Na podlagi določb 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 (v nadaljevanju: Splošna uredba) in na podlagi veljavne zakonodaje, ki ureja varstvo osebnih podatkov, izdaja direktor Juventina Clinic, d.o.o. (v nadaljevanju: organizacija ali upravljavec)

PRAVILNIK
o varstvu osebnih podatkov

I. SPLOŠNE DOLOČBE

1. člen
(namen in vsebina pravilnika)

(1) S tem pravilnikom se določajo pravne podlage za obdelavo osebnih podatkov, organizacijski, tehnični in logično-tehnični postopki in ukrepi za zavarovanje osebnih podatkov v organizaciji z namenom, da se prepreči naključno ali namerno nepooblaščeno uničevanje podatkov, njihovo spremembo ali izgubo, kakor tudi nepooblaščen dostop, obdelava, uporaba ali posredovanje osebnih podatkov.

(2) Odgovorna oseba, vodstvo, zaposleni, delavci oziroma vse osebe, ki so vključene v delovni proces na podlagi pogodbe o zaposlitvi ali drugega pogodbenega razmerja, ki pri delu neposredno ali posredno obdelujejo in uporabljajo osebne, zaupne podatke in/ali se seznanjajo s poslovno skrivnostjo organizacije, morajo spoštovati določila Splošne uredbe, določila veljavne zakonodaje, ki ureja področje varstva osebnih podatkov ter določila drugih predpisov, zavezujočih aktov in pogodb, ki urejajo posamezno področje dela ter z vsebino tega pravilnika.

(3) Po tem pravilniku se varujejo tudi osebni podatki, ki jih na podlagi pogodbe za organizacijo obdeluje zunanji izvajalec (v nadaljnjem besedilu: obdelovalec) oziroma skupni upravljavec.

2. člen
(pomen izrazov)

(1) V tem pravilniku uporabljeni izrazi imajo naslednji pomen:

- *Analiza varnostnih tveganj* je sistematična uporaba informacij za prepoznavanje virov groženj in ranljivosti sredstev ter ocenjevanje tveganj za varnost osebnih podatkov oz. obdelavo;
- *Analiza vpliva na poslovanje* je sistematična uporaba informacij za prepoznavanje virov groženj in ranljivosti sredstev ter ocenjevanje tveganj za neprekinjeno izvajanje obdelave;
- *Biometrični podatki* pomenijo osebne podatke, ki so rezultat posebne tehnične obdelave v zvezi s fizičnimi, fiziološkimi ali vedenjskimi značilnostmi posameznika, ki omogočajo ali potrjujejo edinstveno identifikacijo tega posameznika, kot so podobe obraza ali daktiloskopski podatki;
- *Dokumentiran postopek* pomeni, da je postopek zapisan;
- *Določljivi posameznik* je tisti, ki ga je mogoče neposredno ali posredno določiti, zlasti z navedbo enega ali več identifikatorjev, kot so ime, priimek, identifikacijska številka, podatki o lokaciji in spletni identifikator ali z navedbo enega ali več dejavnikov, ki so značilni za fizično, fiziološko, genetsko, duševno, gospodarsko, kulturno ali družbeno identiteto tega posameznika;
- *Genetski podatki* pomenijo osebne podatke v zvezi s podedovanimi ali pridobljenimi genetskimi značilnostmi posameznika, ki dajejo edinstvene informacije o fiziologiji ali zdravju tega posameznika in so zlasti rezultat analize biološkega vzorca zadevnega posameznika;

- *Grožnja* je možen vzrok za incident, ki lahko povzroči škodo osebnemu podatku, sredstvu za obdelavo ali upravljavcu;
- *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;
- *Informacijski sistem* je programska, strojna, komunikacijska in druga oprema, ki deluje samostojno ali v omrežju in je namenjena zbiranju, procesiranju, distribuciji, uporabi in drugi obdelavi osebnih podatkov;
- *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;
- *Nosilec podatkov* pomeni vse vrste sredstev, na katerih so zapisani ali posneti podatki (listine, akti, gradiva, spisi, računalniška oprema vključno z magnetnimi, optičnimi ali drugi računalniškimi mediji, fotokopije, zvočno in slikovno gradivo, mikrofilmi, naprave za prenos podatkov, ipd.);
- *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 so 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;
- *Obdelovalec* pomeni fizično ali pravno osebo, javni organ, agencijo ali drugo telo, ki obdeluje osebne podatke v imenu upravljavca;
- *Obravnava tveganj* je proces izbora in vpeljave ukrepov za zmanjšanje tveganj;
- *Odgovorna oseba* pomeni fizično osebo, ki je veljavni zakoniti zastopnik oz. direktor;
- *Odgovorna oseba* zbirke je zaposleni ali zunanji sodelavec, odgovoren za obdelavo podatkov iz posamezne zbirke osebnih podatkov;
- *Osebni podatek* pomeni katero koli informacijo v zvezi z določenim ali določljivim posameznikom, na katerega se nanašajo osebni podatki.
- *Podatki o zdravstvenem stanju* pomenijo osebne podatke, ki se nanašajo na telesno ali duševno zdravje posameznika, vključno z zagotavljanjem zdravstvenih storitev in razkrivajo informacije o njegovem zdravstvenem stanju;
- *Posameznik* je določena ali določljiva oseba, na katero se nanaša osebni podatek;
- *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;
- *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;
- *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;
- *Ranljivost* je šibka točka sredstva ali skupine sredstev, ki jo je mogoče izrabiti z eno ali več grožnjami;
- *Sistemski administrator* je oseba, ki skrbi za delovanje sistemske opreme;
- *Škodljiva programska oprema* so računalniški virusi, črvi, trojanski konji in podobna programska oprema, ki se nepooblaščeno namesti v informacijski sistem ali njegov del brez vednosti odgovornih oseb organizacije in posega v integriteto informacijskega sistema;
- *Skrbnik informacijskega sistema* je oseba, ki skrbi za vsebinsko delovanje informacijskega sistema;

- *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;
- *Uporabnik* pomeni fizično ali pravno osebo, javni organ, agencijo ali drugo telo, ki so mu bili osebni podatki razkriti, ne glede na to, ali je tretja oseba ali ne. Vendar pa se javni organi, ki lahko prejmejo osebne podatke v okviru posamezne poizvedbe v skladu s pravom Unije ali pravom države članice, ne štejejo za uporabnike; obdelava teh podatkov s strani teh javnih organov poteka v skladu z veljavnimi pravili o varstvu podatkov glede na namene obdelave;
- *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;
- *Upravljavec zbirke* je zaposleni ali zunanji sodelavec organizacije, zadolžen za obdelavo podatkov iz posamezne zbirke osebnih podatkov;
- *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;
- *Vodstveni pregled* je dokumentiran pregled sistema upravljanja varstva osebnih podatkov, ki ga vodstvo opravi najmanj enkrat letno, da zagotovi skladnost obdelave;
- *Zbirka* pomeni vsak strukturiran niz osebnih podatkov, ki so dostopni v skladu s posebnimi merili, niz pa je lahko centraliziran, decentraliziran ali razpršen na funkcionalni ali geografski podlagi.

II. VARSTVO OSEBNIH PODATKOV

3. člen
(odgovornost vodstva)

(1) Za zagotovitev ustreznih in učinkovitih ukrepov za izvajanje obdelave podatkov v skladu s Splošno uredbo in zakonodajo, ki ureja varstvo osebnih podatkov ter za dokazovanje skladnosti obdelave podatkov, je odgovorno vodstvo.

(2) Vodstvo odgovornosti iz prvega odstavka tega člena uresničuje zlasti:
- s sprejetjem tega pravilnika ter navodil, politik, načrtov in drugih notranjih aktov, s katerimi se določajo:
    - postopki za vzpostavitev zakonitih podlag za obdelavo osebnih podatkov, predvsem z vzpostavitvijo evidenc dejavnosti obdelave;
    - postopki za obravnavanje zahtevkov oziroma ugovorov posameznikov, katerih podatke organizacija obdeluje, vezanih na varstvo njihovih pravic in svoboščin v zvezi z obdelavo osebnih podatkov;
    - izdelave ocen varnostnih tveganj obdelave;
    - izdelave ocen učinka v zvezi z varstvom podatkov;
    - izvajanja 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 imenovanjem pooblaščene osebe za varstvo osebnih podatkov;
- z ustreznim vodenjem seznama in ureditvijo pogodbeno obdelave s strani pogodbenih obdelovalcev;
- z letnim pregledom s strani pooblaščene osebe za varstvo podatkov, ki vključuje notranjo presojo ter pregled ustreznosti in učinkovitosti ukrepov za zagotavljanje varnosti obdelave ter
- z rednimi izobraževanji zaposlenih na področjih varne obdelave osebnih podatkov.

(3) Vodstvo mora zagotoviti, da je omogočeno učinkovito izvajanje, spremljanje in nadziranje ukrepov in postopkov za varnost osebnih podatkov ter njihovo dokazovanje skladnosti obdelave v sodnih, nadzornih in drugih uradnih postopkih.

