Na podlagi 24. in 25. člena Zakona o varstvu osebnih podatkov (Uradni list RS, 94/2007) izdaja

INŠTITUT ZA HIDRAVLIČNE RAZISKAVE
HAJDRIHOVA ULICA 28
1000 LJUBLJANA
(v nadaljevanju: upravljavec osebnih podatkov)

PRAVILNIK O ZAVAROVANJU OSEBNIH PODATKOV

I. SPLOŠNE DOLOČBE

1. člen
Vsebina in namen pravilnika

S tem pravilnikom se določajo organizacijski, tehnični in logično-tehnični postopki in ukrepi za zavarovanje osebnih podatkov pri upravljavcu osebnih podatkov.
Z navedenimi postopki in ukrepi se preprečuje:
- nepooblaščen ali neregistriran dostop do prostorov, strojne in programske opreme,
- slučajno ali namerno nepooblaščeno uničenje podatkov, njihova sprememba ali izguba,
- nepooblaščen dostop, obdelava in posredovanje osebnih podatkov,
- nepooblaščena uporaba osebnih podatkov.

2. člen
Uporaba pravilnika

Ta pravilnik velja za zaposlene in za zunanje sodelavce upravljavca osebnih podatkov.

3. člen
Pomen izrazov

V tem pravilniku uporabljeni izrazi imajo naslednji pomen:
1. Osebni podatek - katerikoli podatek, ki se nanaša na posameznika, ne glede na obliko, v kateri je izražen
2. Občutljivi osebni podatek - podatek o rasnem, narodnem ali narodnostnem poreklu, političnem, verskem, filozofskem prepričanju, članstvu v sindikatu, zdravstvenem stanju, spolnem življenju, vpisu ali izbrisu v ali iz kazenske evidence ali prekrškovne evidence ter biometrične značilnosti.
3. Posameznik - je določena ali določljiva fizična oseba, na katero se nanaša osebni podatek; fizična oseba je določljiva, če se jo lahko neposredno ali posredno identificira, predvsem s sklicevanjem na identifikacijsko številko ali na enega ali več dejavnikov, ki so značilni za njeno fizično, fiziološko, duševno, ekonomsko, kulturno ali družbeno identiteto, pri čemer način identifikacije ne povzroča velikih stroškov, nesorazmerno velikega napora ali ne zahteva veliko časa.;
4. Obdelava osebnih podatkov - pomeni kakršnokoli delovanje ali niz delovanj, ki se izvaja v zvezi z osebnimi podatki, ki so avtomatizirano obdelani ali ki so pri ročni obdelavi del zbirke osebnih podatkov ali so namenjeni vključitvi v zbirko osebnih podatkov, zlasti zbiranje, pridobivanje, vpis, urejanje, shranjevanje, prilagajanje ali spreminjanje, priklicanje, vpogled,

uporaba, razkritje s prenosom, sporočanje, širjenje ali drugo dajanje na razpolago, razvrstitev ali povezovanje, blokiranje, anonimiziranje, izbris ali uničenje; obdelava je lahko ročna ali avtomatizirana (sredstva obdelave).
5. Zbirka osebnih podatkov - je vsak strukturiran niz podatkov, ki vsebuje vsaj en osebni podatek, ki je dostopen na podlagi meril, ki omogočajo uporabo ali združevanje podatkov, ne glede na to, ali je niz centraliziran, decentraliziran ali razpršen na funkcionalni ali geografski podlagi; strukturiran niz podatkov je niz podatkov, ki je organiziran na takšen način, da določi ali omogoči določljivost posameznika.
6. Nosilec podatkov - so vse vrste sredstev, na katerih so sranjeni osebni podatki (listina, akt, gradivo, spis, magnetni, optični ali drugi računalniški mediji, prikazovalnik računalnika, fotokopije, zvočno in slikovno gradivo, mikrofilmi, naprave za prenos podatkov, …)
7. Upravljavec osebnih podatkov - je fizična ali pravna oseba ali druga oseba javnega ali zasebnega sektorja, ki sama ali skupaj z drugimi določa namene in sredstva obdelave osebnih podatkov oziroma oseba, določena z zakonom, ki določa tudi namene in sredstva obdelave.
8. Uporabnik osebnih podatkov - je fizična ali pravna oseba ali druga oseba javnega ali zasebnega sektorja, ki se ji posredujejo ali razkrijejo osebni podatki.
9. Posredovanje osebnih podatkov - je posredovanje ali razkritje osebnih podatkov.

