Na podlagi Splošne Uredbe (EU) 2016/679 Evropskega parlamenta in Sveta z dne 27. aprila 2016 o varstvu posameznikov pri obdelavi osebnih podatkov in o prostem pretoku takih podatkov ter o razveljavitvi Direktive 95/46/ES (Splošna uredba o varstvu podatkov; v nadaljevanju Uredba), v skladu z zakonodajo na področju varstva osebnih podatkov in 18.člena Statuta Onkološkega inštituta Ljubljana je generalna direktorica Zlata Štiblar Kisić dne 3.7.2019 sprejela

P R A V I L N I K
O VARSTVU OSEBNIH IN DRUGIH PODATKOV NA ONKOLOŠKEM INŠTITUTU LJUBLJANA

I. SPLOŠNE DOLOČBE

1. člen
(vsebina in namen pravilnika)

S tem pravilnikom se določajo organizacijski, tehnični in logično-tehnični postopki in ukrepi za zavarovanje osebnih podatkov na Onkološkem inštitutu Ljubljana (v nadaljevanju OI) z namenom, da se:

(1) vzpostavijo ustrezni postopki in ukrepi za zagotovitev zakonitega in odgovornega ravnanja z osebnimi podatki pri delodajalcu,
(2) ozavesti vse zaposlene glede določb zakonodaje o varstvu osebnih podatkov, dolžnem ravnanju in obveznostih delodajalca in zaposlenih,
(3) zagotovi celovitost, zaupnost in razpoložljivost osebnih podatkov, tako da se prepreči slučajno ali namerno nepooblaščeno uničevanje podatkov, njihova sprememba ali izguba ter nepooblaščena obdelava osebnih podatkov.

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 osebnih podatkov** je 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.
(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) **Odgovorna oseba zbirke** je zaposleni ali zunanji sodelavec OI, odgovoren za obdelavo podatkov iz posamezne zbirke osebnih podatkov;
(13) **Informacijski sistem** je programska, strojna, komunikacijska in druga oprema OI, ki deluje samostojno ali v omrežju in je namenjena zbiranju, procesiranju, distribuciji, uporabi in drugi obdelavi osebnih podatkov;
(14) **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 JZZ in posega v integriteto informacijskega sistema;
(15) **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;
(16) **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;
(17) **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;
(18) **Analiza varnostnih tveganj** je sistematična uporaba informacij za prepoznavanje virov groženj in ranljivosti sredstev ter ocenjevanje tveganj za varnost osebnih podatkov oz. obdelavo;
(19) **SUVI** je kratica za krovno politiko varovanja informacij;
(20) **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.
(21) **Sistemski administrator** je oseba, ki skrbi za delovanje sistemske opreme.
(22) **Skrbnik informacijskega sistema** je oseba, ki skrbi za vsebinsko delovanje informacijskega sistema.

3. Člen
(temeljna načela varstva osebnih podatkov)

Osebni podatki:

(1) se obdelujejo zakonito, tako da so v skladu z 9. členom tega pravilnika določene pravne podlage za njihovo konkretno obdelavo, ter da se obdelujejo pošteno in na pregleden način za posameznika, tako da se ne obdelujejo za prikrite ali drugače nepoštene namene, zato da se posamezniki lahko svobodno odločijo, ali bodo sodelovali pri obdelavi njihovih osebnih podatkov oziroma da lahko temu zakonito in učinkovito ugovarjajo (zakonitost, poštenost in preglednost);
(2) se zbirajo za določene, izrecne in zakonite namene ter se ne smejo nadalje obdelovati na način, ki ni združljiv s temi nameni (omejitev namena);
(3) so ustrezni, relevantni in omejeni na to, kar je potrebno za namene, za katere se obdelujejo (najmanjši obseg podatkov);
(4) so točni in, kadar je to potrebno, posodobljeni; sprejeti je treba vse razumne ukrepe za zagotovitev, da se netočni osebni podatki brez odlašanja izbrišejo ali popravijo ob upoštevanju namenov, za katere se obdelujejo (točnost in ažurnost);
(5) se hranijo v obliki, ki dopušča identifikacijo posameznikov, na katere se nanašajo osebni podatki, le toliko časa, kolikor je potrebno za namene, za katere se osebni podatki obdelujejo, razen če je z zakonom določen drug rok hrambe (omejitev roka hrambe);
(6) se obdelujejo na način, ki zagotavlja ustrezno varnost osebnih podatkov, vključno z zaščito pred nedovoljeno ali nezakonito obdelavo, pred nenamerno izgubo, uničenjem, poškodbo ali izgubo razpoložljivosti, z ustreznimi tehničnimi ali organizacijskimi ukrepi (celovitost, zaupnost in razpoložljivost).

II. VARSTVO OSEBNIH PODATKOV

Odgovornost in organiziranost

4. člen
(odgovornost vodstva)

(1) OI zagotavlja ustrezne in učinkovite ukrepe za izvajanje obdelave v skladu s predpisanimi in pogodbeno dogovorjenimi zahtevami ter za dokazovanje skladnosti dejavnosti obdelave z omenjenimi zahtevami.
(2) OI odgovornosti iz prejšnjega odstavka uresničuje zlasti:
s sprejetjem tega pravilnika, navodil, politik, načrtov in drugih notranjih aktov, s katerimi določi:
- postopke za vzpostavitev zakonitih podlag za obdelavo osebnih podatkov, s katerimi OI upravlja;
- postopke za obravnavanje zahtevkov oziroma ugovorov posameznikov, katerih podatke OI 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;
- z ustrezno pogodbeno ureditvijo obdelave s strani obdelovalca;
- z imenovanjem zaposlenih, ki so odgovorni za določene zbirke in zaposlenih, ki upravljajo z osebnimi podatki iz posamezne zbirke;

