	FUNKCIJA	IME IN PRIIMEK	
PRIPRAVILA:	Strokovni sodelavec v FKS	Veronika Zabukovec, mag. poslovnih ved	
SKRBNIK PROCESA:	Strokovni sodelavec v FKS	Veronika Zabukovec, mag. poslovnih ved	
PREGLEDAL:	Direktor	Olga Doles, dr.med.,spec. spl. med.	
ODOBRIL:	Direktor	Olga Doles, dr.med.,spec. spl. med.	

PREGLED ZADNJIH SPREMEMB V DOKUMENTU

Zap. št.	Sprememba v točki:	OPIS SPREMEMBE

KAZALO

I. SPLOŠNE DOLOČBE

1. Vsebina in namen dokumentacije

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 Zdravstveni dom dr. Božidarja Lavriča – Cerknica (kratek naziv ZD Cerknica; 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. Razlaga pojmov

2. člen

V tem pravilniku uporabljeni izrazi imajo naslednji pomen:

- ZVOP-2 – 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;
- privolitev posameznika, na katerega se podatki nanašajo: pomeni vsako prostovoljno, izrecno, informirano in nedvoumno izjavo volje posameznika, o obdelavi njegovih osebnih podatkov;
- nadzorni organ: je informacijski pooblaščenec, določen skladno z zakonom, ki ureja Informacijskega pooblaščenca;
- nadzorne osebe: so informacijski pooblaščenec in nadzorniki za varstvo osebnih podatkov (določeni z zakonom), kadar izvajajo nadzor po določbah zakona, ki ureja varstvo osebnih podatkov;
- javni sektor: so državni organi, samoupravne lokalne skupnosti, nosilci javnih pooblastil v delu, kjer izvršujejo javna pooblastila, javne agencije, javni skladi, javni zavodi, univerze, samostojni visokošolski zavodi, zasebni vrtci in zasebne osnovne ter srednje šole, ki izvajajo javno veljavne vzgojno-izobraževalne programe, samoupravne narodne skupnosti, Svet romske skupnosti RS in druge osebe javnega prava, ustanovljene z zakonom;

- zasebni sektor: so pravne in fizične osebe, ki opravljajo dejavnost v skladu z zakonom, ki ureja gospodarske družbe ali gospodarske javne službe ali obrt, in druge osebe zasebnega prava; zasebni sektor so tudi javni gospodarski zavodi, javna podjetja in gospodarske družbe in izvajalci gospodarskih javnih služb, ne glede na delež oziroma vpliv države ali samoupravne lokalne skupnosti ali samoupravne narodne skupnosti ali dejstvo, da so nosilci javnega pooblastila;
- povezovalni znak: je osebna identifikacijska številka in druge z zakonom opredeljene enolične identifikacijske številke posameznika, z uporabo katerih je mogoče zbrati oziroma priklicati osebne podatke iz zbirk osebnih podatkov, v katerih so enolične identifikacijske številke obdelovanem ter drugi podobni znaki, ki se reno ali sistematično uporabljajo za povezovanje zbirk med različnimi upravljavci ali dveh ali več zbirk znotraj enega upravljavca;
- kazenske evidence: so evidence, določene v zakonu, ki ureja izvrševanje kazenskih sankcij;
- prekrškovne evidence: so evidence o pravnomočnih odločbah o prekrških, evidence pravnomočnih sodb oziroma sklepov o prekrških in kazenskih točk, določenih v zakonu, ki ureja prekrške;
- storitve informacijske družbe: je katerakoli storitev, ki se običajno opravi odplačno, na daljavo (storitev se opravi, ne da bi bile stranke sočasno navzoče), elektronsko (storitev se pošlje na začetnem kraju in sprejme na cilju z elektronsko opremo za obdelavo in shranjevanje podatkov ter se v celoti prenaša, pošilja in sprejema po žici, radijsko, z optičnimi ali drugimi elektromagnetnimi sredstvi) in na posamezno zahtevo prejemnika storitev (storitev opravi s prenosom podatkov na posamezno zahtevo);
- povezovanje zbirk podatkov: je avtomatsko in elektronsko povezovanje zbirk, ki jih upravljajo upravljavci za različne namen ali po različnih pravnih podlagah, in sicer tako, da se določeni osebni podatki samodejno prenesejo ali vključijo v drugo povezano zbirko ali več povezanih zbirk, tudi če se izvaja le enosmeren pretok osebnih podatkov; zbirke so povezane, če se določeni osebni podatki iz ene zbirke neposredno vključijo v drugo zbirko in se tako druga zbirka poveča ali posodobi ali pa se osebni podatki v njen zaradi točnosti spremenijo;
- posebne obdelave: obdelave osebnih podatkov, določenih v zakonih, ki urejajo med drugim tudi področja zdravstvenega varstva, obveznega zdravstvenega zavarovanja ali ko upravljalec ali obdelovalec kot temeljno dejavnost izvaja obsežne obdelave posebnih vrst osebnih podatkov, ali obdelava posebnih vrst osebnih podatkov več kot 10.000 posameznikov, in za obdelavo katerih se smiselno uporabljajo določbe o varnostnih zahtevah in priglasitvi incidentov iz zakona, ki ureja informacijsko varnost, ki se nanašajo na izvajalce bistvenih storitev, če upravljalec glede teh obdelav ni dolžan izvajati ukrepov po zakonu, ki ureja informacijsko varnost;
- SUVI - Sistem za upravljanje varovanja informacij, ki ga opredeljuje eZdravje.