4. člen
Katalog zbirk osebnih podatkov

V katalogu zbirk osebnih podatkov se vodi opis zbirk osebnih podatkov (26. člena ZVOP-1). Katalog zbirke osebnih podatkov se za vsako zbirko osebnih podatkov naredi najmanj 15 dni pred vzpostavitvijo zbirke osebnih podatkov. V roku 15 dni pa se podatki iz 1., 2., 4., 5., 6., 9., 10., 12. in 13. točke prvega odstavka 26. člena ZVOP-1.
Upravljavec osebnih podatkov mora skrbeti za točnost in ažurnost kataloga zbirk osebnih podatkov in ga ob vsaki spremembi redno dopolniti ter spremembe v roku 8 dni posredovati pristojnemu državnemu organu.
Zaposlene, ki obdelujejo zbirke osebnih podatkov, je potrebno seznaniti z vsebino kataloga zbirk osebnih podatkov. Vsem ostalim pa je potrebno na njegovo zahtevo omogočiti vpogled v katalog zbirk osebnih podatkov.
Upravljavec osebnih podatkov mora voditi in po potrebi dopolnjevati seznam zbirk osebnih podatkov iz katerega je razvidno kdo je upravljavec posamezne zbirke osebnih podatkov in katerim osebam je zaradi narave njihovega dela dovoljen dostop do zbirke osebnih podatkov.

II. POOBLAŠČENI DELAVCI

5. člen
Odgovorne osebe

Za zbiranje, obdelavo, shranjevanje in posredovanje osebnih podatkov se določajo odgovorne osebe glede na vsebino osebnih podatkov, ki se obdelujejo, shranjujejo in posredujejo z zakonom pooblaščenim organizacijam ter glede na naravo dela, posameznega delavca.
Zaposleni in zunanji sodelavci, ki pri svojem delu obdelujejo in uporabljajo osebne podatke, oziroma imajo na katerikoli način dostop do osebnih podatkov, morajo biti seznanjeni z ZVOP-1, s področno zakonodajo, ki ureja posamezno področje njihovega dela ter z vsebino tega pravilnika.
Odgovorna oseba za posamezno zbirko osebnih podatkov vzpostavi to zbirko osebnih podatkov in je zanjo odgovorna.

6. člen
Seznam zbirk osebnih podatkov

Naziv zbirke osebnih podatkov in odgovorne osebe za vzpostavitev in obdelavo posamezne zbirke:
Zbirka osebnih podatkov 1: podatki o zaposlenih,
Zbirka osebnih podatkov 2: podatki o članih upravnega odbora,
Zbirka osebnih podatkov 3: podatki o strankah,
Zbirka osebnih podatkov 4: podatki o poslovnih partnerjih.

III. OBDELAVA OSEBNIH PODATKOV

7. člen
Zbirka osebnih podatkov

V zbirki osebnih podatkov se lahko obdelujejo le tisti osebni podatki, ki imajo ustrezno zakonsko podlago po določbah ZVOP-1. Osebne podatke je dovoljeno zbirati samo za določene in zakonite namene. Osebni podatki se ne smejo nadalje obdelovati, če je ta obdelava v nasprotju s temi nameni oziroma, če zakon ne določa drugače.
Pri obdelavi občutljivih osebnih podatkov morajo biti le-ti posebej označeni in zavarovani, tako da se nepooblaščenim osebam prepreči dostop. Obdelovati pa jih je dovoljeno samo na podlagi 13. člena ZVOP-1.
Posameznik (oziroma njegov zakoniti zastopnik, če gre za mladoletno osebo), na katerega osebni podatki se obdelujejo mora biti o tem obveščen v skladu z 19. členom ZVOP-1.