4. člen
(izjava o varovanju osebnih podatkov)

(1) Pred nastopom dela mora zaposleni podpisati izjavo, ki ga zavezuje k varovanju osebnih podatkov.

(2) Iz podpisane izjave mora biti razvidno, da je podpisnik seznanjen z določbami tega pravilnika, Splošne uredbe in zakonodaje. Izjava mora vsebovati tudi pouk o posledicah kršitve določb.

(3) Izjavo iz prvega odstavka tega člena podpišejo tudi zunanji sodelavci, ki se v okviru izvajanja pogodbenih del seznanijo ali bi se lahko seznanili z osebnimi podatki, s katerimi upravlja organizacija.

(4) Izjavo iz prvega odstavka tega člena podpišejo vsi študentje, dijaki, prostovoljci, zunanji pripravniki in specializanti, ki se lahko seznanijo z osebnimi podatki v okviru sodelovanja z organizacijo.

5. člen
(odgovornost za kršitev)

(1) Kršitev določil pravilnika predstavlja hujšo kršitev delovnih obveznosti po pogodbi o zaposlitvi oziroma bistveno kršitev druge pogodbe, zaradi katere lahko organizacija odpove pogodbo o zaposlitvi oziroma drugo pogodbo, ki je podlaga za opravljanje dela pri ali za organizacijo.

(2) V primeru kršitev določil tega pravilnika, je zaposleni odškodninsko odgovoren organizaciji za škodo, ki bi nastala organizaciji oziroma fizičnim ali pravnim osebam, s katerimi organizacija sodeluje.

(3) Kršitev določil pravilnika ima lahko za posledico kazensko, prekrškovno in/ali odškodninsko odgovornost zaposlenega oziroma osebe, ki krši ta pravilnik.

6. člen
(izvajanje postopkov in ukrepov)

(1) Za izvajanje postopkov in ukrepov za zavarovanje osebnih podatkov so odgovorni vsi zaposleni v organizaciji, kot tudi zunanji izvajalci, ki imajo s podjetjem podpisan dogovor o sodelovanju.

(2) Vsak zaposleni, ki obdeluje osebne podatke, je dolžan izvajati predpisane postopke in ukrepe za zavarovanje podatkov in varovati podatke, za katere je izvedel oziroma bil z njimi seznanjen pri opravljanju svojega dela. Obveza varovanja podatkov ne preneha s prenehanjem delovnega razmerja.

7. člen
(nadzor nad izvajanjem postopkov in ukrepov)

(1) Nadzor nad izvajanjem postopkov in ukrepov, določenih s tem pravilnikom opravlja odgovorna oseba organizacije v sodelovanju z delavci, zadolženimi za informacijsko varnost in pooblaščeno osebo za varstvo podatkov.

8. člen
(dokazovanje skladnosti)

(1) Organizacija za potrebe dokazovanja skladnosti obdelave s predpisanimi zahtevami in tem pravilnikom vodi ustrezno dokumentacijo, s katero je sposobna dokazati, da obdelava poteka v skladu z določbami Splošne uredbe in druge zakonodaje, ki urejajo varstvo osebnih podatkov. V organizaciji se ta dokumentacija vodi v okviru dokumentacije pooblaščene osebe za varstvo podatkov, za katero skrbi odgovorna oseba.

III. POOBLAŠČENA OSEBA ZA VARSTVO PODATKO

9. člen
(imenovanje pooblaščene osebe za varstvo osebnih podatkov)

(1) Odgovorna oseba imenuje pooblaščeno osebo za varstvo podatkov s sklepom ali na drug primeren način (npr. s sklenitvijo pogodbe) in poskrbi za objavo informacij o pooblaščeni osebi na spletni strani organizacije.

(2) Za pooblaščeno osebo za varstvo podatkov in njenega namestnika je lahko določen posameznik, ki je poslovno sposoben, ima znanje oziroma praktične izkušnje s področja varstva osebnih podatkov in ni bil pravnomočno obsojen na kazen zapora šestih mesecev oz. ni bil pravnomočno na kaznivo dejanje glede zlorabe osebnih podatkov ter je zmožen izpolnjevanja nalog iz člena 39. Splošne uredbe.

(3) Organizacija zagotavlja, da je pooblaščena oseba za varstvo osebnih podatkov ustrezno in pravočasno vključena v vse zadeve v zvezi z varstvom osebnih podatkov ter da so ji zagotovljena ustrezna sredstva, potrebna za kvalitetno opravljanje svojih nalog ter da ji je omogočen dostop do osebnih podatkov in dejanja obdelave.

(4) O imenovanju ali spremembi funkcije opravljanja pooblaščene osebe za varstvo osebnih podatkov se obvezno seznani Informacijskega pooblaščenca preko za to predvidenega obrazca.

10. člen
(položaj pooblaščene osebe za varstvo podatkov)

(1) Pooblaščena oseba vodstvu strokovno in neodvisno pomaga pri zagotavljanju skladnosti obdelave osebnih podatkov z določbami Splošne uredbe in veljavne zakonodaje s področja varstva osebnih podatkov.

(2) Organizacija zagotovi, da je pooblaščena oseba za varstvo podatkov ustrezno in pravočasno vključena v vse zadeve v zvezi z varstvom osebnih podatkov.

(3) Posamezniki, na katere se nanašajo osebni podatki, lahko s pooblaščeno osebo za varstvo podatkov stopijo v stik glede vseh vprašanj, povezanih z obdelavo njihovih osebnih podatkov in uresničevanjem njihovih pravic na podlagi Splošne uredbe in veljavne zakonodaje s področja varstva osebnih podatkov.

(4) Pooblaščena oseba za varstvo podatkov je pri opravljanju svojih nalog zavezana varovati skrivnost ali zaupnost v skladu s pravom Unije in veljavno zakonodajo o varstvu osebnih podatkov.

11. člen
(naloge pooblaščene osebe)

(1) Pooblaščena oseba za varstvo podatkov ima naslednje naloge:

- obveščanje organizacije, njenih pogodbenih obdelovalcev in zaposlenih, ki izvajajo obdelavo ter svetovanje navedenim o njihovih obveznostih v skladu s Splošno uredbo in veljavno zakonodajo o varstvu osebnih podatkov;
- spremljanje skladnosti s Splošno uredbo in drugo relevantno zakonodajo in politikami upravljavca ali obdelovalca v zvezi z varstvom osebnih podatkov, vključno z dodeljevanjem nalog, ozaveščanjem in usposabljanjem osebja, vključenega v dejanja obdelave ter s tem povezanimi revizijami;
- svetovanje, kadar je to zahtevano, glede ocene učinka v zvezi z varstvom podatkov in spremljanje njenega izvajanja v skladu s členom 35 Splošne uredbe;
- aktivno sodeluje pri pripravi ocen učinkov;
- sodelovanje z nadzornim organom;
- sprejem prijav domnevnih kršitev in njihova obravnava;
- sodeluje pri poročanju o kršitvah varstva osebnih podatkov nadzornemu organu;
- predlaga interna navodila za ravnanje in obvešča zaposlene;
- pripravlja mnenja s področja varstva osebnih podatkov;
- deluje kot kontaktna točka za nadzorni organ pri vprašanjih v zvezi z obdelavo, vključno s predhodnim posvetovanjem iz člena 36 Splošne uredbe in kjer je ustrezno, izvaja posvetovanje glede katere koli druge zadeve;
- sodeluje s posamezniki, na katere se nanašajo osebni podatki, ki se na organizacijo obračajo glede vprašanj, povezanih z obdelavo njihovih osebnih podatkov in uresničevanjem njihovih pravic.

(2) Pooblaščena oseba za varstvo podatkov pri opravljanju svojih nalog upošteva tveganje, povezano z dejanji obdelave ter naravo, obseg, okoliščine in namene obdelave.

IV. OBDELAVA OSEBNIH PODATKOV

12. člen
(pravne podlage obdelave osebnih podatkov)

(1) V organizaciia se lahko na osnovi člena 6 Splošne uredbe obdeluje osebne podatke, v kolikor je izpolnjen vsaj eden od naslednjih pogojev:

– posameznik, na katerega se nanašajo osebni podatki, je privolil v obdelavo njegovih osebnih podatkov v enega ali več določenih namenov;
– obdelava je potrebna za izvajanje pogodbe, katere pogodbena stranka je posameznik, na katerega se nanašajo osebni podatki, ali za izvajanje ukrepov na zahtevo takega posameznika pred sklenitvijo pogodbe;
– obdelava je potrebna za izpolnitev zakonske obveznosti, ki velja za upravljavca;
– obdelava je potrebna za zaščito življenjskih interesov posameznika, na katerega se nanašajo osebni podatki, ali druge fizične osebe;
– obdelava je potrebna za opravljanje naloge v javnem interesu ali pri izvajanju javne oblasti, dodeljene upravljavcu;
– obdelava je potrebna zaradi zakonitih interesov, za katere si prizadeva upravljavec ali tretja oseba, razen kadar nad takimi interesi prevladajo interesi ali temeljne pravice in svoboščine posameznika, na katerega se nanašajo osebni podatki, ki zahtevajo varstvo osebnih podatkov, zlasti kadar je posameznik, na katerega se nanašajo osebni podatki, otrok.