- z imenovanjem pooblaščene osebe za varstvo osebnih podatkov;
- z imenovanjem Komisije za nadzor izvajanja določil Pravilnika o varstvu osebnih podatkov;
- z imenovanjem delovne skupine za informacijsko varnost;
- z notranjo presojo ter vodstvenim pregledom ustreznosti in učinkovitosti ukrepov za zagotavljanje varnosti obdelave

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

(1) Generalni direktor OI imenuje pooblaščeno osebo za varstvo osebnih podatkov (ki pri izvajanju funkcije ne bo prišla v nasprotje interesov) skladno z Uredbo, tem pravilnikom in aktom o sistemizaciji delovnih mest na OI.
(2) Generalni direktor OI 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.
(3) Generalni direktor OI zagotovi, da je pooblaščena oseba ustrezno in pravočasno obveščena o vseh zadevah v zvezi z varstvom osebnih podatkov, ki so del izvajanja registriranih dejavnosti OI. Obveščanje pooblaščene osebe se izvaja:
   - z njenim udeleževanjem na sestankih uprave, oddelkov ali enot ali projektnih 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;
(4) Generalni direktor OI pooblaščeni osebi zagotovi vsa sredstva, potrebna za izvajanje njenih nalog, kamor poleg IT in druge opreme sodijo zlasti dostopi do:
   - osebnih podatkov in revizijskih sledi v zbirkah in drugih oblikah obdelave osebnih podatkov;
   - podatkov o kršitvah varstva osebnih podatkov;
   - zaposlenih v OI in pri obdelovalcu, ki delajo na nalogah, povezanih z varstvom osebnih podatkov; in dostopom do
   - virov in oblik usposabljanj oz. izpopolnjevanj, namenjenih vzdrževanju ustrezne ravni strokovnega znanja pooblaščene osebe.

6. člen
(naloge pooblaščene osebe)

(1) Pooblaščena oseba generalnemu direktorju OI na strokovno neodvisen način pomaga pri zagotavljanju skladnosti obdelave osebnih podatkov s pravili Uredbe in veljavne zakonodaje na področju varstva osebnih podatkov.

(2) Pooblaščena oseba izvaja naslednje naloge:
   - obvešča 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;
   - poroča o kršitvah varstva osebnih podatkov informacijskemu pooblaščencu;

- sodeluje s posamezniki, na katere se nanašajo osebni podatki, ki se na zavod obračajo glede vprašanj, povezanih z obdelavo njihovih osebnih podatkov in uresničevanjem 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 jih obravnava;
- koordinira delo, spodbuja, usmerja in daje navodila v zvezi z zgornjimi nalogami;
- dokumentira naloge.

7. člen
(Komisija za nadzor izvajanja določil Pravilnika o varstvu osebnih podatkov)

(1) Generalni direktor imenuje 5 – člansko komisijo, ki je zadolžena za nadzor nad izvajanjem tega pravilnika in zakona, ki ureja varstvo osebnih podatkov.
(2) Komisija se imenuje za obdobje štirih let. Komisijo sestavljajo zaposleni na OI, po en zaposlen izmed zdravnikov, en s področja zdravstvene nege, zdravstvene administracije, službe za informatiko in pravne službe.
(3) Komisija opravlja nadzore nenapovedano najmanj dva krat letno, izjemoma tudi pogosteje.
(4) Komisija o ugotovitvah zapiše zapisnik, ki ga vroči generalnemu direktorju.

8. člen
(delovna skupina za informacijsko varnost)

(1) Generalni direktor OI imenuje skupino za delo na področju varovanja osebnih podatkov (v nadaljnjem besedilu: delovna skupina za informacijsko varnost), ki svetuje na področju načrtovanja, organiziranja in izvajanja ukrepov s katerimi OI varuje osebne podatke ter preprečuje njihovo slučajno, namerno ali drugače nezakonito uničenje, spremembo, izgubo, nepooblaščeno razkritje, dostop ali drugo nepooblaščeno obdelavo.
(2) 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 odgovornimi osebami zbirk, 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 in podaji končnega mnenja pri oceni učinka v zvezi z varstvom osebnih podatkov.
(3) Delovno skupino sestavljata: dva predstavnika Službe za informatiko, predstavnik Službe za kakovost, predstavnik kadrovske službe, predstavnik Tehnično vzdrževalne službe ter predstavnik Administracije.
(4) Pooblaščena oseba za varstvo osebnih podatkov koordinira delovno skupino za informacijsko varnost. Celotna skupina se sestaja po potrebi in je lahko sklicana tudi le delno, o čemer presodi pooblaščena oseba za varstvo osebnih podatkov.

(5) Delovna skupina za informacijsko varnost je odgovorna za vodenje in ustrezno posodabljanje SUVI.

III. ZAKONITE PODLAGE IN EVIDENTIRANJE OBDELAVE OSEBNIH PODATKOV

Pridobitev zakonite podlage in določitev namena obdelave

9. člen
(pravne podlage obdelave osebnih podatkov)

Osebne podatke je dopustno obdelovati v naslednjih primerih:

