Zdravstveni dom Domžale

Zdravstveni dom Domžale
Mestni trg 2, 1230 Domžale

**Telefon:** (01) 72 45 100
**Telefaks:** (01) 72 14 459
**e-mail:** info@zd-domzale.si

www.zd-domzale.si

ID za DDV: SI88946347
T.R.R: SI56 0110 0600 8353 275

Številka: 15-01–4
Datum: 27. 07. 2023

Na podlagi Zakona o varstvu osebnih podatkov (Uradni list RS, št. 163/22), Splošne uredbo o varstvu podatkov (v nadaljnjem besedilu: GDPR) in 28. člena Statuta Zdravstvenega doma Domžale, št. 15-01–3 z dne 24. 04. 2001, izdajam

# PRAVILNIK O VARSTVU OSEBNIH IN ZAUPNIH PODATKOV V ZRAVSTVENEM DOMU DOMŽALE

## I. SPLOŠNE DOLOČBE

1. člen

S tem pravilnikom se določa:
- način obdelave osebnih podatkov (v nadaljnjem besedilu: obdelava podatkov),
- način obravnavanja zahtevkov in ugovorov posameznika glede obdelave podatkov, ki se nanašajo nanj,
- izvajanje tehničnih in organizacijskih ukrepov, s katerimi Zdravstveni dom Domžale (v nadaljnjem besedilu: ZD Domžale) varuje osebne podatke in njihovo obdelavo,
- določa nosilce, organiziranost in postopke za izvajanje ukrepov iz tega odstavka.

2. člen

(1) Osebne podatke in njihovo obdelavo se varuje s tehničnimi in organizacijskimi ukrepi, ki temeljijo na oceni tveganj, ki jih pomeni obdelava podatkov, zlasti zaradi nenamernega ali nezakonitega uničenja, izgube, spremembe, nepooblaščenega razkritja ali dostopa do osebnih podatkov, ki so poslani, shranjeni ali kako drugače obdelani.

(2) Zaposleni in zunanji sodelavci, ki pri svojem delu obdelujejo osebne podatke ZD Domžale, morajo biti seznanjeni s veljavnimi predpisi s področja varovanja in obdelave osebnih podatkov.

(3) V skladu s tem pravilnikom se varujejo tudi osebni podatki, ki jih na podlagi pogodbe o obdelavi osebnih podatkov obdelujejo zunanji izvajalci.

3. člen

V tem pravilniku uporabljeni izrazi imajo naslednji pomen:

1. **Osebni podatek** pomeni katero koli informacijo v zvezi z določenim ali določljivim posameznikom,

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 alo več dejavnikov, ki so značilni za fizično, fiziološko, gensko, duševno, gospodarsko, kulturno ali družbeno identiteto tega posameznika,

3. **Obdelava podatkov** 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. **Evidenca** 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. **Spisek osebnih podatkov** je skupek osebnih podatkov, ustvarjen za namen organiziranja in izvedbe različnih oblik enkratnih dogodkov, ki jih ob prijavi ali odzivu na dogodek upravljavcu sporoči posameznik, in ki niso uvrščeni v evidenco,

6. **Posebne vrste osebnih podatkov** so zdravstveni podatki posameznika za namene izvajanja storitev v ZD Domžale,

7. **Obdelovalec** pomeni fizične ali pravne osebe, agencije ali drugi zunanji izvajalci, ki obdelujejo osebne podatke za ZD Domžale,

8. **Uporabnik** pomeni fizično ali pravno osebo, javni organ, agencijo ali drugo telo, ki so mu bili osebni podatki razkriti. 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 VOP glede na namene obdelave,

9. **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 katero izrazi strinjanje z obdelavo osebnih podatkov, ki se nanašajo nanj,

10. **Nosilec podatkov** so vse vrste sredstev, na katerih so zapisani ali posneti podatki evidenc,

11. **Končni uporabnik osebnih podatkov** (v množinski obliki za te posameznike v pravilniku se uporablja tudi izraz: osebje) je zaposleni ali zunanji sodelavec, ki zaradi narave svojega dela lahko obdeluje določene osebne podatke, s katerimi upravlja ali jih v okviru izvajanja poslovnih dejavnosti obravnava,

12. **Skrbnik evidence** je zaposleni ali zunanji sodelavec, odgovoren za obdelavo podatkov iz posamezne evidence osebnih podatkov,

13. **Informacijski sistem** je programska, strojna, komunikacijska in druga oprema, ki je namenjena obdelavi osebnih podatkov,

14. **Kršitev varnosti 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,

15. **Vodstveni pregled** je dokumentiran pregled SUVI, ki ga vodstvo opravi najmanj enkrat letno, da zagotovi skladnost obdelave podatkov.

16. **Poslovna skrivnost** se označujejo podatki skladno s klasifikacijskimi stopnjami zaupnosti informacij.

17. **SUVI** je sistem upravljanja varovanja informacij.

## II. VARSTVO OSEBNIH PODATKOV

### 1. Odgovornost nosilcev in organiziranost obdelave osebnih podatkov

4. člen

(1) Za zagotovitev ustreznih in učinkovitih tehničnih in organizacijskih ukrepov za izvajanje obdelave v skladu s predpisanimi in pogodbeno dogovorjenimi zahtevami ter za dokazovanje skladnosti dejavnosti obdelave z omenjenimi zahtevami je odgovorno vodstvo.

(2) Vsi tehnični in organizacijski ukrepi za izvajanje obdelave v skladu s predpisanimi in pogodbeno dogovorjenimi zahtevami morajo biti 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.

(3) Način izvajanja ukrepov iz prejšnjega odstavka določata Navodilo za ravnanje z informacijami različnih stopenj zaupnosti in Navodilo za uporabo informacijskih sistemov, ki ga sprejme direktor ZD Domžale ter ga objavi na spletni strani ZD Domžale in na intranetu ZD Domžale.

### 2. Pooblaščena oseba za varstvo osebnih podatkov

5. člen

(1) Za pooblaščeno osebo za varstvo osebnih podatkov, se določa posameznika, ki izpolnjuje z zakonom predpisane pogoje za pooblaščeno osebo za varstvo osebnih podatkov (v nadaljnjem besedilu: DPO).