(2) Osebni podatki se smejo obdelovati samo za določene in zakonite namene ter se ne smejo nadalje obdelovati tako, da bi bila njihova obdelava v neskladju s temi nameni, če zakon ne določa drugače.

13. člen
(namen obdelave osebnih podatkov)

(1) Osebni podatki se smejo obdelovati samo za namene, določene v zakonski podlagi ali določene v informacijah posredovanih posamezniku, na katerega se nanašajo obdelovani podatki, v okviru pridobivanja privolitve za obdelavo ali sklenitev pogodbe, na podlagi katere se izvaja obdelava.

(2) Obdelava osebnih podatkov za drug namen kot za tistega, za katerega so bili podatki 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. V primeru, da se načrtuje obdelava za drug namen na podlagi privolitve, se lahko izvede le na podlagi nove privolitve posameznika, na katerega se nanašajo osebni podatki, če zakon ne določa drugače.

14. člen
(pogoji za privolitev)

(1) Kadar obdelava temelji na privolitvi, mora biti upravljavec zmožen dokazati, da je posameznik, na katerega se nanašajo osebni podatki, privolil v obdelavo svojih osebnih podatkov.

(2) Če je privolitev posameznika, na katerega se nanašajo osebni podatki, dana v pisni izjavi, ki se nanaša tudi na druge zadeve, se zahteva za privolitev predloži na način, ki se jasno razlikuje od drugih zadev, v razumljivi in lahko dostopni obliki ter v jasnem in preprostem jeziku. Deli take izjave, ki predstavljajo kršitev te uredbe, niso zavezujoči.

(3) Posameznik, na katerega se nanašajo osebni podatki, ima pravico, da svojo privolitev kadar koli prekliče. Preklic privolitve ne vpliva na zakonitost obdelave na podlagi privolitve pred njenim preklicem. O tem se pred privolitvijo obvesti posameznika, na katerega se nanašajo osebni podatki. Privolitev je enako enostavno preklicati kot dati.

(4) Pri ugotavljanju, ali je bila privolitev dana prostovoljno, se med drugim zlasti upošteva, ali je izvajanje pogodbe, vključno z zagotavljanjem storitve, pogojeno s privolitvijo v obdelavo osebnih podatkov, ki ni potrebna za izvedbo zadevne pogodbe.

15. člen
(obdelava posebnih vrst osebnih podatkov)

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

(2) Posebne vrste osebnih podatkov se smejo iz evidenc posredovati osebam iz javnega ali zasebnega sektorja ter tretjim le, če to določa zakon, ali na podlagi pisne zahteve ali pisne privolitve posameznika, na katerega se nanašajo. Privolitev mora biti izrecna in praviloma pisna.

(3) Pri obdelavi posebnih vrst osebnih podatkov morajo biti zaposleni še posebej vestni in skrbni. Posebne vrste osebnih podatkov morajo biti varovane tako, da se nepooblaščenim osebam prepreči dostop do njih.

V. OBVEŠČANJE IN VARSTVO PRAVIC POSAMEZNIKA GLEDE OBDELAVE PODATKOV

16. člen
(obveščanje o obdelavi osebnih podatkov)

(1) Organizacija posameznika, čigar osebne podatke bo zbiral, obvesti o obstoju izvajanja obdelave in namenih obdelave. Besedila informacij morajo obsegati najmanj naslednje informacije:
- imena in kontaktne podatke upravljavca;
- kontaktne podatke pooblaščene osebe;
- namene, za katere se osebni podatki obdelujejo;
- obstoju pravice do vložitve prijave pri Informacijskem pooblaščencu in njegove kontaktne podatke;
- obstoju pravice do dostopa do podatkov in do tega, da upravljavec popravi ali izbriše podatke ali omeji obdelavo podatkov posameznika, na katerega se osebni podatki nanašajo;

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

(3) Predlog besedil informacij iz prejšnjega odstavka pripravi pooblaščena oseba za varstvo osebnih podatkov v sodelovanju z organizacijo.

17. člen
(pravice posameznika, na katerega se nanašajo osebni podatki)

(1) Posameznik, na katerega se nanašajo osebni podatki, ima pravico od organizacije dobiti potrditev, ali se v zvezi z njim obdelujejo osebni podatki in kadar je temu tako, mu organizacija nudi dostop do osebnih podatkov in informacije iz 1. odstavka člena 15 Splošne uredbe ter zagotavlja naslednje pravice, v kolikor je to v skladu s Splošno uredbo:
- pravica do popravka;
- pravica do izbrisa („pravica do pozabe“);
- pravica do omejitve obdelave;
- obveznost obveščanja v zvezi s popravkom ali izbrisom osebnih podatkov ali omejitvijo obdelave;
- pravica do prenosljivosti podatkov;
- pravica do ugovora in avtomatizirano sprejemanje posameznih odločitev.

(2) Posamezniku, na katerega se nanašajo osebni podatki, se zagotovi vse informacije iz členov 13 in 14 ter sporočila iz členov 15 do 22 in 34 Splošne uredbe, povezana z obdelavo, v jedrnati, pregledni, razumljivi in lahko dostopni obliki ter jasnem in preprostem jeziku, kar velja zlasti za vse informacije, namenjene posebej otroku. Informacije se posredujejo v pisni obliki ali z drugimi sredstvi, vključno, kjer je ustrezno, z elektronskimi sredstvi. Na zahtevo posameznika, na katerega se nanašajo osebni podatki, se lahko informacije predložijo ustno, pod pogojem, da se identiteta posameznika, na katerega se nanašajo osebni podatki, dokaže z drugimi sredstvi.

(3) Posameznik uveljavlja svoje pravice tako da pošlje zahtevek po elektronski pošti na info@juventina.si ali z redno pošto na naslov organizacije.

(4) Organizacija posameznika, ki z zahtevo uveljavlja svoje pravice, seznani z odločitvijo in z osebnimi podatki, če je to predmet zahteve, najkasneje v enem mesecu po prejemu zahteve. Ta rok se lahko po potrebi podaljša za največ dva dodatna meseca ob upoštevanju kompleksnosti in števila zahtev. O podaljšanju roka organizacija obvesti posameznika. Odločitev organizacije mora vsebovati razloge in informacijo o pravici do pritožbe pri Informacijskem pooblaščencu v roku 15 dni do seznanitve z odločitvijo.

(5) Dostop do lastnih osebnih podatkov in uveljavljanje pravic je za posameznika brezplačno, vendar lahko organizacija zaračuna razumno plačilo, kadar so zahtevki očitno neutemeljeni ali pretirani, zlasti ker se ponavljajo. Če je posameznikova zahteva za dostop očitno neutemeljena ali pretirana, lahko organizacija v takšnem primeru zavrne zahtevo.

(6) V primeru uveljavljanja pravic iz tega naslova bo organizacija morda morala od posameznika zahtevati določene informacije, ki ji bodo pomagale pri potrditvi posameznikove identitete, kar je le varnostni ukrep, ki zagotavlja, da se osebni podatki ne razkrijejo nepooblaščenim osebam.

(7) V primeru, da posameznik meni, da so njegove pravice kršene, se lahko za zaščito ali pomoč obrne na nadzorni organ oz. na Informacijskega pooblaščenca: gp.ip@ip-rs.si ali poišče informacije na spletni strani: www.ip-rs.si.

18. člen
(pravica dostopa posameznika, na katerega se nanašajo osebni podatki)

(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:
- namene obdelave;
- vrste zadevnih osebnih podatkov;
- uporabnike ali kategorije uporabnikov, ki so jim bili ali jim bodo razkriti osebni podatki, zlasti uporabnike v tretjih državah ali mednarodnih organizacijah;
- kadar je mogoče, predvideno obdobje hrambe osebnih podatkov ali, če to ni mogoče, merila, ki se uporabijo za določitev tega obdobja;
- obstoj pravice, da se od upravljavca zahteva popravek ali izbris osebnih podatkov ali omejitev obdelave osebnih podatkov v zvezi s posameznikom, na katerega se nanašajo osebni podatki, ali obstoj pravice do ugovora taki obdelavi;
- pravico do vložitve pritožbe pri nadzornem organu;
- kadar osebni podatki niso zbrani pri posamezniku, na katerega se ti nanašajo, vse razpoložljive informacije v zvezi z njihovim virom.

(2) Kadar se osebni podatki prenesejo v tretjo državo ali mednarodno organizacijo, ima posameznik, na katerega se nanašajo osebni podatki, pravico biti obveščen o ustreznih zaščitnih ukrepih.

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

19. člen
(pravica do popravka)

(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, vključno s predložitvijo dopolnilne izjave.

