Na podlagi Uredbe EU (2916/679) Evropskega parlamenta in sveta z dne 27.4.2016 (v nadaljevanju Uredba) in 22. člena Statuta Zdravstvenega doma Radlje ob Dravi direktor Zdravstvenega doma Radlje ob Dravi izdaja

P R A V I L N I K

o varstvu osebnih podatkov v Zdravstvenem domu Radlje ob Dravi

I. SPLOŠNE DOLOČBE

1. člen
(vsebina in namen pravilnika)

S Pravilnikom o varstvu osebnih podatkov v Zdravstvenem domu Radlje ob Dravi (v nadaljevanju: Pravilnik) se določa način zagotavljanja zakonitih podlag za obdelavo osebnih podatkov (v nadaljnjem besedilu: obdelava), s katerimi upravlja Zdravstveni dom Radlje ob Dravi (v nadaljevanju: ZD Radlje ob Dravi), način obravnavanja zahtevkov in ugovorov posameznika glede obdelave podatkov, ki se nanašajo nanj, ter izvajanje tehničnih in organizacijskih ukrepov, s katerimi ZD Radlje ob Dravi varuje obdelavo v skladu s Splošno uredbo o varstvu podatkov (v nadaljnjem besedilu: Uredba), Zakonom, ki ureja varstvo osebnih podatkov (v nadaljnjem besedilu: ZVOP-1), ter drugimi predpisi, zavezujočimi akti in pogodbami, ki določajo ukrepe in postopke varstva osebnih podatkov in zagotavljanja varne obdelave teh podatkov.

ZD Radlje ob Dravi obdelavo varuje s tehničnimi in organizacijskimi varnostnimi ukrepi, ki temeljijo na oceni tveganj za pravice in svoboščine posameznika, ki jih pomeni obdelava podatkov, ki se nanašajo nanj, zlasti zaradi nenamernega ali nezakonitega uničenja, izgube, spremembe, nepooblaščenega razkritja ali dostopa do osebnih podatkov, ki so poslani, shranjeni ali kako drugače obdelani.

ZD Radlje ob Dravi s tem Pravilnikom ter s politikami, načrti in navodili, ki sestavljajo sistem upravljanja varstva osebnih podatkov (v nadaljnjem besedilu SUVOP), določa nosilce, organizacijo in postopke za izvajanje ukrepov iz prejšnjih dveh odstavkov tega člena.

Zaposleni v ZD Radlje ob Dravi in zunanji sodelavci, ki pri svojem delu obdelujejo in uporabljajo osebne podatke, s katerimi upravlja ZD Radlje ob Dravi, morajo biti seznanjeni z Uredbo, ZVOP-1, z drugimi zakoni, ki urejajo obdelavo osebnih podatkov na področju poslovanja ZD Radlje ob Dravi, ter z vsebino tega Pravilnika in Sistemom za upravljanje in varovanje informacij (v nadaljevanju: SUVI politike).

Po tem Pravilniku se varujejo tudi osebni podatki, ki jih na podlagi pogodbe za ZD Radlje ob Dravi obdeluje zunanji izvajalec (v nadaljnjem besedilu: obdelovalec).

Ta pravilnik določa tudi postopke in ukrepe za varovanje zaupnih podatkov, ki predstavljajo poslovno oz.poklicno skrivnost.

2. člen
(pomen izrazov)

V tem pravilniku uporabljeni izrazi imajo naslednji pomen:

1. **Osebni podatek** pomeni katero koli informacijo v zvezi z določenim ali določljivim posameznikom, na katerega se nanašajo osebni podatki. Določljiv posameznik je tisti, ki ga je mogoče neposredno ali posredno določiti, zlasti z navedbo identifikatorja, kot je ime,

identifikacijska številka, podatki o lokaciji, spletni identifikator, ali z navedbo enega ali več dejavnikov, ki so značilni za fizično, fiziološko, gensko, duševno, gospodarsko, kulturno ali družbeno identiteto tega posameznika;

2. **Posameznik** je določena ali določljiva oseba, na katero se nanaša osebni podatek; posameznik je določljiv, če ga je mogoče neposredno ali posredno določiti, zlasti z navedbo identifikatorja, kot je ime, identifikacijska številka, podatki o lokaciji, spletni identifikator, ali z navedbo enega/več dejavnikov, ki so značilni za fizično, fiziološko, gensko, duševno, gospodarsko, kulturno ali družbeno identiteto tega posameznika;
3. **Obdelava** pomeni vsako dejanje ali niz dejanj, ki se izvaja v zvezi z osebnimi podatki ali nizi osebnih podatkov z avtomatiziranimi sredstvi ali brez njih, kot je zbiranje, beleženje urejanje, strukturiranje, shranjevanje, prilagajanje ali spreminjanje, priklic, vpogled, uporaba, razkritje s posredovanjem, razširjanje ali drugačno omogočanje dostopa, prilagajanje ali kombiniranje, omejevanje, izbris ali uničenje;
4. **Zbirka** pomeni vsak strukturiran niz osebnih podatkov, ki so dostopni v skladu s posebnimi merili, niz pa je lahko centraliziran, decentraliziran ali razpršen na funkcionalni ali geografski podlagi;
5. **Posebne vrste osebnih podatkov** so osebni podatki, ki razkrivajo rasno ali etično poreklo, politično mnenje, versko ali filozofsko prepričanje ali članstvo v sindikatu, genski podatki, biometrični podatki za namene edinstvene identifikacije posameznika, podatki v zvezi z zdravjem ali podatki v zvezi s posameznikovim spolnim življenjem ali spolno usmerjenostjo;
6. **Upravljavec** pomeni fizično ali pravno osebo, javni organ, agencijo ali drugo telo, ki samo ali skupaj z drugimi določa namene in sredstva obdelave; kadar namene in sredstva obdelave določa pravo Unije ali pravo države članice, se lahko upravljavec ali posebna merila za njegovo imenovanje določijo s pravom Unije ali pravom države članice;
7. **Obdelovalec** pomeni fizično ali pravno osebo, javni organ, agencijo ali drugo telo, ki obdeluje osebne podatke v imenu upravljavca;
8. **Uporabnik** pomeni fizično ali pravno osebo, javni organ, agencijo ali drugo telo, ki so mu bili osebni podatki razkriti, ne glede na to, ali je tretja oseba ali ne. Vendar pa se javni organi, ki lahko prejmejo osebne podatke v okviru posamezne poizvedbe v skladu s pravom Unije ali pravom države članice, ne štejejo za uporabnike; obdelava teh podatkov s strani teh javnih organov poteka v skladu z veljavnimi pravili o varstvu podatkov glede na namene obdelave;
9. **Tretja oseba** pomeni fizično ali pravno osebo, javni organ, agencijo ali telo, ki ni posameznik, na katerega se nanašajo osebni podatki, upravljavec, obdelovalec in osebe, ki so pooblaščene za obdelavo osebnih podatkov pod neposrednim vodstvom upravljavca ali obdelovalca;
10. **Privolitev posameznika** na katerega se nanašajo osebni podatki, pomeni: vsako prostovoljno, konkretno, informirano in nedvoumno ravnanje v obliki izjave ali drugačnega jasnega aktivnega delovanja, iz katerega je mogoče sklepati na želje posameznika, na katerega se nanašajo osebni podatki, s katerimi izrazi strinjanje z obdelavo osebnih podatkov, ki se nanašajo nanj;
11. **Nosilec podatkov** so vse vrste sredstev, na katerih so zapisani ali posneti podatki evidenc;
12. **Končni uporabnik osebnih podatkov** je zaposleni ali zunanji sodelavec ZD Radlje ob Dravi, ki zaradi narave svojega dela lahko obdeluje določene osebne podatke, s katerimi upravlja ali jih v okviru izvajanja poslovnih dejavnosti obravnava ZD Radlje ob Dravi;
13. **Upravljavec zbirke** je zaposleni ali zunanji sodelavec ZD Radlje ob Dravi, zadolžen za obdelavo podatkov iz posamezne zbirke osebnih podatkov;
14. **Odgovorna oseba zbirke** je zaposleni ali zunanji sodelavec ZD Radlje ob Dravi, odgovoren za obdelavo podatkov iz posamezne zbirke osebnih podatkov;

