24. maj 2018

Na podlagi 25. člena Zakona o varstvu osebnih podatkov (Uradni list RS, št. 94/07) in ob upoštevanju vsebine Uredbe (EU) 2016/679 Evropskega parlamenta in Sveta z dne 27. aprila 2016 o varstvu posameznikov pri obdelavi osebnih podatkov (v nadaljevanju Splošna uredba) je **ZDRAVSTVENI ZAVOD FLIS MARIBOR**, dne 24.05.2018 sprejel naslednji

P R A V I L N I K
O ZAVAROVANJU OSEBNIH PODATKOV

I. SPLOŠNE DOLOČBE

1. člen

S tem Pravilnikom se določajo postopki in ukrepi za zavarovanje vseh vrst osebnih podatkov, vodenih v zbirkah osebnih podatkov, s katerimi upravlja izvajalec zdravstvene dejavnosti (v nadaljevanju izvajalec). Določijo se tehnični in organizacijski ukrepi za zagotovitev skladnosti obdelave osebnih podatkov z določbami Splošne uredbe, zakona, ki ureja varstvo osebnih podatkov in drugih predpisov, ki urejajo varstvo osebnih podatkov.

S tem Pravilnikom se določijo osebe, ki so odgovorne za posamezne zbirke osebnih podatkov, in osebe, ki lahko zaradi narave njihovega dela obdelujejo posamezne osebne podatke, s katerimi upravlja izvajalec in jih obdeluje.

Ta Pravilnik določa ukrepe za zavarovanje pri zbiranju, obdelovanju, shranjevanju, posredovanju in uporabi osebnih podatkov pri izvajalcu.

V zadevah, ki jih ne ureja ta Pravilnik, se neposredno uporabljajo določbe Zakona o varstvu osebnih podatkov, Zakona o pacientovih pravicah, Zakona o zdravstveni dejavnosti, Zakona o zbirkah podatkov s področja zdravstvenega varstva, Zakona o arhivskem gradivu, ki vsebuje podatke o zdravljenju pacienta ter Zakona o varstvu dokumentarnega in arhivskega gradiva ter arhivih, Zakonom o zdravniški službo, Zakonom o zdravstvenem varstvu in zdravstvenem zavarovanju.

V Pravilniku uporabljeni in zapisan izrazi v slovnični obliki za moški spol, se uporabljajo kot nevtralni za ženski in moški spol.

2. člen

Izvajalec vodi katalog zbirk in podatkov v katerem so opisane vse zbirke (osebnih) podatkov, ki jih izvajalec vodi. Katalog podatkov se redno dopolnjuje ob vsaki spremembi podatkov, ki jih ta vsebuje. Zbirke osebnih podatkov so določene v prilogi (Priloga 9) tega Pravilnika.

3. člen

Določbe tega Pravilnika veljajo za vse vodene zbirke podatkov pri izvajalcu, ne glede na obliko, v kateri je osebni podatek izražen.

Varstvo osebnih podatkov se zagotavlja vsaki posameznici ali posamezniku, ne glede na narodnost, raso, barvo kože, veroizpoved, etnično pripadnost, spol, jezik, politično ali drugo prepričanje, spolno usmerjenost, spolno identiteto, premoženjsko stanje, kraj rojstva, izobrazbo, družbeni položaj, državljanstvo, kraj oziroma vrsto prebivališča, zdravstvene ali genske predispozicije ali katerokoli drugo osebno okoliščino.

4. člen

Vsi zaposleni in zunanji sodelavci pri izvajalcu, ki pri svojem delu uporabljajo osebne podatke, ki jih obdeluje izvajalec ali podatke, ki predstavljajo poslovno oziroma poklicno skrivnost ali imajo iz kakršnihkoli razlogov možnost dostopa do teh podatkov, morajo biti seznanjeni z zakonom o varstvu osebnih podatkov, s področno zakonodajo, ki jim dovoljuje obdelavo osebnih podatkov, s tem Pravilnikom in s splošnimi akti, ki opredeljujejo poslovno oziroma poklicno skrivnost.

5. člen

Za varovane osebne podatke štejejo tisti podatki, ki predstavljajo katerokoli informacijo v zvezi z določenim ali določljivim posameznikom, ne glede na obliko, v katero so izraženi. 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 posameznika.

V smislu določbe 1. odstavka tega člena štejejo za osebne podatke o posamezniku zlasti:
• identifikacijski podatki o posamezniku,
• podatki, ki se nanašajo na rasno poreklo in pripadnost narodu ali narodnosti,
• podatki, ki se nanašajo na družinska razmerja,
• podatki, ki se nanašajo na stanovanjske in bivalne pogoje posameznika,
• podatki o zaposlitvi,
• podatki o socialnem in ekonomskem stanju posameznika,
• podatki o izobrazbi in pridobljenih znanjih,
• slikovni (in glasovni) podatki nadzornih video sistemov,
• podatki o uporabi komunikacijskih sredstev,
• podatki o aktivnostih v prostem času,
• podatki o zdravstvenem stanju posameznika,
• podatki o ideoloških in verskih prepričanjih,
• podatki o posamezniku na področju notranjih zadev,
• podatki o navadah posameznika.

6. člen

Zavarovanje osebnih podatkov zajema pravne, organizacijske in ustrezne logistično-tehnične postopke in ukrepe za zagotavljanje skladnosti obdelave osebnih podatkov z določbami Splošne uredbe, zakona, ki ureja varstvo osebnih podatkov in drugih predpisov, ki urejajo varstvo osebnih podatkov, s katerimi se:
- varujejo prostori, strojna in sistemska programska oprema;
- varuje aplikativna programska oprema, s katero se obdelujejo osebni podatki;
- zagotavlja varnost posredovanja in prenosa osebnih podatkov;
- onemogoča nepooblaščenim osebam dostop do računalniških sistemov, na katerih se obdelujejo osebni podatki in dostop do podatkovnih zbirk;

- omogoča naknadno ugotavljanje, kdaj so bili posamezni podatki vneseni v podatkovne zbirke, oziroma računalniške sisteme, kdaj in kdo je dostopal do njih in to v obdobju, za katero se posamezni podatki shranjujejo.

7. člen

Obdelava in zavarovanje posebnih vrst osebnih podatkov, med katere sodijo podatki o rasnem ali etničnem poreklu, politično mnenje, versko ali filozofsko prepričanje ali članstvo v sindikatu in obdelava genskih podatkov, biometričnih podatkov za namene edinstvene identifikacije posameznika, podatkov v zvezi z zdravjem ali podatkov v zvezi s posameznikovim spolnim življenjem ali spolno usmerjenostjo, morata biti izvajana posebno vestno in skrbno.
Podatki o zdravstvenem stanju so osebni podatki, ki se nanašajo na telesno ali duševno zdravje posameznika, vključno z zagotavljanjem zdravstvenih storitev in razkrivajo informacije o njegovem zdravstvenem stanju.

Genski podatki so osebni podatki v zvezi s podedovanimi ali pridobljenimi genskimi značilnostmi posameznika, ki dajejo edinstvene informacije o fiziologiji ali zdravju tega posameznika in so zlasti rezultat analize biološkega vzorca zadevnega posameznika.

Biometrični podatki so osebni podatki, 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.