Vrste podatkov, lastništvo, skrbništvo in dovoljenje do dostopa opredeljuje Politika o navodilih za klasifikacijo, označevanje in ravnanje z informacijami.

II. VSEBINSKE IN POSTOPKOVNE DOLOČBE

3. Zbirka osebnih podatkov

3. 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.

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.

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

ZD Cerknica vodi seznam, iz katerega je za vsako zbirko osebnih podatkov jasno razvidno, katera oseba je odgovorna za posamezno zbirko osebnih podatkov ter katere osebe lahko zaradi narave svojega dela obdelujejo osebne podatke, ki se nanašajo na posamezno zbirko osebnih podatkov. V seznam se vpisujejo sledeči podatki: naziv zbirke osebnih podatkov, delovno mesto osebe, ki je odgovorna za zbirko osebnih podatkov delovna mesta oseb, ki lahko zaradi narave njihovega dela obdelujejo osebne podatke, ki se nanašajo na zbirko osebnih podatkov.

4. člen

Varstvo osebnih podatkov se zagotavlja vsakemu posamezniku, ne glede na narodnost, raso, barvo kože, veroizpoved, etično 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.

Obdelava osebnih podatkov je prepovedana, če se izvaja na način diskriminacije glede na narodnost, raso, barvo kože, veroizpoved, etično pripadnost, spol, jezik, politično ali drugo prepričanje, spolno usmerjenost, spolno identiteto, premoženjsko stanje, kraj rojstva, izobrazbo, družbeni položaj, državljanstvo, kraj oziroma vrsto prebivališča, zdravstveno stanje, genske dispozicije ali katero koli drugo osebno okoliščino posameznika.

5. 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 kakršnokoli razlogov možnosti dostopa do teh podatkov, morajo biti seznanjeni s Splošno uredbo, z veljavnim 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.

6. člen

Za varovane osebne podatke štejejo tisti podatki, ki predstavljajo katerokoli informacijo v zvezi z določenim ali določljivim posameznikom, na katerega se osebni podatki nanašajo, in to ne glede na obliko, v kateri so takšni podatki 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.

4. Zavarovanje osebnih podatkov

7. člen

Zavarovanje osebnih podatkov zajema ustrezne tehnične in organizacijske ukrepe za zagotavljanje skladnosti obdelave osebnih podatkov, glede na naravo, obseg, okoliščine in namen obdelave pa tudi tveganj za pravice in svoboščine posameznikov, z določbami Splošne uredbe in veljavnim zakonom, ki ureja varstvo osebnih podatkov in drugih predpisov, ki urejajo varstvo osebnih podatkov.