(2) Vodstvo lahko za pomoč DPO pri opravljanju njegovih nalog izmed zaposlenih ali zunanjih strokovnjakov določi tudi druge osebe, ki pa so pri izvajanju pomoči vezane na navodila DPO.

(3) Vodstvo zagotovi, da je DPO ustrezno in pravočasno vključen v vse zadeve v zvezi z varstvom osebnih podatkov (v nadaljnjem besedilu: VOP). Vključevanje DPO v zadeve VOP se zagotovi predvsem z:
- neposrednim dostopom do vodstva, kadar vodstvo ali DPO ocenita, da določena zadeva VOP zahteva tak način obravnave,
- neposrednim dostopom do zaposlenih, ki obdelujejo osebne podatke,
- dostopom do podatkov, ki jih potrebuje za izvajanje svojih delovnih nalog.

(4) DPO vodstvu na strokovno neodvisen način pomaga pri zagotavljanju skladnosti obdelave osebnih podatkov s predpisi, ki urejajo obdelavo in VOP.

(5) DPO izvaja naslednje naloge:

- vodstvo in osebje obvešča ter jim svetuje o njihovih obveznostih v skladu z GDPR in drugimi predpisi,
- spremlja skladnost z GDPR, drugimi predpisi in SUVI, vključno z dodeljevanjem nalog, ozaveščanjem in usposabljanjem osebja, ter s tem povezanimi presojami SUVI in revizijami,
- svetuje, kadar je to zahtevano, glede ocene učinka v zvezi z VOP in spremljanja njenega izvajanja,
- sodeluje z Informacijskim pooblaščencem,
- deluje kot kontaktna točka za Informacijskega pooblaščenca pri vprašanjih v zvezi z obdelavo, vključno s predhodnim posvetovanjem ali posvetovanjem glede katere koli druge zadeve,
- svetuje razvijalcem novih rešitev za obdelavo osebnih podatkov glede načina obvladovanja tveganj za pravice in svoboščine, ki bi jih glede na uporabljene tehnologije ter naravo, obseg, okoliščine in namen obdelave lahko imela nova rešitev obdelave,
- nudi strokovno podporo pri obravnavi zahtevkov in ugovorov posameznikov, katerih podatke ZD Domžale obdeluje, vezanih na varstvo njihovih pravic in svoboščin v zvezi z obdelavo osebnih podatkov,
- vodi evidenco dejavnosti obdelave osebnih podatkov in skrbi za njeno dostopnost notranji in zunanji javnosti,
- daje mnenje k oceni učinka v zvezi z VOP, ki jo pripravi ZD Domžale v okviru načrtovanja obdelave, ki bi lahko povzročila veliko tveganje za pravice in svoboščine posameznikov, katerih podatki bodo predmet obdelave,
- organizira in izvaja usposabljanja in ozaveščanja osebja in obdelovalcev, ki so vključeni v dejanja obdelave, v zvezi z VOP,
- izvaja notranje kontrolne preglede s področja VOP skladno z letnim načrtom preverjanja skladnosti obdelave s predpisanimi in interno določenimi zahtevami.

## 3. Skrbniki evidenc obdelav osebnih podatkov

6. člen

(1) Za vsako evidenco obdelav osebnih podatkov, s katero upravlja ZD Domžale, se določi skrbnika, ki je odgovoren za zakonito in varno obdelavo osebnih podatkov v evidencah, ter za izvajanje postopkov in ukrepov opisanih v tem pravilniku in na njegovi podlagi izdanih notranjih aktih. Skrbnika posamezne evidence ter njegove naloge določi direktor ZD Domžale.

(2) Skrbnik evidence je odgovoren zlasti za:
- obdelavo osebnih podatke le za namene, za katere so bili zbrani,
- pridobitev predhodnega mnenja DPO v primeru obdelave osebnih podatkov za drug (dodaten) namen, zagotovitev informacije posamezniku o tem drugem namenu in za pridobitev privolitve posameznika za obdelavo,
- zbiranje najmanjšega možnega obsega osebnih podatkov, ki se jih potrebuje za uresničitev namena obdelave,
- določitev obsega dostopnih pravic končnih uporabnikov osebnih podatkov do evidence,
- posodabljanje opisov evidence v Evidenci dejavnosti obdelave in obveščanje DPO o posamični posodobitvi,
- obravnavanje zahtevkov posameznika v povezavi z evidenco, za katero skrbi (seznanitev, popravek, izbris, preklic ali ugovor obdelavi) ter obveščanje posameznika o izvedbi ali zavrnitvi zahtevka,
- brisanje podatkov v evidenci osebnih podatkov po poteku roka hrambe,
- pripravo in podpis pogodb z obdelovalci,
- učinkovito in skladno obravnavo kršitev VOP v sodelovanju s DPO.

## 4. Uporabniki osebnih podatkov

7. člen

(1) Uporabniki osebnih podatkov morajo imeti dostop do tistih vrst osebnih podatkov v določenih evidencah, ki jih nujno potrebujejo za izvedbo svojih delovnih nalog.

(2) Obseg nujno potrebnih dostopnih pravic za končnega uporabnika, na predlog njegovega nadrejenega, določi in odobri skrbnik evidence, dodelitev odobrenih dostopnih pravic v informacijskem sistemu pa izvede strokovnjak za IT ZD Domžale.

(3) Končni uporabnik osebnih podatkov mora posamične dostope do evidenc izvesti v skladu z navodili za obdelavo oziroma uporabo določene evidence in v skladu s SUVI. Pri tem mora zlasti paziti, da:

- ne razkriva osebnih podatkov, s katerimi se je seznanil pri svojem delu, sodelavcem, ki niso pooblaščeni za delo z osebnimi podatki, ali uporabnikom,
- ne opušča ravnanj, s katerim bi lahko preprečil:
    1. nepooblaščen vpogled v nosilce osebnih podatkov,
    2. nedovoljeno odnašanje nosilcev osebnih podatkov iz prostorov,
    3. ogrožanje integritete, zaupnosti in razpoložljivosti osebnih podatkov,
    4. postopke in ukrepe za evidentiranje vseh dejavnosti obdelav osebnih podatkov,
- o zlorabi osebnih podatkov ali vdoru v evidenco osebnih podatkov obvesti skrbnika evidence in druge zaposlene, odgovorne za obravnavanje kršitev VOP,
- ne opusti vestnega in skrbnega nadzora varovanih prostorov.