20. člen
(pravica do izbrisa („pravica do pozabe“))

(1) Posameznik, na katerega se nanašajo osebni podatki, ima pravico doseči, da upravljavec brez nepotrebnega odlašanja izbriše osebne podatke v zvezi z njim, upravljavec pa ima obveznost osebne podatke brez nepotrebnega odlašanja izbrisati, kadar velja eden od 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;
- posameznik, na katerega se nanašajo osebni podatki, obdelavi ugovarja, za njihovo obdelavo pa ne obstajajo nobeni prevladujoči zakoniti razlogi;
- osebni podatki so bili obdelani nezakonito.

(2) Prvi odstavek tega člena se ne uporablja, če je obdelava potrebna:

- za uresničevanje pravice do svobode izražanja in obveščanja;
- za izpolnjevanje pravne obveznosti obdelave na podlagi prava Unije ali prava države članice, ki velja za upravljavca, ali za izvajanje naloge v javnem interesu ali pri izvajanju javne oblasti, ki je bila dodeljena upravljavcu;
- za namene arhiviranja v javnem interesu, za znanstveno- ali zgodovinskoraziskovalne namene ali statistične namene;
- za uveljavljanje, izvajanje ali obrambo pravnih zahtevkov.

21. člen
(pravica do omejitve obdelave)

(1) Posameznik, na katerega se nanašajo osebni podatki, ima pravico doseči, da upravljavec omeji obdelavo, kadar velja eden 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 dokler se ne 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 z odstavkom 1, 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) Upravljavec, ki je dosegel omejitev obdelave v skladu z odstavkom 1, pred preklicem omejitve obdelave o tem obvesti posameznika, na katerega se nanašajo osebni podatki.

22. člen
(obveznost obveščanja v zvezi s popravkom ali izbrisom osebnih podatkov ali omejitvijo obdelave)

(1) Upravljavec vsakemu uporabniku, ki so mu bili osebni podatki razkriti, sporoči vse popravke ali izbrise osebnih podatkov ali omejitve obdelave, razen če se to izkaže za nemogoče ali vključuje nesorazmeren napor. Upravljavec o teh uporabnikih obvesti posameznika, na katerega se nanašajo osebni podatki, če ta posameznik tako zahteva.

23. člen
(pravica do prenosljivosti podatkov)

(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, kadar:
- obdelava temelji na privolitvi,
- se obdelava izvaja z avtomatiziranimi sredstvi.

(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.

24. člen
(pravica do ugovora)

(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. 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.

(2) Posameznika, na katerega se nanašajo osebni podatki, se na pravico izrecno opozori najpozneje ob prvem komuniciranju z njim in se mu to pravico predstavi jasno in ločeno od vseh drugih informacij.

(3) Kadar se osebni podatki obdelujejo v znanstveno- ali zgodovinskoraziskovalne 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.

25. člen
(dolžnost obvestitve posameznikov o pravicah)

(1) Odgovorna oseba organizacije je dolžna poskrbeti za to, da so posamezniki na primeren način, ki je skladen z zahtevami Splošne uredbe in zakonodajo o varstvu podatkov, obveščeni o pravicah. Organizacija poskrbi za enotno kontaktno točko, na katero se lahko obrnejo posamezniki pri uveljavljanju svojih pravic.

26. člen
(postopek posredovanja osebnih podatkov)

(1) Zdravstveni dom posreduje osebne podatke drugim osebam javnega sektorja ali drugim fizičnim ali pravnim osebam, če je za posredovanje dana ustrezna pravna podlaga v skladu z zakonodajo, razen če drug zakon določa drugače. Prejemnik podatkov sme osebne podatke obdelovati samo za namen, za uresničevanje katerega se mu posredujejo.

(2) Posredovanje osebnih podatkov mora vlagatelj zahtevati pisno. Zahteva mora vsebovati:
- podatke o vlagatelju zahteve (za fizično osebo: osebno ime, 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 vlagatelja oziroma 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;
- identifikacijo zadeve, v zvezi s katero so osebni podatki potrebni, ter navedbo organa ali drugega subjekta, ki obravnava zadevo;
- vrste osebnih podatkov, ki naj se mu posredujejo;
- obliko in način pridobitve zahtevanih osebnih podatkov.

(3) Zdravstveni dom vlagatelju, če drug 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. Zdravstveni dom in vlagatelj se v roku lahko dogovorita za njegovo podaljšanje. Če zdravstveni dom v roku 15 dni ne posreduje podatkov oz. se rok ne podaljša, se šteje, da je zahteva zavrnjena.

27. člen
(način posredovanja podatkov)

(1) Osebni podatki, ki se posredujejo uporabniku v fizični obliki, morajo biti posredovani v ovojnici, ki ne omogoča, da bi bila ob normalni svetlobi ali pri osvetlitvi ovojnice z običajno lučjo vidna vsebina ovojnice. Ovojnica mora tudi zagotoviti, da odprtja ovojnice in seznanitve z njeno vsebino ni mogoče opraviti brez vidne sledi odpiranja ovojnice.

(2) Osebne podatke je dovoljeno prenašati z informacijskimi, telekomunikacijskimi in drugimi sredstvi le ob izvajanju postopkov in ukrepov, ki nepooblaščenim preprečujejo prilaščanje ali uničenje podatkov ter neupravičeno seznanjanje z njihovo vsebino.

(3) Posebne vrste osebnih podatkov se v fizični obliki pošilja naslovnikom v zaprtih ovojnicah. V primeru, da se posebne vrste osebnih podatkov pošilja v elektronski obliki, mora biti med prenosom zagotovljena njihova nečitljivost, tako da so šifrirani in zavarovani z geslom. Podrobnosti o načinu pošiljanja posebnih vrst osebnih podatkov predpiše z navodilom odgovorna oseba organizacije po posvetu s pooblaščeno osebo za varstvo podatkov.

28. člen
(evidenca posredovanj podatkov)

(1) Vsakršno koli posredovanje osebnih podatkov se zaznamuje z navedbo naslednjih podatkov:
- osebno ime/firmo in naslov/sedež osebe, kateri so bili posredovani osebni podatki,
- navedba, če je bilo posredovanje opravljeno po uradni dolžnosti,
- pravna podlaga, na podlagi katere so bili posredovani osebni podatki,
- kateri osebni podatki so bili posredovani,
- datum posredovanja podatkov,
- oseba, ki je posredovala podatek.

(2) Seznam iz prejšnjega odstavka se vodi v fizični ali v elektronski obliki.

VI. EVIDENTIRANJE OBDELAVE OSEBNIH PODATKOV

29. člen
(evidenca dejavnosti obdelave)

(1) Organizacija vodi evidenco dejavnosti obdelave v skladu z določbami člena 30 Splošne uredbe.

(2) Ta evidenca vsebuje vse naslednje informacije:
- naziv evidence;
- 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, 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.

(3) Vsak obdelovalec in predstavnik obdelovalca, kadar ta obstaja, vodita evidenco vseh vrst dejavnosti obdelave, ki jih izvajata v imenu upravljavca, ki vsebuje:
- naziv ali ime in kontaktne podatke obdelovalca ali obdelovalcev in vsakega upravljavca, v imenu katerega deluje obdelovalec ter, kadar obstajajo, predstavnika upravljavca ali obdelovalca in pooblaščene osebe za varstvo podatkov;
- vrste obdelave, ki se izvaja v imenu posameznega upravljavca;
- kadar je ustrezno, prenose osebnih podatkov v tretjo državo ali mednarodno organizacijo, v primeru prenosov pa tudi dokumentacijo o ustreznih zaščitnih ukrepih;
- kadar je mogoče, splošni opis tehničnih in organizacijskih varnostnih ukrepov.

(4) Evidence iz drugega in tretjega odstavka tega člena se vodi v pisni obliki, vključno z elektronsko obliko.

(5) Upravljavec, obdelovalec ali predstavnik upravljavca ali obdelovalca, kadar ta obstaja, nadzornemu organu na zahtevo omogočijo dostop do evidenc.

(6) Zaposleni, ki obdelujejo osebne podatke, morajo biti seznanjeni z evidenco dejavnosti obdelave, vpogled v evidenco dejavnosti obdelave je omogočana vsakemu zaposlenemu na zahtevo.

30. člen
(vloga obdelovalca)

(1) Z vsako zunanjo pravno ali fizično osebo, ki opravlja posamezna opravila v zvezi z obdelavo osebnih podatkov za upravljavca, se sklene pisna pogodba o opravljanju storitev, katera vsebuje tudi določila o predmetu obdelave (zlasti vsebino in trajanje obdelave, naravo in namen obdelave, vrste osebnih podatkov in kategorije posameznikov), pravicah in obveznostih pogodbenega obdelovalca in upravljavca ter postopke in ukrepe za zavarovanje osebnih podatkov skladno s Splošno uredbo in zakonom, ki ureja varstvo osebnih podatkov.

(2) Obdelovalci so tudi zunanji sodelavci, ki vzdržujejo strojno in programsko opremo ter izdelujejo in nameščajo novo strojno ali programsko opremo, v kolikor imajo pri svojem delu dostop do osebnih podatkov.

(3) Zunanje pravne ali fizične osebe smejo opravljati storitve obdelave osebnih podatkov samo v okviru pooblastil upravljavca in osebnih podatkov ne smejo obdelovati ali drugače uporabljati za noben drug namen.