8. člen
Obdelava osebnih podatkov uporabnikov spletnih strani

Osebne podatke (npr. podatki o uporabniku, gesla in uporabniška imena, naslove elektronske pošte, ...), ki jih uporabniki spletnih strani upravljavca osebnih podatkov posredujejo z namenom dostopa do posameznih vsebin je potrebno varovati v skladu z ZVOP-1. Dostop do teh podatkov ima samo s strani upravljavca osebnih podatkov pooblaščena oseba. Tako pridobljene osebne podatke je dovoljeno uporabljati samo za namene dostopa uporabnikov do spletnih vsebin. Če je uporabnik na spletni strani izrazil tudi željo o obveščanju, je osebne podatke dovoljeno uporabljati tudi v te namene. Kakršnakoli uporaba in obdelava tako pridobljenih osebnih podatkov, ki ni neposredno povezana z uporabo vsebin, za katere je uporabnik spletnih strani izrazil željo, ni dovoljena.

IV. VAROVANJE PROSTOROV IN RAČUNALNIŠKE OPREME

9. člen
Varovanje osebnih podatkov

Nosilci zbirk osebnih podatkov, strojna in programska oprema se morajo hraniti v posebej določenih prostorih, ki morajo biti varovani z organizacijskimi ter fizičnimi oziroma tehničnimi ukrepi, ki onemogočajo nepooblaščenim osebam dostop do podatkov.
Nosilci osebnih podatkov in morajo biti shranjeni in zavarovani tako, da nepooblaščenim osebam onemogočajo vpogled.

V prisotnosti nepooblaščenih oseb morajo biti nosilci osebnih podatkov in računalniški prikazovalniki nameščeni tako, da te nepooblaščene osebe nimajo vpogleda. Enako velja tudi za prostore, ki so namenjeni poslovanju s strankami.

10. člen
Dostop v zavarovane prostore

Dostop v varovane prostore je mogoč le v rednem delovnem času, izven tega časa pa samo na podlagi posebne dovolilnice s strani pooblaščenega delavca.
Varovani prostori morajo biti ves čas nadzorovani, oziroma se morajo v primeru odsotnosti delavcev, ki jih nadzorujejo zakleniti, ključe pa je potrebno hraniti na predvidenem mestu, ki nepooblaščenim delavcem preprečuje dostop do njih.

11. člen
Osebni podatki v skupnih prostorih

Nosilci osebnih podatkov, ki se nahajajo v skupnih prostorih morajo biti vedno zaklenjeni oziroma kako drugače ustrezno zavarovani pred nepooblaščenim vpogledom zaklenjeni.

12. člen
Varovanje občutljivih osebnih podatkov

Občutljive osebne podatke je dovoljeno hraniti samo v varovanih prostorih.

13. člen
Vzdrževanje

Vzdrževanje strojne opreme ter dobava in instalacija nove strojne in programske opreme lahko poteka samo z vednostjo pooblaščene osebe. Te storitve lahko opravljajo samo pooblaščeni servisi in vzdrževalci na podlagi sklenjene pogodbe.
Vzdrževalci strojne opreme, dobavitelji in instalaterji nove strojne in programske opreme, vzdrževalci prostorov, obiskovalci in poslovni partnerji so lahko prisotni v varovanih prostorih samo z vednostjo pooblaščene osebe.

14. člen
Varovanje izven delovnega časa

Izven delovnega časa morajo biti omare in pisalne mize z nosilci osebnih podatkov zaklenjene, računalniki in druga strojna oprema pa izklopljeni in fizično ali programsko zaklenjeni.
Izven delovnega časa se lahko zaposleni kot so na primer čistilke in varnostniki gibljejo v varovanih prostorih, samo pod pogojem, da so osebni podatki zavarovani tako, da jim onemogočajo vpogled. Nosilci podatkov morajo biti zaklenjeni, računalniki in druga strojna oprema pa izklopljeni in fizično ali programsko zaklenjeni.

V. VAROVANJE PROGRAMSKE OPREME TER OSEBNIH PODATKOV, KI SO NAMENJENI OBDELAVI

15. člen

Zavarovanje programske opreme

Zavarovanje programske opreme obsega sistemsko in aplikativno programsko opremo, s katero se osebni podatki obdelujejo.
Programska oprema mora biti ustrezno zavarovana na način, ki nepooblaščenim osebam onemogoča dostop. Dostop je dovoljen samo pooblaščenim osebam ter zunanjim pravnim oziroma fizičnim osebam, ki na podlagi pogodbe opravljajo posamezne storitve.