Posebne vrste osebnih podatkov (med katere sodijo tudi podatki o zdravstvenem stanju in v zvezi z zdravljenjem) morajo biti pri obdelavi posebej označeni in zavarovani tako, da se nepooblaščenim osebam prepreči dostop do njih.

8. člen

V tem Pravilniku uporabljeni izrazi imajo naslednji pomen:
- ZVOP – Zakon o varstvu osebnih podatkov;
- Splošna uredba – Uredba (EU) 2016/679 Evropskega parlamenta in Sveta z dne 26. aprila 2016 o varstvu posameznikov pri obdelavi osebnih podatkov (GDPR);
- ZPacP – Zakon o pacientovih pravicah;
- ZZDej – Zakon o zdravstveni dejavnosti;
- osebni podatek pomeni: katero koli informacijo v zvezi z določenim ali določljivim posameznikom; 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;
- posebna vrsta osebnih podatkov: podatki, ki razkrivajo rasno ali etnično poreklo, politično mnenje, versko ali filozofsko prepričanje ali članstvo v sindikatu, in obdelava genskih podatkov, biometričnih podatkov za namene edinstvene identifikacije posameznika, podatkov v zvezi z zdravjem ali podatkov v zvezi s posameznikovim spolnim življenjem ali spolno usmerjenostjo;
- posameznik: je določena ali določljiva fizična oseba na katero se nanaša osebni podatek;
- 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;
- 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;
- 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;
- upravljavec pomeni: fizično ali pravno osebo, javni organ, agencijo ali drugo telo, ki samo ali skupaj z drugimi obdeluje osebne podatke in določa namene in sredstva obdelave;
- obdelovalec pomeni: fizično ali pravno osebo, javni organ, agencijo ali drugo telo, ki obdeluje osebne podatke v imenu upravljavca;
- uporabnik pomeni: fizično ali pravno osebo, javni organ, agencijo ali drugo telo, ki so mu bili osebni podatki razkriti, ne glede na to, ali gre za posameznika, na katerega se podatki nanašajo ali na tretjo osebo. Javni organi, ki lahko prejmejo osebne podatke v okviru posamezne poizvedbe se ne štejejo za uporabnike.;
- nosilec podatkov: vse vrste sredstev, na katerih so zapisani ali posneti podatki, ne glede na obliko, v kateri so izraženi (listina, akt, gradivo, spis, magnetni, optični ali drugi računalniški mediji, prikazovalnik računalnika, fotokopije, zvočno ali slikovno gradivo, mikrofilmi, naprave za prenos podatkov);
- strojna oprema: oprema za vnos, obdelavo, prikaz, shranjevanje in posredovanje podatkov;
- računalniška strojna oprema: oprema za prenos podatkov, oprema za kriptografijo, oprema za zvočno in slikovno gradivo, merilni instrumenti, mikrofilmska oprema ipd.;
- programska oprema sistemska: programi, ki jih računalnik uporablja za krmiljenje svoje opreme in za komunikacije z okoljem (operacijski sistem) in druga programska orodja, ki so del operacijskega sistema in so namenjena vzdrževalcem in uporabnikom računalnika;
- programska oprema aplikativna: programi, s katerimi se izvaja obdelava podatkov;
- zavarovani prostori: prostori, kjer se nahajajo nosilci podatkov, preko katere je mogoč dostop do zbirk podatkov;
- pooblaščeni delavec: s strani odgovorne osebe imenovan delavec, ki skrbi za izvajanje postopkov in ukrepov za izvajanje zavarovanja podatkov;
- pooblaščena oseba za varstvo osebnih podatkov – s strani izvajalca imenovana oseba z ustreznimi poklicnimi odlikami in zlasti strokovnim znanjem ter dejanskimi izkušnjami o zakonodaji in praksi na področju varstva osebnih podatkov ali na primerljivem področju, ki upravljavcu ali obdelovalcu na neodvisen način pomaga pri zagotavljanju skladnosti obdelave osebnih podatkov s pravili Splošne uredbe ter določbami zakona, ki ureja področje varstva osebnih podatkov in drugih zakonov, ki urejajo obdelavo in varstvo osebnih podatkov.

II. TAJNOST PODATKOV

9. člen

Kot tajni podatki so opredeljeni podatki, ki jih obdeluje izvajalec, in ki so tako pomembni, da bi z njihovo izdajo nastale ali lahko nastale hujše škodljive posledice za izvajalca ali za posameznika.
Ti podatki so označeni kot :
- poslovna skrivnost in
- poklicna skrivnost.

10. člen

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

Za poslovno skrivnost se štejejo :
- podatki, listine in informacije, ki jih kot skrivnost določi izvajalec;
- rezultati raziskovanj, ki še niso verificirani;
- podatki in listine, ki vsebujejo ponudbo in povpraševanje poslovnih partnerjev,
- informacije o načinu dostopa v varovane objekte, kjer dejavnost izvaja izvajalec.

Za poklicno skrivnost se štejejo :
- vsi medicinski oz. zdravstveni in administrativni podatki do katerih imajo dostop zdravstveni delavci in drugi delavci pri opravljanju svojega dela, na podlagi katerih je mogoče identificirati osebo oz. diagnozo ali prognozo njene bolezni ali postopkov zdravljenja.

11. člen

Podatke, ki predstavljajo poslovno ali poklicno skrivnost, lahko sporočajo tretjim osebam samo zakoniti zastopnik izvajalca oz. od njega pooblaščene osebe, v skladu s tem Pravilnikom in ob upoštevanju določb o varovanju osebnih podatkov.

III. VAROVANJE PROSTOROV IN NOSILCEV OSEBNIH PODATKOV

12. člen

Prostori, kjer se nahajajo nosilci varovanih osebnih podatkov (vsak dokument, na katerem je zapisan osebni podatek in vsak drug računalniški ali elektronski nosilec podatka) in strojna ter programska oprema (v nadaljevanju besedila: varovani prostori) morajo biti varovani z organizacijskimi ter fizičnimi in tehničnimi ukrepi, ki onemogočajo nepooblaščenim osebam dostop do podatkov (npr. zaščita s ključavnicami, varovalni sistemi, alarmni sistemi, videonadzor).

Dostop v prostore iz 1. odstavka tega člena je mogoč in dopusten le v delovnem času, izven delovnega časa pa le na podlagi dovoljenja zakonitega zastopnika izvajalca ali od njega pooblaščene osebe.

13. člen

Nosilci osebnih podatkov (dokumenti, listine) morajo biti v delovnem času praviloma v zaklenjenih omarah v delovnih prostorih. Delovni prostori pa morajo biti izven delovnega časa zaklenjeni. Nosilci osebnih podatkov (dokumentov), hranjeni izven delovnih prostorov, oziroma izven varovanih prostorov, morajo biti stalno zaklenjeni v omari.

Dostop do programske opreme mora biti varovan tako, da z ustreznim kodiranjem dovoljuje dostop samo za to vnaprej določenim zaposlenim ali s strani izvajalca pooblaščenim osebam, ki v skladu s pogodbo opravljajo dogovorjene storitve pri izvajalcu ali za izvajalca. Če več oseb uporablja isti računalnik, naj ima vsak, ki dostopa do podatkov svoje geslo, v kolikor programska oprema to omogoča.