(4) Pooblaščena pravna ali fizična oseba, ki za upravljavca opravlja dogovorjene storitve izven prostorov upravljavca, mora imeti vsaj enako strog način zagotavljanja varnosti osebnih podatkov, kakor ga določa ta pravilnik.

31. člen
(evidenca obdelovalcev)

(1) Organizacija vodi evidenco obdelovalcev, ki se preverja najmanj en krat letno. Evidenca vsebuje vsaj naslednje podatke:
- naziv obdelovalca;
- interna številka krovne pogodbe z obdelovalcem, če obstaja;
- interna številka pogodbe o pogodbeni obdelavi, če obstaja in datum sklenitve in poteka pogodbe;
- druga oblika zaveze za izpolnjevanje zahtev v skladu z zakonodajo (aneks h krovni pogodbi, enostranska izjava, posebna pogodba ...);
- datum zadnjega preverjanja seznama.

VII. VARNOST OBDELAVE OSEBNIH PODATKOV IN ORGANIZACIJSKI UKREPI

32. člen
(vgrajeno in privzeto varstvo podatkov)

(1) Organizacija v okviru lastnega razvoja oziroma pri naročanju programske opreme za rešitve in storitve obdelave sledi načelu vgrajenega in privzetega varstva osebnih podatkov, ki obsegajo predvsem:
- minimizacijo obdelave osebnih podatkov;
- čimprejšnjo psevdomizacijo osebnih podatkov;
- preglednost pri nalogah in obdelavi osebnih podatkov;
- omogočanje posameznikom, na katere se nanašajo osebni podatki, da spremljajo obdelavo osebnih podatkov in
- omogočanje upravljavcu, da vzpostavi in izboljša varnostne ukrepe.

(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, se organizacija zavezuje, da bo proizvajalce produktov, storitev in aplikacij spodbujal, da pri razvoju in oblikovanju takih produktov, storitev in aplikacij upoštevajo pravico do varstva podatkov ter ob ustreznem upoštevanju najnovejšega tehnološkega razvoja, zagotovijo, da so upravljavci in obdelovalci zmožni izpolnjevati svoje obveznosti varstva podatkov. Načeli vgrajenega in privzetega varstva podatkov se morata upoštevati tudi pri javnih razpisih.

(3) Organizacija se v zvezi z zagotavljanjem vgrajenega in privzetega varstva podatkov iz prvega in drugega odstavka tega člena posvetuje s pooblaščeno osebo za varstvo podatkov.

33. člen
(kakovost obdelave podatkov)

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

VIII. OCENA UČINKA V ZVEZI Z VARSTVOM PODATKOV

34. 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 osebnih podatkov, povzročila veliko tveganje za pravice in svoboščine posameznikov, se na to opozori vodstvo organizacije.

(2) V tem primeru se opravi presoja glede izvedbe, ocena učinka v zvezi z varstvom osebnih podatkov, kot jo predvideva člen 35 Splošne uredbe in veljavna zakonodaja s področja varstva osebnih podatkov.

(3) Po potrebi se v okviru priprave ocene učinkov v zvezi z varstvom podatkov zaprosi za mnenje posameznike, na katere bi se nanašali obdelovani podatki oziroma ponudnika informacijske rešitve oziroma poklicna združenja (npr. Zdravniška zbornica ali Združenje zdravstvenih zavodov).

(4) Oceno učinka izdela odgovorna oseba oddelka, kjer evidenca dejavnosti obdelave nastaja oz. se pojavi potreba po izvedbi ocen učinka. Pri oceni učinka sodeluje tudi pooblaščena oseba za varstvo osebnih podatkov.

IX. BRISANJE PODATKOV

35. člen
(rok hrambe podatkov)

(1) Osebni podatki se lahko obdelujejo le toliko časa, kolikor je določen rok hrambe oziroma dokler obstaja pravna podlaga iz člena 6 Splošne uredbe. Rok hrambe osebnih podatkov organizacija omeji na najkrajše možno obdobje in le, dokler je hramba potrebna za dosego namena obdelave, zaradi katerega so se podatki ali nadalje obdelave, zaradi katerega so se podatki zbirali ali nadalje obdelovali. Po preteku roka hranjenja se osebni podatki zbrišejo, uničijo, blokirajo ali anonimizirajo oz. se izvede drug postopek, ki onemogoča identifikacijo posameznika, razen če zakon ali drug akt ne določa drugače.

(2) Osebne podatke, ki jih organizacija obdeluje na osnovi pogodbenega odnosa s posameznikom, ta hrani za obdobje, ki je potrebno za izvršitev pogodbe in še 6 let po njenem prenehanju, razen v primerih, ko pride med posameznikom in organizacijo do spora v zvezi s pogodbo. V takem primeru hrani podatke še 10 let po pravnomočnosti sodne odločbe, arbitraže ali poravnave ali, če sodnega spora ni bilo, 6 let od dneva mirne razrešitve spora.

(3) Tiste osebne podatke, ki jih organizacija obdeluje na podlagi osebne privolite posameznika ali zakonitega interesa, bo ta hranil do preklica te privolitve oziroma do zahteve do izbrisa. V

primeru preklica privolitve ali utemeljene zahteve za izbris se podatki izbrišejo brez nepotrebnega odlašanja, po tem ko organizacija odloči o zahtevku posameznika. Organizacija lahko te podatke izbriše tudi pred preklicem, kadar je bil dosežen namen obdelave osebnih podatkov ali če tako določa zakon.

(4) V primeru ko zdravstveni dom prejme zahtevo posameznika v zvezi z njegovimi pravicami iz 15. do 22. člena Splošne uredbe, zdravstveni dom ne sme izbrisati, odsvojiti ali spremeniti zahtevanih osebnih podatkov, ki so predmet postopka, dnevnikov obdelav in drugih povezanih informacij, ne glede na potek predpisanih ali interno določenih rokov hrame, dokler o zadevi ni pravnomočno odločeno, po pravnomočnosti pa ravna skladno s pravnomočno odločitvijo v zadevi.

(5) Izjemoma lahko zdravstveni dom zavrne zahtevo za izbris razlogov iz Splošne uredbe, kot jih našteva:
- uresničevanje pravice do svobode izražanja in obveščanja,
- izpolnjevanje pravne obveznosti obdelave,
- razlogi javnega interesa na področju javnega zdravja,
- nameni arhiviranja v javnem interesu,
- znanstveno- ali zgodovinskoraziskovalni nameni ali statistični nameni,
- izvajanje ali obramba pravnih zahtevkov.

36. člen
(brisanje podatkov)

(1) Za brisanje podatkov iz nosilcev podatkov se uporabi takšna metoda brisanja, da je nemogoča restavracija vseh ali dela brisanih podatkov.

(2) Podatki na klasičnih medijih (listine, kartoteke, register, seznam ...) se uničijo na način, ki onemogoča branje vseh ali dela uničenih podatkov. Na enak način se uničuje pomožno gradivo (npr. matrice, izračune in grafikone, skice, poskusne oziroma neuspešne izpise ipd.).

(3) Prepovedano je odmetavati odpadne nosilce podatkov z osebnimi podatki v koše za smeti.

(4) Pri prenosu nosilcev osebnih podatkov na mesto uničenja je potrebno zagotoviti ustrezno zavarovanje tudi v času prenosa. Prenos nosilcev podatkov na mesto uničenja ter uničevanje nosilcev osebnih podatkov nadzoruje posebna komisija, ki o uničenju sestavi tudi ustrezen zapisnik oziroma se uničenje preda ustrezni zunanji službi na osnovi sklenjene pogodbe.

(5) Organizacija načine hrambe, arhiviranja in uničenja zdravstvene dokumentacije v fizični ali elektronski obliki sprejme v posebnem dokumentu.

X. VAROVANJE PROSTOROV IN RAČUNALNIŠKE OPREME

37. člen
(varovanje prostorov)

(1) Prostori, v katerih se nahajajo nosilci osebnih podatkov, strojna in programska oprema (varovani prostori), morajo biti varovani z organizacijskimi ter fizičnimi in/ali tehničnimi ukrepi, ki onemogočajo nepooblaščenim osebam dostop do podatkov.

(2) Kot varovani prostor so opredeljeni prostori vodstva, strežniške sobe, pisarne in drugi prostori, v katere nepooblaščene osebe nimajo vstopa.

(3) Dostop do varovanih prostorov je mogoč le v rednem delovnem času, izven tega časa pa samo na podlagi dovoljenja odgovorne osebe organizacije.

(4) Ključi varovanih prostorov se uporabljajo in hranijo v skladu s hišnim redom. Ključi se ne puščajo v ključavnici v vratih iz zunanje strani.

(5) Varovani prostori ne smejo ostajati nenadzorovani oziroma se morajo zaklepati ob odsotnosti delavcev, ki jih nadzorujejo.

(6) 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 morajo biti izklopljeni oz. fizično ali programsko zaklenjeni.