16. člen
Posodabljanje programske opreme

Posodabljanje, popravljanje in spreminjanje programske opreme je dovoljeno samo na podlagi dovoljenja pooblaščenega delavca. Te storitve lahko opravljajo samo pooblaščeni servisi na podlagi sklenjene pogodbe. Vse opravljene spremembe in dopolnitve programske opreme morajo biti s strani izvajalca ustrezno dokumentirane.

17. člen
Preverjanje računalniških virusov in programske opreme

Programska oprema, ki jo imajo nameščeno zaposleni na svojih računalnikih, kakor tudi vsebina mrežnega strežnika, kjer se nahajajo osebni podatki, se redno preverja glede na prisotnost računalniških virusov. V primeru pojava virusa se le-tega s pomočjo ustrezne strokovne službe čim prej odpravi. Preveri se tudi vzrok pojava virusa.
Osebni podatki in programska oprema, ki se uporablja za pregled ali obdelavo osebnih podatkov mora biti pred uporabo preverjeni zaradi morebitne prisotnosti računalniškega virusa.
Zaposleni ne smejo inštalirati programske opreme, ki bi jim omogočila vpogled ali obdelavo osebnih podatkov na računalniški informacijski sistem brez vednosti pooblaščene osebe.

18. člen
Gesla za dostop do osebnih podatkov

Dostop do osebnih podatkov je v okviru uporabe programske opreme mogoč samo z geslom. Sistem omogoča avtorizacijo in naknadno identifikacijo uporabnikov ter programov in podatkov, ki jih je uporabljal, kakor tudi naknadno ugotavljanje kdaj so bili posamezni podatki vneseni, spremenjeni ali uporabljeni. Seznam gesel je zaupne narave in mora biti varovan tako, da je preprečen dostop nepooblaščenim osebam. Seznam je dovoljeno imeti samo pooblaščenim delavcem.
Gesla za dostop do osebnih podatkov je potrebno spreminjati najmanj vsakih šest mesecev. Aktualna in pretekla gesla je potrebno hraniti v za to primernih prostorih, ki morajo biti zaklenjeni, varni pred ognjem in poplavami in zavarovani pred elektromagnetnimi motnjami Gesla, ki se uporabljajo za vstop in administriranje računalniške mreže podatkov se hranijo v zapečatenih ovojnicah. Vsaka uporaba zapečatenih ovojnic se evidentira. Po uporabi se gesla spremenijo tako da gesta, ki jih je uporabil administrator ne veljajo več.

19. člen
Restavriranje računalniškega sistema

Ob restavriranju računalniškega sistema oziroma ob okvarah in ob drugih izjemnih situacijah se izdela varnostna kopija celotne vsebine osebnih podatkov. Za izdelavo kopij je odgovoren pooblaščeni delavec.

20. člen
Katalog strojne in programske opreme za uporabo osebnih podatkov

Pooblaščeni delavec izda in sproti dopolnjuje katalog strojne in programske opreme, ki omogoča stik uporabnika z osebnimi podatki. Katalog je dostopen samo pooblaščenim delavcem.

VI. ZUNANJE PRAVNE ALI FIZIČNE OSEBE

21. člen
Zunanje pravne ali fizčne osebe in varovanje osebnih podatkov

Če zunanja pravna ali fizična oseba opravlja posamezna opravila v zvezi z zbiranjem, obdelovanjem, shranjevanjem ali posredovanjem osebnih podatkov in je registrirana za opravljanje takšne dejavnosti, se v skladu z 11. členom ZVOP-1 z njo sklene pisna pogodba. Pogodba mora vsebovati tudi predpisane pogoje in ukrepe za zagotovitev varstva osebnih podatkov in njihovega zavarovanja. Podobno je potrebno določiti tudi v pogodbah z vzdrževalci strojne in programske opreme ter z dobavitelji, ki izdelujejo in instalirajo novo strojno ali programsko opremo.
Zunanje pravne ali fizične osebe lahko opravljajo samo tiste storitve na področju obdelave osebnih podatkov, za katere jih je pooblastil naročnik. Podatkov, ki so jih pridobili na podlagi pogodbe z naročnikom pa ne smejo uporabljati in obdelovati za noben drug namen.
Če pooblaščena pravna ali fizična oseba opravlja z osebnimi podatki zunaj prostorov naročnika njenih storitev mora zagotoviti varovanje osebnih podatkov, ki je enako ali strožje od varovanja pri naročniku njenih storitev.