15. **Informacijski sistem** je programska, strojna, komunikacijska in druga oprema ZD Radlje ob Dravi, ki deluje samostojno ali v omrežju in je namenjena zbiranju, procesiranju, distribuciji, uporabi in drugi obdelavi osebnih podatkov;
16. **Škodljiva programska oprema** so računalniški virusi, črvi, trojanski konji in podobna programska oprema, ki se namesti v informacijski sistem ali njegov del brez vednosti direktorja oz. drugih odgovornih oseb ZD Radlje ob Dravi in posega v integriteto informacijskega sistema;
17. **Kršitev varstva osebnih podatkov** pomeni kršitev varnosti, ki povzroči nenamerno ali nezakonito uničenje, izgubo, spremembo, nepooblaščeno razkritje ali dostop do osebnih podatkov, ki so poslani, shranjeni ali kako drugače obdelani;
18. **Varnostni dogodek** je zaznano dogajanje v obdelavi osebnih podatkov, ki kaže na morebitno kršitev varstva osebnih podatkov oziroma odpoved postopkov in ukrepov za zavarovanje osebnih podatkov ali na do tedaj še neznano okoliščino, ki bi lahko bila pomembna za varnost;
19. **Incident** je eden ali več neželenih ali nepričakovanih dogodkov, za katere je zelo verjetno, da bodo ogrozili varnost obdelave osebnih podatkov ali sredstev, s katerimi se obdelava izvaja;
20. **Grožnja** je možen vzrok za incident, ki lahko povzroči škodo osebnemu podatku, sredstvu za obdelavo ali upravljavcu;
21. **Ranljivost** je šibka točka sredstva ali skupine sredstev, ki jo je mogoče izrabiti z eno ali več grožnjami.
22. **Analiza varnostnih tveganj** je sistematična uporaba informacij za prepoznavanje virov groženj in ranljivosti sredstev ter ocenjevanje tveganj za varnost osebnih podatkov oz. obdelavo;
23. **Analiza vpliva na poslovanje** je sistematična uporaba informacij za prepoznavanje virov groženj in ranljivosti sredstev ter ocenjevanje tveganj za neprekinjeno izvajanje obdelave;
24. **Obravnava tveganj** je proces izbora in vpeljave ukrepov za zmanjšanje tveganj;
25. **Dokumentiran postopek** pomeni, da je postopek zapisan;
26. **Vodstveni pregled** je dokumentiran pregled sistema upravljanja varstva osebnih podatkov, ki ga vodstvo opravi najmanj enkrat letno, da zagotovi skladnost obdelave;
27. **SUVI** je kratica za sistem upravljanja varovanja informacij;
28. **Psevdonimizacija** pomeni obdelavo osebnih podatkov na tak način, da osebnih podatkov brez dodatnih informacij ni več mogoče pripisati specifičnemu posamezniku, na katerega se nanašajo osebni podatki, če se take dodatne informacije hranijo ločeno ter zanje veljajo tehnični in organizacijski ukrepi za zagotavljanje, da se osebni podatki ne pripišejo določenemu ali določljivemu posamezniku.
29. **Sistemski administrator** je oseba, ki skrbi za delovanje sistemske opreme.
30. **Skrbnik informacijskega sistema** je oseba, ki skrbi za vsebinsko delovanje informacijskega sistema

3. člen

ZD Radlje ob Dravi vodi Evidenco dejavnosti obdelave, v kateri morajo biti opisane vse zbirke osebnih podatkov, ki jih ZD Radlje ob Dravi vodi. Evidenca dejavnosti obdelave se ob vsaki spremembi podatkov redno dopolnjuje.

4. člen

Določbe tega pravilnika veljajo za vse klasične in računalniško vodene zbirke podatkov.

5. člen

Kot **uradna tajnost** so opredeljeni podatki, ki so tako pomembni, da bi z njihovo izdajo nastale ali lahko nastale hude škodljive posledice za ZD Radlje ob Dravi ali za posameznika. Podatki, ki so določeni za uradno tajnost imajo oznako **zaupno.** Ti podatki so v 8. členu označeni kot

- poslovna skrivnost in
- poklicna skrivnost.

6. člen

Za poslovno in poklicno skrivnost se smatrajo listine in podatki, ki predstavljajo poslovno, medicinsko in znanstveno raziskovalno delo, ter listine in podatki katerih sporočanje bi bilo zaradi njihove narave in pomena v nasprotju z interesi zavoda

Za poslovno skrivnost se štejejo:

- Podatki, listine in informacije, ki jih kot takšne določi Svet zavoda;
- Rezultati raziskovanj, ki še niso verificirani;
- Podatki in listine, ki vsebujejo ponudbo in povpraševanje poslovnih partnerjev, razpis ali javni natečaj do objave rezultatov natečaja ali javnega razpisa;
- Vsebinski del dogovorov o poslovno - tehničnem sodelovanju z drugimi zavodi, podjetji in drugimi pravnimi osebami;
- Plan finančno – tehničnega zavarovanja objektov in premoženja;
- Informacije o pogojih, prejetih in danih kratkoročnih kreditih, razen tistih, ki jih vodstvo zavoda nameni kot informacijo internim in eksternim javnostim;
- Informacije o načinu dostopa v katerikoli del informacijskega sistema zavoda;
- Informacije o načinu dostopa v varovane objekte zavoda;

Direktor ZD Radlje ob Dravi ali od njega pooblaščena oseba je pooblaščen za sporočanje podatkov, ki imajo značaj poslovne skrivnosti in so označeni kot zaupni.

Za poklicno skrivnost se štejejo:

- vsi medicinski oz. zdravstveni in administrativni osebni podatki ter podatki njihovih osebnih in družinskih zadev do katerih pridejo zdravstveni delavci in zdravstveni sodelavci ter drugi delavci pri opravljanju svojega dela, na podlagi katerih je mogoče identificirati osebo oz. diagnozo ali prognozo njene bolezni.

II. VARSTVO OSEBNIH PODATKOV

Odgovornost in organiziranost

7. člen

(odgovornost vodstva)

Za zagotovitev ustreznih in učinkovitih ukrepov za izvajanje obdelave v skladu s predpisanimi in pogodbeno dogovorjenimi zahtevami ter za dokazovanje skladnosti dejavnosti obdelave z omenjenimi zahtevami je odgovorno vodstvo ZD Radlje ob Dravi.

Vodstvo ZD Radlje ob Dravi odgovornosti iz prejšnjega odstavka uresničuje zlasti:

a) s sprejetjem tega pravilnika ter navodil, politik, načrtov in drugih notranjih aktov, s katerimi določi:

- postopke za vzpostavitev zakonitih podlag za obdelavo osebnih podatkov, s katerimi ZD Radlje ob Dravi upravlja;
- postopke za obravnavanje zahtevkov oziroma ugovorov posameznikov, katerih podatke ZD Radlje ob Dravi obdeluje, vezanih na varstvo njihovih pravic in svoboščin v zvezi z obdelavo osebnih podatkov;
- izdelavo ocene varnostnih tveganj obdelave;
- izdelavo ocene učinka v zvezi z varstvom podatkov;
- izvajanje ustreznih tehničnih in organizacijskih ukrepov, s katerimi se varujejo osebni podatki ter preprečuje njihovo slučajno, namerno ali drugače nezakonito uničenje, spremembo, izgubo, nepooblaščeno razkritje, dostop ali drugo nepooblaščeno obdelavo;

b) z ustrezno pogodbeno ureditvijo obdelave s strani obdelovalca;
c) z imenovanjem zaposlenih, ki so odgovorni za določene zbirke in zaposlenih, ki upravljajo z osebnimi podatki iz posamezne zbirke;
d) z imenovanjem pooblaščene osebe za varstvo osebnih podatkov;
e) z imenovanjem delovne skupine za informacijsko varnost;
f) z notranjo presojo ter vodstvenim pregledom ustreznosti in učinkovitosti ukrepov za zagotavljanje varnosti obdelave ter
g) z rednimi usposabljanji osebja, ki izvaja obdelavo na področju zagotavljanja zakonsko skladne in varne obdelave osebnih podatkov.

Vodstvo ZD Radlje ob Dravi mora zagotoviti, da so vsi ukrepi in postopki za izvajanje obdelave v skladu s predpisanimi in pogodbeno dogovorjenimi zahtevami dokumentirani tako, da je omogočeno njihovo učinkovito izvajanje, spremljanje in nadziranje, ter dokazovanje skladnosti obdelave v sodnih in drugih uradnih postopkih oziroma na zahtevo nadzornega ali drugih pristojnih organov.

8. člen
(imenovanje in položaj pooblaščene osebe za varstvo osebnih podatkov)

Vodstvo ZD Radlje ob Dravi imenuje pooblaščeno osebo za varstvo osebnih skladno z Uredbo, in tem pravilnikom.

Vodstvo ZD Radlje ob Dravi lahko za pomoč pooblaščeni osebi pri opravljanju njenih nalog izmed svojih zaposlenih določi tudi druge osebe, ki so pri izvajanju pomoči vezane na navodila pooblaščene osebe.