(7) Obiskovalci se smejo v poslovnih prostorih, v katerih se nahajajo nosilci podatkov, gibati samo v spremstvu zaposlenega. To določilo ne velja za zunanje sodelavce organizacije, katerih vstop in gibanje v prostorih, v katerih se nahajajo nosilci podatkov, je urejeno s pogodbo ter jim je dodeljeno vstopno sredstvo.

38. člen
(vhodna kontrola zaposlenih)

(1) Če organizacija za kontrolo vhodov uporablja kartice, je vsak zaposleni, ki mu je dodeljena kartica za vhodno kontrolo, dolžan z njo ravnati z vso skrbnostjo in z zavedanjem, da je namenjena samo njegovi osebni uporabi. Izgubo ali odtujitev kartice mora takoj javiti kadrovski oziroma ustrezni službi, ki kartico nemudoma prekliče.

(2) Vsak zaposleni je bil opozorjen in seznanjen z varnostnimi zahtevami pri ravnanju s kartico.

(3) Seznam zaposlenih, ki uporabljajo kartico za vhodno kontrolo, obsega ime in priimek zaposlenega ter interno številko zaposlenega, če obstaja. Seznam, skupaj z izjavo in datumom ter podpisom prevzema kartice, hrani kadrovska služba.

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

(1) Zaposleni svojega delovnega mesta ne smejo pustiti nenadzorovanega oziroma morajo poskrbeti, da so takrat originalne listine in nosilci osebnih podatkov shranjeni tako, da nepooblaščene osebe do njih nimajo dostopa. Izven delovnega časa morajo biti omare in pisalne mize z nosilci osebnih podatkov zaklenjene (politika čiste mize).

(2) Računalniški zasloni morajo biti nameščeni tako, da nepooblaščene osebe nimajo vpogleda v prikazovane podatke.

(3) Računalniki in druga informacijska tehnologija oziroma oprema, ki omogoča dostop do osebnih podatkov morajo biti v času odsotnosti zaposlenega bodisi izklopljeni bodisi fizično ali programsko zaklenjeni (politika čistega zaslona).

(4) Zaposleni ne smejo brez nadzora puščati nosilcev osebnih podatkov na mizah v prisotnosti oseb, ki nimajo pravice vpogleda vanje.

(5) Nosilci osebnih podatkov, ki se nahajajo izven varovanih prostorov (npr. avla, hodniki, skupni prostori, učilnice, predavalnice, jedilnice) morajo biti zaklenjeni v omarah.

(6) Posebnih vrst osebnih podatkov se ne sme hraniti izven varovanih prostorov. Iznos nosilcev podatkov, ki vsebujejo posebne vrste osebnih podatkov iz prostorov organizacije ni dovoljen, razen v primerih, ko je to nujno potrebno oziroma določeno z zakonom.

(7) V prostorih, ki so namenjeni poslovanju s strankami oziroma nimajo statusa varovanega prostora in je vanje dovoljen dostop nezaposlenim (npr. sprejemna pisarna, tajništvo), morajo biti nosilci podatkov nameščeni tako, da stranke nimajo neposrednega vpogleda vanje. V takih prostorih na oglasnih deskah ali kakorkoli drugače ne smejo biti izpostavljeni taki podatki, na osnovi katerih bi se lahko nepooblaščene osebe seznanile z osebnimi podatki posameznika in za katere organizacija nima pravne podlage za njihovo objavo oziroma obdelavo.

(8) Vzdrževalci prostorov, informacijske tehnologije oziroma strojne in programske opreme, obiskovalci in poslovni partnerji se smejo gibati v varovanih prostorih samo z vednostjo odgovorne osebe. Delavci, kot so čistilke, varnostniki idr., se lahko izven delovnega časa gibljejo samo v tistih varovanih prostorih, kjer je onemogočen vpogled v osebne podatke (nosilci podatkov so shranjeni v zaklenjenih omarah in pisalnih mizah, računalniki in druga strojna oprema so izklopljeni ali kako drugače fizično ali programsko zaklenjeni).

40. 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) V primeru, da se navedeni dokumenti ne shranijo, se trajno uničijo.

41. člen
(vzdrževanje in popravila informacijske tehnologije in elektronskih storitev)

(1) Vzdrževanje in popravila informacijske tehnologije in elektronskih storitev ter druge opreme je dovoljeno samo z vednostjo odgovorne osebe oziroma ga lahko izvajajo pooblaščeni servisi ali vzdrževalci, ki imajo z organizacijo sklenjeno ustrezno pogodbo.

42. člen
(revizijske sledi)

(1) Organizacija v zvezi z dostopi do podatkov, postopkov obdelave in do sistemov obdelave tvori, beleži in hrani zapise, ki omogočajo ugotavljanje, kdo, kdaj in kje je dostopal do določenega podatka, postopka obdelave oz. sistema za obdelavo.

(2) Zapisi iz prejšnjega odstavka 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 so odgovorni skrbniki informacijskih sistemov oz. rešitev, ki na podlagi posveta s pooblaščeno osebo za varstvo osebnih podatkov določijo, kdo in v katerih primerih

sme dostopati do zapisov revizijskih sledi. Način zbiranja zapisov, hrambo in uporabo revizijskih sledi organizacija določi v posebnem dokumentu.

43. člen
(mehanizmi za zaščito pred zlonamerno programsko opremo)

(1) Organizacija uporablja ustrezne mehanizme za zaščito pred zlonamerno programsko opremo, da tako zmanjšuje možnost, da bi le-ta ogrozila neoporečnost in zaupnost informacij in programske opreme. Organizacija uporablja programsko opremo za zaščito pred virusi in drugo neželeno programsko opremo (spyware, adware, grayware itd.). Omenjena programska oprema mora biti nameščena na vse odjemalce.

(2) Način uporabe mehanizmov za zaščito pred zlonamerno programsko opremo se določi v posebnem dokumentu.

XI. INFORMACIJSKO VARNOSTNA POLITIKA

44. člen
(varovanje dostopa do sistemske in aplikativno programske računalniške opreme)

(1) Dostop do elektronskih storitev oziroma do programske opreme mora biti varovan tako, da dovoljuje dostop samo za to vnaprej določenim zaposlenim v organizaciji ali zunanjim sodelavcem - fizičnim ali pravnim osebam - ki v skladu s pogodbo opravljajo dogovorjene storitve.

(2) Zaposlenemu oziroma zunanjim sodelavcem se dodeljujejo ali ukinjajo pravice dostopa do informacij, aplikacij in sistemov, ki jih potrebujejo glede na dodeljeno delovno mesto, kar določi in odobri nadrejena oseba. Način dodeljevanja ali ukinjanja dostopa do sistemske in aplikativne računalniške opreme se določi v posebnem dokumentu.

(3) Popravljanje, spreminjanje in dopolnjevanje sistemske in aplikativne programske opreme je dovoljeno samo na podlagi odobritve odgovorne osebe ali od nje pooblaščene osebe, izvajajo ga lahko samo pooblaščeni servis ali vzdrževalec, ki ima z organizacijo sklenjeno ustrezno pogodbo. Izvajalci morajo izvedene spremembe in dopolnitve sistemske in aplikativne programske opreme ustrezno dokumentirati. V primeru, da je potrebno za delo izdelati kopije, morajo biti le-te po prenehanju namena, s katerim so bile izdelane, ustrezno uničene. Enako velja za ostale izpise, izvoze podatkov ali druge pripomočke za izvedbo storitve servisiranja.

(4) Vsebine na nosilcih podatkov na mrežnih strežnikih in lokalnih delovnih postajah, kjer se nahajajo osebni podatki, se mora redno preverjati zaradi potencialne prisotnosti računalniških virusov in druge oblike zlonamerne kode. V primeru odkritja virusa, se ta odpravi s strani ustrezne strokovne službe oziroma pristojne osebe, zadolžene za delovanje računalniškega informacijskega sistema, obenem pa se skuša ugotovi tudi vzrok pojava virusa.

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

(6) Zaposleni ne smejo nameščati programske opreme brez odobritve osebe, zadolžene za delovanje računalniškega informacijskega sistema. Prav tako ne smejo odnašati programske

opreme iz organizacije brez odobritve odgovorne osebe organizacije ali vodje organizacijske enote in vednosti osebe, zadolžene za delovanje računalniškega informacijskega sistema.

(7) Dostop do podatkov in uporaba sistemske in aplikativno programske opreme se varuje s sistemom gesel za avtorizacijo in identifikacijo uporabnikov programske opreme in podatkov. Vsak uporabnik ima svoje geslo za dostopanje do posameznih elektronskih storitev, ki ga prejme ob nastopu delovnega mesta. Posojanje gesel in uporaba skupinskih gesel je prepovedana.

45. člen
(uporaba naprav za obdelavo osebnih podatkov)

(1) Zaposleni uporabljajo različno informacijsko tehnologijo (računalnik, telefon, tablica in druge elektronske naprave) ter različne elektronske storitve (dostop do interneta, elektronska pošta, dostop do oblaka, skupni imeniki in mape ter druga programska oprema oziroma storitve), ki jim jo dodeli delodajalec, izključno za službene namene.