## 5. Dokazila o skladnosti obdelave

8. člen

(1) Za potrebe dokazovanja skladnosti obdelave s predpisanimi zahtevami, pogodbenimi obveznostmi in tem pravilnikom se vodi ustrezno dokumentacijo, s katero je sposoben dokazati, da obdelava poteka v skladu z določbami GDPR, drugih predpisov in SUVI.

(2) Dokumentacija iz prejšnjega odstavka obsega tako dokazila o razvoju, upravljanju in vzdrževanju informacijske infrastrukture za obdelavo, uporabniško dokumentacijo rešitev, storitev in sistemov za obdelavo, evidenco dejavnosti obdelave, ocene tveganj, ocene učinkov, poročila o obravnavanju kršitev VOP, varnostne politike, kakor tudi revizijske sledi postopkov obdelave in poročila o notranjih presojah in zunanjih revizijah, inšpekcijskih nadzorih in drugih preverjanjih skladnosti poslovanja s strani pristojnih organov oz. pooblaščenih organizacij.

(3) Način vodenja dokumentacije SUVI je opredeljen v Politiki varovanja, ki jo sprejme direktor ZD Domžale in jo objavi na spletni strani ZD Domžale in na intranetu ZD Domžale.

III. ZAKONITE PODLAGE IN EVIDENTIRANJE OBDELAVE OSEBNIH PODATKOV

## 1. Pridobitev zakonite podlage in določitev namena obdelave

### a) Pravne podlage obdelave osebnih podatkov

9. člen

Osebni podatki se lahko obdelujejo, kadar je izpolnjen vsaj eden izmed naslednjih pogojev:
- če je obdelava potrebna za izpolnitev zakonske obveznosti,
- če je za obdelavo podana osebna privolitev posameznika,
- če se obdelujejo osebni podatki posameznikov, ki so sklenili pogodbo ali pa so na podlagi zahteve posameznika z njim v fazi pogajanj za sklenitev pogodbe ali če je obdelava osebnih podatkov potrebna in primerna za izvajanje ukrepov pred sklenitvijo pogodbe ali za izvajanje pogodbe ali,
- če je obdelava osebnih podatkov potrebna zaradi uresničevanja zakonitih interesov, razen kadar nad takimi interesi prevladajo interesi ali človekove pravice in temeljne svoboščine posameznika, na katerega se nanašajo osebni podatki, ki zahtevajo VOP, zlasti kadar je posameznik, na katerega se nanašajo osebni podatki, otrok.

### b) Privolitev posameznika

10. člen

(1) Osebne podatke na podlagi osebne privolitve posameznika se obdeluje takrat, ko obdelave, ki je potrebna za zakonito poslovanje, ni mogoče izvajati na podlagi zakona, pogodbe ali zakonitega interesa.

(2) Utemeljitev uporabe osebne privolitve posameznika kot pravne podlage za obdelavo in osnutek besedila privolitve, ki bo v zvezi z obdelavo posredovana posamezniku, pripravi skrbnik procesa, v okviru katerega bodo obdelovani s privolitvijo posameznika zbrani osebni podatki. K utemeljitvi in osnutku besedila privolitve mora pridobiti tudi mnenje DPO.

### c) Zakoniti interes

11. člen

(1) Obdelavo podatkov na podlagi zakonitega interesa utemelji z oceno učinka, s katero se opredeli zakoniti interes in oceni morebitno prevlado interesov posameznikov, katerih podatki naj bi se obdelovali, nad zakonitim interesom ZD Domžale.

(2) Nosilec izdelave ocene iz prejšnjega odstavka je skrbnik procesa, katerega del naj bi bila predmetna obdelava. Mnenje k oceni mora podati tudi DPO.

### č) Namen in obseg obdelave osebnih podatkov

12. člen

(1) Osebni podatki se zbirajo 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 sklenitve pogodbe, na podlagi katere se bo izvajala obdelava.

(2) Obdelava osebnih podatkov za druge namene od tistih, 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 ta zakon. Za ugotovitev, ali je namen nadaljnje obdelave združljiv z namenom, za katerega so bili osebni podatki prvotno zbrani, mora odgovorna oseba predmetne evidence pred začetkom obdelave za druge namene pisno oceniti, ali je obdelava za drug namen združljiva z namenom, za katerega so bili osebni podatki prvotno zbrani ter pridobiti tudi mnenje DPO. DPO pisno oceno skupaj s svojim mnenjem posreduje v potrditev direktorju ZD Domžale. Pisna ocena, mnenje in odločitev direktorja ZD Domžale morajo biti v pisni obliki shranjeni v okviru dokumentacije SUVI.

(3) 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.

### d) Obdelava posebnih vrst osebnih podatkov

13. člen

(1) Posebne vrste osebnih podatkov se lahko 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.

(2) Posebne vrste osebnih podatkov se iz evidenc obdelav smejo posredovati drugim posameznikom ali osebam javnega ali zasebnega sektorja le, če to določa zakon, ali na podlagi pisne zahteve ali pisne privolitve posameznika, na katerega se nanašajo.

## 2. Vzpostavitev evidenc obdelav in evidentiranje dejavnosti obdelave

### a) Vzpostavitev evidenc obdelav

14. člen

(1) Za vsako evidenco obdelav osebnih podatkov se pisno določi:
- naziv evidence,
- odgovorno osebo evidence, če to potrebno,
- pravno podlago za obdelavo,
- namen(e) obdelave,
- opis kategorij posameznikov, na katere se nanašajo osebni podatki,
- vrste osebnih podatkov,
- kategorije uporabnikov, ki so jim bodo razkriti osebni podatki, vključno z uporabniki v tretjih državah ali mednarodnih organizacijah,
- kadar je mogoče, predvidene roke za izbris različnih vrst podatkov.