Zavarovanje osebnih podatkov zajema pravne, organizacijske in ustrezne logistično-tehnične postopke in ukrepe, s katerimi se:

- varujejo prostori, strojna in sistemska programska oprema, kjer se nahajajo osebni podatki;
- varuje aplikativna programska oprema, s katero se obdelujejo osebni podatki;
- zagotavlja varnost posredovanja in prenosa osebnih podatkov;
- onemogoča nepooblaščenim osebam dostop do naprav, na katerih se obdelujejo osebni podatki in do njihovih zbirk;
- omogoča naknadno ugotavljanje kdaj so bili posamezni podatki uporabljeni in vneseni v zbirko podatkov oziroma računalniške sisteme, kdaj in kdo jih je vnesel, kdo dostopa do teh podatkov in to v obdobju, za katero se posamezni podatki shranjujejo (sledljivost podatkov). Sledljivosti podatkov v obstoječi aplikativni programski opremi je zagotovljena.

Pri tem se uporabljajo sprejete varnostne politike iz Sistema za upravljanje varovanja informacij (SUVI), ki ga opredeljuje eZdravje. Področne varnostne politike so Izvedbeni dokumenti tega pravilnika.

8.člen

Obdelava in zavarovanje posebnih vrst osebnih podatkov, med katere sodijo podatki o rasnem ali etničnem poreklu, politično mnenje, versko, ali fiziološko prepričanje ali članstvo v sindikatu in obdelava genskih podatkov, biometričnih podatkov za namene edinstvene identifikacije posameznika, podatkov v zvezi z zdravjem (zdravstveno stanje, zdravljenje) ali podatkov v zvezi posameznikovim spolnim življenjem ali spolno usmerjenostjo, morata biti izvajana posebno vestno in skrbno.

Posebne vrste osebnih podatkov morajo biti pri obdelavi posebej označeni in zavarovani tako, da se nepooblaščenim osebam prepreči dostop do njih oziroma seznanitev z njimi.

9. člen

Za varnost osebnih podatkov na področju posebnih obdelav, kar vključuje obdelavo osebnih podatkov v informacijskih sistemih, v katerih:

- se izvajajo obdelave osebnih podatkov, določenih v zakonih, ki urejajo področja upravnih notranjih zadev, finančne uprave, državljanstva, Slovenske obveščevalno-varnostne agencije, zdravstvenega varstva, obveznega zdravstvenega zavarovanja, uveljavljanja pravic iz javnih sredstev ter kazenskih in prekrškovnih evidenc, ali
- - se obdelujejo podatki več kot 100.000 posameznikov na podlagi veljavnega zakon, razen obdelav osebnih podatkov (3. poglavje ZVOP-2) ali
- Upravljalec ali obdelovalec kot svojo temeljno dejavnosti izvaja obsežne obdelave posebnih vrst osebnih podatkov, ali
- Se obdeluje posebne vrste osebnih podatkov več kot 10.000 posameznikov;

se smiselno uporabljajo določbe o varnostnih zahtevah in priglasitvi incidentov iz zakona, ki ureja informacijsko varnost, ki se nanašajo na izvajalce bistvenih storitev, če upravljalec glede teh obdelav ni dolžan izvajati ukrepov po zakonu, ki ureja informacijsko varnost.

V kolikor se obdelujejo biometrični osebni podatki, zdravstveni osebni podatki ali podatki iz kazenskih in prekrškovnih evidenc in obdelav o izvajajo državni organi, samoupravne lokalne skupnosti, javne agencije, javni zavodi, javna podjetja, izvajalci javnih služb ali nosilci javnih pooblastil, mora biti podatek o fizični lokaciji hrambe teh podatkov znan v vseh fazah hrambe in obdelave in tako zbirko podatkov je dovoljeno hraniti le znotraj ozemlja RS.