(2) V omejenem obsegu in razumnih mejah se s strani organizacije dodeljena informacijska tehnologija in elektronske storitve lahko uporabljajo tudi v zasebne namene. Pri tem morajo delavci varovati ugled organizacije, tehnologije in storitev pa se ne sme uporabljati za neprimerne ali žaljive namene. Vodstvo lahko po lastni presoji delavcu kadarkoli prepove uporabo v zasebne namene.

(3) Zasebne naprave iz prejšnjega odstavka morajo biti vključene v popisu informacijskih sredstev ter opremljene z ustreznimi informacijskimi varnostnimi rešitvami (šifriranje, razmejitev obdelave zasebnih podatkov).

46. člen
(uporaba zasebne opreme zaposlenega)

(1) Delavec lahko za namene opravljanja dela poleg službene opreme uporablja svojo zasebno opremo in druge tehnične naprave (predvsem telefon), če takšno uporabo odobri odgovorna oseba in delavec poda prostovoljno pisno soglasje, da lahko delodajalec za namene izvajanja delovnega procesa pri tem obdeluje njegovo zasebno telefonsko številko oziroma zasebni elektronski naslov.

(2) V primeru prenehanja delovnega razmerja je delavec dolža z zasebne oreme ali drugih naprav in njihovih nosilcev podatkov, ki jih je v soglasju z delodajalcem uporabljal za službene namene, izbrisati vse osebne podatke, ki so bili preneseni v okviru opravljanja delovnega procesa, in vse datoteke, ki jih je zaposleni uporabljal v službene namene, ne glede na to, ali vsebujejo osebne podatke.

47. člen
(uporaba svetovnega spleta)

(1) Dostop do svetovnega spleta je omogočen zaposlenim za njihovo delo, izobraževanje in informiranje.

(2) Zaposleni v organizaciji morajo uporabljati svetovni splet v skladu z etičnimi in moralnimi normami. Vsi uporabniki informacijskih sistemov se morajo zavedati, da se v medmrežju izkazujejo z mrežnim naslovom organa javnega zavoda (IP naslov).

(3) V omrežju organizacije se na zahtevo odgovorne osebe lahko izdeluje statistika obiskanih spletnih strani, ki mora biti anonimizirana in ni za javno objavo. Statistika se lahko uporablja izključno za načrtovanje in varovanje informacijskega sistema.

(4) Vodstvo organizacije lahko zaradi zagotavljanja informacijske varnosti in razpoložljivosti informacijskih virov ter zaradi preprečevanja kršitev s posebno odredbo odredi blokado določenih spletnih strani. Blokado dostopa do določenih spletnih strani izvede oseba, zadolžena za delovanje računalniškega informacijskega sistema, na podlagi pisne odredbe odgovorne osebe. O blokadi se obvesti vse zaposlene po elektronski pošti.

48. člen
(službena elektronska pošta)

(1) Službena elektronska pošta se v organizaciji lahko uporablja kot orodje za komunikacijo s posamezniki, pacienti, strankami, zaposlenimi in zunanjimi izvajalci. Pri tem se morajo delavci držati ne le etičnih in moralnih norm, temveč tudi bontona. Pošiljatelj se mora zavedati, da se vsako sporočilo s službenega elektronskega naslova pri prejemniku lahko razloži kot mnenje organizacije, v katerem je pošiljatelj zaposlen.

(2) Zaposleni po elektronski pošti ne smejo pošiljati verižnih pisem in obsežnih datotek (glasba, filmi, zagonske datoteke in skripte ipd.), razen ko to zahtevajo potrebe delovnih procesov.

(3) Posredovanje službenih elektronskih naslovov na zunanje spletne strežnike za namene prijave zaposlenega na določeno storitev (npr. pošte liste, prijava na izobraževanja ipd.) ni dovoljeno, razen če je povezano s poslovnim procesom organizacije.

(4) Zaposleni svojega službenega elektronskega naslova ne smejo uporabljati v trženjske namene in z njega ne smejo pošiljati oglasne pošte na znane in/ali neznane naslove. Prav tako se zaposleni ne smejo prijavljati na oglasno pošto ali novice z elektronskimi naslovi organizacije, razen če je to povezano s potrebami delovnega mesta.

(5) Zaposleni morajo biti previdni pri odpiranju elektronske pošte s priponkami neznanih pošiljateljev. Če sumijo, da gre za nezaželeno pošto, ki bi lahko bila škodljiva, naj je ne odpirajo, temveč naj o tem obvestijo pristojno osebo, zadolženo za delovanje računalniškega informacijskega sistema.

(6) Zaposleni nikakor ne smejo pošiljati posebnih vrst osebnih podatkov ali gesel po elektronski pošti razen v ustrezno akreditiranih sistemih, oziroma mora biti podatkom med prenosom zagotovljena njihova nečitljivost, tako da so šifrirani in zavarovani z geslom.

(7) Uporaba zasebne elektronske pošte (npr. Gmail, Yahoo ipd.) za službene namene je prepovedana, saj potencialno predstavlja neupravičeno obdelavo osebnih podatkov. Izjemoma je izključno za namene komuniciranja med zaposlenimi na osnovi dovoljenja odgovorne osebe dovoljeno uporabljati zasebno elektronsko pošto.

49. člen
(generiranje gesel)

(1) Pri generiranju oziroma določanju gesel je treba spoštovati pravila:
- gesla morajo biti dolžine minimalno 8 znakov ali ustrezno daljša, v kolikor je to določeno za posamezno uporabniško rešitev;
- gesla ne smejo vsebovati smiselnih alfanumeričnih zaporedij znakov;
- gesla morajo biti kvalitetna (priporoča se uporaba ustrezne dolžine, posebni znaki, velike in male črke, številke);
- gesla ne smejo vsebovati besed iz različnih slovarjev;
- gesla naj ne bodo ciklična in naj se ne ponavljajo iz predhodnih obdobij;
- uveljavljeno mora biti obvezno redno spreminjanje gesel (najmanj na 6 mesecev);
- začetna gesla se ob prvi prijavi spremenijo;

- gesla, ki jih je generiral zunanji dobavitelj, je potrebno takoj spremeniti ob prvi uporabi v produkcijskem okolju;
- uporabniško ime ne sme kazati posebnih pooblastil uporabnika.

50. člen
(ravnanje z gesli)

(1) Pri ravnanju z gesli je treba obvezno spoštovati napotke:
- pooblaščena oseba, ki dodeljuje gesla, jih mora obravnavati zaupno, preprečiti mora možnost nepooblaščenega vpogleda in jih posredovati na varen način;
- uporabnikom mora biti omogočeno, da kadarkoli spremenijo svoje uporabniško geslo;
- geslo ne sme biti nikdar prikazano na zaslonu;
- gesla, ki se hranijo v elektronski obliki, morajo biti obvezno shranjena v šifrirani obliki;
- vsak uporabnik mora imeti svoje uporabniško ime in geslo izključno za osebno rabo;
- geslo je potrebno hraniti na način, ki drugi osebi popolnoma onemogoči možnost vpogleda;
- vsak uporabnik je odgovoren za zaupnost gesla in ga ne sme v nobenem primeru zaupati drugi osebi;
- v nobenem primeru uporabnik ne sme izdati gesla nadrejenemu, podrejenemu ali osebi, ki ga nadomešča ali IT osebju;
- v primeru razkritja gesla ali suma razkritja gesla mora to nemudoma sporočiti pooblaščeni osebi za dodeljevanje gesel.

(2) Vsa gesla in postopki, ki se uporabljajo za vstop in administriranje mreže osebnih računalnikov (supervizorska oziroma nadzorna gesla), administriranje elektronske pošte in administriranje aplikativnih programov, se hranijo v sefu v zaprti kuverti ali na drug ustrezen način, tako, da je dostop nepooblaščenih oseb onemogočen. Uporabi se jih samo v izrednih okoliščinah oziroma ob nujnih primerih. Vsako uporabo teh gesel sme dovoliti odgovorna oseba organizacije. Po vsaki takšni uporabi se določi nova vsebina gesel.

51. člen
(varnostno kopiranje podatkov)

(1) Organizacija zagotovi rezervno kopijo podatkov in omogoči ponovno vzpostavitev sistema ter uspešno nadaljevanje dela po množici različnih dogodkov oz. varnostnih incidentov, ki povzročijo poškodovanje ali izgubo podatkov. To so problemi s strojno opremo, problemi s programsko opremo, človeške napake, naravne nesreče ipd. Vsi pomembni elektronski podatki se redno shranjujejo na medije daljše trajnosti. Praviloma se enkrat letno izvede test obnove varnostnih kopij, kar se ustrezno dokumentira.

(2) Varnostne kopije podatkov se hranijo zaklenjene v zavarovanih ognjevarnih omarah, zaščitene pred nepooblaščenim dostopom ter drugimi vplivi kot so poplave ali elektromagnetne motnje.

(3) Način izvajanja varnostnega kopiranja podatkov se določi v posebnem dokumentu.