(1) če obdelavo osebnih podatkov določa zakon;
(2) če gre za obdelavo osebnih podatkov posameznika, ki je z javnim sektorjem sklenil pogodbo ali ki je na svojo zahtevo v pogajanjih z javnim sektorjem za sklenitev pogodbe, če je obdelava osebnih podatkov potrebna za izvajanje pogodbe ali za izvedbo pogajanj za sklenitev pogodbe;
(3) posameznik, na katerega se nanašajo osebni podatki, je privolil v obdelavo njegovih osebnih podatkov v enega ali več določenih namenov;
(4) obdelava je potrebna za zaščito življenjskih interesov posameznika, na katerega se nanašajo osebni podatki, ali druge fizične osebe;
(5) obdelava je potrebna za opravljanje naloge v javnem interesu ali pri izvajanju javne oblasti, dodeljene upravljavcu;
(6) Izjemoma se v javnem sektorju lahko obdelujejo osebni podatki, ki so potrebni za uresničevanje zakonitih interesov javnega sektorja, če pri tem ne gre za izvajanje zakonskih pristojnosti, nalog ali obveznosti javnega sektorja ter če nad temi interesi ne prevladajo človekove pravice in temeljne svoboščine ali interesi posameznika, na katerega se nanašajo osebni podatki;
(7) Privolitev za uporabo in drugo obdelavo osebnih podatkov po tretjem odstavku tega člena ni potrebna:
   - če za namene epidemioloških in drugih raziskav, izobraževanja, medicinskih objav ali druge namene pacientova istovetnost ni ugotovljiva,
   - če za namene spremljanja kakovosti in varnosti zdravstvene obravnave pacientova istovetnost ni ugotovljiva,
   - kadar se zaradi potreb zdravljenja podatki posredujejo drugemu izvajalcu zdravstvene dejavnosti,

10. člen
(namen in obseg obdelave osebnih podatkov)

(1) Osebni podatki se smejo zbirati samo za namene, ki imajo podlago v zakonu ali za namene, ki so določeni v okviru privolitve za obdelavo v kolikor ta obstaja oziroma v pogodbi, na podlagi katere se obdelava izvaja.
(2) 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.
(3) Če je načrtovana obdelava za drug namen, kot za tistega za katerega so bili dotični osebni podatki zbrani, le-ta ni dopustna na podlagi prvotne privolitve, temveč le na podlagi nove privolitve posameznika, v kolikor druga zakonska podlaga ne določa drugače.

11. člen
(obdelava posebnih vrst osebnih podatkov)

(1) Posebne vrste osebnih podatkov se lahko v OI obdelujejo le, če tako obdelavo določa zakon, ali če je posameznik za to podal izrecno pisno privolitev.
(2) Posebne vrste osebnih podatkov se iz evidenc OI, 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.

12. Člen
(posebno varstvo osebnih podatkov umrlih posameznikov)

(1) Osebni podatki umrlih posameznikov se varujejo v skladu zakonom o varstvu podatkov (ZVOP-2) in drugimi zakoni.
(2) OI lahko podatke o umrlem posamezniku posreduje le tistim uporabnikom, ki so za obdelavo osebnih podatkov pooblaščeni z zakonom in tistim, ki izkažejo pravni interes za uveljavljanje pravic pred subjekti javnega sektorja.
(3) Ne glede na določbe prejšnjega odstavka OI osebne podatke o umrlem posamezniku posreduje zakoncu, partnerju v zunajzakonski skupnosti ter partnerjem z njima izenačenih skupnosti, otrokom ali staršem ali dedičem, če umrli posameznik ni pisno prepovedal posredovanja njegovih osebnih podatkov.
(4) Če zakon ne določa drugače, lahko upravljavec podatke o umrlem posamezniku posreduje tudi drugi osebi, ki namerava te podatke uporabljati za zgodovinsko-raziskovalne, znanstveno-raziskovalne, statistične ali arhivske namene.
(5) V zgodovinskih in drugih izobraževalnih publikacijah v fizični ali elektronski obliki se lahko objavljajo zakonito pridobljeni osebni podatki umrlih posameznikov, če tako določa zakon, če je privolitev pred smrtjo dal posameznik sam ali če je za takšno objavo v času po smrti posameznika podana pisna privolitev naslednjih oseb v izključujočem vrstnem redu: zakonec ali partner iz zunajzakonske skupnosti ali partner z njima z zakonom izenačene skupnosti, otroci ali starši umrlega posameznika.

Vzpostavitev zbirke in evidentiranje dejavnosti obdelave

13. člen
(vzpostavitev zbirke)

Pred začetkom zbiranja osebnih podatkov je potrebno vzpostaviti zbirko, ki jo hrani, pooblaščena oseba za varstvo osebnih podatkov.

Ob vzpostavitvi zbirke 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;

14. člen
(vodenje evidence dejavnosti obdelave)

(1) OI vodi evidenco dejavnosti obdelave osebnih podatkov v okviru svoje odgovornosti. Ta evidenca vsebuje vse naslednje informacije:
- naziv ali ime in kontaktne podatke upravljavca in,
- kadar obstajajo, skupnega upravljavca, predstavnika upravljavca in pooblaščene osebe za varstvo podatkov;
- namene obdelave;
- opis kategorij posameznikov, na katere se nanašajo osebni podatki, in vrst osebnih podatkov;
- kategorije uporabnikov, ki so jim bili ali jim bodo razkriti osebni podatki, vključno z uporabniki v tretjih državah ali mednarodnih organizacijah;
- kadar je ustrezno, informacije o prenosih osebnih podatkov v tretjo državo ali mednarodno organizacijo, vključno z identifikacijo te tretje države ali mednarodne organizacije, v primeru prenosov pa tudi dokumentacijo o ustreznih zaščitnih ukrepih;
- kadar je mogoče, predvidene roke za izbris različnih vrst podatkov;
- kadar je mogoče, splošni opis tehničnih in organizacijskih varnostnih ukrepov.

(2) Evidence dejavnosti obdelave, ki je sestavljena iz vseh zbirk osebnih podatkov iz 8. člena tega pravilnika, in jo ureja ter posodablja pooblaščena oseba za varstvo osebnih podatkov na podlagi informacij, pridobljenih s strani odgovorne osebe posameznih evidenc.

Pogodbena obdelava osebnih podatkov

15. člen
(vloga obdelovalca)

(1) Z vsako zunanjo pravno ali fizično osebo, ki opravlja posamezna opravila v zvezi z obdelavo osebnih podatkov, ki jih zbira OI, in ki zagotavljajo zadostna jamstva za izvedbo ustreznih tehničnih in organizacijskih ukrepov (v nadaljevanju pogodbeni obdelovalec), OI sklene pisni sporazum, ki vsebuje tudi določila o načinu varstva in zavarovanja osebnih podatkov pri pogodbenem obdelovalcu.