Vodstvo ZD Radlje ob Dravi zagotovi, da je pooblaščena oseba ustrezno in pravočasno obveščena o vseh zadevah v zvezi z varstvom osebnih podatkov, ki so del izvajanja registriranih dejavnosti ZD Radlje ob Dravi. Obveščanje pooblaščene osebe se izvaja:

- z neposrednim dostopom do vodstva ZD Radlje ob Dravi, kadar vodstvo ali pooblaščena oseba ocenita, da določena zadeva varstva osebnih podatkov zahteva tak način obravnave;
- z njenim udeleževanjem sestankov vodstev ZD Radlje ob Dravi oz. delovnih skupin, ki obravnavajo varstvo osebnih podatkov;
- z neposrednim dostopom do zaposlenih, ki obdelujejo osebne podatke;
- z dostopom do dokumentarnega gradiva, ki obravnava zadeve varstva osebnih podatkov;
- z neposrednim dostopom do zbirk osebnih podatkov in zapisov revizijskih sledi, ki jih potrebuje za izvajanje svojih nalog;

Vodstvo ZD Radlje ob Dravi pooblaščeni osebi zagotovi dostop do:

- osebnih podatkov in revizijskih sledi v zbirkah in drugih oblikah obdelave osebnih podatkov;
- podatkov o kršitvah varstva osebnih podatkov;
- zaposlenih v ZD Radlje ob Dravi in pri obdelovalcu, ki delajo na nalogah, povezanih z varstvom osebnih podatkov.

9. člen
(naloge pooblaščene osebe)

Pooblaščena oseba vodstvu ZD Radlje ob Dravi na strokovno neodvisen način pomaga pri zagotavljanju skladnosti obdelave osebnih podatkov s pravili Uredbe, določbami ZVOP-1 in drugih zakonov, ki urejajo obdelavo in varstvo osebnih podatkov.

Pooblaščena oseba izvaja naslednje naloge:

- obvešča zavod in zaposlene ter pogodbene delavce o pravicah in dolžnostih na področju varstva osebnih podatkov;
- spremlja skladnosti poslovanja oziroma obdelav podatkov s predpisi o varstvu osebnih podatkov in internimi politikami o varnosti;
- pripravlja predloge za izvedbo ukrepov;
- organizira in/ali izvaja notranja usposabljanja po programu, če to narekujejo potrebe;
- občasne revizije obdelav in procesov v organizacijskih enotah po programu;
- občasno spremlja izvajanja ocen učinkov po programu;
- daje mnenja glede ocen učinkov v zvezi z varstvom podatkov;
- sodeluje z nadzornim organom pri nadzorih ali pri posvetovanjih;
- sodeluje s posamezniki, na katere se nanašajo osebni podatki, ki se na zavod obračajo glede vprašanj, povezanih z obdelavo njihovih osebnih podatkov, in uresničevanjem njihovih pravic;
- vodi evidenco dejavnosti obdelave;
- aktivno sodeluje pri pripravi ocen učinkov;
- poroča o kršitvah varstva osebnih podatkov nadzornemu organu;
- dokumentira zaznane in sporočene kršitve;
- pripravlja interna navodila za ravnanje in obvešča zaposlene;
- daje pobude za odpravo pomanjkljivosti ali zmanjšanje tveganj na področju varstva osebnih podatkov;
- pripravlja zaprosila za mnenja s področja varstva osebnih podatkov;
- sprejema prijave domnevnih kršitev in njihova obravnava;
- koordinira delo, spodbuja, usmerja in daje navodila v zvezi z zgornjimi nalogami;
- dokumentira naloge.

V primeru, da ima ZD Radlje ob Dravi pogodbeno določeno pooblaščeno osebo za varstvo osebnih podatkov, se dela in naloge pooblaščene osebe za varstvo osebnih podatkov posebej določijo v pogodbi.

10. člen
(delovna skupina za informacijsko varnost)

Vodstvo ZD Radlje ob Dravi imenuje skupino za delo na področju varovanja osebnih podatkov, ki bo odgovorna za informacijsko varnost (v nadaljnjem besedilu: delovna skupina za informacijsko varnost), ki vodstvu svetuje na področju načrtovanja, organiziranja in izvajanja ukrepov s katerimi ZD Radlje ob Dravi varuje osebne podatke ter preprečuje njihovo slučajno, namerno ali drugače

nezakonito uničenje, spremembo, izgubo, nepooblaščeno razkritje, dostop ali drugo nepooblaščeno obdelavo.

Delovna skupina za informacijsko varnost izvaja zlasti naslednje naloge:

- skrbi za učinkovito obravnavanje ter dokumentiranje varnostnih dogodkov in incidentov in zagotavlja zakonsko skladne obdelave podatkov, ter sprejete popravne ukrepe;
- skrbi, da so pri razvoju novih rešitev za obdelavo osebnih podatkov izvedeni oz. vgrajeni ustrezni tehnični in organizacijski ukrepi za odpravo ali zmanjšanje tveganj;
- v sodelovanju s pooblaščeno osebo in zaposlenimi, odgovornimi za izvajanje dejanj obdelave, ocenjuje varnostne dogodke in incidente, v okviru katerih je bilo kršeno varstvo osebnih podatkov, ter, če iz ocene izhaja, da bi bile s kršitvijo ogrožene pravice in svoboščine posameznikov, na katere so se nanašali podatki, ki so bili predmet kršitve, pripravi obvestilo o kršitvi, ki ga pooblaščena oseba za varstvo osebnih podatkov najkasneje v 72 urah od seznanitve z incidentom pošlje Informacijskemu pooblaščencu;
- sodeluje pri izdelavi ocene učinka v zvezi z varstvom osebnih podatkov.

Pooblaščena oseba za varstvo osebnih podatkov koordinira delovno skupino za informacijsko varnost.

Delovna skupina za informacijsko varnost je odgovorna za vodenje in ustrezno posodabljanje dokumentacije SUVI.

Dokaziła o skladnosti

11. člen

(dokazovanje skladnosti)

ZD Radlje ob Dravi za potrebo dokazovanja skladnosti obdelave s predpisanimi zahtevami in tem pravilnikom vodi ustrezno dokumentacijo, s katero je sposobna dokazati, da obdelava poteka v skladu z določbami Uredbe, Zakona o varstvu osebnih podatkov, oziroma drugih predpisov, ki urejajo varstvo osebnih podatkov. V ZD Radlje ob Dravi je ta dokumentacija vodena v okviru SUVI.

III. ZAKONITE PODLAGE IN EVIDENTIRANJE OBDELAVE OSEBNIH PODATKOV

Pridobitev zakonite podlage in določitev namena obdelave

12. člen

(pravne podlage obdelave osebnih podatkov)

Osebni podatki se v ZD Radlje ob Dravi lahko obdelujejo, če obdelavo osebnih podatkov in osebne podatke, ki se obdelujejo določa zakon, ali, če je za obdelavo določenih osebnih podatkov podana osebna privolitev posameznika.

Ne glede na prejšnji odstavek se lahko v ZD Radlje ob Dravi obdelujejo osebni podatki posameznikov, ki so z ZD Radlje ob Dravi sklenili pogodbo ali pa so na podlagi zahteve posameznika z njim v fazi pogajanj za sklenitev pogodbe, če je obdelava osebnih podatkov potrebna in primerna za izvajanje ukrepov pred sklenitvijo pogodbe ali za izvajanje pogodbe.

Ne glede na prvi odstavek tega člena se lahko v ZD Radlje ob Dravi obdelujejo tisti osebni podatki, ki so potrebni za zaščito življenjskih interesov posameznika, na katerega se nanašajo osebni podatki.

Ne glede na prvi odstavek tega člena se lahko v javnem sektorju obdelujejo osebni podatki, če je obdelava potrebna zaradi uresničevanja zakonito upravičenih interesov, za katere si prizadeva upravljavec ali tretja oseba, razen kadar nad takimi interesi prevladajo interesi ali človekove pravice in temeljne svoboščine posameznika, na katerega se nanašajo osebni podatki, ki zahtevajo varstvo osebnih podatkov, zlasti kadar je posameznik, na katerega se nanašajo osebni podatki, otrok.

13. člen
(namen in obseg obdelave osebnih podatkov)

Osebni podatki se smejo v ZD Radlje ob Dravi zbirati samo za namene, določene v zakonski podlagi, ali opredeljene v informaciji, posredovani posamezniku, na katerega se nanašajo obdelovani podatki, v okviru pridobivanja privolitve za obdelavo ali sklenitev pogodbe, na podlagi katere se izvaja obdelava.