52. člen
(oddaljen dostop do sistemov)

(1) Oddaljen dostop do informacijskega sistema organizacije je dovoljen le na podlagi odobrene metode z ustrezno ravnjo varnosti, in sicer za tiste delavce, ki dostop potrebujejo zaradi opravljanja delovnih nalog, vendar le v omejenem obsegu. Treba je upoštevati tudi načelo praznega zaslona. Po končanem delu se je treba obvezno odjaviti iz sistema in zagotoviti, da katerikoli podatki in sledi ne ostanejo na delovni postaji.

(2) Za uveljavitev oddaljenega varnega dostopa je na strojni opremi zagotovljena prepoznava ustrezne programske opreme, ki omogoča zaščito končne točke pred internetnimi grožnjami. Za zagotavljanje zaupnosti se šifrira ves promet iz končne točke oddaljenega omrežja do omrežja organizacije.

53. člen
(uporaba naprav za komunikacijo na daljavo)

(1) Zdravstvene storitve, glede katerih sta lahko ob upoštevanju pravil medicinske doktrine bolnik in izvajalec ali več izvajalcev zdravstvene dejavnosti prostorsko ločena, lahko opravijo z uporabo informacijskih in telekomunikacijskih tehnologij (v nadaljnjem besedilu: telemedicina). Zdravstvena dokumentacija se v tem primeru posreduje v skladu s predpisi o varstvu osebnih podatkov, ki se nanašajo na prenos občutljivih osebnih podatkov prek telekomunikacijskih omrežij.

(2) V primeru opravljanja zdravstvene dejavnosti v obliki telemedicine se šteje, da je zdravstveno varstvo zagotovljeno v državi, v kateri ima sedež izvajalec zdravstvene dejavnosti, ki opravlja telemedicino.

(3) Zaposleni lahko za potrebe komunikacije na daljavo uporabljajo storitve telemedicine v skladu z zakonodajo, tem pravilnikom in z navodili odgovorne osebe organizacije.

54. člen
(vpogled v službeno informacijsko tehnologijo zaposlenega)

(1) Oseba, zadolžena za delovanje informacijskega sistema v organizaciji, lahko na posebej utemeljeno pisno zahtevo odgovorne osebe v prisotnosti tričlanske komisije v izrednih primerih (nenadna odpoved delavca, smrt delavca, nepričakovane, nenadne in dalj časa trajajoče ali trajne odsotnosti delavca, odpoved delovnega razmerja s strani zaposlenega brez odpovednega roka, odpoved delovnega razmerja iz krivdnih razlogov zaradi neopravičene odsotnosti in podobni izredni primeri) vpogleda v informacijsko tehnologijo (npr. v računalnik) ali druge elektronske storitve (npr. v elektronsko pošto) delavca le, če je to nujno potrebno za izpolnjevanje zakonskih obvez organizacije oziroma za vodenje delovnega procesa.

(2) Vpogled opravi tričlanska komisija, ki jo vsakokrat imenuje odgovorna oseba organizacije. V njej mora biti vsaj en predstavnik zaposlenih, ki ni vodstveni delavec. O vpogledu mora komisija napisati zapisnik, ki vsebuje:
- obrazložitev razloga vpogleda,
- zapisnik o vstopu z morebitnimi pripombami delavca, če je ta navzoč,
- navedbe prisotnih oseb,
- seznam oziroma izpis pridobljenih podatkov.

(3) Če se pojavi utemeljen sum, da zaposleni ne spoštujejo določil informacijsko varnostne politike tega pravilnika, lahko oseba, zadolžena za delovanje računalniškega informacijskega sistema, na posebej utemeljeno pisno zahtevo odgovorne osebe opravi nadzor uporabe elektronskih storitev, a zgolj z vidika pregleda dnevniških zapisov o količini prometa in shranjenih podatkov, ki obremenjujejo strežnik. Pri tem se ne sme pregledovati vsebin.

(4) O namenu uporabe informacijske tehnologije in elektronskih storitev iz tega člena ter možnosti vpogleda mora biti zaposleni pisno obveščen. Kot zadostno obvestilo se šteje obvestilo skupaj s temi pravili poslano vsem zaposlenim po elektronski pošti.

55. člen
(ravnanje zaposlenih ob prenehanju delovnega razmerja)

(1) Ob prenehanju delovnega razmerja oziroma po izčrpanju temelja za opravljanje dela je delavec dolžan vrniti službeno informacijsko tehnologijo, ki jo je uporabljal v službene namene, pri čemer mora pred vrnitvijo delavec sam poskrbeti, da so iz uporabljane informacijske opreme in elektronskih storitev očiščene oziroma izbrisane vse njegove zasebne vsebine, službene pa ohranjene v celoti.

(2) V primeru prenehanja delovnega razmerja je delavec dolžan z zasebne opreme ali drugih naprav in njihovih nosilcev podatkov, ki jih je v soglasju z delodajalcem uporabljal za službene namene, izbrisati vse osebne podatke, ki so bili preneseni v okviru opravljanja delovnega procesa in vse datoteke, ki jih je zaposleni uporabljal v službene namene, ne glede na to, ali vsebujejo osebne podatke.

XII. UKREPANJE OB SUMU KRŠITVE VARSTVA OSEBNIH PODATKOV

56. člen
(obvestilo o kršitvah)

(1) Zaposleni so dolžni o aktivnostih, ki so povezane z odkrivanjem, nepooblaščenim dostopom ali uničenjem podatkov, zlonamerni ali nepooblaščeni uporabi, prilaščanju, spreminjanju ali poškodovanju takoj obvestiti pooblaščeno osebo, sami pa poskušajo takšno aktivnost preprečiti.

(2) 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. Kršitev je lahko storjena nehote (npr. iz malomarnosti) ali pa je načrtovana oziroma naklepna. Na splošno ta kršitev pomeni varnostni incident, ki ogroža zaupnost, celovitost in dostopnost osebnih podatkov.

(3) Zaposleni so dolžni pri svojem delu spremljati in biti pozorni na morebitne varnostne incidente ter v skladu s tem pravilnikom ustrezno ravnati.

57. člen
(ukrepanje ob varnostnem incidentu)

(1) Nemudoma, ko zaposleni zasledijo, da se je v organizaciji zgodil varnostni incident, morajo nujno o tem obvestiti nadrejenega delavca oziroma vodstvo.

(2) Vodstvo mora najprej izvedeti, kaj se je zgodilo, oceniti, kakšne so potencialne škodljive posledice za pravice in svoboščine posameznikov in sprejeti ustrezne ukrepe za odpravo posledic ali vsaj zmanjšanje tveganj. Priporočljivo je, da se vodstvo za pripravo ocene verjetnosti in resnosti posledic za pravice in svoboščine posameznikov posvetuje s pooblaščeno osebo za varstvo podatkov.

(3) V primeru, da vodstvo organizacije oceni, da bo zaradi incidenta nastalo tveganje za pravice in svoboščine posameznikov, mora o tem obvestiti Informacijskega pooblaščenca brez odlašanja, najkasneje pa v 72 urah po zaznani kršitvi. V primeru, da se je incident zgodil v zvezi s podatki, pri katerih je organizacija v vlogi obdelovalca, mora o kršitvi obvestiti upravljavca v najkrajšem možnem času po zaznani kršitvi.

(4) Za prijavo se uporabi obrazec, ki vsebuje vsaj naslednje informacije, kot to zahteva Splošna uredba:

- opis vrste kršitve, kategorije in približno število posameznikov, na katere se nanašajo osebni podatki, vrste in približno število evidenc osebnih podatkov;
- kontaktne podatke pooblaščene osebe za varstvo podatkov;
- opis verjetnih posledic kršitve varstva osebnih podatkov;
- opis ukrepov, ki jih je upravljavec sprejel ali pa predvidenih ukrepov za ublažitev tveganj za kršitve.

58. člen
(obveznost obveščanja Informacijskega pooblaščenca)

(1) Za obveščanje Informacijskega pooblaščenca o kršitvah varstva osebnih podatkov po členu 33 Splošne uredbe je pristojna odgovorna oseba organizacije.

(2) Organizacija lahko s posebnim aktom podrobneje predpiše ravnanje in ukrepanje v primerih kršitve varstva osebnih podatkov.

XIII. KONČNE DOLOČBE

59. člen
(seznanitev zaposlenih s pravilnikom)

(1) S pravilnikom so seznanjeni zaposleni in sodelavci v organizaciji, tako da se pravilnik objavi na oglasnih deski ali na omrežju organizacije ter se pošlje vsem zaposlenim in sodelavcem preko elektronske pošte.

(2) Zaposleni in ostali pogodbeni sodelavci se redno, praviloma 1 krat letno, udeležijo izobraževanja s področja varstva osebnih podatkov, ki ga izvede pooblaščena oseba za varstvo podatkov.

60. člen
(začetek veljavnosti pravilnika)

(1) Z dnem, ko je sprejet ta pravilnik, preneha veljati obstoječi Pravilnik o varstvu osebnih podatkov.

(2) Ta pravilnik prične veljati in se začne uporabljati dne 15.10.2024

Ljubljana, 14.10.2024

Juventina Clinic d.o.o.
Prof.dr. Uroš Ahčan, direktor