(2) Pisna pogodba določa obveznosti obdelovalca do upravljavca, vsebino in trajanje obdelave, naravo in namen obdelave, vrste osebnih podatkov, kategorije posameznikov, na katere se nanašajo osebni podatki, ter obveznosti in pravice upravljavca. Pogodba zlasti določa, da obdelovalec:
- osebne podatke obdeluje samo po dokumentiranih navodilih upravljavca, vključno glede prenosov osebnih podatkov v tretjo državo ali mednarodno organizacijo, razen če to od njega zahteva zakonodaja, ki velja za obdelovalca; v slednjem primeru obdelovalec o tej pravni zahtevi pred obdelavo podatkov obvesti upravljavca, razen če zadevno pravo prepoveduje takšno obvestilo na podlagi pomembnih razlogov v javnem interesu;
- zagotovi, da so osebe, ki so pooblaščene za obdelavo osebnih podatkov, zavezane k zaupnosti ali jih k zaupnosti zavezuje ustrezen zakon;
- sprejme vse ukrepe za zagotovitev varnosti osebnih podatkov;
- spoštuje pogoje iz prejšnjega odstavka glede najemanja drugega obdelovalca;
- ob upoštevanju narave obdelave pomaga upravljavcu z ustreznimi tehničnimi in organizacijskimi ukrepi, kolikor je to mogoče, pri izpolnjevanju njegovih obveznosti, da

odgovori na zahteve za uresničevanje pravic posameznika, na katerega se nanašajo osebni podatki, iz poglavja III;
- upravljavcu pomaga pri izpolnjevanju obveznosti iz členov 32 do 36 Splošne uredbe ob upoštevanju narave obdelave in informacij, ki so dostopne obdelovalcu;
- v skladu z navodili upravljavca izbriše ali vrne vse osebne podatke upravljavcu po zaključku storitev v zvezi z obdelavo ter uniči obstoječe kopije, razen če zakonodaja predpisuje shranjevanje osebnih podatkov;
- upravljavcu na voljo vse informacije, potrebne za dokazovanje izpolnjevanja obveznosti iz tega člena, ter upravljavcu ali drugemu revizorju, ki ga pooblasti upravljavec, omogoči izvajanje revizij, tudi pregledov, in pri njih sodeluje.

(3) Določbe tega člena veljajo tudi za pogodbene obdelovalce, ki vzdržujejo obstoječo strojno in programsko opremo ali izdelujejo in inštalirajo novo strojno ali programsko opremo, s katero se obdelujejo osebni podatki

(4) Pogodbeni obdelovalci lahko opravljajo storitve obdelave osebnih podatkov samo v okviru pooblastil iz pogodbe po tem členu in podatkov ne smejo obdelovati ali drugače uporabljati za noben drug namen.

(5) Odgovorne osebe se pri pripravi pogodb s pogodbenimi obdelovalci posvetujejo s pooblaščeno osebo za varstvo osebnih podatkov.

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

Obveščanje posameznika o obdelavi podatkov, ki se nanašajo nanj

16. člen
(obveščanje o obdelavi osebnih podatkov)

(1) OI posameznika, čigar osebne podatke bo zbiral, obvesti o obstoju izvajanja obdelave in namenih obdelave.

(2) Obvestilo iz prejšnjega odstavka morajo obsegati najmanj naslednje informacije:
- imena in kontaktne podatke upravljavca;
- kontaktne podatke pooblaščene osebe;
- namene, za katere se osebni podatki obdelujejo;
- pravno podlago obdelave;
- rok hrambe osebnih podatkov;
- kategorije prejemnikov osebnih podatkov;
- obstoju pravice do vložitve prijave pri Informacijskem pooblaščencu in njegove kontaktne podatke;
- o obstoju pravice do seznanitve z lastnimi osebnimi podatki ter zdravstveno dokumentacijo in pravice do ugovora, izbrisa, popravka, omejitve obdelave ter prenosljivosti podatkov, če so za to izpolnjeni pogoji (41. člen Zakona o pacientovih pravicah ter 15. do 22. člen Splošne uredbe (EU) o varstvu podatkov);

(3) Obvestilo iz prejšnjega odstavka pripravi in posodablja pooblaščena oseba.
(4) Pred vsako obdelavo osebnih podatkov je zaposleni dolžan presoditi ali imajo za obdelavo ustrezno zakonsko podlago. V primeru dvomov se lahko posvetuje s pooblaščeno osebo za varstvo osebnih podatkov.

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

17. člen
(pravica posameznika do seznanitve glede obdelave njegovih podatkov)

(1) 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;

(2) 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;

(3) Upravljavec zagotovi kopijo osebnih podatkov, ki se obdelujejo.

(4) 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.

(5) Odgovorna oseba posamezne zbirke podatkov je dolžan prizadetega posameznika obvestiti o omejitvi obdelave podatkov v najkrajšem možnem času, brez nepotrebnega odlašanja.

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

(1) 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.

(2) Za izvedbo posameznikovega zahtevka je zadolžena odgovorna oseba posamezne zbirke podatkov, na katere se nanaša zahtevek ali pooblaščena oseba za varstvo osebnih podatkov.

(3) Odgovorna oseba posamezne zbirke podatkov je dolžan prizadetega posameznika obvestiti o omejitvi obdelave podatkov v najkrajšem možnem času, brez nepotrebnega odlašanja.

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

(1) 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.

(2) 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.

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

(4) Odgovorna oseba posamezne zbirke podatkov je dolžan prizadetega posameznika obvestiti o omejitvi obdelave podatkov v najkrajšem možnem času, brez nepotrebnega odlašanja.

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

(1) 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.

(2) 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.