Računalniki ali druga strojna oprema, na kateri se obdelujejo ali hranijo osebni podatki, mora biti izven delovnega časa izklopljena in fizično ali programsko zaklenjena, dostop do osebnih podatkov, hranjenih na disku računalnika pa kodiran z geslom.

Ključi prostorov, v katerih se hranijo nosilci osebnih podatkov in računalniška oprema, hrani vsak zaposleni ali od izvajalca pooblaščena oseba pri izvajalcu s skrbnostjo kot v lastnih zadevah in še posebej na način, da onemogočijo dostop do ključa nepooblaščenim osebam.

14. člen

V varovane prostore, kjer se obdelujejo osebni podatki, osebe, ki ne delajo v varovanih prostorih in ki niso zaposlene ali v pogodbenem razmerju pri izvajalcu ali s strani izvajalca pooblaščene, ne smejo vstopati brez spremstva ali prisotnosti izvajalca ali zaposlenega delavca ali pooblaščene osebe pri izvajalcu.

Izvajalec, zaposleni ali pooblaščena oseba, ki dela v varovanih prostorih, mora vestno in skrbno nadzorovati prostor in ob zapustitvi prostora zakleniti prostor ali ga zapreti na način, da je onemogočen tretjim in nepooblaščenim osebam vstop v varovane prostore.

Zaposlen ali pooblaščena oseba pri izvajalcu, ki pri svojem delu uporablja osebne podatke ali jih kakorkoli obdeluje, ne sme med delovnim časom puščati nosilcev osebnih podatkov na pisalnih mizah ali jih kako drugače izpostavljati nevarnosti vpogleda vanje nepooblaščenim osebam.

V prostorih, kjer imajo vstop tretji (nepooblaščene osebe, kot npr. pacienti) oziroma osebe, ki niso zaposlene pri izvajalcu ali od izvajalca pooblaščene, morajo biti nosilci podatkov in računalniški prikazovalniki nameščeni v času obdelave ali dela na njih tako, da tretjim osebam ni omogočen vpogled v osebne podatke, ki se obdelujejo.

15. člen

Nosilcev osebnih podatkov zaposleni ali pooblaščene osebe pri izvajalcu ne smejo odnašati izven varovanih prostorov brez izrecnega dovoljenja zakonitega zastopnika izvajalca oz. od njega pooblaščene osebe.

Obdelovanje osebnih podatkov iz zbirk osebnih podatkov je dovoljeno le v prostorih izvajalca.

Izvajalec oz. od njega pooblaščena oseba lahko dovoli zaposlenemu iznos nosilcev osebnih podatkov iz varovanih prostorov izvajalca, ko predhodno zaposleni pri izvajalcu vpiše namen in razlog za iznos podatkov v knjigo evidenc o ravnanju z osebnimi podatki (priloga št. 7), ki se vodi pri izvajalcu.

Posredovanje osebnih podatkov pooblaščenim zunanjim institucijam in drugim, ki izkažejo zakonsko podlago za pridobitev osebnih podatkov, dovoli zakoniti zastopnik izvajalca. Posredovanje osebnih podatkov se vpiše v knjigo evidenc o ravnanju z osebnimi podatki (priloga št. 7).

16. člen

Vzdrževanje in popravilo strojne računalniške in druge opreme, s katero se obdelujejo osebni podatki, je dovoljeno samo z vednostjo in odobritvijo zakonitega zastopnika izvajalca ali pooblaščene osebe pri izvajalcu, izvajajo pa ga lahko samo pooblaščeni servisi in njihovi vzdrževalci, ki imajo z izvajalcem sklenjeno pogodbo o servisiranju računalniške oziroma strojne opreme.

17. člen

Vzdrževalci prostorov in druge opreme v varovanih prostorih, poslovni partnerji in drugi obiskovalci, se smejo gibati v varovanih prostorih le ob prisotnosti izvajalca, zaposlenega pri izvajalcu ali pooblaščene osebe izvajalca.

18. člen

Zaposleni tehnično-vzdrževalni delavci in čistilke pri izvajalcu se lahko gibljejo v varovanih prostorih izven delovnega časa in brez prisotnosti pooblaščene osebe pri izvajalcu le, če so nosilci podatkov shranjeni v zaklenjenih omarah in programski nosilci ustrezno kodirani, na način, kot to določa ta Pravilnik za čas izven delovnega časa.

IV. ZAVAROVANJE SISTEMSKE IN APLIKATIVNE PROGRAMSKE RAČUNALNIŠKE OPREME TER PODATKOV, KI SE OBDELUJEJO Z RAČUNALNIŠKO OPREMO

19. člen

Dostop do računalniške programske opreme mora biti varovan, na način, ki omogoča dostop samo zaposlenim pri izvajalcu ali pooblaščenim osebam pri izvajalcu in tretjim, ki za izvajalca po pogodbi opravljajo servisiranje računalniške strojne in programske opreme ali drugih pogodbenih storitev.

20. člen

Popravljanje, spreminjanje in dopolnjevanje sistemske in aplikativne programske opreme je dovoljeno samo na podlagi odobritve zakonitega zastopnika izvajalca oz. od njega pooblaščene osebe, izvajajo pa ga lahko samo pooblaščeni servis in organizacije, oziroma njihovi delavci, ki imajo z izvajalcem sklenjeno ustrezno pogodbo, ki je skladna z zahtevami iz področja varstva osebnih podatkov.

Izvajalec mora vse spremembe in dopolnitve sistemske in aplikativne programske opreme ustrezno dokumentirati.

21. člen

Za shranjevanje in varovanje aplikativne programske opreme veljajo enaka določila kot za ostale podatke iz tega Pravilnika.
Izvajalec mora skrbeti, da se v primeru servisiranja, popravila, spreminjanja ali dopolnjevanja sistemske ali aplikativne programske opreme, ob morebitnem kopiranju osebnih podatkov, po prenehanju potrebe po kopiji, kopija uniči.

Izvajalec ali od njega pooblaščena oseba mora biti v času servisiranja računalnika in programske opreme, v kolikor se le ta izvaja v varovanih prostorih ves čas prisoten in mora nadzirati, da ne pride do nedopustnega ravnanja z osebnimi podatki in dostopanja do podatkov izven namena.

V primeru izkazane potrebe po popravilu računalnika s shranjenimi osebnimi podatki na disku, na način, da se popravilo vrši izven zavarovanih prostorov izvajalca, mora izvajalec predhodno, pred izročitvijo računalnika v popravilo, z izvajalcem računalniških storitev (obdelovalec) skleniti pisno pogodbo, s katero obdelovalec zagotovi jamstvo o tem, da bo izvajal ustrezne tehnične in organizacijske ukrepe za zagotavljanje skladnosti prevzetih opravil z določbami zakona, ki ureja varstvo osebnih podatkov in določbami Splošne uredbe.

22. člen

Vsebina diskov mrežnega strežnika in lokalnih delovnih postaj, kjer se nahajajo osebni podatki, se sprotno (vsaj 1x tedensko) preverja na morebitno prisotnost računalniških virusov.

Ob pojavu računalniškega virusa je potrebno storiti vse, da se s pomočjo strokovnjakov virus odpravi in da se ugotovi vzrok pojava virusa in odpravi nevarnost zlorabe osebnih podatkov.