(2) Opis evidence se v pisni obliki shrani v dokumentacijo SUVI.

### b) Vodenje evidence dejavnosti obdelave

15. člen

(1) ZD Domžale za namen dokazovanja skladnosti postopkov obdelave osebnih podatkov z veljavnimi predpisi hrani evidenco zapisov o dejavnostih obdelav, s katerimi upravlja. Podatki evidence so dostopni zaposlenim ZD Domžale in nadzornim organom.

(2) Evidenca dejavnosti obdelave osebnih podatkov obsega najmanj naslednje podatke:
- kontaktne podatke ZD Domžale,
- naziv evidence,
- odgovorno osebo dejavnosti obdelave,
- pravno podlago za obdelavo,
- namene obdelave,
- morebitno obdelavo za namene avtomatiziranega odločanja in profiliranja,
- opis kategorij posameznikov, na katere se nanašajo osebni podatki, in vrst osebnih podatkov,
- pravice posameznikov, na katere se nanašajo osebni podatki,
- kategorije uporabnikov, ki jim bodo razkriti osebni podatki, vključno z uporabniki v tretjih državah ali mednarodnih organizacijah,
- informacije o prenosih osebnih podatkov v tretjo državo ali mednarodno organizacijo, vključno z identifikacijo te tretje države ali mednarodne organizacije, v primeru prenosov v tretjo državo ali mednarodno organizacijo, za katero še ni bil izdan sklep o skladnosti pa tudi dokumentacijo o ustreznih zaščitnih ukrepih,
- predvidene roke za izbris podatkov,
- splošni opis tehničnih in organizacijskih varnostnih ukrepov.

**c) Pogodbena obdelava osebnih podatkov**

16. člen

(1) ZD Domžale lahko obdelavo osebnih podatkov zaupa pogodbenemu obdelovalcu, ki zagotovi zadostna jamstva, zlasti v smislu strokovnega znanja, zanesljivosti in virov za izvajanje tehničnih in organizacijskih ukrepov, vključno z varnostjo obdelave. Pred sklenitvijo pogodbe se od obdelovalca zahteva, da predstavi organizacijske in tehnične ukrepe, s katerimi zagotavlja varno obdelavo v skladu s predpisanimi zahtevami.

(2) V zvezi z obdelavo, ki se jo zaupa obdelovalcu, ZD Domžale z obdelovalcem sklene pisno pogodbo o obdelavi, s katero določi kontaktne podatke in DPO pogodbenih strank, vrsto in način izvajanja obdelave ter navodila obdelovalcu glede obdelave osebnih podatkov, morebitne prenose obdelovanih podatkov v tretje države, opis tehničnih in organizacijskih varnostnih ukrepov, ki se morajo izvajati v zvezi z obdelavo, ter druge obveznosti in pravice obeh strank.

(3) Pogodba iz prejšnjega odstavka zlasti določa, da obdelovalec:
1. obdeluje le tiste osebne podatke in le za namen kot je določeno v pogodbi ter osebne podatke obdeluje samo po dokumentiranih navodilih ZD Domžale, vključno glede prenosov osebnih podatkov v tretjo državo ali mednarodno organizacijo, razen če to od njega zahteva veljavna zakonodaja, vendar mora v takšnem primeru obdelovalec obstoj takih pravnih podlag sporočiti ZD Domžale še pred začetkom izvajanja pogodbe, razen, če zakon določa drugače zaradi bistvenega javnega interesa,
2. zagotovi, da so osebe, ki bodo izvajale obdelavo, zavezane k varovanju zaupnosti,
3. sprejme vse ukrepe za varnost obdelave, predvidene s predpisi, ki urejajo varstvo osebnih podatkov in s tem pravilnikom,
4. morebitnega drugega (pod)obdelovalca zaposli samo na podlagi predhodnega dovoljenja ZD Domžale,
5. ob upoštevanju narave obdelave z ustreznimi tehničnimi in organizacijskimi ukrepi ZD Domžale pomaga pri izpolnjevanju njegovih obveznosti, da odgovori na zahteve za uresničevanje pravic posameznika, na katerega se nanašajo osebni podatki,
6. ZD Domžale pomaga pri izpolnjevanju zahtev, vezanih na avtomatizirano odločanje in profiliranje, spoštovanju varstva posameznikov pri prenosu njihovih podatkov v tretje države ali mednarodne organizacije in pri izpolnjevanju obveznosti glede zagotavljanja varnosti obdelave, ki je predmet

pogodbe, ter obravnavi posameznikove zahteve, da se mu nemudoma posreduje vse podatke, ki se nanašajo na obdelavo,

7. na zahtevo ZD Domžale po zaključku storitve obdelave izbriše ali ZD Domžale vrne vse podatke ter uniči morebitne kopije, če veljavni predpisi ne določajo drugače,
8. revizorju, ki ga pooblasti ZD Domžale, ali Informacijskemu pooblaščencu, na voljo vse informacije, potrebne za dokazovanje skladnosti obdelave s predpisanimi zahtevami, in pri dokazovanju sodeluje ter omogoči preverjanja, vključno s kontrolami, ki jih izvede ZD Domžale ali z njene strani DPO ter sodeluje pri njihovi izvedbi,
9. da ZD Domžale pravočasno obvesti, če meni, da je določeno navodilo iz pogodbe ali dogovora ali na njuni podlagi v nasprotju z določbami predpisov, ki urejajo varstvo osebnih podatkov.

(4) Pogodbeni obdelovalec ne sme zadolžiti drugega obdelovalca brez predhodnega dovoljenja ZD Domžale.

(5) Pogodbeni obdelovalec in katera koli oseba, ki pri njem izvaja obdelavo in ima dostop do osebnih podatkov, teh podatkov ne sme obdelati brez navodil ZD Domžale, če ni z veljavnimi predpisi določeno drugače. Za obdelovalca in njegove zaposlene veljajo enake obveznosti VOP kot za zaposlene ZD Domžale.