(3) Za izvedbo posameznikovega zahtevka je zadolžena odgovorna oseba posamezne zbirke podatkov na katere se nanaša zahtevek posameznika ali pooblaščena oseba za varstvo osebnih podatkov.

(4) Odgovorna oseba posamezne zbirke podatkov je dolžan prizadetega posameznika obvestiti o omejitvi obdelave podatkov v najkrajšem možnem času, brez nepotrebnega odlašanja.

21. člen
(Seznanitev z lastnimi osebnimi podatki)

(1) Posameznik, na katerega se nanašajo osebni podatki, ima pravico, da prejme osebne podatke v zvezi z njim, ki jih je posredoval 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.

(2) 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.

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

(4) Za izvedbo posameznikovega zahtevka je zadolžen odgovorna oseba posamezne zbirke podatkov na katere se nanaša zahtevek posameznika ali pooblaščena oseba za varstvo osebnih podatkov.
(5) Odgovorna oseba posamezne zbirke podatkov je dolžan prizadetega posameznika obvestiti o omejitvi obdelave podatkov v najkrajšem možnem času, brez nepotrebnega odlašanja.

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

(1) 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
(2) 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.
(3) 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.
(4) 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

23. člen
(vgrajeno in privzeto varstvo podatkov)

(1) OI si prizadeva izvesti ustrezne tehnične in organizacijske ukrepe, s katerimi zagotovi, da se privzeto obdelajo le tisti osebni podatki, ki so potrebni za vsak poseben namen obdelave. Ta obveznost velja za količino zbranih osebnih podatkov, obseg njihove obdelave, obdobje njihove hrambe in njihovo dostopnost. S takšnimi ukrepi se zagotovi zlasti, da osebni podatki niso samodejno dostopni nedoločenemu številu posameznikov brez posredovanja zadevnega posameznika.
(2) OI si prizadeva že tekom načrtovanja nove obdelave predvideti ustrezne tehnične in organizacijske ukrepe ter varovalke, ki bi zagotavljale, da bo obdelava potekala v skladu s temeljnimi načeli varstva osebnih podatkov še zlasti pa z načelom sorazmernosti. Ukrepi morajo biti primerni glede na stanje najnovejšega tehnološkega razvoja na tem področju, naravo, obseg, okoliščine in namene obdelave ter tveganja za poseg v človekove pravice in temeljne svoboščine posameznikov, ki nastajajo pri obdelavi. Pri izvajanju ukrepov se upošteva tudi tehnologijo, ki je dejansko na razpolago upravljavcu.

24. člen
(kakovost obdelovanih podatkov)

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

25. člen
(popis informacijskih sredstev)

(1) OI pregled nad rešitvami, napravami, sistemi in drugo infrastrukturo (v nadaljevanju: sredstvo), ki jo uporablja za obdelavo zbirk, vodi v popisu informacijskih sredstev kot priloga Krovne politike varovanja informacij. Za vzdrževanje podatkov popisa informacijskih sredstev je odgovoren vodja službe za informatiko.
(2) Izdelavo in vzdrževanje informacijskih sredstev koordinira vodja službe za informatiko.

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

(1) OI s posebno politiko, ki je del SUVI, 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.
(2) Zasebne naprave iz prejšnjega odstavka morajo biti vključene v popisu informacijskih sredstev.

Ocena tveganj in ocena učinka na varstvo osebnih podatkov

27. člen
(ocena tveganj informacijske varnosti)

(1) Služba za informatiko redno izvaja oceno tveganja informacijske varnosti OI, 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.

(2) Ocena tveganja informacijske varnosti se popravi in dopolni 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.

(3) Način izvedbe ocene tveganj OI določi z Navodili za izvajanje ocen učinkov na varstvo osebnih podatkov in je priloga temu pravilniku.
(4) Za pripravo ocene tveganja informacijske varnosti je odgovoren vodja Službe za informatiko. Gre za timsko delo, v katerem sodeluje tudi pooblaščena oseba za varstvo osebnih podatkov in skupina za informacijsko varnost.

28. člen
(ocena učinkov na varstvo osebnih podatkov)

(1) 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, OI pred obdelavo opravi oceno učinka na varstvo osebnih podatkov. V eni oceni je lahko obravnavan niz podobnih dejanj obdelave, ki predstavljajo podobna velika tveganja.
(2) Namen izvajanja ocen učinkov za varstvo osebnih podatkov so podrobneje opredeljeni v Navodilih za izvajanje ocen učinkov na varstvo osebnih podatkov, ki je priloga temu pravilniku.
(3) Oceno učinka izdela notranja organizacijska enota za njeno koordinacijo rednega izvajanja je odgovorna oseba službe/oddelka/enote, 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 in skupina za informacijsko varnost.

Spremembe načina obdelave

29. člen
(uvajanje sprememb)

(1) Sprememba informacijskih rešitev ali rokovanja z dokumentacijo, 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.

(2) Razvojno, preizkusno in produkcijsko okolje informacijskih rešitev, s katerimi se izvaja obdelava podatkov, so ločeni glede na specifiko rešitve.
(3) Seznam verzij se nahaja pri skrbniku informacijske rešitve.
(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 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.
(6) Nadzor sprememb informacijskih sistemov je podrobneje opisan v Politiki razvoja, spreminjanja in vzdrževanja programske opreme, v okviru SUVI.

Zagotavljanje neprekinjenega poslovanja

30. člen
(načrt neprekinjenega poslovanja)

(1) Odgovornost, organiziranje in izvedba postopkov za zagotovitev neprekinjene obdelave in ohranjanje celovitosti obdelovanih podatkov se 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 OI.
(2) Načrt neprekinjenega poslovanja je podrobneje opisan v Politiki upravljanja z varnostnimi incidenti v okviru SUVI.
(3) Za koordiniranje in vzdrževanje načrta neprekinjenega poslovanja je odgovoren vodja službe za informatiko skupaj s pooblaščeno osebo za varstvo osebnih podatkov ter skupino za informacijsko varnost.