Vsi podatki in programska oprema, ki so namenjeni uporabi na računalnikih pri izvajalcu in v računalniškem informacijskem sistemu izvajalca in prispejo k izvajalcu na medijih za prenos računalniških podatkov ali preko telekomunikacijskih kanalov, morajo biti pred uporabo preverjeni na morebitno prisotnost računalniških virusov.

23. člen

Zaposleni delavci ali pooblaščene osebe ne smejo brez izrecnega dovoljenja zakonitega zastopnika izvajalca inštalirati nobene programske opreme na računalnike, ki se uporabljajo pri izvajalcu za potrebe opravljanja zdravstvene dejavnosti.
Zaposleni delavci ne smejo odnašati programske opreme iz prostorov izvajalca brez izrecnega dovoljenja zakonitega zastopnika izvajalca oz. od njega pooblaščene osebe.

24. člen

Pristop do podatkov prek aplikativne programske opreme mora biti varovan s sistemom profesionalnih kartic ter s sistemom gesel za avtorizacijo in identifikacijo uporabnikov programov in podatkov, sistem gesel pa mora omogočati tudi možnost naknadnega ugotavljanja, kdaj so bili posamezni osebni podatki vneseni v zbirko podatkov, uporabljeni ali drugače obdelovani in kdo jih je obdeloval.

Gesla so zaupni podatki, katere je prepovedano sporočati nepooblaščenim osebam.

25. člen

Vsa gesla in postopki, ki se uporabljajo za vstop in za administriranje v mreži osebnih računalnikov, administriranje z elektronsko pošto in administriranje prek aplikativnih programov, se hranijo v zapečatenih ovojnicah in varujejo v zaklenjenih omarah ali predalnikih v varovanem prostoru izvajalca (priloga št. 8). Zakoniti zastopnik izvajalca določi režim dodeljevanja in spreminjanja gesel.

26. člen

Za potrebe restavriranja osebnih podatkov oziroma računalniškega sistema po okvarah ali izgubi podatkov iz drugih razlogov mora izvajalec, ali po zaposlenem ali pooblaščeni osebi, ki vodi zbirke osebnih podatkov, redno izdelovati kopije vsebine osebnih podatkov, ki jih vodi. Vse izdelane kopije vsebin zbirk osebnih podatkov se morajo vpisati v knjigo evidenc o ravnanju z osebnimi podatki (priloga št. 6).

Računalniške kopije vsebin zbirk osebnih podatkov se hranijo v prostorih, ki morajo biti ognjevarni, varovani pred poplavami in elektromagnetnim motnjami ter zaklenjeni.

V. OBDELAVA OSEBNIH PODATKOV IN ZBIRKE OSEBNIH PODATKOV

27. člen

Osebni podatki v zasebnem sektorju (v to skupino spadajo tudi zasebni izvajalci zdravstvene dejavnosti s koncesijo ali brez koncesije) se lahko obdelujejo, če obdelavo osebnih podatkov in osebne podatke, ki se obdelujejo, določa zakon ali če je za obdelavo določenih osebnih podatkov podana privolitev posameznika.

V določenih primerih pa lahko izvajalec obdeluje osebne podatke tudi v primerih, kadar ne obstoji zakonsko pooblastilo ali ni podane privolitve posameznika, in sicer:
- ko je posameznik z izvajalcem sklenil pogodbo ali pa je na podlagi zahteve tega posameznika v fazi pogajanj za sklenitev pogodbe z njim, če je obdelava osebnih podatkov potrebna in primerna za izvajanje ukrepov pred sklenitvijo pogodbe ali za izvajanje pogodbe;
- kadar gre za obdelavo tistih osebnih podatkov, ki so potrebni za zaščito življenjskih interesov posameznika, na katerega se nanašajo osebni podatki, ali druge fizične osebe;
- kadar je obdelava potrebna zaradi uresničevanja zakonitih upravičenih interesov, za katere si prizadeva upravljavec ali tretja oseba, razen kadar nad takimi interesi prevladajo interesi ali človekove pravice in temeljne svoboščine posameznika, na katerega se nanašajo osebni podatki, ki zahtevajo varstvo osebnih podatkov, zlasti kadar je posameznik, na katerega se nanašajo osebni podatki, otrok.

28. člen

Izvajalec vodi osebne podatke v zbirkah osebnih podatkov, ki jih ustanovi na podlagi zakona ter vodi osebne podatke v zbirkah osebnih podatkov na podlagi soglasja osebe, na katero se podatki nanašajo (priloga št. 9).

Vrste in vsebina posameznih zbirk podatkov s področja zdravstvenega varstva, njihov namen, obdobna poročila, kdo mora posredovati podatke in kdaj, upravljavec zbirke, način dajanja podatkov in čas hranjenja podatkov, so določene z Internim seznamom katalogov zbirk osebnih podatkov, ki je priloga tega pravilnika (priloga št. 9).

Zaposleni pri izvajalcu ali pooblaščene osebe, ki obdelujejo osebne podatke, morajo biti seznanjeni z vsebino katalogov podatkov.

VI. SPREJEM IN POSREDOVANJE OSEBNIH PODATKOV TRETJIM

29. člen

Izvajalec, zaposlen ali pooblaščena oseba, ki je zadolžena za sprejem in evidenco pošte, mora izročiti poštno pošiljko z osebnimi podatki direktno posamezniku, ali službi, na katero je ta pošiljka naslovljena.

Izvajalec, zaposlen ali pooblaščena oseba, ki je zadolžena za sprejem in evidenco pošte, odpira in pregleduje vse poštne pošiljke in pošiljke, ki prispejo naslovljene na izvajalca.

Zaposlen ali pooblaščena oseba, ki je zadolžena za sprejem in evidenco pošte, ne odpira tistih pošiljk, ki so naslovljene na drug organ ali organizacijo in so pomotoma dostavljena ter pošiljk, ki so označene kot osebni podatki, ampak takšno pošto izroči izvajalcu. Prav tako ne sme odpirati pošiljk, naslovljenih na delavca, na katerih je na ovojnici navedeno, da se vročijo osebno naslovniku, ter pošiljk, na katerih je najprej navedeno osebno ime delavca brez označbe njegovega uradnega položaja in šele nato naslov izvajalca.

30. člen

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.

Izvajalec nikoli naslovniku ne posreduje originalov dokumentov, razen v primeru pisne odredbe sodišča. Originalni dokument se mora v času odsotnosti nadomestiti s kopijo.

31. člen

Pisemske pošiljke, s katerimi izvajalec pošilja naslovnikom posebne vrste osebnih podatkov, se pošiljajo naslovniku priporočeno s povratnico ali po kurirju z oznako »zaupno« na kuverti.

Pisemske pošiljke, s katerimi izvajalec pošilja osebne podatke, ki niso posebne vrste osebnih podatkov, se pošiljajo naslovniku priporočeno.

Pisemska ovojnica, v kateri se posredujejo osebni podatki, mora biti izdelana na takšen način, da ovojnica ne omogoča, da bi bila ob normalni svetlobi ali pri osvetlitvi ovojnice z običajno lučjo vidna vsebina iz ovojnice. Prav tako mora ovojnica zagotavljati, da odprtje ovojnice in seznanitve z njeno vsebino ni mogoče opraviti brez vidne sledi odpiranja ovojnice.