TAJNOST PODATKOV

10. 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.

11. 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.

12.člen

Zakonit zastopnik izvajalca oziroma pooblaščena oseba lahko podatke, ki predstavljajo poslovno ali poklicno skrivnost, posreduje tretjim osebam, ko le-te izkažejo pravni interes in v skladu s tem Pravilnikom, ZVOP-2 in zakonom o dostopu do informacij javnega značaja (ZDIJZ).

5. Pravice posameznikov, na katere se nanašajo osebni podatki

13. člen

Izvajalec mora posamezniku na njegovo zahtevo:
- omogočiti seznanitev in dostop do osebnih podatkov,
- potrditi, ali se podatki v zvezi z njim obdelujejo, omogoči se mu vpogled v njegove osebne podatke, katere izvajalec poseduje in mu omogočiti kopiranje le-teh (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 nasprotju z zakonom;
- obvestiti posameznika o vseh popravkih ali izbrisih osebnih podatkov ali omejitev obdelave;
- posredovati osebne podatke, ki jih je posameznik posredoval izvajalcu, v strukturirani splošno uporabljeni in strojno berljivi obliki, drugemu upravljalcu, ne da bi ga izvajalec pri tem oviral;
- prenehati z obdelavo osebnih podatkov v primeru podanega ugovora posameznika (npr. umik soglasja), razen če upravljalec dokaže nujne legitimne razloge za obdelavo, ki prevladajo nad interesi, pravicami in svoboščinami posameznika, na katerega se nanašajo osebni podatki in
- pravica do vložitve pritožbe pri nadzornem organu (pravica do pritožbe).

14. člen

Izvajalec (obdelovalec) posameznikovih osebnih podatkov mora posamezniku na njegovo zahtevo:

- zagotoviti kopijo osebnih podatkov, katere obdeluje;
- posredovati izpis osebnih podatkov, ki jih poseduje izvajalec v svoji zbiri;
- 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 in vsa potrebna pojasnila v zvezi s tem;
- dati informacije o rokih hrambe dokumentacije, če le-tega lahko opredeli in
- pojasniti tehnične postopke odločanja, če izvaja avtomatizirano odločanje z obdelavo osebnih podatkov posameznika.

15. člen

Izvajalec od prejeman zahteve posameznika, ki izvira iz njegovih pravic v zvezi z obdelavo osebnih podatkov in so opredeljene v 13.členu tega Pravilnika, 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 hrambe, dokler o zadevi ni pravnomočno odločeno, po pravnomočnosti pa skladno s pravnomočno odločitvijo v zadevi.

16.člen

Izvajalec na zahtevo posameznika slednjemu posreduje izpis, seznam, informacije ter pojasnilo v zvezi s pravicami posameznika, ki se nanašajo na obdelavo osebnih podatkov v 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.

17. člen

Kadar izvajalec obravnava zahtevke posameznika, ki so njegova pravica (kot predeljeno v 13.členu tega Pravilnika) in druge zahteve posameznika s področja varstva osebnih podatkov, dostopa do osebnih podatkov, njihovega pridobivanja in obdelave po določbah ZVOP-2 ali drugem zakonu, posameznika seznani z odločitvijo v pisni obliki, če pa posameznik to zahteva, tudi ustno. Odločitev mora vsebovati razloge in informacijo o pravici do pritožbe pri nadzornem organu v roku 15 dni od seznanitve z odločitvijo. Odločitev ima lahko obliko uradnega zaznamka, ki se pošlje posamezniku na način, ki omogoča seznanitev z odločitvijo in dokazovanje njenega prejema.

18. člen

Izvajalec je dolžan informacije posamezniku, ki izvirajo iz njegovih pravic c zvezi z obdelavo osebnih podatkov, in so opredeljene v 13. členu tega Pravilnika, zagotoviti brezplačno.