31. člen
(varnostno kopiranje podatkov)

(1) OI 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.
(2) Varnostno kopiranje podatkov je podrobneje opredeljeno v Politiki izdelave in shranjevanja varnostnih kopij, v okviru SUVI.

(3) Dejanja oz. dogodki iz prejšnjega odstavka so lahko uvrščeni med varnostne dogodke ali incidente.
(4) 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.
(5) Bolnišnica 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.
(6) 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 v skladu s 33. členom Uredbe.

Posredovanje osebnih podatkov

32. člen
(postopek posredovanja)

(1) Osebni podatki s katerimi upravlja OI, se na zahtevo posredujejo samo tistim uporabnikom, ki se izkažejo z ustrezno zakonito podlago za obdelavo podatkov.
(2) OI je dolžan uporabniku osebnih podatkov posredovati osebne podatke brez plačila stroškov posredovanja, razen če zakon določa drugače ali če gre za uporabo za zgodovinsko, statistično ali znanstveno-raziskovalne namene.
(3) OI mora pravico iz prvega odstavka tega člena pacientu omogočiti takoj ali najpozneje pet delovnih dni po prejemu zahteve. Pacient lahko pri istem izvajalcu zdravstvene dejavnosti vloži zahtevo največ dvakrat mesečno.
(4) Poleg pravic iz prejšnjih odstavkov tega člena ima pacient pravico zahtevati:
- da se dodajo njegove pripombe k zapisom v zdravstveni dokumentaciji,
- osnovna ustna pojasnila o vsebini zdravstvene dokumentacije, razen kadar pacient že prejme izčrpna pojasnila po zdravnikovi pojasnilni dolžnosti,
- izčrpna ustna pojasnila o vsebini zdravstvene dokumentacije, če glede posameznih delov dokumentacije ni prejel pojasnil po zdravnikovi pojasnilni dolžnosti.

Izvajalec zdravstvene dejavnosti mu mora omogočiti uresničitev pravice iz prve in druge alineje tega odstavka v roku iz tretjega odstavka tega člena, uresničitev pravice iz tretje alineje tega odstavka pa v 15 dneh od prejema zahteve.

(5) Posredovanje osebnih podatkov 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. Pacient ima pravico določiti osebe, ki se lahko seznanijo z njegovo zdravstveno dokumentacijo, in osebe, katerim seznanitev z njegovo zdravstveno dokumentacijo prepoveduje, če to ni v nasprotju z zakonom.
(6) 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.
(7) 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). Navodila za šifriranje vsebin z orodjem 7zip so objavljena na spletni strani OI pod zavihkom *Varstvo osebnih podatkov*.

33. člen
(seznanitev z zdravstveno dokumentacijo pokojnika)

(1) Po smrti pacienta imajo pravico do seznanitve z njegovo zdravstveno dokumentacijo osebe, ki so za obdelavo podatkov pooblaščene z zakonom ter osebe, za katere je pacient predhodno dal izrecno privolitev v pisni obliki. Pravico do seznanitve z njegovo zdravstveno dokumentacijo na podlagi zakona imajo:
- pacientov zakonec;
- zunajzakonski partner;
- partner iz istospolne skupnosti;
- otroci in posvojenci;
- kadar teh oseb ni imajo pravico pacientovi starši;
- druge osebe, ki izkažejo pravni interes z ustrezno listino;
- drugi osebi, ki namerava te podatke uporabljati zgodovinsko, statistično ali v znanstveno-raziskovalne namene, v kolikor posameznik ni prepovedal posredovanja teh osebnih podatkov.

(2) Zahteva za seznanitev oseb iz prejšnjega odstavka se delno ali v celoti zavrne, če tako določa zakon ali če je pacient seznanitev pred smrtjo pisno ali ustno v navzočnosti dveh prič izrecno prepovedal.

(3) Ne glede na izrecno prepoved umrlega pacienta imajo pravico do seznanitve z zdravstveno dokumentacijo v delu, ki se nanaša na razloge, ki utegnejo bistveno vplivati na njihovo zdravje, pacientovi starši, pacientovi potomci do katerega koli kolena, pacientov zakonec, zunajzakonski partner ali partner iz istospolne skupnosti, bratje in sestre ali druge osebe, ki so bile z umrlim pacientom v posebnem razmerju in to z gotovostjo izkažejo.

(4) O tem, ali je zahteva za seznanitev utemeljena ali ne, bo odločila pravna služba OI v 15 dneh od prejema obrazložene zahteve. Pravna služba bo ocenila, ali je zahtevo podala upravičena oseba ali je izkazan pravni interes ter ocenila, kateri so tisti podatki, ki so potrebni za dosego zakonitega namena seznanitve. Tako bo odločila, ali se zahteva za seznanitev delno ali v celoti zavrne ali pa se zahtevi ugodi ter v kakšnem obsegu. Če je zahteva delno ali v celoti zavrnjena, imajo naštete osebe iz prvega odstavka, pravico vložiti pritožbo pri Informacijskem pooblaščencu.

(5) Seznanitev se izvede prek pacientovega izbranega osebnega zdravnika ali zdravnika, ki je bil kako drugače udeležen v postopku zdravljenja, če tega ni, pa zdravnika določi strokovni direktor.

(6) V kolikor upravičena oseba želi le fotokopije zdravstvene dokumentacije se mu ta izroči preko pravne službe OI.

(7) Zdravniki na poziv pravne službe pisno podajo zahtevane podatke, najkasneje v roku treh (3) delovnih dni, v izrednih utemeljenih primerih pa se lahko rok tudi skrajša.

(8) Osebam, ki so upravičene do podatkov po zakonu, se omogoča dostop le do tistih podatkov, ki so potrebni za dosego zakonitega namena seznanitve.

