrezno pogodbo.

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

#### 44. člen

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

#### 45. člen

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

Ob pojavu računalniškega virusa se nemudoma obvesti organizator informacijskih sistemov, ki odpravi virus, hkrati pa ugotovi tudi vzrok pojava virusa v računalniškem informacijskem sistemu zavoda.

Vsebina diskov mrežnega strežnika in lokalnih delovnih postaj, kjer so shranjeni pomembni podatki, se morajo vsaj enkrat tedensko preveriti glede na prisotnost računalniških virusov.

#### 46. člen

Zaposleni ne smejo sami nameščati programske opreme brez vednosti in dovoljenja organizatorja informacijskih sistemov, izven zavoda pa tudi ne smejo odnašati programske opreme, če nimajo odobritve pristojnega vodje sektorja in brez vednosti organizatorja informacijskih sistemov .

#### 47. člen

Pristop do podatkov preko aplikativne programske opreme se varuje s sistemom gesel za avtorizacijo in identifikacijo uporabnikov programov in podatkov.

Organizator informacijskih sistemov izdela organizacijsko navodilo, s katerim se določi režim dodeljevanja, hranjenja, vzdrževanja in spreminjanja gesel.

#### 48. clen

Vsa gesla in postopki, ki se uporabljajo za vstop in administriranje mreže osebnih racunalnikov (nadzorna gesla), elektronske pošte in aplikativnih programov se loceno hranijo v zapечатnih ovojnica. Varujejo se kot poslovno skrivnost. Uporabi se jih samo v izrednih okoliščinah oziroma ob nujnih primerih. Vsaka izredna uporaba vsebine zapечатnih ovojnic se dokumentira.

#### 49. clen

Za potrebe obnavljanja racunalniškega sistema ob okvarah in ob drugih izjemnih situacijah se mora zagotoviti redna izdelava kopij vsebine mrežnega strežnika in lokalnih postaj (ce so podatki tam).

Kopije se hranijo v za to določenih arhivskih omarah, ki morajo biti ognjevarne in zavarovane proti poplavam in elektromagnetnim motnjam, v okviru predpisanih klimatskih pogojev ter zaklenjene.

### **V. BRISANJE IN UNICENJE PODATKOV**

#### 50. clen

Po preteku roka hranjenja podatkov, se le-ti brišejo.

Za brisanje podatkov iz racunalniških medijev se uporabi takšna metoda brisanja, da je nemogoca restavracija vseh ali dela brisanih podatkov.

Podatki na klasicnih medijih (listine, kartoteke, register, seznam ...) se unicijo na nacin, ki onemogoca branje unicjenih podatkov. Na enak nacin se unicuje pomožno gradivo (npr.: matrice, izracune in grafikone, skice, poskusne oziroma neuspešne izpise, ipd.).

#### 51. clen

Odpadnih in poškodovanih nosilcev podatkov z zaupno vsebino ni dovoljeno odmetavati v koše za smeti.

### **VI. UKREPANJE OB SUMU NEPOOBLAŠČENEGA DOSTOPA DO PODATKOV IN ODGOVORNOST ZA IZVAJANJE VARNOSTNIH UKREPOV IN POSTOPKOV**

#### 52. clen

Zaposleni so dolžni takoj obvestiti o nepravilnosti organizatorja informacijskih sistemov, direktorja ali drugo pooblašceno osebo, ce ugotovijo, da se izvajajo aktivnosti, ki so povezane z:

- odkrivanjem ali nepooblašceni unicenjem zaupnih in osebnih podatkov,
- zlonamernim ali nepooblašceni uporabljanjem podatkov ali
- prilašcanjem, spreminjanjem ali poškodovanjem podatkov.

#### 53. člen

Za izvajanje postopkov in ukrepov za varovanje zaupnih in osebnih podatkov so odgovorni direktor, vodje sektorjev, področij in timov, organizator informacijskih sistemov, drugi strokovni sodelavci in druge določene osebe.

#### 54. 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 z njimi seznanjen pri opravljanju svojega dela. Obveza varovanja zaupnih podatkov ne preneha s prenehanjem delovnega razmerja.

Pred nastopom dela na delovnem mestu, kjer se obdelujejo podatki s stopnjo zaupnosti, ki je višja ali enaka od »POSLOVNA SKRIVNOST – ZAUPNO«, mora zaposleni podpisati posebno izjavo, ki ga zavezuje k varovanju poklicne skrivnosti in vsebuje pouk o posledicah kršitve.

#### 55. člen

Zunanji sodelavci smejo opravljati storitve obdelave zaupnih in osebnih podatkov v okviru pogodbenih pooblastil in jih ne smejo obdelovati ali drugače uporabljati za noben drug namen. Medsebojne pravice in obveznosti določene s pogodbo morajo vsebovati tudi določila o pogojih in ukrepih za zagotovitev varstva zaupnih ali osebnih podatkov.

### **VII. KONCNI DOLOČBI**

#### 56. člen

Za kršitev določil o obveznostih določenih s tem pravilnikom so zaposleni lahko tudi disciplinsko odgovorni v skladu z določili Pravidnika o disciplinski in odškodninski odgovornosti (št. 1069-IV/03), zunanji sodelavci pa skladno s pogodbo.

#### 56. člen

Ta pravilnik začne veljati osem dni po objavi na oglasnih deskah zavoda.

**dr. Iztok PURIC,**  
**direktor**

Pravilnik je bil objavljen na oglasnih deskah zavoda 07. 05. 2004!