(6) Pogodbeni obdelovalec zagotovi vsaj takšno raven varnosti obdelave, kot jih zahtevajo GDPR in drugi predpisi ter ta pravilnik. V zvezi s postopki obdelave mora izvajati ukrepe, ki omogočajo naknadno ugotavljanje, kdo in kdaj je izvedel obdelovalni postopek na določenem osebnem podatku.

(7) Če pride do varnostnega incidenta, ki se nanaša na obdelavo osebnih podatkov po pogodbi, je pogodbeni obdelovalec dolžan nemudoma, najpozneje pa v roku 12 ur, o incidentu pisno obvestiti ZD Domžale, in sicer na kontaktno točko, določeno v pogodbi ter navesti aktivnosti, ki jih je izvedel, da je zavaroval osebne podatke in ukrepe, ki jih je po varnostnem incidentu izvedel, da do tovrstnih varnostnih incidentov ne bi več prišlo.

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

### Obveščanje posameznika o obdelavi podatkov, ki se nanašajo nanj

17. člen

(1) ZD Domžale posameznika, v zvezi s katerim se bodo zbirali podatki, obvesti o obstoju izvajanja obdelave in namenih obdelave. Obveščanje posameznika o obdelavi se izvaja:

- z informiranjem o obdelavi osebnih podatkov v fazi sklepanja pogodbe, katere del bo obdelava osebnih podatkov, s posameznikom, na katerega se bodo nanašali obdelovani podatki,
- z vključitvijo informacij o obdelavi v besedilo privolitve posameznika v obdelavo podatkov, ki se nanašajo nanj,
- z obveščanjem posameznikov v primeru, da so osebni podatki pridobljeni od tretjih oseb.

(2) Besedila informacij iz prejšnjega odstavka morajo obsegati najmanj obvestila o:

- imenu in kontaktnih podatkih ZD Domžale,
- kontaktnih podatkih DPO,
- namenih, za katere se osebni podatki obdelujejo in pravni podlagi za njihovo obdelavo,
- obstoju pravice do vložitve pritožbe pri Informacijskem pooblaščencu in njegove kontaktne podatke,

- obstoju pravice posameznika, na katerega se nanašajo osebni podatki, do popravka ali izbrisa podatkov, omejitve obdelave ter do prenosljivosti podatkov,
- roku hrambe osebnih podatkov,
- kategorijah uporabnikov osebnih podatkov, tudi uporabnikov v tretjih državah in mednarodnih organizacijah,
- obstoju avtomatiziranega sprejemanja odločitev, vključno z oblikovanjem profilov ter vsaj v takih primerih smiselne informacije o razlogih zanj, kot tudi pomen in predvidene posledice take obdelave za posameznika, na katerega se nanašajo osebni podatki, in
- pravici ugovora v zvezi z obdelavo iz prejšnje alineje.

(3) Besedila informacij iz prejšnjega odstavka pripravi in vzdržuje DPO.

## V. VARNOST OBDELAVE OSEBNIH PODATKOV

### 1. Organizacijski ukrepi

#### a) Vgrajeno in privzeto varstvo podatkov

18. člen

(1) ZD Domžale dosledno sledi pravilu vgrajenega in privzetega VOP, ki obsega predvsem:
- minimizacijo obdelave osebnih podatkov,
- čimprejšnjo psevdonimizacijo ali anonimizacijo osebnih podatkov, kjer je to mogoče,
- preglednost pri nalogah in obdelavi osebnih podatkov,
- omogočanje posameznikom, na katere se nanašajo osebni podatki, da spremljajo obdelavo podatkov, in
- omogočanje upravljavcu, da vzpostavi in izboljša varnostne ukrepe.

(2) Pri razvoju, oblikovanju, izboru in uporabi aplikacij, storitev in produktov, ki temeljijo na obdelavi osebnih podatkov, ali ki pri opravljanju svoje funkcije obdelujejo osebne podatke, morajo razvijalci oziroma izdelovalci rešitev oziroma produktov ali storitev, namenjenih obdelavi, ki jih izvaja ZD Domžale ali njeni obdelovalci, pri razvoju in oblikovanju takih rešitev, produktov ali storitev upoštevati pravico do VOP ter ob upoštevanju najnovejših tehnoloških možnosti, zagotoviti, da bo ZD Domžale in njeni obdelovalci zmožni izpolnjevati svoje obveznosti VOP. Pravilo vgrajenega in privzetega VOP, ZD Domžale upošteva tudi pri zunanjih naročilih izdelave rešitev oziroma pri nabavi opreme za obdelavo.

(3) Za izvajanje pravila vgrajenega in privzetega VOP so v ZD Domžale odgovorni vodje projektov za izdelavo rešitev oziroma uvedbo produktov in storitev obdelave podatkov oziroma skrbniki procesov, katerih poslovanje bodo nove rešitve/produkti/storitve podprli.

(4) Svetovanje in nadzor nad upoštevanjem oziroma spoštovanjem pravila vgrajenega in privzetega VOP v okviru obdelave osebnih podatkov izvaja DPO.

#### b) Kakovost obdelovanih podatkov

19. člen

Osebni podatki, ki se obdelujejo v ZD Domžale, morajo biti točni, ažurni, ustrezni in po obsegu primerni glede na namene, za katere se obdelujejo, za kar so dolžni poskrbeti skrbniki evidenc in končni uporabniki osebnih podatkov.

## 2. Ocena tveganj in ocena učinka

### a) Ocena tveganj informacijske varnosti

20. člen

(1) ZD Domžale redno izvaja oceno tveganja, ki vpliva ali bi lahko vplivalo na varnost obdelave podatkov, in sicer po postopku, ki obsega zlasti:
- identifikacijo oziroma odkrivanje groženj ali nevarnosti,
- ugotovitev, kateri viri bi bili lahko izpostavljen 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.

(2) Za koordinacijo izvajanje ocen tveganja vezanega je odgovoren skrbnik SUVI.