34. člen
(evidentiranje posredovanj)

(1) 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:
- datum posredovanja podatkov ter
- pravna podlaga na podlagi katere so bili posredovani osebni podatki;

(2) V primeru posredovanja osebnih podatkov iz medicinske dokumentacije se v mapo pacienta, katerega podatki so bili posredovani, vloži izpolnjen obrazec »Potrdilo o izdaji zdravstvene dokumentacije pacienta«. Naveden obrazec je priloga tega pravilnika.
(3) OI nikoli ne posreduje izvirnih listin, razen v primeru pisne odredbe sodišča.

Fizični in tehnični ukrepi varovanja obdelave

35. člen
(varovanje prostorov)

(1) Vsi prostori OI, v katerih se nahajajo nosilci podatkov, ki vsebujejo osebne podatke ter strojna in programska oprema za obdelovanje teh podatkov, so varovani prostori.
(2) 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.
(3) Obiskovalci se smejo v poslovnih prostorih OI, v katerih se nahajajo nosilci podatkov gibati samo v spremstvu zaposlenega. To določilo ne velja za stalne zunanje sodelavce OI, 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). Med pogodbene sodelavce štejejo tudi osebe, ki na OI opravljajo delo preko študentskega servisa, pogodbe o usposabljanju oziroma katerega koli drugega pogodbena razmerja
(4) Ukrepi za varovanje prostorov so podrobneje opredeljeni v Politiki fizične zaščite in fizičnega dostopa v okviru SUVI.

36. člen
(vhodna kontrola zaposlenih)

(1) OI, zaradi varovanja osebnih in drugih varovanih podatkov ter opreme za njihovo obdelavo, vstope zaposlenih v prostore, kjer je že vzpostavljena vhodna kontrola, kontrolira s terminalom za elektromehansko odpiranje vrat s pomočjo šifrirane kartice.
(2) Vsak zaposleni oz. pogodbeni sodelavec, ki mu je dodeljena kartica za registracijo prisotnosti na delu, ki se, ko so dodeljene pravice pristopa, uporablja tudi za vhodno kontrolo pristopa (v nadaljevanju: uporabnik kartice), je dolžan z njo ravnati z vso skrbnostjo in z zavedanjem, da je namenjena samo njegovi osebni uporabi. Morebitna izguba ali odtujitev kartice mora takoj javiti kadrovski ali tehnično vzdrževalni ali službi, ki kartico nemudoma prekliče. Zaposlenemu kadrovska služba izda novo kartico, ki je kopija izgubljene kartice (prenesejo se vsi podatki, vključno z dovoljenji na omejena območja).
(4) Vsakega uporabnika kartice je kadrovska služba ob izdaji kartice na registracijo prisotnosti dolžna opozoriti in seznaniti z varnostnimi zahtevami pri ravnanju s kartico.
(5) Kadrovska služba izdajo kartice za registracijo vpiše v sistem, tehnično vzdrževalna služba pa, v skladu z navodili nadrejenega uporabniku kartice oziroma skrbnika pogodbe, dodeli pravice vstopa na omejena območja, ki pa ne smejo preseči obsega pravic določenega s pravilnikom (v nadaljevanju: kartica za vhodno kontrolo pristopa).
(6) Seznam zaposlenih uporabnikov kartice za registracijo prisotnosti, obsega ime in priimek uporabnika, matični indeks, služben e-naslov, organizacijsko enoto ter pravno podlago za delo. Seznam, skupaj z izjavo in datumom ter podpisom prevzema kartice hrani kadrovska služba.
(7) Seznam uporabnikov kartice za vhodno kontrolo pristopa obsega ime in priimek uporabnika, matični indeks uporabnika, služben e-naslov, organizacijsko enoto ter pravno podlago za delo. Seznam, skupaj z izjavo nadrejenega oziroma skrbnika pogodbe hrani tehnično vzdrževalna služba.
(8) Kartico za vhodno kontrolo lahko v izjemnih primerih, ki jih predhodno odobri generalni direktor, uporablja več pogodbenih delavcev. Seznam vseh uporabnikov kartice se vodi v tehnično vzdrževalni službi.

37. člen
(videonadzor vstopa v prostore)

(1) Vstop v prostore OI je pod videonadzorom v obsegu, ki je nujno potreben 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.
(2) Pregled posnetkov videonadzora je dopusten le v primeru incidenta, katerega posledica je poškodovanje dobrin iz prejšnjega odstavka, kršitve pravic in obveznosti iz naslova sklenjenega delovnega razmerja in kršitve pravil varnega vstopanja v prostore OI. Vsak pregled posnetkov videonadzora mora biti ustrezno argumentiran in voden v Evidenci videonadzora.
(3) Zaposleni in obiskovalci so z videonadzorom seznanjeni z ustreznimi obvestilnimi napisi. Šteje se, da je bil posameznik na podlagi obvestila obveščen o obdelavi osebnih podatkov.
(4) Videonadzorni sistem, s katerim se izvaja videonadzor, mora biti zavarovan pred dostopom nepooblaščenih oseb.
(5) Posnetki videonadzora se, če ni zaznanih posebnosti, avtomatsko izbrišejo v 20 dneh.
(6) Za Evidenco uporabe video nadzornega sistema je odgovorna Pooblaščena oseba video sistema, ki jo imenuje direktor s sklepom.

Varovanje dostopa do IT opreme in infrastructure

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

(1) 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.
(2) Računalniški zasloni morajo biti nameščeni tako, da nepoklicani nimajo vpogleda v prikazovane podatke.
(3) Iznos nosilcev podatkov, ki vsebujejo posebne vrste osebnih podatkov iz prostorov OI ni dovoljen.
(4) V sklopu SUVI je OI sprejela področne politike – predpise, ki temeljijo na zakonih in predpisih, ki jih je predpisalo Ministrstvo za zdravje. Vse podatkovne baze in dostopi do njih preko aplikacij so varovani in predpisani v njih.