Obdelava osebnih podatkov za druge namene kot tiste, za katere so bili osebni podatki prvotno zbrani, je dovoljena le, kadar je združljiva z nameni, za katere so bili osebni podatki prvotno zbrani, ali kadar to določa Zakon o varstvu osebnih podatkov. Za ugotovitev, ali je namen nadaljnje obdelave združljiv z namenom, za katerega so bili osebni podatki prvotno zbrani, mora upravljavec predmetne zbirke pred začetkom obdelave za druge namene opraviti presojo v skladu s četrtim odstavkom 6. člena Uredbe ter pridobiti mnenje pooblaščene osebe. Presoja mora biti opravljena v pisni obliki in shranjena v okviru dokumentacije SUVI.

Obdelava osebnih podatkov za drug namen kot za tistega, za katerega so bili zbrani, ni dopustna na podlagi prvotne privolitve, če je bila ta privolitev podana za določen namen, ki lahko vsebuje eno ali več delovanj obdelave v skladu z določenim namenom. Če je načrtovana obdelava za drug namen na podlagi privolitve, se lahko izvede le na podlagi nove privolitve posameznika, na katerega se nanašajo osebni podatki, če druga zakonska podlaga ne določa drugače.

14. člen
(obdelava posebnih vrst osebnih podatkov)

Posebne vrste osebnih podatkov se lahko v ZD Radlje ob Dravi obdelujejo le, če tako obdelavo določa zakon, ali če je posameznik za to podal izrecno pisno privolitev in je bila privolitev podana za enega ali več določenih namenov.

Posebne vrste osebnih podatkov se iz evidenc ZD Radlje ob Dravi drugim posameznikom ali osebam javnega ali zasebnega sektorja smejo posredovati le, če to določa zakon, ali na podlagi pisne zahteve ali pisne privolitve posameznika, na katerega se nanašajo.

Vzpostavitev zbirke in evidentiranje dejavnosti obdelave

15. člen
(vzpostavitev zbirke)

Zbirko s sklepom vzpostavi vodstvo ZD Radlje ob Dravi.

V sklepu iz prejšnjega odstavka se določi:

- naziv zbirke;
- odgovorno osebo zbirke;
- upravljavca zbirke;
- pravno podlago za obdelavo;

- namen/e obdelave;
- kategorije posameznikov, na katere se nanašajo osebni podatki;
- kategorije uporabnikov, ki jim bodo razkriti osebni podatki
- vrste osebnih podatkov v zbirki;
- informacija o prenosih v tretje države;
- kadar je mogoče, predvidene roke za izbris različnih vrst podatkov;
- tehnične in organizacijske varnostne ukrepe za zagotavljanje varnosti;

Sklep o vzpostavitvi zbirke služi kot podlaga za prvi vpis zbirke v evidenco dejavnosti obdelave.

16. člen
(vodenje evidence dejavnosti obdelave)

ZD Radlje ob Dravi za namen dokazovanja skladnosti z Uredbo, Zakonom o varstvu osebnih podatkov in drugimi predpisi, ki urejajo obdelavo, hrani evidenco zapisov o dejavnosti obdelav, s katerimi upravlja. Podatki evidence so dostopni odgovornim osebam posamezne zbirke, osebi pooblaščeni za varstvo osebnih podatkov, vodstvu zdravstvenega doma in na njegovo zahtevo tudi nadzornemu organu.

Evidenca dejavnosti obdelave poleg vrst podatkov, ki jih določa Uredba, obsega dodatne podatke, namenjene učinkovitejšemu izvajanju ukrepov varstva osebnih podatkov in zagotavljanja varnosti obdelave.

Zbirko evidence dejavnosti obdelave ureja in posodablja strokovna oseba v sodelovanju s pooblaščeno osebo za varstvo osebnih podatkov na podlagi informacij, pridobljenih s strani upravljavca posameznih evidenc. Vsaka posodobitev evidence je vnaprej obravnavana v skupini za informacijsko varnost.

Pogodbena obdelava osebnih podatkov
17. člen
(vloga obdelovalca)

Če ZD Radlje ob Dravi izvaja obdelavo, varuje osebne podatke, ki so predmet obdelave ali se nanjo nanašajo za drugo organizacijo (naročnika), to počne skladno z določili tega pravilnika in pogodbe, s katero uredita medsebojna razmerja.

Vsebina pogodbe in medsebojne pravice in obveznosti glede izvajanja obdelave smiselno sledi določbam prejšnjega člena tega pravilnika.

IV.OBVEŠČANJE IN VARSTVO PRAVIC POSAMEZNIKA GLEDE OBDELAVE PODATKOV, KI SE NANAŠAJO NANJ

Obveščanje posameznika o obdelavi podatkov, ki se nanašajo nanj
18. člen
(obveščanje o obdelavi osebnih podatkov)

ZD Radlje ob Dravi posameznika, čigar osebne podatke bo zbirala, obvesti o obstoju izvajanja obdelave in namenih obdelave. Obveščanje posameznika o obdelavi se izvaja z:

- ustrezno informacijo o izvajanju storitve ali uporabe rešitve, katerih del je obdelava osebnih podatkov;

- vključitvijo informacij o obdelavi v pogajanja za sklenitev pogodbe, katere del bo obdelava osebnih podatkov posameznika;
- vključitvijo informacij o obdelavi k privolitvi posameznika v obdelavo podatkov, ki se nanašajo nanj, s strani ZD Radlje ob Dravi in/ali tretje osebe.

Besedila informacij iz prejšnjega odstavka morajo obsegati najmanj naslednje informacije:
- imena in kontaktne podatke upravljavca;
- kontaktne podatke pooblaščene osebe;
- namene, za katere se osebni podatki obdelujejo;
- obstoju pravice do vložitve prijave pri Informacijskem pooblaščencu in njegove kontaktne podatke;
- obstoju pravice do dostopa do podatkov in do tega, da upravljavec popravi ali izbriše podatke ali omeji obdelavo podatkov posameznika, na katerega se osebni podatki nanašajo;

Poleg teh informacij, mora upravljavec posamezniku, na katerega se nanašajo podatki, v posebnih primerih zagotoviti dodatne informacije, da s tem omogoči izvajanje pravic posameznika, na katerega se nanašajo podatki:
- pravno podlago obdelave;
- rok hrambe osebnih podatkov;
- kategorije prejemnikov osebnih podatkov;
- druge informacije, zlasti, če so bili osebni podatki pridobljeni brez vednosti posameznika na katerega se nanašajo;

Besedila informacij iz prejšnjega odstavka pripravi in vzdržuje strokovna oseba v sodelovanju s skupino za informacijsko varnost.

Postopki varstva pravic posameznika v zvezi z obdelavo podatkov, ki se nanašajo nanj

19. člen

(zahtevek posameznika do informacij o obdelavi njegovih podatkov)

Posameznik, na katerega se nanašajo osebni podatki, ima pravico od upravljavca dobiti potrditev, ali se v zvezi z njim obdelujejo osebni podatki, in kadar je temu tako, dostop do osebnih podatkov in naslednje informacije:
- namen obdelave;
- vrste osebnih podatkov;
- uporabnike, ki so jim bili osebni podatki posredovani;
- kadar je mogoče, predvideno obdobje hrambe osebnih podatkov oz. če to ni mogoče, merila, ki se uporabljajo za določitev tega obdobja;
- obstoj pravice, da se od upravljavca zahteva popravek, izbris ali omejitev obdelave osebnih podatkov v zvezi s posameznikom, na katerega se nanašajo , ali obstoj do pravice ugovora taki obdelavi;
- pravico do vložitve pritožbe pri nadzornem organu;
- obstoj avtomatiziranega sprejemanja odločitev, vključno z oblikovanjem profilov, ter v vsaj takih primerih smiselne informacije o razlogih zanj, kot tudi pomen in predvidene posledice take obdelave za posameznika, na katerega se nanašajo;

Kadar se podatki prenesejo v tretjo državo ali mednarodno organizacijo, ima posameznik, na katerega se nanašajo osebni podatki, pravico biti obveščen o ustreznih zaščitnih ukrepih v zvezi s prenosom;

Upravljavec zagotovi kopijo osebnih podatkov, ki se obdelujejo. Za dodatne kopije, ki jih zahteva posameznik, na katerega se nanašajo osebni podatki lahko upravljavec zaračuna razumno pristojbino ob upoštevanju upravnih stroškov. Kadar posameznik zahtevo predloži v elektronski obliki in, če posameznik ne zahteva drugače se informacije zagotovijo v elektronski obliki.