VII. SPREJEM OSEBNIH PODATKOV

22. člen
Sprejem osebnih podatkov po pošti

Delavec, ki je zadolžen za sprejem pošte mora poštno pošiljko z osebnimi podatki izročiti direktno posamezniku, ali službi, na katero je naslovljena.
Delavec, ki je zadolžen za sprejem pošte, ne sme odpirati pošiljk, ki so naslovljene na drug organ ali organizacijo in so dostavljene na napačen naslov. Prav tako ne sme odpirati pošiljk, ki so označene kot osebni podatki ali za katere iz označb na ovojnici izhaja, da se nanašajo na natečaj ali razpis ter pošiljk na katerih je označeno, da se naj vročijo osebno osebi, čigar ime je na pošiljki navedeno pred imenom inštituta.
Delavec, ki je zadolžen za sprejem pošte in je ob odpiranju ovojnice, ki ni bila naslovljena v skladu z določili prejšnjega odstavka, ugotovil, da se vsebina nanaša na osebne podatke, mora pošiljko direktno dostaviti osebi, na katero se osebni podatki nanašajo, oziroma delavcu, ki je pooblaščen za obdelavo osebnih podatkov.

VIII. POSREDOVANJE OSEBNIH PODATKOV

23. člen
Posredovanje pooblaščenim osebam

Osebni podatki se smejo posredovati samo tistim uporabnikom samo na podlagi ustrezne zakonske podlage oziroma na podlagi pisne zahtevo ali privolitvijo posameznika (oziroma njegovega zakonitega zastopnika, če gre za mladoletno osebo), na katerega se podatki nanašajo. Posredovanje se lahko opravi na podlagi pisne zahteve, v kateri mora biti jasno navedena zakonska podlaga, na podlagi katere se mu bodo posredovali osebni podatki. Če se posredovanje osebnih podatkov zahteva ustno, je pooblaščeni delavec v primeru dvoma o obstoju pisne izjave oziroma privolitve posameznika (oziroma njegovega zakonitega zastopnika, če gre za mladoletno osebo)na katerega se podatki nanašajo dolžan zahtevati pisno izjavo.
Osebne podatke je potrebno posredovati v obliki, ki nepooblaščeni osebi preprečuje vpogled. Kadar gre za podatke v fizični obliki jih je potrebno posredovati v ovojnici, ki ne omogoča, da bi bila ob normalni svetlobi ali pri osvetlitvi ovojnice z običajno lučjo vidna vsebina ovojnice. Ovojnica mora tudi zagotoviti, da odprtja ovojnice in seznanitve z njeno vsebino ni mogoče opraviti brez vidne sledi odpiranja ovojnice. Osebne podatke je z informacijskimi, komunikacijskimi in drugimi sredstvi dovoljeno poslati le ob izvajanju postopkov in ukrepov, ki nepooblaščenim osebam preprečujejo prilaščanje ali uničenje podatkov ter neupravičeno seznanjanje z njihovo vsebino.
Občutljivi osebni podatki se lahko posredujejo samo na podlagi pisne zahteve. Občutljive osebne podatke je preko komunikacijskih omrežij dovoljeno posredovati samo v primeru, če so posebej zavarovani s kriptografskimi metodami in elektronskim podpisom tako, da je zagotovljena nečitljivost podatkov med njihovim prenosom.
Pri posredovanju osebnih podatkov se nikoli ne posredujejo originalni dokumenti, razen v primeru pisne odredbe sodišča. V tem primeru se originalni dokument začasno nadomesti s kopijo.

24. člen
Posredovanje osebam, na katere se podatki nanašajo

Posamezniku (oziroma njegovemu zakonitemu zastopniku, če gre za mladoletno osebo), o katerem se v zbirki osebnih podatkov hranijo osebni podatki, je potrebno na njegovo zahtevo posredovati osebne podatke, ki se nanašajo nanj.