32. člen

Prenašanje osebnih podatkov preko telekomunikacijskih sredstev, elektronske pošte ali drugih računalniških medijev izven prostorov izvajalca mora biti zavarovano s postopki in ukrepi na način, ki nepooblaščenim preprečuje prilaščanje, uničenje ali nedovoljeno seznanjanje z njihovo vsebino.

Prenos osebnih podatkov po elektronski pošti mora biti zavarovan z geslom za identifikacijo ali kodiranjem.
Vsebina osebnih podatkov, ki jih izvajalec prenaša do naslovnika po komunikacijskih kanalih, po elektronski pošti ali fizično na računalniških medijih izven prostorov

izvajalca, se mora med prenosom napraviti nečitljiva z ustreznimi standardnimi kriptografskimi metodami in elektronskim podpisom tako, da je zagotovljena nečitljivost podatkov med njihovim prenosom. V primeru, da izvajalec pošilja občutljiv osebni podatek po elektronski pošti, mora podatek ustrezno šifrirati oz. kriptirati, pri tem pa gesla za dostop do vsebine podatkov, ne sme posredovati po istem informacijskem kanalu (če torej izvid posreduje v kriptirani obliki pacientu, ne sme šifrirnega gesla pacientu sporočiti po elektronski pošti, ampak ga mora sporočiti po telefonu, uporaba sms,…).

33. člen

Osebne podatke, vodene v zbirki osebnih podatkov izvajalca, lahko izvajalec posreduje drugim uporabnikom zgolj na podlagi utemeljene zahteve iz katere izhaja veljavna pravna podlaga za pridobitev podatkov ter utemeljenost zahteve, pri čemer pa mora zahteva vsebovati vsaj:
1. podatke o uporabniku ali upravljavcu (za fizično osebo: osebno ime, naslov opravljanja dejavnosti ali naslov stalnega ali začasnega prebivališča; za samostojnega podjetnika ter za pravno osebo: naziv oziroma firmo in naslov oziroma sedež in matično številko) ter podpis pooblaščene osebe;
2. pravno podlago za pridobitev zahtevanih osebnih podatkov;
3. namen obdelave osebnih podatkov oziroma razloge, ki izkazujejo potrebnost in primernost osebnih podatkov za dosego namena pridobitve;
4. predmet in številko ali drugo identifikacijo zadeve, v zvezi s katero so osebni podatki potrebni;
5. vrste osebnih podatkov, ki naj se mu posredujejo;
6. obliko in način pridobitve zahtevanih osebnih podatkov.

Izvajalec mora uporabniku ali upravljavcu, če zakon ne določa drugače, zahtevane osebne podatke posredovati najpozneje v 15 dneh od dne prejema popolne zahteve, ali pa ga v tem roku pisno obvestiti o razlogih, zaradi katerih mu zahtevanih osebnih podatkov ne bo posredoval.

V primeru ugoditve zahtevi za posredovanje osebnih podatkov, mora izvajalec uporabnika opozoriti, da sme prejete osebne podatke uporabiti samo za namene, za katere so bili posredovani.

Izvajalec pa mora za vsako posredovanje osebnih podatkov zagotoviti, da je mogoče pozneje ugotoviti, katere vrste osebnih podatkov so bile posredovane, komu, kdaj in po kateri pravni podlagi, za kateri namen oziroma iz katerih razlogov oziroma za potrebe katerega postopka. Revizijsko sled posredovanih osebnih podatkov mora izvajalec hraniti za obdobje pet (5) let. V ta namen se posredovanje osebnih podatkov iz zbirk osebnih podatkov, ki jih vodi izvajalec, drugim upravičencem vpiše v knjigo evidenc o ravnanju z osebnimi podatki, s čimer se zagotavlja možnost naknadnega ugotavljanja, kateri osebni podatki, kdaj in na kakšen način, komu in za kakšne namene so bili posredovani (priloga št. 6).

VII. BRISANJE PODATKOV OZIROMA UNIČENJE NOSILCEV OSEBNIH PODATKOV

34. člen

Osebni podatki lahko izvajalec vodi v zbirki osebnih podatkov le toliko časa, kolikor je potrebno, da se doseže namen, za katerega se podatki obdelujejo.

Po prenehanju potrebe po vodenju in zakonske podlage za obdelavo osebnih podatkov, se podatki zbrišejo oziroma nosilci podatkov uničijo, blokirajo ali anonimizirajo, razen če zakon ali drug akt ne določa drugače.

Roki, po katerih se osebni podatki, ki jih obdeluje izvajalec izbrišejo iz zbirke podatkov, so določeni v Notranjih pravilih in klasifikacijskem načrtu izvajalca.

35. člen

Brisanje osebnih podatkov na računalniških medijih se opravi na način, po postopku in metodi, ki onemogoča restavriranje brisanih podatkov.

Osebni podatki, vsebovani na klasičnih nosilcih (listine, kartoteke, register, seznam) se brišejo z uničenjem nosilcev. Nosilci se fizično uničijo (pokurijo, razrežejo) v prostorih izvajalca pod nadzorom zakonitega zastopnika izvajalca ali s predajo dokumentacije v uničenje organizaciji, ki se ukvarja z uničevanjem zaupne dokumentacije in ima z izvajalcem sklenjeno ustrezno pogodbo o izvajanju storitev, s podanim jamstvom izvajalca storitve, da bo ravnal v skladu s pravili o varstvu osebnih podatkov.

Uničevanje posameznih dokumentov, ki dnevno nastajajo v delovnem procesu se uničuje v prostorih izvajalca z razrezom. Uničuje jih pooblaščena oseba, ki dela s temi dokumenti.

Prepovedano je odmetavati odpadne nosilce podatkov z osebnimi podatki v koše za smeti, brez, da so nosilci podatkov predhodno ustrezno uničeni, da ne omogočajo dostopa do osebnih podatkov.

36. člen

Z vestnostjo in skrbnostjo določeno s tem pravilnikom za uničevanje osebnih podatkov, vodenih v zbirkah oziroma na posameznih nosilcih podatkov, se mora brisati in uničevati tudi pomožna dokumentacija ali računalniški produkti oziroma predloge, ki vsebujejo posamezne osebne podatke.

VIII. STORITVE, KI JIH OPRAVLJAJO ZUNANJE PRAVNE ALI FIZIČNE OSEBE

37. člen

Izvajalec lahko zaupa posamezna opravila v zvezi z obdelavo osebnih podatkov zunanji pravni ali fizični osebi (pogodbeni obdelovalec), pri tem pa si mora izvajalec prizadevati, da pogodbeni obdelovalec zagotavlja zadostna jamstva o tem, da bo izvajal ustrezne tehnične in organizacijske ukrepe za zagotavljanje skladnosti prevzetih opravil obdelave s Splošno uredbo, zakonom, ki ureja področje varstva osebnih podatkov in tem Pravilnikom.