Za izvedbo posameznikovega zahtevka je zadolžen upravljavec/odgovorna oseba posamezne zbirke podatkov na katere se nanaša zahtevek posameznika ali pooblaščena oseba za varstvo osebnih podatkov.

20. člen
(zahtevek posameznika za popravek podatkov v zvezi z njim)

Posameznik na katerega se nanašajo osebni podatki, ima pravico doseči, da upravljavec brez nepotrebnega odlašanja popravi netočne osebne podatke v zvezi z njim. Posameznik, na katerega se nanašajo osebni podatki, ima ob upoštevanju namenov obdelave, pravico do dopolnitve nepopolnih osebnih podatkov.

Za izvedbo posameznikovega zahtevka je zadolžen upravljavec/odgovorna oseba posamezne zbirke podatkov na katere se nanaša zahtevek ali pooblaščena oseba za varstvo osebnih podatkov.

Upravljavec/odgovorna oseba posamezne zbirke podatkov je dolžan prizadetega posameznika obvestiti v najkrajšem možnem času, brez nepotrebnega odlašanja.

21. člen
(zahtevek posameznika za izbris podatkov v zvezi z njim)

Posameznik na katerega se nanašajo osebni podatki, ima pravico doseči, da upravljavec brez nepotrebnega odlašanja izbriše osebne podatke v zvezi z njim, kadar velja eden izmen naslednjih razlogov:

- osebni podatki niso več potrebni v namene, za katere so bili zbrani ali kako drugače obdelani;
- posameznik na katerega se nanašajo osebni podatki, prekliče privolitev na podlagi katere poteka obdelava in kadar za obdelavo ne obstaja nobena druga pravna podlaga;
- osebni podatki so bili obdelani nezakonito.

Posameznik nima pravice zahtevati izbrisa osebnih podatkov v primerih, ko je obdelava potrebna:

- za uresničevanje pravic do svobode izražanja in obveščanja;
- za izpolnjevanje pravne obveznosti obdelave na podlagi prava Unije ali Zakona o varstvu osebnih podatkov ali za izvajanje naloge v javnem interesu javnega zdravja;
- za namene arhiviranja v javnem interesu, za znanstveno- ali zgodovinsko -raziskovalne ali statistične namene
- za uveljavljanje, izvajanje ali obrambo pravnih zahtevkov.

Za izvedbo posameznikovega zahtevka je zadolžen upravljavec/odgovorna oseba posamezne zbirke podatkov na katere se nanaša zahtevek posameznika ali pooblaščena oseba za varstvo osebnih podatkov.

Upravljavec/odgovorna oseba posamezne zbirke podatkov je dolžan prizadetega posameznika obvestiti v najkrajšem možnem času, brez nepotrebnega odlašanja.

22. člen
(zahtevek posameznika za omejitev obdelave podatkov v zvezi z njim)

Posameznik, na katerega se nanašajo osebni podatki, ima pravico doseči, da upravljavec omeji obdelavo, kadar velja en od naslednjih primerov:

- posameznik, na katerega se nanašajo osebni podatki, oporeka točnosti podatkov, in sicer za obdobje, ki upravljavcu omogoča preveriti točnost osebnih podatkov;
- je obdelava nezakonita in posameznik, na katerega se nanašajo osebni podatki, nasprotuje izbrisu osebnih podatkov ter namesto tega zahteva omejitev njihove uporabe;
- upravljavec osebnih podatkov ne potrebuje več za namene obdelave, temveč jih posameznik, na katerega se nanašajo osebni podatki, potrebuje za uveljavljanje, izvajanje ali obrambo pravnih zahtevkov;
- je posameznik, na katerega se nanašajo osebni podatki, vložil ugovor v zvezi z obdelavo za obdobje v katerem se preveri, ali zakoniti razlogi upravljavca prevladajo nad razlogi posameznika, na katerega se nanašajo osebni podatki.

Kadar je bila obdelava osebnih podatkov omejena v skladu s 1. odstavkom, se taki osebni podatki z izjemo njihovega shranjevanja obdelujejo le s privolitvijo posameznika, na katerega se ti nanašajo, ali za uveljavljanje, izvajanje ali obrambo pravnih zahtevkov ali zaradi varstva pravic druge fizične ali pravne osebe ali zaradi pomembnega javnega interesa Unije ali države članice.

Za izvedbo posameznikovega zahtevka je zadolžen upravljavec/odgovorna oseba posamezne zbirke podatkov na katere se nanaša zahtevek posameznika ali pooblaščena oseba za varstvo osebnih podatkov.

Upravljavec/odgovorna oseba posamezne zbirke podatkov je dolžan prizadetega posameznika obvestiti o omejitvi obdelave podatkov v najkrajšem možnem času, brez nepotrebnega odlašanja.

23. člen
(zahtevek posameznika da prejme podatke v zvezi z njim)

Posameznik, na katerega se nanašajo osebni podatki, ima pravico, da prejme osebne podatke v zvezi z njim, ki jih je posedoval upravljavcu, v strukturirani, splošno uporabljani in strojno berljivi obliki, in pravico, da te podatke posreduje drugemu upravljavcu, ne da bi ga upravljavec, ki so mu bili osebni podatki zagotovljeni, pri tem oviral.

Pri uresničevanju pravice do prenosljivosti podatkov v skladu z odstavkom 1 ima posameznik, na katerega se nanašajo osebni podatki, pravico, da se osebni podatki neposredno prenesejo od enega upravljavca k drugemu, kadar je to tehnično izvedljivo.

Ta pravica se ne uporablja za obdelavo, potrebno za opravljanje naloge, ki se izvaja v javnem interesu ali pri izvajanju javne oblasti, dodeljene upravljavcu.

Za izvedbo posameznikovega zahtevka je zadolžen upravljavec/odgovorna oseba posamezne zbirke podatkov na katere se nanaša zahtevek posameznika ali pooblaščena oseba za varstvo osebnih podatkov.

Upravljavec/odgovorna oseba posamezne zbirke podatkov je dolžan prizadetega posameznika obvestiti o omejitvi obdelave podatkov v najkrajšem možnem času, brez nepotrebnega odlašanja.

24. člen
(ugovor posameznika zoper obdelavo podatkov o njem)

Posameznik, na katerega se nanašajo osebni podatki, ima na podlagi razlogov, povezanih z njegovim posebnim položajem, pravico, da kadar koli ugovarja obdelavi osebnih podatkov v zvezi z njim

Upravljavec preneha obdelovati osebne podatke, razen če dokaže nujne legitimne razloge za obdelavo, ki prevladajo nad interesi, pravicami in svoboščinami posameznika, na katerega se nanašajo osebni podatki, ali za uveljavljanje, izvajanje ali obrambo pravnih zahtevkov.

Kadar se osebni podatki obdelujejo v znanstveno - ali zgodovinsko - raziskovalne namene ali statistične namene, ima posameznik, na katerega se ti podatki nanašajo, pravico, da iz razlogov, povezanih z njegovim posebnim položajem, ugovarja obdelavi osebnih podatkov v zvezi z njim, razen če je obdelava potrebna za opravljanje naloge, ki se izvaja zaradi razlogov javnega interesa.

Za izvedbo ukrepa za izvedbo posameznikovega zahtevka je upravljavec/odgovorna oseba posamezne zbirke podatkov na katere se nanaša zahtevek posameznika ali pooblaščena oseba za varstvo osebnih podatkov.

Upravljavec/odgovorna oseba posamezne zbirke podatkov je dolžan prizadetega posameznika obvestiti o prenehanju obdelave podatkov v najkrajšem možnem času, brez nepotrebnega odlašanja.

V. VARNOST OBDELAVE OSEBNIH PODATKOV

Organizacijski ukrepi

25. člen
(vgrajeno in privzeto varstvo podatkov)

ZD Radlje ob Dravi v okviru lastnega razvoja programske opreme za rešitve in storitve obdelave ter pri postopkih nabave dosledno sledi načelu vgrajenega in privzetega varstva osebnih podatkov, ki obsegajo predvsem:

- minimizacijo obdelave osebnih podatkov;
- čimprejšnjo psevdomizacijo osebnih podatkov;
- preglednost pri nalogah in obdelavi osebnih podatkov;
- omogočanje posameznikom, na katere se nanašajo osebni podatki, da spremljajo obdelavo osebnih podatkov, in
- omogočanje upravljavcu, da vzpostavi in izboljša varnostne ukrepe.