Kadar so zahtevki posameznika v zvezi z obdelavo osebnih podatkov neutemeljeni ali pretirani, zlasti ker se ponavljajo, lahko izvajalec zahtevi ugodi, če je utemeljena, posamezniku pa zaračuna stroške, ki vključujejo materialne stroške posredovanja informacij, sporočil, odgovorov oziroma izvajanja zahtevanega ukrepanja, v višini v skladu s predpisom ministrstva. O nastalih stroških izvajalec obvesti posameznika vnaprej.

19. člen

Posameznik, ki meni, da izvajalec krši njegove pravice, določene s Splošno uredbo in z zakoni, ki urejajo obdelavo ali varstvo osebnih podatkov, lahko zahteva sodno varstvo svojih pravic ves čas trajanja kršitve, brez predhodnega uveljavljanja pravic po drugih določbah ZVOP-2 ali uporabe drugih pravnih sredstev. S sodnim varstvom lahko poleg prenehanja kršitve ali vzpostavitve zakonitega stanja zahteva tudi povrnitev škode.

20. člen

Izvajalec lahko posreduje osebne podatke posameznika drugim fizičnim ali pravnim osebam ali osebam javnega sektorja na podlagi prejete zahteve, iz katere mora izhajati veljavna pravna podlaga za pridobitev podatkov in utemeljenost zahteve, ki pa mora vsebovati naslednje podatke:
1. 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.
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, ter navedbo organa ali drugega subjekta, ki obravnava zadevo.
5. Vrste osebnih podatkov, ki naj se mu posredujejo.
6. oblika in način pridobitve zahtevanih osebnih podatkov.

Izvajalec vlagatelju zahteve, če zakon ne določa drugače, zahtevane osebne podatke posreduje najpozneje v 15 dneh od prejemna popolne zahteve ali pa ga v tem roku pisno obvesti o razlogih, zaradi katerih mu zahtevanih osebnih podatkov ne bo posredoval. Dopustno je podaljšanje roka v primeru dogovora med izvajalcem in vlagateljem zahteve.

21. člen

Pri pridobivanju osebnih podatkov iz zbirk osebnih podatkov s področja zdravstva ni dovoljeno uporabljati povezovalnega znaka na način, da bi se za pridobitev osebnega podatka uporabil izključno ta znak, razen, če zakon tega ne določa drugače.

Izjemoma se lahko uporabi povezovalni znak za pridobivanje osebnih podatkov, če je ta podatek v konkretni zadevi, ki lahko omogoči, da se odkrije storilec ali kaznivo dejanje, ki se preganja po uradni dolžnosti, ali da se zavaruje življenje ali telo posameznika. O tem se brez odlašanja napravi uradni zaznamek ali drug ustrezen zapis, ki omogoča naknadno preverjanje nujnosti uporabe povezovalnega znaka.

22. člen

Osebni podatki umrlih posameznikov se obdelujejo v skladu z določili ZVOP-2 in zakonom o pacientovih pravicah.

6. Varovanje prostorov in računalniške opreme in opredelitev

VAROVANJE PROSTOROV IN NOSILCEV OSEBNIH PODATKOV

23. 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.

24. 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.

25. 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.

26. 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 evidenco, 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 evidenco.

27. 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 in pogodbo o obdelavi osebnih podatkov, s katerimi se seznanijo pri izvajanju svojega dela po krovni pogodbi z izvajalcem.

28. 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.

29. 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.

V varovane prostore ZD nezaposlene osebe ne smejo vstopati brez spremstva ali prisotnosti zaposlenega delavca. Delavec, ki dela v varovanih prostorih, mora vestno in skrbno nadzorovati prostor in ob zapustitvi prostora zakleniti prostor oziroma drugače zavarovati nosilce osebnih podatkov.

Delavec, ki pri svojem delu uporablja osebne podatke ali jih kakorkoli obdeluje, ne sme med delovnim časom puščati nosilcev osebnih podatkov na pisalnih mizah (v skladu s Politiko fizične zaščite in fizičnega dostopa) ali jih kako drugače izpostavljati nevarnosti vpogleda vanje nepooblaščenim osebam oziroma delavcem.