### b) Ocena učinka v zvezi z varstvom osebnih podatkov

21. člen

(1) Predhodna ocena učinka v zvezi z VOP (v nadaljnjem besedilu: DPIA) je obvezna za vsako novo obdelavo osebnih podatkov v ZD Domžale, če je na seznamu vrst dejanj obdelave, za katere je DPIA obvezna, ki ga pripravi Informacijski pooblaščenec (nove tehnologije, oblikovanje profilov ter sprejemanje odločitev, ki imajo pravne učinke na posameznika, obsežno spremljanje javno dostopnega območja, obsežna obdelava posebnih vrst osebnih podatkov…). DPIA se pripravi tudi kadar ZD Domžale oceni, da bi lahko določena obdelava osebnih podatkov, četudi ni na seznamu obvezne izdelave DPIA, povzročila veliko tveganje za pravice in svoboščine posameznikov. V eni oceni je lahko obravnavan niz podobnih dejanj obdelave, ki predstavljajo podobna velika tveganja.

(2) DPIA zajema vsaj:
- sistematičen opis predvidenih dejanj obdelave in namenov obdelave, kadar je ustrezno pa tudi zakonitih interesov, za katere si prizadeva ZD Domžale,
- oceno potrebnosti in sorazmernosti dejanj obdelave glede na njihov namen,
- oceno tveganj za pravice in svoboščine posameznikov, na katere se nanašajo osebni podatki,
- ukrepe za obravnavanje tveganj, vključno z zaščitnimi ukrepi, varnostne ukrepe ter mehanizme za zagotavljanje VOP in za dokazovanje skladnosti s to GDPR, ob upoštevanju pravic in zakonitih interesov posameznikov, na katere se nanašajo osebni podatki, ter drugih oseb, ki jih to zadeva.

(3) ZD Domžale lahko, po potrebi, glede ocenjevane obdelave, zaprosi za mnenje posameznike, na katere bi se nanašali obdelovani podatki, ali njihove predstavnike (npr. združenja, zbornice).

(4) Ugotovitve DPIA se dokumentirajo v poročilu, ki obsega oceno ali:
- je predlagani način skladen s predpisanimi zahtevami,
- bo za zagotovitev skladnosti treba izvesti dodatne ukrepe, ali je potrebno v zvezi z ocenjevano obdelavo izvesti predhodno posvetovanje z Informacijskim pooblaščencem,
- so ugotovljena tveganja tako visoka, da ocenjevane obdelave ni mogoče izvesti v skladu s predpisanimi zahtevami.

(5) DPIA izdela DPO.

### 3. Spremembe načina obdelave

22. člen

(1) Spremembe informacijskih rešitev ali dokumentacije, ki vplivajo na VOP, lahko izvirajo iz:
- razlogov za izboljšavo ali uvedbo novih rešitev,
- odprave napak na informacijskih rešitvah,
- organizacijskih sprememb ali
- pravnih sprememb.

(2) Razvojno, preizkusno in produkcijsko okolje informacijskih rešitev, s katerimi se izvaja obdelava osebnih podatkov, so vedno popolnoma ločeni.

(3) Vsaka sprememba informacijskih rešitev ali dokumentacije, ki vplivajo na VOP, se najprej preizkuša izključno v razvojnem okolju in izključno z imaginarnimi podatki ali javno dostopnimi digitalnimi vsebinami. Vsaka sprememba se mora ustrezno dokumentirati, in sicer tako, da se označi nova različica, opisno opredelijo vzroki spremembe in bistvene dopolnitve ter določi mesto hrambe nove in prejšnje različice. Vedno se varno hranijo vse različice informacijske rešitve in dokumentacije za nazaj.

(4) 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.

(5) Pred vsakokratno namestitvijo nove različice informacijske rešitve se:
- predvidi način in morebitni problemi namestitve in delovanja v sistemu,
- uspešno preizkusi nova različica v testnem okolju, kar se ustrezno dokumentira,
- skladno s spremembami dopolni oziroma drugače popravi projektna dokumentacija.

(6) Novih različic informacijskih rešitev, ki vplivajo na VOP, ni dopustno nameščati, preden se uspešno in pravilno izvedejo vsa opravila v skladu s prejšnjim odstavkoma.

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

(8) Nadzor nad spoštovanjem pravil upravljanja sprememb izvaja skrbnik SUVI.

### 4. Zagotavljanje neprekinjene obdelave

### a) Načrt neprekinjene obdelave

23. člen

ZD Domžale odgovornost, organiziranje in izvedbo postopkov za zagotovitev neprekinjene obdelave in ohranjanje celovitosti obdelovanih podatkov določi z kot del SUVI, ki temelji na sposobnosti ZD Domžale, 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.

**b) Varnostne kopije**

24. člen

(1) Za potrebe okrevanja ali povratka informacijskega sistema ob hudih okvarah, uničenju ali ob drugih incidentih, ki povzročijo izgubo osebnih podatkov ali prekinitev obdelave, ZD Domžale redno izdelujejo kopije vsebine strežnikov oziroma druge infrastrukture, na katerih se hranijo podatki in programska oprema za obdelavo podatkov.

(2) Informacije o izdelavi elektronskih kopij evidenc so vodene v okviru postopka kontrole sprememb na informacijskem sistemu ZD Domžale, ki določa tudi pogostost izdelave varnostnih kopij, ter v okviru Evidence dejavnosti obdelave.

**c) Varnostni dogodki in incidenti**

25. člen

(1) ZD Domžale določi ukrepe in postopke obravnavanja v primeru kršitev pravil varnosti, določenih v tem pravilniku in drugih aktih ZD Domžale ter v primeru drugih dogodkov, 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 oziroma uničenje opreme za izvajanje obdelave.

(2) Kadar zaradi varnostnega dogodka ali incidenta pride do kršitve VOP, zaradi katere bi bile lahko ogrožene pravice in svoboščine posameznikov, mora biti izdelano in Informacijskemu pooblaščencu poslano obvestilo o kršitvi VOP, skladno z GDPR.