Pri razvoju, oblikovanju, izboru in uporabi aplikacij in storitev, ki temeljijo na obdelavi osebnih podatkov ali ki pri opravljanju svoje funkcije obdelujejo osebne podatke, bi bilo treba proizvajalce storitev in aplikacij spodbujati, da pri razvoju in oblikovanju takih storitev in aplikacij upoštevajo pravico do varstva podatkov ter ob ustreznem upoštevanju najnovejšega tehnološkega razvoja

zagotovijo, da so upravljavci in obdelovalci zmožni izpolnjevati svoje obveznosti varstva podatkov. Načeli vgrajenega in privzetega varstva podatkov bi morali biti upoštevani tudi na javnih razpisih.

26. člen
(kakovost obdelovanih podatkov)

Osebni podatki, ki se obdelujejo v ZD Radlje ob Dravi, morajo biti točni, ažurni, ustrezni in po obsegu primerni glede na namene, za katere se obdelujejo.

27. člen
(popis informacijskih sredstev)

ZD Radlje ob Dravi pregled nad rešitvami, napravami, sistemi in drugo infrastrukturo (v nadaljevanju: sredstvo), ki jo uporablja za obdelavo zbirk, vodi v popisu informacijskih sredstev kot prilogo Krovne politike varovanja informacij.

Informacijska sredstva so sestavni del SUVI politike.

28. člen
(uporaba zasebnih naprav za obdelavo osebnih podatkov)

ZD Radlje ob Dravi s posebno politiko določi pravila uporabe zasebnih naprav (računalnikov, tablic, pametnih telefonov) za obdelavo podatkov, s katerimi upravlja. Politika mora obsegati tudi postopke za zagotavljanje varnosti obdelave na zasebnih napravah in ukrepanje v primeru odtujitve ali pogrešitve naprave.

Zasebne naprave iz prejšnjega odstavka morajo biti vključene v popisu informacijskih sredstev in v delu, ki je namenjen obdelavi, obvladovane s sistemi podjetja za upravljanje mobilnih naprav ter opremljene z ustreznimi informacijskimi varnostnimi rešitvami (šifriranje, razmejitev obdelave zasebnih podatkov/storitev od podatkov/storitev ZD Radlje ob Dravi, SUVI politika).

Ocena tveganj in ocena učinka na varstvo osebnih podatkov
29. člen
(ocena tveganj informacijske varnosti)

ZD Radlje ob Dravi redno izvaja oceno tveganja, ki bi lahko vplivala na varnost obdelave podatkov in sicer po postopku, ki obsega zlasti:

- identifikacijo oziroma odkrivanje groženj ali nevarnosti;
- ugotovitev, kateri viri bi bili lahko izpostavljeni identificiranim grožnjam ali nevarnostim;
- oceno tveganja, v kateri sta upoštevana verjetnost nastanka dogodka in resnost nastalih posledic;
- sprejetje odločitev o tem, ali je tveganje sprejemljivo;
- odločitev o uvedbi ukrepov za zmanjšanje nesprejemljivega tveganja.

ZD Radlje ob Dravi popravi in dopolni oceno tveganja vsakokrat ko:

- obstoječi preventivni ukrepi varovanja niso zadostni oziroma niso več ustrezni;
- se spremenijo podatki, na katerih je ocenjevanje temeljilo;
- obstajajo možnosti in načini za dopolnitev ocenjevanja.

Način izvedbe ocene tveganj ZD Radlje ob Dravi določi s Politiko izvajanja ocen učinkov na varstvo osebnih podatkov – upravljanje komunikacij in informacij, katerega del je metodologija izdelave ocene tveganj in obsega ocenjevanje tveganj, identificiranje, kriterije ovrednotenja, vire ogrožanj in postopke obvladovanja tveganj.

Za koordinacijo rednega izvajanja ocene tveganja je odgovorna oseba posamezne službe/ambulante, kjer se evidence dejavnosti obdelave obdelujejo oz. spreminjajo. Gre za timsko delo, v katerem sodeluje tudi pooblaščena oseba za varstvo osebnih podatkov. Pripravljene ocene učinkov pred predvideno obdelavo ali spremembo pregleda in potrdi skupina za informacijsko varnost.

30. člen
(ocena učinkov na varstvo osebnih podatkov)

Kadar je možno, da bi lahko vrsta obdelave osebnih podatkov, zlasti z uporabo novih tehnologij, ob upoštevanju narave, obsega, okoliščin in namenov obdelave povzročila veliko tveganje za pravice in svoboščine posameznikov, ZD Radlje ob Dravi pred obdelavo opravi oceno učinka na varstvo osebnih podatkov. V eni oceni je lahko obravnavan niz podobnih dejanj obdelave, ki predstavljajo podobna velika tveganja.

Namen politike izvajanja ocen učinkov za varstvo osebnih podatkov so podrobneje opredeljeni v Politiki izvajanja ocen učinkov na varstvo osebnih podatkov.

Po potrebi ZD Radlje ob Dravi glede ocenjevanja obdelave zaprosi za mnenje posameznike, na katere bi se nanašali obdelovani podatki, ali njihove predstavnike (npr. Združenje Zdravstvenih zavodov, Zdravniška zbornica...).

Oceno učinka izdela odgovorna oseba službe/ambulante, kjer evidenca dejavnosti obdelave nastaja oz. se pojavi potreba po izvedbi ocen učinka. Gre za timsko delo, v katerem sodeluje tudi pooblaščena oseba za varstvo osebnih podatkov. Pripravljene ocene učinkov pred predvideno obdelavo ali spremembo pregleda in potrdi skupina za informacijsko varnost.

Spremembe načina obdelave
31. člen
(uvajanje sprememb)

Sprememba informacijskih rešitev ali dokumentacije, ki vplivajo na varstvo podatkov, lahko izvirajo iz:

- razlogov za izboljšavo ali uvedbo novih rešitev,
- odprave napak na informacijskih rešitvah,
- organizacijskih sprememb, ki vplivajo na rešitve ali
- pravnih sprememb, ki vplivajo na rešitve.

Razvojno, preizkusno in produkcijsko okolje informacijskih rešitev, s katerimi se izvaja obdelava podatkov, so ločeni glede na specifiko rešitve.
Vsaka sprememba informacijskih rešitev ali dokumentacije se mora ustrezno dokumentirati.

Seznam verzij se nahaja pri skrbniku informacijske rešitve.

Realni podatki ne smejo nikoli zapustiti produkcijskega okolja in se ne smejo prenašati v nobeno drugo okolje ali posredovati drugim osebam brez izrecne podlage v veljavnem zakonu ali brez

izrecnega soglasja vseh pogodbenih strank, na katero se podatki nanašajo, ter po vnaprejšnji presoji, ali je takšno ravnanje v skladu z vsemi veljavnimi predpisi.

Pred namestitvijo nove oz. spremembo že obstoječe informacijske rešitve oz. aplikativne podpore za storitve, ki vplivajo na varstvo podatkov, odgovorna oseba (vodja projekta, vodja enote) določi potrebne aktivnosti za usposabljanje oziroma informiranje vseh uporabnikov.

Nadzor sprememb informacijskih sistemov je podrobneje opisan v Politiki razvoja, spreminjanja in vzdrževanja programske opreme – upravljanje komunikacij in informacij.

Zagotavljanje neprekinjenega poslovanja
32. člen
(načrt neprekinjenega poslovanja)

Odgovornost, organiziranje in izvedba postopkov za zagotovitev neprekinjene obdelave in ohranjanje celovitosti obdelovanih podatkov se v ZD Radlje ob Dravi določi s pravili neprekinjenega poslovanja, ki temeljijo na sposobnosti organizacije, da pripravi načrt za primere incidentov in motenj pri obdelavi ter se nanje odzove tako, da lahko zagotovi neprekinjeno obdelavo in s temi obdelavami povezanih poslovnih procesov ZD Radlje ob Dravi.

Za koordiniranje in vzdrževanje načrta neprekinjenega poslovanja je odgovoren informatik skupaj s pooblaščeno osebo za varstvo osebnih podatkov ter skupino za informacijsko varnost.

33. člen
(varnostno kopiranje podatkov)

ZD Radlje ob Dravi določi postopke obravnavanja kršitev pravil varnosti, ki bi lahko povzročila ali povzročijo namerno ali nenamerno uničenje, izgubo, spremembo, nepooblaščeno razkritje ali dostop do osebnih podatkov, ki so poslani shranjeni ali kako drugače obdelani, ali katastrofalen izpad oz. uničenje opreme za izvajanje obdelave (SUVI politika).

Dejanja oz. dogodki iz prejšnjega odstavka so lahko uvrščeni med varnostne dogodke ali incidente.