V prostor, kjer imajo vstop stranke oziroma osebe, ki niso zaposlene v zavodu, morajo biti nosilci podatkov in računalniški prikazovalniki, v kolikor je to izvedljivo, nameščeni v času obdelave ali dela na njih tako, da strankam ni omogočen vpogled vanje.

30.člen

Nosilcev osebnih podatkov delavci zavoda ne smejo odnašati izven zavoda ali jih posredovati tretjim osebam brez izrecnega dovoljenja direktorja, razen zdravstvene dokumentacije.
Za iznos zdravstvene dokumentacije (kartonov) odgovarja zdravnik, ki je skrbnik teh podatkov.

Posredovanje osebnih podatkov pooblaščenim zunanjim institucijam in drugim, ki izkažejo zakonsko podlago za pridobitev osebnih podatkov, dovoli direktor, razen zdravstvene dokumentacije, ki jo posreduje skrbnik teh podatkov.

Predhodno vsi delavci vpišejo namen in tehten razlog za iznos podatkov iz zavoda v **seznam posredovanih osebnih podatkov**.

Z vsako zunanjo pravno ali fizično osebo, ki opravlja posamezna opravila v zvezi z zbiranjem, obdelovanjem, shranjevanjem ali posredovanjem osebnih podatkov in je registrirana za opravljanje takšne dejavnosti (pogodbeni obdelovalec), se sklene pisna pogodba OB PRSKS03 10), predvidena z ZVOP. V takšni pogodbi morajo biti obvezno predpisani tudi pogoji in ukrepi za zagotovitev varstva osebnih podatkov in njihovega zavarovanja. Omenjeno velja tudi za zunanje osebe, ki vzdržujejo strojno in programsko opremo ter izdelujejo in namestijo novo strojno ali programsko opremo.

31. člen

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

7. Zavarovanje sistemske in aplikativne programske opreme ter podatkov, ki se obdelujejo z računalniško opremo

32. 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.

Pristop do podatkov prek aplikativne programske opreme in dostop v mrežo mora biti varovan s sistemom gesel za avtorizacijo in identifikacijo uporabnikov programov in podatkov v skladu s Politiko nadzora dostopa do aplikacij, informacij in sistemov.

Direktor v sodelovanju z informatikom določi v skladu s Politiko upravljanja in varovanja gesel režim dodeljevanja, hranjenja in spreminjanja gesel.
Za shranjevanje in varovanje nosilcev osebnih podatkov, shranjenih v elektronski obliki, veljajo enaka določila kot za ostale podatke iz tega pravilnika.

33. 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.

34. 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.

35. 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.

36. 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.

37. 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.

38. 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. Zakoniti zastopnik izvajalca določi režim dodeljevanja in spreminjanja gesel.

Varovana administratorska gesla odgovorna oseba informacijskega sistema hrani v ovojnicah in se smejo uporabljati v izjemnih in nujnih primerih. Vsako uporabo vsebine ovojnic ustrezno nadzira in dokumentira. Preverja tudi redno menjavanje gesel (14 znakov, menjava na 90 dni). To predstavlja Politiko upravljanja in varovanja gesel.

39. člen

Odgovorna oseba za informacijski sistem opredeli procedure za varnostno kopiranje in restavriranje podatkov.
Za potrebe restavriranja osebnih podatkov oziroma računalniškega sistema po okvarah ali izgubi podatkov in drugih razlogov mora imeti informacijski sistem zavoda zagotovljen mehanizem izdelave varnostnih kopij, pri čemer se uporablja Politika varnostnega kopiranja.

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.