V kolikor pogodbena obdelava pri zunanji osebi ni določena na podlagi izrecnega zakonskega pooblastila, mora izvajalec z zunanjo osebo skleniti pogodbo ali drug dogovor, s katerim izvajalec in zunanja oseba določita predmet, trajanje, vrsto in namen obdelave, vrsto osebnih podatkov, kategorije posameznikov, na katere se nanašajo osebni podatki ter pravice in obveznosti zunanje osebe. Pogodba ali dogovor mora zlasti določiti, da zunanja oseba:
1. osebne podatke obdeluje samo po izkazanih navodilih izvajalca,

2. zagotovi, da so osebe, pooblaščene za obdelavo osebnih podatkov, zavezane k varovanju tajnosti ali zaupnosti ali da za njih velja ustrezna zakonska dolžnost varovanja tajnosti;
3. izvede vse potrebne ukrepe za varnost osebnih podatkov;
4. po koncu zagotavljanja storitev pogodbene obdelave vse podatke po navodilu izvajalca vrne ali izbriše, če ne obstaja pravna obveznost glede hrambe osebnih podatkov.

38. člen

Zunanje osebe (pogodbeni obdelovalci) smejo opravljati storitve obdelave osebnih podatkov samo v okviru namena, ki je določen v pogodbi ali dogovoru o pogodbeni obdelavi podatkov z izvajalcem in podatkov ne smejo obdelovati ali drugače uporabljati za noben drug namen.

IX. UKREPI ZA VAROVANJE OSEBNIH PODATKOV IN UKREPANJE OB UGOTOVITVI O ZLORABI OSEBNIH PODATKOV ALI VDORU V ZBIRKE OSEBNIH PODATKOV

39. člen

Izvajalec mora zagotoviti ustrezne tehnične in organizacijske ukrepe, s katerimi se varujejo osebni podatki ter preprečuje njihovo slučajno, namerno ali drugače nezakonito uničenje, spremembo, izgubo, nepooblaščeno razkritje, dostop ali drugo nepooblaščeno obdelavo.

Ukrepi morajo biti primerni glede na stanje najnovejšega tehnološkega razvoja na tem področju, na naravo, obseg, okoliščine in namene obdelave ter resnost in verjetnost tveganj za človekove pravice in temeljne svoboščine posameznikov, ki nastajajo pri obdelavi, kar vključuje zlasti:
(a) psevdonimizacijo in šifriranje osebnih podatkov;
(b) ukrepe za zagotovitev stalne zaupnosti, celovitosti, dostopnosti in odpornosti sistemov in storitev za obdelavo;
(c) ukrepe za zmožnost pravočasne povrnitve razpoložljivosti osebnih podatkov v primeru varnostnega incidenta;
(d) postopke rednega testiranja, ocenjevanja in vrednotenja učinkovitosti tehničnih in organizacijskih ukrepov teh ukrepov;
(e) v primeru dosegljivosti osebnih podatkov preko telekomunikacijskega sredstva ali omrežja, morajo strojna, sistemska in aplikativno programska oprema zagotavljati, da je obdelava osebnih podatkov v zbirkah osebnih podatkov v mejah pooblastil uporabnika takšnega sredstva oziroma omrežja;
(f) ukrepe, ki omogočajo poznejše ugotavljanje, kdaj so bile posamezne vrste osebnih podatkov vnesene v zbirko osebnih podatkov, uporabljene ali drugače obdelane in kdo je to storil, in sicer za obdobje 5 let od zaključka leta, v katerem je potekala obdelava, razen če za obdelave posameznih vrst osebnih podatkov drug zakon ne določa drugače.

V primeru obdelave posebnih vrst osebnih podatkov mora izvajalec poleg ukrepov iz prejšnjega odstavka ozaveščati osebe, udeležene v postopkih obdelave podatkov o varnostnih politikah ter postopkih in ukrepih za zagotavljanje varnosti osebnih podatkov (kot npr.: odjavljanje iz sistema po zaključku dela, uporaba programskega zaklepanja računalnika ob odsotnosti od računalnika, zaklepanje prostorov ali stalni nadzor, politika čiste in urejene delovne mize in delovnega prostora, pomen zagotavljanja sledljivosti obdelave, vsak uporabnik uporablja svoje uporabniško ime in geslo, fizično varovanje gesel, previdnost pri izbiri gesel, občasno spreminjanje gesel, kriptirano pošiljanje podatkov po elektronskih medijih, pazljivost in skrbnost pri

posredovanju podatkov po telefonu, takojšnje obveščanje o incidentu, posvetovanje s Pooblaščeno osebo za varstvo osebnih podatkov, upoštevanje notranjih pravil in aktov,…).

40. člen

Izvajalec določi in imenuje Pooblaščeno osebo za varstvo osebnih podatkov, ki izvajalcu na neodvisen način pomaga pri zagotavljanju skladnosti obdelave osebnih podatkov s pravili Splošne uredbe ter določbami zakona, ki ureja varstvo osebnih podatkov in drugih zakonov, ki urejajo obdelavo in varstvo osebnih podatkov pri opravljanju zdravstvene dejavnosti.
Pooblaščena oseba za varstvo podatkov ima vsaj naslednje naloge:
- obveščanje izvajalca in pri njem zaposlenih, ki izvajajo obdelavo, ter svetovanje navedenim o njihovih obveznostih v skladu s Splošno Uredbo in drugimi določbami prava Unije ali nacionalne zakonodaje iz področja varstvu osebnih podatkov;
- spremljanje skladnosti s Splošno Uredbo, drugimi določbami prava Unije ali nacionalne zakonodaje iz področja varstva osebnih podatkov in politikami izvajalca v zvezi z varstvom osebnih podatkov, vključno z dodeljevanjem nalog, ozaveščanjem in usposabljanjem osebja, vključenega v dejanja obdelave, ter s tem povezanimi revizijami;
- svetovanje pri izvajanju ocene učinka tveganja;
- sodelovanje z nadzornim organom (Informacijskim pooblaščencem);
- delovanje kot kontaktna točka za nadzorni organ pri vprašanjih v zvezi z obdelavo osebnih podatkov pri izvajalcu.

41. člen

Izvajalec, zaposleni in pooblaščene osebe pri izvajalcu so dolžni izvajati ukrepe za zagotavljanje varovanja osebnih podatkov, s katerimi se seznanijo pri svojem delu, ravnati vestno in skrbno na način in po postopkih, ki jih določa ta Pravilnik.

Zaposleni, ki izve ali opazi, da je prišlo do zlorabe osebnih podatkov (odkrivanje osebnih podatkov, nepooblaščeno uničenje, nepooblaščeno spreminjanje, poškodovanje zbirke, prilaščanje osebnih podatkov) ali do vdora v zbirko osebnih podatkov, mora takoj o tem obvestiti zakonitega zastopnika izvajalca.

42. člen

Za zlorabo osebnih podatkov šteje vsaka uporaba osebnih podatkov v namene, ki niso v skladu z nameni zbiranja, določenimi v zakonu, na podlagi katerega se zbirajo ali nameni, določenimi v katalogu zbirk osebnih podatkov. Za poskus zlorabe šteje poskus uporabe osebnih podatkov v nedovoljene namene.

43. člen

V primeru, da izvajalec ugotovi, da je v procesu obdelave osebnih podatkov prišlo do slučajnega, namernega ali drugačnega nezakonitega uničenja, spremembe, izgube, nepooblaščenega razkritja, dostopa ali druge oblike nepooblaščene obdelave, je dolžan izvajalec brez nepotrebnega odlašanja, oziroma najpozneje v 72 urah po seznanitvi s kršitvijo, o kršitvi uradno obvesti pristojni nadzorni organ (Informacijskega pooblaščenca).