(3) Kadar je verjetno, da kršitev VOP povzroči veliko tveganje za pravice in svoboščine posameznikov, mora ZD Domžale brez nepotrebnega odlašanja o tem obvestiti posameznike, katerih osebni podatki so bili kršeni ali je verjetno, da so bili kršeni. ZD Domžale ne obvesti posameznika o kršitvi, kadar obveščanje skladno z GDPR ni potrebno.

**5. Posredovanje osebnih podatkov**

**a) Postopek posredovanja**

26. člen

(1) Osebni podatki, s katerimi upravlja ZD Domžale, 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.

(2) Posredovanje osebnih podatkov iz prejšnjega odstavka lahko uporabnik zahteva pisno ali ustno. Zahteva za posredovanje vsebuje:

- identifikacijske podatke (za fizično osebo: osebno ime, naslov opravljanja dejavnosti ali naslov stalnega ali začasnega prebivališča, za samostojnega podjetnika posameznika, posameznika, ki samostojno opravlja dejavnost, ter za pravno osebo: naziv oziroma firmo in naslov oziroma sedež in matično številko) ter podpis pooblaščene osebe,
- pravno podlago za pridobitev zahtevanih osebnih podatkov,
- namen obdelave osebnih podatkov oziroma razloge, ki izkazujejo potrebnost in primernost osebnih podatkov za dosego namena pridobitve,
- predmet in številko ali drugo identifikacijo zadeve, v zvezi s katero so osebni podatki potrebni,

- vrste osebnih podatkov, ki naj se mu posredujejo, in
- obliko in način pridobitve zahtevanih osebnih podatkov.

(3) 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. Če uporabnik zahteva posredovanje osebnih podatkov ustno, sme odgovorna oseba v primeru dvoma o obstoju pisnega soglasja posameznika, na katerega se podatki nanašajo, od uporabnika zahtevati, naj ga predloži.

(4) Podjetje vlagatelju zahteve, če zakon ne določa drugače, zahtevane osebne podatke posreduje najpozneje v 15 dneh od prejema popolne zahteve, ali pa ga v tem roku pisno obvesti o razlogih, zaradi katerih mu zahtevanih osebnih podatkov ne bo posredoval.

### b) Evidentiranje posredovanj

27. člen

(1) Vsako posredovanje osebnih podatkov se vpiše v evidenco posredovanj z navedbo naslednjih podatkov:
- kateri osebni podatki so bili posredovani,
- osebno ime/firmo in naslov/sedež osebe, ki so ji bili posredovani osebni podatki, oziroma navedba, da je bilo posredovanje opravljeno po uradni dolžnosti,
- datum posredovanja osebnih podatkov in
- pravna podlaga, na podlagi katere so bili posredovani osebni podatki.

(2) Evidenca posredovanj se hrani neizbrisno v elektronski obliki, vpis pa opravi končni uporabnik podatkov, ki je osebne podatke posredoval uporabniku. Podatki o posameznem posredovanju se hranijo tri leta.

## 6. Fizični in tehnični ukrepi varovanja obdelave

### a) Varovanje poslovnih prostorov

28. člen

Varovanje poslovnih prostorov je določeno z dokumentacijo SUVI.

### b) Varovanje dostopa do IT opreme in infrastrukture

29. Člen

(1) Varovanje dostopa do strojne in programske opreme je določeno z dokumentacijo SUVI. 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.

(2) Vzdrževanje in popravila strojne računalniške in druge opreme je dovoljeno samo z vednostjo osebe, odgovorne za delovanje informacijskega sistema ZD Domžale, izvajajo pa ga lahko samo pooblaščeni zaposleni oziroma serviserji in vzdrževalci, ki imajo s ZD Domžale sklenjeno ustrezno pogodbo.

(3) Dostopi do programske opreme morajo biti beleženi z revizijsko sledjo.

(4) Popravljanje, spreminjanje in dopolnjevanje sistemske in aplikativne programske opreme je dovoljeno samo na podlagi odobritve osebe, odgovorne za delovanje informacijskega sistema, izvajajo pa ga lahko samo organizacije in posamezniki (v nadaljnjem besedilu: izvajalci), ki imajo s ZD Domžale sklenjeno ustrezno pogodbo. Izvajalci morajo spremembe in dopolnitve sistemske in aplikativne programske opreme ustrezno dokumentirati.

(5) Za shranjevanje in varovanje aplikativne programske opreme veljajo enake zahteve, kot za podatke.

(6) Vsebina diskov omrežnega strežnika in delovnih postaj, povezanih v omrežje, na katerih se nahajajo osebni podatki, se vsakodnevno preveri z vidika prisotnosti računalniških virusov. Zaznava računalniškega virusa se obravnava kot varnostni incident.

(7) Vsi podatki in programska oprema, ki so namenjeni uporabi v računalniškem informacijskem sistemu, in prispejo v ZD Domžale na prenosnih medijih ali preko komunikacijskih kanalov, morajo biti pred uporabo pregledani, da na njih ni računalniških virusov.

(8) Zaposleni na informacijsko opremo ne smejo namestiti programske opreme brez vednosti osebe, odgovorne za delovanje informacijskega sistema. Prav tako iz prostorov ZD Domžale brez odobritve in vednosti osebe, odgovorne za informacijski sistem ne smejo odnašati programske opreme ZD Domžale.

## 7. Nadzor dostopa do obdelovanih osebnih podatkov

30. člen

(1) Dostop končnih uporabnikov do osebnih podatkov mora biti kontroliran s sistemom gesel oziroma drugih avtentikacijskih sredstev, povezanih s sistemom za upravljanje pravic posameznika za uporabo določenih informacijskih rešitev/sistemov in določenih vrst/evidenc osebnih podatkov.

(2) Zaposlenemu obseg dostopnih pravic za obdelavo osebnih podatkov oziroma uporabo informacijskega sistema, ki je nujno potreben za izvajanje njegovih delovnih nalog, določi po postopku, določenem v dokumentaciji SUVI.