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

(1) Zaposleni, 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.
(2) 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.
(3) Dokumenti, ki vsebujejo osebne podatke (razni seznami, zapisi ipd.), ki jih pri svojem delu ne potrebujemo več in ki jih lahko zavržemo, se trajno uničijo (uničevalniki dokumentacije).

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

(1) 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 vodje službe za informatiko, izvajajo pa ga lahko samo pooblaščeni zaposleni oz. serviserji in vzdrževalci, ki imajo s OI sklenjeno ustrezno pogodbo.
(3) Vsi dostopi do programske opreme morajo biti obeleženi z revizijsko sledjo.
(4) Popravljanje, spreminjanje in dopolnjevanje sistemske programske opreme je dovoljeno samo na podlagi odobritve vodje službe za informatiko, izvajajo pa ga lahko samo organizacije in posamezniki (v nadaljnjem besedilu: izvajalci), ki imajo z OI sklenjeno ustrezno pogodbo. Izvajalci morajo spremembe in dopolnitve sistemske programske opreme ustrezno dokumentirati.
(5) 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 z OI sklenjeno ustrezno pogodbo. Izvajalci morajo spremembe in dopolnitve aplikativne programske opreme ustrezno dokumentirati.
(6) Vsebina diskov omrežnega strežnika in delovnih postaj, povezanih v omrežje, na katerih se nahajajo osebni podatki, se preverjajo samodejno z vidika prisotnosti računalniških virusov.
(7) V primeru, da zaposleni pri uporabi podatkov in programske opreme, ki so namenjeni uporabi v računalniškem informacijskem sistemu, in prispejo v OI na prenosnih medijih ali preko komunikacijskih kanalov, zazna računalniški virus, ga je dolžan sporočiti službi za informatiko.
(8) Zaposleni na informacijsko opremo ne smejo namestiti programske opreme brez vednosti vodje službe za informatiko.

41. člen
(kontrola dostopa do informacijskega sistema)

(1) 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.
(2) Vsi dostopi do informacijskega sistema in podatkov se beležijo z revizijsko sledjo.
(3) Zaposlenemu se dodeli obseg dostopnih pravic za uporabo informacijskega sistema, ki je nujno potreben za izvajanje delovnih nalog.
(4) Vzpostavitev nadzora dostopa do aplikacij, informacij in sistemov ter namen dostopa do omrežja zaradi preprečitve nepooblaščenega dostopa do omrežnih storitev je podrobneje opisana v SUVI.

42. člen
(revizijske sledi)

(1) OI 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.
(2) Zapisi iz prejšnjega odstavka, vezani na dostope do osebnih podatkov, se hranijo za obdobje 5 let od zaključka leta, v katerem je bil zapis ustvarjen, razen, če za obdelavo posameznih vrst osebnih podatkov drug zakon ne določa drugače.
(3) Za revizijske sledi je odgovoren skrbnik SUVI, ki na podlagi posveta z pooblaščeno osebo za varstvo osebnih podatkov v konkretnem primeru določi, kdo in v katerih primerih sme

dostopati do zapisov revizijskih sledi. Način zbiranja zapisov, hrambo in uporabo revizijskih sledi OI določi v Politiki revizijskih sledi, v okviru SUVI.

VI. VARNOST OBDELAVE OSEBNIH PODATKOV

43. 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 OI, takoj obvestiti neposredno nadrejenega, on pa pooblaščeno osebo za varstvo osebnih podatkov. V kolikor je mogoče pa si morajo zaposleni prizadevati z zakonitimi ukrepi takšno aktivnost preprečiti.

44. člen
(izvajanje postopkov in ukrepov)

Vsi zaposleni v OI 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.

45. 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 OI skupaj s Komisijo za nadzor nad izvajanjem določil Pravilnika o varstvu osebnih in drugih podatkov na OI.

46. člen
(izjava)

(1) Pred nastopom dela v OI mora zaposleni podpisati posebno izjavo, ki ga zavezuje k varovanju osebnih podatkov.
(2) 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.
(3) Izjavo iz prvega odstavka tega člena podpišejo tudi zunanji sodelavci OI, ki se v okviru izvajanja pogodbenih del seznanijo ali bi se lahko seznanili z osebnimi podatki, s katerimi upravlja OI.
(4) Izjavo iz prvega odstavka tega člena podpišejo vsi dijaki, študentje, zunanji pripravniki, specializanti, ki opravljajo del obveznega programa izobraževanja/kroženja v OI, sekundariji in delavci na usposabljanju.
(5) Izjava iz prvega odstavka tega člena predstavlja Prilogo temu Pravilniku.

47. člen
(odgovornost za kršitev)

(1) Kršitev določil tega pravilnika s strani zaposlenih pomeni kršitev obveznosti iz delovnega razmerja, ostali pa za kršitve odgovarjajo na temelju pogodbenih obveznosti.
(2) Odgovornost iz prejšnjega odstavka ne izključuje prekrškovne, kazenske ali odškodninske odgovornosti, kadar tako določa zakon

KONČNE DOLOČBE

48. člen
(seznanitev zaposlenih s pravilnikom)

Vsebina pravilnika se po sprejemu objavi na intranetu OI.

49. člen
(začetek veljavnosti)

Ta pravilnik prične veljati, ko ga sprejme generalna direktorica in z objavo na intranetu.

Z veljavnostjo tega pravilnika preneha veljati Pravilnik o varstvu osebnih in drugih podatkov na OI z dne 14.4.2016.

Generalna direktorica:

Zlata Štiblar Kisić

1. Podrejeni dokumenti

- NAV – 662 Izvajanje ocen učinkov na varstvo osebnih podatkov
  - NAV – 663 Izjava o seznanjenosti s pravilnikom o varstvu osebnih podatkov
    - OBR – 1017 Potrdilo o izdaji zdravstvene dokumentacije pacienta