Ta obveznost izvajalca ni podana, če ni izkazana verjetnost, da bi bile s kršitvijo varstva osebnih podatkov ogrožene pravice in svoboščine posameznikov, na katere se kršitev nanaša.

Uradno obvestilo iz 1. odstavka tega člena Pravilnika nadzornemu organu mora vsebovati vsaj naslednje podatke:
- opis vrste kršitve varstva osebnih podatkov, po možnosti tudi kategorije in približno število zadevnih posameznikov, na katere se nanašajo osebni podatki, ter vrste in približno število zadevnih evidenc osebnih podatkov;
- sporočilo o imenu in kontaktnih podatkih pooblaščene osebe za varstvo podatkov ali druge kontaktne točke, pri kateri je mogoče pridobiti več informacij;
- opis verjetnih posledic kršitve varstva osebnih podatkov;
- opis ukrepov, ki jih izvajalec sprejme ali katerih sprejetje predlaga za obravnavanje kršitve varstva osebnih podatkov, pa tudi ukrepov za ublažitev morebitnih škodljivih učinkov kršitve.

44. člen

V primeru, da bi kršitev varstva osebnih podatkov povzročila veliko tveganje za pravice in svoboščine posameznikov, je izvajalec brez nepotrebnega odlašanja o kršitvi varstva osebnih podatkov, dolžan obvestiti posameznika, na katerega se nanašajo osebni podatki.

X. PRAVICE POSAMEZNIKOV, NA KATERE SE NANAŠAJO OSEBNI PODATKI

45. člen

Izvajalec mora posamezniku na njegovo zahtevo:
- omogočiti vpogled v katalog zbirke osebnih podatkov;
- potrditi, ali se podatki v zvezi z njim obdelujejo ali ne in mu omogočiti vpogled v osebne podatke, ki so vsebovani v zbirki osebnih podatkov in se nanašajo nanj, ter njihovo prepisovanje ali kopiranje (pravica do dostopa);
- dopolniti, popraviti, izbrisati ali omejiti uporabo osebnih podatkov, za katere posameznik dokaže, da so nepopolni, netočni ali neažurni ali da so bili zbrani ali obdelani v nasprotju z zakonom (pravica do popravka, do izbrisa, do omejitve obdelave),
- posredovati osebne podatke, ki jih je posameznik posedoval izvajalcu, v strukturirani, splošno uporabljani in strojno berljivi obliki, in ima posameznik pravico, da te podatke posreduje drugemu upravljavcu, ne da bi ga izvajalec, ki so mu bili osebni podatki zagotovljeni, pri tem oviral (pravica do prenosljivosti podatkov).

Izvajalec na zahtevo posameznika do seznanitve z osebnimi podatki zagotovi kopijo osebnih podatkov, ki se obdelujejo. 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, izvajalec informacije zagotovi v elektronski obliki, ki je splošno uporabljana in je skladna s pravili posredovanja osebnih podatkov s tem Pravilnikom.

46. člen

Izvajalec osebnih podatkov mora posamezniku na njegovo zahtevo tudi:
- posredovati izpis osebnih podatkov, ki so vsebovani v zbirki osebnih podatkov in se nanašajo nanj;

- posredovati seznam uporabnikov, katerim so bili posredovani osebni podatki, kdaj, na kakšni podlagi in za kakšen namen;
- dati informacijo o virih, na katerih temeljijo zapisi, ki jih o posamezniku vsebuje zbirka osebnih podatkov, in o metodi obdelave;
- dati informacije o namenu obdelave in vrsti osebnih podatkov, ki se obdelujejo, ter vsa potrebna pojasnila v zvezi s tem;
- pojasniti tehnične oziroma logično-tehnične postopke odločanja, če izvaja avtomatizirano odločanje z obdelavo osebnih podatkov posameznika.

47. člen

Izvajalec na zahtevo posameznika slednjemu posreduje izpis, seznam, informacije ter pojasnilo v petnajstih (15) dneh od dneva, ko je prejel zahtevo, ali ga v istem roku pisno obvesti o razlogih, zaradi katerih mu izpisa, seznama, informacij ali pojasnila ne bo posredoval.

XI. ODGOVORNOST ZA IZVAJANJE UKREPOV ZAVAROVANJA OSEBNIH PODATKOV

48. člen

Izvajalec je dolžan zagotoviti, da se pred nastopom dela zaposlenega na delovnem mestu, kjer se zbirajo, urejajo, obdelujejo, spreminjajo, shranjujejo, posredujejo ali uporabljajo osebni podatki ali nosilci osebnih podatkov, zaposleni seznani s pravili o varovanju osebnih podatkov, kot tudi poklicne skrivnosti in v ta namen podpiše tudi ustrezno izjavo, ki ga opozarja na posledice kršitve pravil o varovanju osebnih podatkov (priloga št. 1). Iz podpisane izjave mora biti razvidno, da je podpisnik seznanjen z določbami tega Pravilnika ter določbami zakona, ki ureja področje varstva osebnih podatkov in vsebine Splošne uredbe.

Izjavo morajo podpisati tudi zaposleni, ki prihajajo posredno v stik z obdelavo osebnih podatkov pri izvajalcu, to so specializanti, študentje, pripravniki, dijaki na praksi in drugi delavci, ki se izobražujejo pri izvajalcu (priloga št. 2).

Obveza varovanja osebnih podatkov, s katerimi se zaposleni seznani pri svojem delu pri izvajalcu traja tudi po prenehanju delovnega razmerja pri izvajalcu.

49. člen

Ravnanje zaposlenega v nasprotju z določili tega Pravilnika pomeni kršitev delovnih obveznosti.

Kot lažja kršitev delovnih obveznosti se šteje kršitev zaposlenega:
- če opusti vestno in skrbno nadzorovanje varovanih prostorov,
- če opusti ravnanja za preprečitev vpogleda v ali na nosilce osebnih podatkov,
- če ne uniči kopije osebnih podatkov,
- če ne izvaja preventive v zvezi z računalniškimi virusi,
- če ne vodi evidence kopij vsebin zbirk osebnih podatkov v knjigi evidenc o ravnanju z osebnimi podatki,
- če ne obvesti zakonitega zastopnika izvajalca v primeru zlorabe osebnih podatkov ali vdora v zbirko osebnih podatkov.

50. člen

Kot hujša kršitev delovnih obveznosti se šteje kršitev zaposlenega:
- če sporoča osebne podatke, s katerimi se je seznanil pri svojem delu, nepooblaščenim osebam,
- če opusti skrb in nadzor nad nosilci osebnih podatkov med delovnim časom in tako dopusti možnost vpogleda vanje nepooblaščenim osebam,
- če brez izrecnega dovoljenja odnaša iz prostorov izvajalca nosilce osebnih podatkov,
- če posreduje osebne podatke pooblaščenim zunanjim institucijam brez dovoljenja zakonitega zastopnika izvajalca,
- če ne vpiše v knjigo evidenc o ravnanju z osebnimi podatki dejstva o posredovanju osebnih podatkov zunanjim institucijam,
- če popravlja, spreminja ali dopolnjuje sistemsko ali aplikativno programsko opremo,
- če inštalira ali odnese programsko opremo iz prostorov izvajalca brez izrecnega dovoljenja zakonitega zastopnika izvajalca,
- če ne izdeluje redno kopije vsebine osebnih podatkov,
- če ne hrani računalniških kopij vsebin zbirk osebnih podatkov v zavarovanih zaklenjenih omarah.