Namen varnostnega kopiranja podatkov je zagotoviti rezervno kopijo podatkov in omogočiti ponovno vzpostavitev sistema in uspešno nadaljevanje dela po množici različnih dogodkov oziroma varnostnih incidentov, ki povzročijo poškodovanje ali izgubo podatkov – kot so problemi s strojno opremo, problemi s programsko opremo, človeške napake, naravne nesreče ipd. Zato se vsi pomembni elektronski podatki redno shranjujejo na medije daljše trajnosti.

ZD Radlje ob Dravi zagotavlja, da so izdelani postopki za varnostno kopiranje in restavriranje podatkov. S tem se zagotovi, da se delo na sistemu lahko uspešno nadaljuje po namernem ali naključnem izpadu.

Kadar zaradi varnostnega dogodka ali incidenta pride do kršitve varstva osebnih podatkov, zaradi katere bi bile lahko ogrožene pravice in svoboščine posameznikov, mora biti izdelano in informacijskemu pooblaščencu poslano obvestilo o kršitvi varstva osebnih podatkov, izdelano v skladu s 33. členom Uredbe.

Posredovanje osebnih podatkov

34. člen

(postopek posredovanja)

Osebni podatki s katerimi upravlja ZD Radlje ob Dravi, se na zahtevo posredujejo samo tistim uporabnikom, ki se izkažejo z ustrezno zakonito podlago za obdelavo podatkov, ki se nanašajo na določenega posameznika ali določene kategorije posameznikov.

Posredovanje osebnih podatkov iz prejšnjega odstavka tega člena lahko uporabnik zahteva pisno. Ob vložitvi pisne vloge mora uporabnik jasno navesti zakonito podlago, ki ga pooblašča za pridobitev osebnih podatkov, ali pa mora k vlogi priložiti pisno zahtevo oziroma privolitev posameznika, na katerega se podatki nanašajo.

Ovojnica v kateri se posredujejo osebni podatki v fizični obliki, mora biti izdelana tako, da ne omogoča, da bi bila ob normalni svetlobi ali pri osvetlitvi z običajno lučjo vidna vsebina ovojnice. Ovojnica mora tudi zagotoviti, da je ni mogoče odpreti in se seznaniti z njeno vsebino brez vidne sledi odpiranja.

Osebne podatke je dovoljeno posredovati z informacijskimi, komunikacijskimi in drugimi sredstvi le ob izvajanju postopkov in ukrepov, ki nepooblaščenim osebam preprečujejo prilaščanje ali uničenje podatkov ter neupravičeno seznanjanje z njihovo vsebino.

Posebne vrste osebnih podatkov je dovoljeno posredovati preko elektronskih komunikacij samo, če so šifrirani tako, da je zagotovljena njihova neprepoznavnost med prenosom (7Zip in geslo).

35. člen

(evidentiranje posredovanj)

Vsako posredovanje osebnih podatkov iz prejšnjega člena se zaznamuje z navedbo naslednjih podatkov:

- kateri osebni podatki so bili posredovani,
- osebno ime/firmo in naslov/sedež osebe, ki so ji bili posredovani osebni podatki, oz. navedba, da je bilo posredovanje opravljeno po uradni dolžnosti,
- datum in ura posredovanja podatkov ter
- pravna podlaga, na podlagi katere so bili posredovani osebni podatki.

Seznam iz prejšnjega odstavka je v elektronski obliki.

Fizični in tehnični ukrepi varovanja obdelave

36. člen

(varovanje prostorov)

Vsi prostori ZD Radlje ob Dravi, v katerih se nahajajo nosilci podatkov, ki vsebujejo osebne podatke ter strojna in programska oprema za obdelovanje teh podatkov, so varovani prostori.

Vsak vstop v varovane prostore ZD Radlje ob Dravi mora biti kontroliran.

Prostori ZD Radlje ob Dravi so varovani s protivlomnim alarmom, ki mora biti vključen vedno, ko v prostoru ni nobenega zaposlenega.

Zaposleni morajo ob zaključku delovnega časa oziroma po končanem delu izven delovnega časa omare in pisalne mize z nosilci podatkov, ki vsebujejo osebne podatke zakleniti. Računalniki in druga strojna oprema pa izklopljeni oz. fizično ali programsko zaklenjeni.

Obiskovalci se smejo v poslovnih prostorih ZD Radlje ob Dravi, v katerih se nahajajo nosilci podatkov gibati samo v spremstvu zaposlenega. To določilo ne velja za stalne zunanje sodelavce ZD Radlje ob Dravi, katerih vstop in gibanje v prostorih, v katerih se nahajajo nosilci podatkov je urejeno s pogodbo in jim je dodeljeno vstopno sredstvo (kartica za vhodno kontrolo, identifikacijska kartica).

37. člen
(vstopi in izstopi iz prostorov v nočnem času)

Vstopi v ZD Radlje ob Dravi v nočnem času med 22:00 uro in 6:00 uro so možni le preko dežurne službe.

Varovanje ljudi in premoženja je podrobneje opredeljeno v Pogodbi št. 3-500DS/03PG o sprejemu signala alarma vloma in intervenciji Varnosti Maribor d.d. z dne 12.05.2003.

38. člen
(podaljšano oko - nadzor vstopa v prostore)

Vstop in gibanje v prostoru dežurne ambulante je nadzorovano z nadzorom – podaljšano oko, ki je nujno potrebno za varovanje in varnost zaposlenih, pacientov, obiskovalcev in poslovnih partnerjev, zaradi varovanja premičnin in opreme, zaradi zagotavljanja varnosti službenih prostorov in nadzora vstopa ali izstopa v službene prostore ali, če zaradi narave dela obstaja možnost ogrožanja zaposlenih, pacientov, obiskovalcev in poslovnih partnerjev.

Nadzor – podaljšano oko se ne snema in se ne hrani.

Zaposleni in obiskovalci so z videonadzorom seznanjeni z ustreznimi obvestilnimi napisi.

39. člen
(varovanje nosilcev podatkov, ki vsebujejo osebne podatke)

Zaposleni ne smejo puščati nosilcev podatkov, ki vsebujejo osebne podatke, na vidnem mestu (npr. na pisalnih mizah) v prisotnosti oseb, ki nimajo pravice vpogleda vanje.

Računalniški zasloni morajo biti nameščeni tako, da nepoklicani nimajo vpogleda v prikazovane podatke.

Iznos nosilcev podatkov, ki vsebujejo posebne vrste osebnih podatkov iz prostorov ZD Radlje ob Dravi ni dovoljen. V sklopu krovne politike varovanja informacij je ZD Radlje ob Dravi sprejela področne politike – predpise, ki temeljijo na zakonih in predpisih SUVI, ki jih je predpisalo Ministrstvo za zdravje. Vse podatkovne baze in dostopi do njih preko aplikacij so varovani in predpisani v njih.

40. člen
(kopiranje in tiskanje osebnih podatkov s strani zaposlenih)

Zaposleni v ZD Radlje ob Dravi, ki pri izvajanju svojih delovnih nalog kopirajo ali na drug tehnični način razmnožujejo ali tiskajo dokumente, ki vsebujejo osebne podatke, na napravah, ki jih uporablja večje

število zaposlenih, po končanem kopiranju ali tiskanju ne smejo puščati dokumentov v, na ali ob napravah.

Kopiranje in tiskanje dokumentov, ki vsebujejo posebne vrste osebnih podatkov, se lahko opravi samo na napravah, ki so v času kopiranja ali tiskanja pod kontrolo zaposlenega, ki izvaja omenjeni opravili.

Dokumenti, ki vsebujejo osebne podatke in se potrebujejo kot pomoč (razni seznami, zapisi ipd.) pri opravljanju del in nalog, se hranijo kot del osnovne dokumentacije posameznika. V primeru, da se navedeni dokumenti ne shranijo, se trajno uničijo (uničevalniki dokumentacije).

41. člen
(varovanje dostopa do strojne in programske opreme)

Dostop do programske opreme mora biti varovan tako, da dovoljuje dostop samo zaposlenim, ki jih določi oseba, odgovorna za delovanje informacijskega sistema, ali osebju zunanjega izvajalca, ki v skladu s pogodbo izvaja dogovorjena dela.

Vzdrževanje in popravila strojne računalniške in druge opreme je dovoljeno samo z vednostjo vodje službe za informatiko, izvajajo pa ga lahko samo pooblaščeni zaposleni oz. serviserji in vzdrževalci, ki imajo z ZD Radlje ob Dravi sklenjeno ustrezno pogodbo.

Vsi dostopi do programske opreme morajo biti obeleženi z revizijsko sledjo.