Računalniške kopije vsebin zbirk osebnih podatkov na disketah ali drugih medijih se hranijo v zavarovanih zaklenjenih omarah odpornih proti ognju, poplavam in v predpisanih klimatskih razmerah. Odgovorna oseba za informacijski sistem v sodelovanju z zunanjimi sodelavci v rednih časovnih presledkih preverja izdelavo varnostnih kopij (na 3 mesece) in preizkusi postopke restavriranja (na 6 mescev). Dnevno se prenese varnostne kopije na oddaljeno lokacijo.

40. člen

Za oddaljeni dostop do programske opreme zunanjih pogodbenih izvajalcev mora biti zagotovljena sledljivost in seznanjenost zavoda o vsakokratnih dostopih v skladu s Politiko oddaljenega dostopa.

41. člen

Notranji informacijski sistem zavoda, kjer se nahajajo nosilci osebnih podatkov, je potrebno ustrezno varovati pred virusi, zlonamernimi kodami, poskusi vdorov, ter drugimi nevarnostmi, ki vplivajo na varnost in varovanje v skladu s Politiko zaščite pred zlonamerno programsko opremo.

Vsi podatki in programska oprema, ki so namenjeni uporabi na računalnikih zavoda in v računalniškem informacijskem sistemu zavoda in prispejo v zavod na medijih za prenos računalniških podatkov ali prek telekomunikacijskih kablov, morajo biti pred uporabo preverjeni glede prisotnosti računalniških virusov ali drugih nevarnosti.

8. Manipulacija z osebnimi podatki in zbirkami osebnih podatkov

OBDELAVA OSEBNIH PODATKOV IN EVIDENCA OBDELAVE OSEBNIH PODATKOV

42. člen

Osebni podatki v javnem sektorju 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,
- obdelava je povezana s posameznikovimi osebnimi podatki, katere le-ta sam objavi,
- obdelava je potrebna za uveljavljanje, izvajanje ali obrambo pravnih zahtevkov ali kadarkoli sodišča izvajajo svojo sodno pristojnost,
Obdelava je potrebna za namene preventivne medicine ali medicine dela, oceno delovne sposobnosti zaposlenega, zdravstveno diagnozo, zagotovitev zdravstvene ali socialne oskrbe ali zdravljenja ali upravljanje sistemov in storitev zdravstvenega ali socialnega varstva in
- obdelava je potrebna za namene arhiviranja v javnem interesu, za znanstveno – ali zgodovinsko-raziskovalne namene ali statistične namene.

43. člen

Izvajalec je dolžan posameznika natančno obvestiti o tem, v kakšnem obsegu poteka obdelava osebnih podatkov pri izvajalcu in kakšne so posledice te obdelave in mu je dolžan v jedrnati, pregledni, razumljivi in lahko dostopni obliki zagotoviti naslednje informacije:
- informacije upravljavcu,
- informacije o namenu obdelovanja osebnih podatkov in pravno podlago za le-ta namen;
- zakonite interese, za uveljavljanje katerih si prizadeva izvajalec ali tretja oseba,
- kadar obdelava temelji na privolitvi, obstoju pravice o preklicu privolitve;
- informacije o uporabnikih osebnih podatkov,
- informacije o morebitnem prenosu osebnih podatkov v tretjo državo ali mednarodno organizacijo;
- informacijo o obdobju hrambe osebnih podatkov,
- informacije glede obstoja pravic posameznika skladno z Uredbo (pravica do dostopa, popravka, izbrisa, omejitve obdelave, ugovora obdelavi in prenosljivost podatkov);
- informacijo glede pravice do vložitve pritožbe pri nadzornem organu;
- informacijo o tem, ali je zagotovitev osebnih podatkov zakonska ali pogodbena obveznost ali obveznost, ki je potrebna za sklenitev pogodbe in ali le-te zagotovi posameznik in kakšne so posledice, če jih ne zagotovi;
- informacije o obstoju avtomatiziranega sprejemanja odločitev (razlogi, pomen in posledice);

- kadar osebni podatki niso pridobljeni od posameznika, na katerega se nanašajo, mora izvajalec posamezniku zagotoviti podatek p vrstah zadevnih osebnih podatkov, ki se obdelujejo te rod kje izvirajo osebni podatki in po potreb, ali izvirajo iz javno dostopnih virov in
- obveščanje posameznika glede stroškov pri uveljavljanju pravic (ZVOP-2).