XII. POSEBNE UREDITVE ZA ZBIRKE OSEBNIH PODATKOV VODENIH PRI IZVAJALCU

51. člen
Obdelava osebnih podatkov za katere je potrebna privolitev

Pisno privolitev zaposlenih in tretjih oseb mora izvajalec pridobiti za vzpostavitev in vodenje zbirke osebnih podatkov ali osebnega podatka, ki jo ali ga namerava izvajalec voditi, pa taka zbirka ali obdelava osebnega podatka ni predpisana z zakonom (priloga št. 3).

52. člen

Pisno soglasje iz predhodnega člena mora vsebovati:
- jasno opredeljeno voljo za izdajo soglasja,
- navedbo podatkov, ki se zbirajo,
- natančno opredeljen namen zbiranja podatkov,
- zagotovilo, da se bodo podatki uporabljali le za namen za katerega so zbrani,
- čas shranjevanja podatkov,
- seznanitev z možnostjo preklica soglasja,
- datum podpisa izjave in podpis osebe.

53. člen
Zbirke osebnih podatkov zaposlenih

Zbirke osebnih podatkov zaposlenih se vzpostavijo ob sklenitvi delovnega razmerja z delavcem oziroma ažurirajo ob vsaki spremembi, ki jo javi delavec ali je povezana z delavcem.

54. člen
Videonadzor

Izvajalec kot upravljavec osebnih podatkov mora v primeru izvajanega videonadzora o izvajanju videonadzora objaviti obvestilo. Obvestilo mora biti vidno in razločno

objavljeno na način, ki omogoča posamezniku, da se seznani z njegovim izvajanjem najkasneje, ko se nad njim začne izvajati videonadzor.

Obvestilo iz prejšnjega odstavka mora vsebovati naslednje informacije:
- da se izvaja videonadzor;
- naziv upravljavca osebnih podatkov ter
- telefonsko številko za pridobitev informacije, kje in koliko časa se shranjujejo posnetki iz videonadzornega sistema.

Videonadzorni sistem, s katerim se izvaja videonadzor, mora biti zavarovan pred dostopom nepooblaščenih oseb.

55. člen

Videonadzor dostopa v uradne službene oziroma poslovne prostore se lahko izvaja, če je to potrebno za varnost ljudi in premoženja, zaradi zagotavljanja nadzora vstopa ali izstopa v ali iz službenih oziroma poslovnih prostorov ali če zaradi narave dela obstaja možnost ogrožanja delavcev.

O izvajanju videonadzora je potrebno pisno obvestiti vse zaposlene, ki opravljajo delo v nadzorovanem prostoru.

Zbirka osebnih podatkov po tem členu vsebuje posnetek posameznika (slika oziroma glas), datum in čas vstopa in izstopa iz prostora, lahko pa tudi osebno ime posnetega posameznika, naslov njegovega stalnega ali začasnega prebivališča, zaposlitev, številko in podatke o vrsti njegovega osebnega dokumenta ter razlogu vstopa, če se navedeni osebni podatki zbirajo poleg ali s posnetkom videonadzornega sistema.

56. člen

Videonadzor znotraj delovnih prostorov se lahko izvaja le v izjemnih primerih, kadar je to nujno potrebno za varnost ljudi in premoženja ali za varovanje tajnih podatkov ter poslovne skrivnosti, tega namena pa ni možno doseči z milejšimi sredstvi.

Videonadzor se lahko izvaja le glede tistih delovnih prostorov, kjer je potrebno varovati interese iz prejšnjega odstavka.

Prepovedano je izvajati videonadzor v delovnih prostorih izven delovnega mesta, zlasti v garderobah, dvigalih in sanitarnih prostorih.

Zaposleni morajo biti pred začetkom izvajanja videonadzora po tem členu vnaprej pisno obveščeni o njegovem izvajanju.

XIII. PRAVICE IZVEDENCA DO PODATKOV IZ MEDICINSKE DOKUMENTACIJE

57. člen

Izvedenec, ki ga postavi sodišče, ima pravico do vpogleda v medicinsko dokumentacijo in mu mora izvajalec omogočiti in zagotoviti vpogled v medicinsko dokumentacijo.
Pred pregledom medicinske dokumentacije se mora izvedenec dokazati s sklepom sodišča, da je v konkretni zadevi postavljen za izvedenca. Fotokopijo sklepa sodišča je potrebno priložiti k preostali medicinski dokumentaciji ambulantnega kartona posameznika.

Pravica do vpogleda v medicinsko dokumentacijo zajema:
- pravico do vpogleda,
- pravico do izpisa,
- pravico do fotokopiranja.

58. člen

Medicinsko dokumentacijo predloži izvedencu izvajalec ali od njega pooblaščena oseba. Na poseben obrazec je potrebno napisati uro, ko je bila zdravstvena dokumentacija dana izvedencu na vpogled, katere podatke je izvedenec izpisal in katera zdravstvena dokumentacija mu je bila izdana v obliki fotokopije. Označiti je potrebno tudi uro predaje fotokopije medicinske dokumentacija (priloga št. 4).

Izvedenec je dolžan kriti stroške izpisa ali fotokopije medicinske dokumentacije ter ostale stroške, ki zajemajo zamudo časa izvajalca, ki pripravi medicinsko dokumentacijo.

59. člen

V primeru, da sodišče v sklepu odredi, da je potrebno izvedencu izročiti original medicinske dokumentacije oz. njene posamezne dele, mora izvajalec za čas do vrnitve originalne medicinske dokumentacije s strani sodišča pripraviti fotokopije medicinske dokumentacije in prav tako na posebnem obrazcu vpisati, kdaj, ob kateri uri in katera medicinska dokumentacije je bila predana izvedencu v originalu.

XIV. PREHODNE IN KONCNE DOLOCBE

60. člen

Ta pravilnik prične veljati in se uporabljati z dnem 25.5.2018.

61. člen

Priloga tega Pravilnika so naslednji obrazci:
- izjava delavca, zaposlenega pri izvajalcu o varovanju osebnih podatkov (priloga št. 1),
- izjava delavca, ki opravlja delo pri izvajalcu kot specializant, pripravnik, študent, dijak na praksi (priloga št. 2),
- soglasje delavca/tretje osebe za vzpostavitev in vodenje zbirk osebnih podatkov (priloga št. 3),
- potrdilo o izročitvi medicinske dokumentacije izvedencu (priloga št. 4),
- obvestilo posamezniku o posredovanju podatkov (priloga št. 5),
- knjiga evidenc o ravnanju z osebnimi podatki – posredovanje in iznos osebnih podatkov pri izvajalcu (priloga št. 6),
- evidenca o spremembah in dopolnitvah sistemske in aplikativne programske opreme (priloga št. 7),
- evidenca gesel za uporabo računalniške opreme (priloga št. 8),
- seznam katalogov – evidenc zbirk osebnih podatkov (priloga št. 9).

Izvajalec zdravstvene dejavnosti:

ZDRAVSTVENI ZAVOD FLIS MARIBOR
Ivica Flis Smaka