## 8. Sledljivost dostopov do podatkov

31. člen

(1) ZD Domžale v zvezi z dostopi do podatkov izvaja ukrepe, ki omogočajo poznejše ugotavljanje, kdaj so bile posamezne vrste osebnih podatkov vnesene v evidenco osebnih podatkov, uporabljene ali drugače obdelane in kdo je to storil, in sicer za obdobje, ko je mogoče zakonsko varstvo pravice posameznika zaradi nedopustnega posredovanja ali obdelave osebnih podatkov.

(2) Ukrepi iz prejšnjega odstavka morajo biti primerni glede na tehnološko stanje informacijskega sistema ZD Domžale, na naravo, obseg, okoliščine in namene obdelave ter resnost in verjetnost tveganj za človekove pravice in temeljne svoboščine posameznikov, ki nastajajo pri obdelavi, lahko pa se upošteva tudi stroške njihovega izvajanja. ZD Domžale mora odločitev o načinu zagotavljanja sledljivosti obdelave pisno dokumentirati.

(3) Kadar se ukrepi iz prvega odstavka izvajajo s tvorjenjem sledilnega zapisa o dostopih do avtomatsko obdelanih podatkov, se zapisi hranijo v obliki evidence revizijskih sledi. Pravna podlaga za vodenje in obdelavo evidence revizijskih sledi je zakoniti interes ZD Domžale, da je sposoben dokazati, da obdelavo izvaja v skladu z GDPR in predpisi, ki urejajo varstvo osebnih podatkov.

(4) Odgovorna osebe evidence revizijskih sledi je DPO, ki določi, kdo in v katerih primerih dostopa do zapisov revizijskih sledi.

## VI. KRŠITEV VARSTVA OSEBNIH PODATKOV

32. člen

(1) Zaposleni mora v zvezi s kršitvijo VOP, ki lahko povzroči fizično, premoženjsko ali nepremoženjsko škodo, kot je izguba nadzora nad njihovimi osebnimi podatki ali omejitev njihovih pravic, diskriminacija, kraja ali zloraba identitete, finančna izguba, okrnitev ugleda, izguba zaupnosti osebnih podatkov, zaščitenih s poklicno skrivnostjo, ali katera koli druga znatna gospodarska ali socialna škoda, ukrepati v skladu z dokumentacijo SUVI.

(2) Kadar obdelavo izvaja pogodbeni obdelovalec, je potrebno zahteve iz prejšnjega odstavka vključiti v pogodbo o obdelavi osebnih podatkov in k njihovem izvajanju zavezati tudi osebje pogodbenega obdelovalca.

## VII. ODGOVORNOST ZA IZVAJANJE POSTOPKOV IN UKREPOV ZA ZAVAROVANJE OSEBNIH PODATKOV

### a) Izvajanje postopkov in ukrepov varstva in varovanja podatkov

33. člen

(1) Vsi zaposleni so dolžni izvajati določene ukrepe za VOP skladno s SUVI ter varovati zaupnost osebnih podatkov, s katerimi so se seznanili pri opravljanju svojega dela. Obveza varovanja podatkov ne preneha s prenehanjem delovnega razmerja.

(2) Kadar obdelavo izvaja obdelovalec, je potrebno zahteve iz prejšnjega odstavka vključiti v pogodbo o obdelavi osebnih podatkov in k njihovem izvajanju zavezati tudi osebje obdelovalca.

### b) Obvestilo o dolžnosti varstva osebnih podatkov

34. člen

(1) Pogodba o zaposlitvi v ZD Domžale mora obsegati obvestilo o obveznostih zaposlenega glede varstva in varovanja osebnih podatkov.

(2) Zaposleni pred nastopom dela podpiše izjavo, iz katere izhaja, da je seznanjen z veljavno zakonodajo, ki ureja področje varovanja osebnih podatkov, ter z vsebino tega pravilnika.

(3) Zunanji sodelavci ZD Domžale, ki se v okviru izvajanja pogodbenih del seznanijo ali bi se lahko seznanili z osebnimi podatki, s katerimi upravlja ZD Domžale, pred začetkom izvajanja pogodbenih del podpišejo izjavo, ki vsebuje obvestilo iz prvega odstavka tega člena.

### c) Odgovornost za kršitev

35. člen

(1) Zaposleni so dolžni o aktivnosti, ki je usmerjena v odkrivanje ali nepooblaščeno uničenje osebnih podatkov, kakor tudi o nepravilni, zlonamerni ali nepooblaščeni uporabi, prilaščanju, odstopanju, prikrivanju, spreminjanju ali poškodovanju osebnih podatkov, takoj obvestiti pooblaščenega delavca ali svojega vodjo, sami pa poskušajo tako aktivnost odpraviti.

(2) Kršitev določil tega pravilnika s strani zaposlenih pomeni kršitev obveznosti iz delovnega razmerja, pogodbeni obdelovalci in zunanji pogodbeni partnerji ZD Domžale pa za kršitve odgovarjajo na temelju pogodbenih obveznosti.

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

### d) Izvajanje notranjega nadzora nad varstvom osebnih podatkov

36. člen

(1) Redni nadzor nad izvajanjem postopkov in ukrepov VOP in varnosti obdelave, določenih s tem pravilnikom, relevantnimi predpisi in veljavnimi pogodbami izvaja DPO.

(2) Letne presoje izvajanja ukrepov VOP izvaja delovna skupina, sestavljena iz zaposlenih ZD Domžale in, če je potrebno, zunanjih sodelavcev, ki jih za izvedbo posamezne letne presoje imenuje direktor ZD Domžale.

(3) Na podlagi ugotovitev nadzorov in presoj DPO pripravi letno poročilo o stanju VOP v ZD Domžale, ki ga enkrat letno v obliki vodstvenega pregleda varstva osebnih podatkov obravnava direktor ZD Domžale in svet zavoda.

Mag. Renata Rajapakse, dr. med. spec.
direktorica

ZDRAVSTVENI DOM DOMŽALE Mestni trg 2 1230 DOMŽALE

Digitalno podpisal RENATA RAJAPAKSE