25. člen
Evidenca posredovanj

Vsako posredovanje osebnih podatkov je potrebno zabeležiti v evidenco posredovanj osebnih podatkov.
Iz evidence mora biti razvidno:
- kateri osebni podatki so bili posredovani,
- komu so bili osebni podatki posredovani: oseba, naslov oziroma oseba, podjetje, naslov ki so ji bili podatki posredovani,
- kdaj so bili osebni podatki posredovani: datum in ura,
- pravna podlaga na podlagi katere so bili posredovani osebni podatki

26. člen

Posredovanje osebnih podatkov informacijskemu pooblaščencu

Upravljavec osebnih podatkov mora v skladu z Zakonom o informacijskem pooblaščencu (Uradni list 113/05) redno obveščati informacijskega pooblaščenca o svojih zbirkah osebnih podatkov.

IX. BRISANJE OSEBNIH PODATKOV

27. člen
Čas hranjenja osebnih podatkov

Osebni podatki se hranijo le toliko časa, dokler je to potrebno za dosego namena, zaradi katerega so se zbirali ali nadalje obdelovali. Po izpolnitvi namena obdelave se osebni podatki zbrišejo, uničijo, blokirajo ali anonimizirajo, če niso na podlagi zakona, ki ureja arhivsko gradivo in arhive, opredeljeni kot arhivsko gradivo, oziroma če zakon za posamezne vrste osebnih podatkov ne določa drugače (21. člen ZVOP-1).

28. člen
Načini brisanja osebnih podatkov

Za brisanje podatkov iz računalniških medijev se uporabi takšna metoda brisanja, da je nemogoča restavracija vseh ali dela izbrisanih osebnih podatkov.
Podatki na klasičnih medijih (listine, register, seznam, kartoteke, izračuni, grafikone, skice, slike, poskusne oziroma neuspešne izpisi, ...) se uničijo na način, ki onemogoča branje vseh ali dela uničenih osebnih podatkov.
Pri prenosu osebnih podatkov na mesto uničenja in pri postopku uničenja je potrebno zagotoviti ustrezno varovanje osebnih podatkov pred dostopom nepooblaščenih oseb. Prenos in uničenje osebnih podatkov nadzoruje s strani upravljavca osebnih podatkov pooblaščena komisija, ki o tem sestavi ustrezni zapisnik.

X. ODGOVORNOST ZA IZVAJANJE VARNOSTNIH UKREPOV IN POSTOPKOV

29. člen
Odgovornost za izvajanje in nadzor nad varnostnimi ukrepi in postopki

Za izvajanje varnostnih ukrepov in postopkov je odgovorno vodstvo. Nadzor nad izvajanjem ukrepov in postopkov opravlja vodstvo.

30. člen
Dolžnosti zaposlenih

Predpisane postopke in ukrepe za zavarovanje osebnih podatkov so dolžni izvajati vsi zaposleni, ki obdelujejo osebne podatke oziroma so bili z njimi seznanjeni pri opravljanju svojega dela. Ta obveza varovanja podatkov ne preneha s prenehanjem delovnega razmerja.
Pred pridobitvijo pooblastila za obdelavo osebnih podatkov oziroma pred nastopom dela na delovnem mestu, ki vključuje tudi obdelavo osebnih podatkov mora posameznik podpisati izjavo o varovanju osebnih podatkov, ki ga zavezuje k varovanju osebnih podatkov. Iz izjave mora biti tudi razvidno, da je seznanjen z določbami ZVOP in tega pravilnika.

Za kršitev je pooblaščeni delavec disciplinsko odgovoren. Disciplinska odgovornost vključuje tudi prekrškovne, kazenske ali odškodninske odgovornosti.

31. člen
Ukrepanje ob sumu nepooblaščenega dostopa

O nepooblaščenem odkrivanju, uporabi, prilaščanju, spreminjanju, poškodovanju ali brisanju osebnih podatkov so zaposleni dolžni nemudoma obvestiti pooblaščeno osebo. Sami pa so dolžni po svojih močeh takšno aktivnost preprečiti.

XI. KONČNA DOLOČBA

32. člen

Ta pravilnik začne veljati dne 18.11.2011.

V Ljubljani, dne 10.11.2011.

Ime in priimek odgovorne osebe

__ Jurij Mlačnik_____