Popravljanje, spreminjanje in dopolnjevanje sistemske programske opreme je dovoljeno samo na podlagi odobritve skrbnika informacijskega sistema, izvajajo pa ga lahko samo organizacije in posamezniki (v nadaljnjem besedilu: izvajalci), ki imajo z ZD Radlje ob Dravi sklenjeno ustrezno pogodbo. Izvajalci morajo spremembe in dopolnitve sistemske programske opreme ustrezno dokumentirati.

Popravljanje, spreminjanje in dopolnjevanje aplikativne programske opreme je dovoljeno samo na podlagi odobritve skrbnika informacijskega sistema, izvajajo pa ga lahko samo organizacije in posamezniki (v nadaljnjem besedilu: izvajalci), ki imajo s ZD Radlje ob Dravi sklenjeno ustrezno pogodbo. Izvajalci morajo spremembe in dopolnitve aplikativne programske opreme ustrezno dokumentirati.

Vsebina diskov omrežnega strežnika in delovnih postaj, povezanih v omrežje, na katerih se nahajajo osebni podatki, se preverjajo samodejno z vidika prisotnosti računalniških virusov. Zaznava računalniškega virusa se obravnava kot incident.

Vsi podatki in programska oprema, ki so namenjeni uporabi v računalniškem informacijskem sistemu, in prispejo v ZD Radlje ob Dravi na prenosnih medijih ali preko komunikacijskih kanalov, so pred uporabo pregledani s strani zaposlenega ki jih uporablja, da na njih ni računalniških virusov. V primeru, da zaposleni pri uporabi zazna računalniški virus, ga je dolžan obravnavati kot incident.

Zaposleni na informacijsko opremo ne smejo namestiti programske opreme brez vednosti službe za informatiko. Prav tako iz prostorov ZD Radlje ob Dravi brez odobritve direktorja in vednosti skupine za informacijsko varnost ne smejo odnašati programske opreme.

42. člen
(kontrola dostopa do informacijskega sistema)

Dostop do uporabnikov informacijskega sistema je kontroliran s sistemom gesel ali z drugimi avtentikacijskimi (npr. digitalna potrdila ...) sredstvi, ki v povezavi s sistemom tvorjenja in beleženja revizijskih sledi omogoča naknadno ugotavljanje, kdaj so bili posamezni podatki vneseni v zbirko podatkov, uporabljeni ali drugače obdelani ter kdo je to storil.

Vsi dostopi do informacijskega sistema in podatkov se beležijo z revizijsko sledjo.

Zaposlenemu se dodeli obseg dostopnih pravic za uporabo informacijskega sistema, ki je nujno potreben za izvajanje delovnih nalog.

Vsa gesla in postopki, ki se uporabljajo za administriranje operacijskih sistemov, baz, podatkov, lokalnega in drugih omrežij ter elektronske pošte in drugih aplikativnih programov (t.i. administratorska gesla), se varno hranijo pri sistemskem administratorju. Uporabi se jih samo v izrednih okoliščinah oziroma v nujnih primerih. Vsaka uporaba vsebine mesta hrambe gesel in postopkov se dokumentira. Pri vsaki takšni uporabi se določi nova vsebina gesel.

43. člen
(revizijske sledi)

ZD Radlje ob Dravi v zvezi z dostopi do podatkov, postopkov obdelave in do sistemov obdelave tvori, beleži in hrani zapise (t.i. revizijske sledi), ki omogočajo poznejše ugotavljanje, kdaj in kdo je dostopal do določenega podatka, postopka obdelave oz. sistema za obdelavo.

Za revizijske sledi so odgovorni skrbniki posameznih informacijskih sistemov oz. rešitev, ki na podlagi posveta z pooblaščeno osebo za varstvo osebnih podatkov določi, kdo in v katerih primerih sme dostopati do zapisov revizijskih sledi. Način zbiranja zapisov, hrambo in uporabo revizijskih sledi ZD Radlje ob Dravi določi v Politiki revizijskih sledi – upravljanje komunikacij in informacij. V politiki se določi sledljivost obdelav podatkov.

44. člen

Dostop v zavarovane prostore je mogoč le v rednem delovnem času, izven tega časa pa samo na podlagi pisnega dovoljenja pooblaščene osebe enote. Vodi se evidenca izdaje in vrnitve ključev izven delovnega časa. Rezervni ključi prostorov, v katerih se hranijo varovani podatki, se hranijo pri delavcih dežurne službe v ZD Radlje ob Dravi, ki smejo izdati ključe samo osebi, ki v tem prostoru dela oz. v skladu s prvim odstavkom tega člena. Zaposleni ne smejo puščati nezavarovanih nosilcev osebnih podatkov na hodnikih, na mizah ali policah. Nosilci osebnih podatkov, ki se nahajajo izven zavarovanih prostorov, morajo biti shranjeni in zaklenjeni v omarah.

VI. VARNOST OBDELAVE OSEBNIH PODATKOV

45. člen
(obveščanje o kršitvah varstva ali varnosti)

Zaposleni so dolžni o aktivnostih, ki so povezane z odkrivanjem ali nepooblaščenim uničenjem osebnih podatkov, zlonamerni ali nepooblaščeni uporabi, prilaščanju, spreminjanju ali poškodovanju osebnih podatkov, oziroma o kršitvi pravil varovanja poslovnih in službenih prostorov ali strojne in programske opreme informacijskega sistema ZD Radlje ob Dravi takoj obvesti neposredno

nadrejenega, on pa pooblaščeno osebo za varstvo osebnih podatkov, sami pa morajo z zakonitimi ukrepi takšno aktivnost preprečiti.

46. člen
(izvajanje postopkov in ukrepov)

Vsi zaposleni v ZD Radlje ob Dravi so dolžni izvajati s tem pravilnikom predpisane postopke in ukrepe za varstvo in zavarovanje osebnih podatkov in varovati osebne podatke, za katere so izvedeli oz. bili z njimi seznanjeni pri opravljanju svojega dela. Obveza varovanja podatkov ne preneha s prenehanjem delovnega razmerja.

47. člen
(izvajanje in nadzor nad izvajanjem postopkov in ukrepov)

Nadzor nad izvajanjem postopkov in ukrepov, določenih s tem pravilnikom, opravlja pooblaščena oseba za varstvo osebnih podatkov v ZD Radlje ob Dravi, skupaj s skupino za informacijsko varnost.

48. člen
(izjava)

Pred nastopom dela v ZD Radlje ob Dravi mora zaposleni podpisati posebno izjavo, ki ga zavezuje k varovanju osebnih podatkov.

Iz podpisane izjave mora biti razvidno, da je podpisnik seznanjen z določbami tega pravilnika in zakona, izjava pa mora vsebovati tudi pouk o posledicah kršitve določb pravilnika in zakona.

Izjavo iz prvega odstavka tega člena podpišejo tudi zunanji sodelavci ZD Radlje ob Dravi, ki se v okviru izvajanja pogodbenih del seznanijo ali bi se lahko seznanili z osebnimi podatki, s katerimi upravlja ZD Radlje ob Dravi.

Izjavo iz prvega odstavka tega člena podpišejo vsi dijaki, študentje, zunanji pripravniki in specializanti, ki opravljajo del obveznega programa izobraževanja/kroženja v ZD Radlje ob Dravi, ter volonterji.

49. člen
(odgovornost za kršitev)

Kršitev določil tega pravilnika s strani zaposlenih pomeni kršitev obveznosti iz delovnega razmerja, ostali pa za kršitve odgovarjajo na temelju pogodbenih obveznosti.

Odgovornost iz prejšnjega odstavka ne izključuje prekrškovne, kazenske ali odškodninske odgovornosti, kadar tako določa zakon.

VII. KONČNE DOLOČBE

50. člen
(izvajanje nadzora)

Nadzor nad izvajanjem določb tega pravilnika izvaja direktor oziroma od njega pooblaščena oseba.

51. člen
(seznanitev zaposlenih s pravilnikom)

Z vsebino pravilnika se seznanijo vsi zaposleni preko elektronske pošte. Vsebina pravilnika se po sprejemu izobesi na oglasni deski. Kršitev določil trga pravilnika predstavlja kršitev delovnih obveznosti.

52. člen
(začetek veljavnosti)

Ta pravilnik prične veljati po podpisu direktorja.

Z veljavnostjo tega pravilnika preneha veljati Pravilnik o varovanju osebnih in drugih zaupnih podatkov ter dokumentarnega gradiva v ZD Radlje ob Dravi z dne 6.12.2001.

Radlje, dne 1. 12. 2018

Direktor:
Lidija GOLOB, univ. dipl. ekon.

ZDRAVSTVENI DOM RADLJE OB DRAVI Mariborska cesta 37