Posameznik mora prejeti navedene informacije, ko izvajalec pridobi njegove osebne podatke.

44. 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.

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.

Zaposleni pri izvajalcu ali pooblaščene osebe, ki obdelujejo osebne podatke, morajo biti seznanjeni z vsebino evidenc dejavnosti obdelav osebnih podatkov.

Evidenca dejavnosti obdelav osebnih podatkov vsebuje vse naslednje informacije:

- naziv/ime in kontaktne podatke upravljavca, ali skupnega upravljavca, predstavnika upravljavca in pooblaščene osebe za varstvo podatkov;
- namen obdelave;
- opis kategorij posameznikov, katere se nanašajo osebni podatki, in vrste osebnih podatkov;
- kategorije uporabnikov, ki so jim bili oziroma jim bodo razkriti osebni podatki;
- kadar je ustrezno, informacije o prenosih osebnih podatkov v tretjo državo ali mednarodno organizacijo (z ustrezno identifikacijo) in dokumentacijo o ustreznih zaščitnih ukrepih;
- kadar je mogoče, predvidene roke za izbris različnih vrst podatkov:
- splošni opis tehničnih in organizacijskih varnostnih ukrepov in
- kontaktne podatke pooblaščene osebe za varstvo osebnih podatkov.

SPREJEM IN POSREDOVANJE OSEBNIH PODATKOV TRETJIM

45. 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.

Zaposleni 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.

46. 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.

Vsako posredovanje osebnih podatkov se beleži v evidenco posredovanih osebnih podatkov, iz katere mora biti razvidno, kateri osebni podatki so bili posredovani, komu, kdaj in na kakšni podlagi (ZVOP-2).

47. 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.

48. 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,…).

49. 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.

9. Fizična zaščita, fizični dostop in brisanje podatkov

BRISANJE PODATKOV OZIROMA UNIČENJE NOSILCEV OSEBNIH PODATKOV

50. 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 rokov hrambe in klasifikacijskem načrtu izvajalca.

51. 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.

52. 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.

Uničevanje osebnih podatkov na nosilcih iz predhodnega odstavka se mora izvajati tekoče in ažurno. Uničenje ali odstranjevanje nosilcev osebnih podatkov lahko izvaja le od direktorja pooblaščena oseba (notranja ali zunanja) oz. se lahko formira komisija za uničenje v skladu s Pravilnikom o arhiviranju in Politiko izdelave in hrambe arhivskih kopij.

53. člen

Izvajalec je dolžan, ob upoštevanju narave obdelovanih podatkov in tveganj občasno in na dokumentiran način preverjati, ali se upoštevajo določbe omejevanja roka hrambe.

STORITVE, KI JIH OPRAVLJAJO ZUNANJE PRAVNE ALI FIZIČNE OSEBE

54. 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.

55. 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.

10. Ukrepanje ob ugotovitvi zlorabe osebnih podatkov ali vdoru v zbirke osebnih podatkov

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

56. 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,…).

57. 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.

58. člen

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.

Izvajalec imenuje Pooblaščeno osebo za varstvo osebnih podatkov s posebnim sklepom:

1. **Podlaga**
   - člen 37 (odstavek 1) Splošne uredbe (EU) o varstvu podatkov in
   - ustrezni člen ZVOP-2 in
   - lahko tudi ustrezna podlaga iz ZDR-1

2. **Podatki o pooblaščeni osebi**
   - osebno ime
   - naziv
   - delovno mesto, funkcija, lahko dodatno tudi šifra iz sistemizacije
   - organizacijska enota
   - kontakt (telefon in e-pošta)

3. **Kratka obrazložitev izpolnjevanja pogojev** *(odvisno tudi od ZVOP-2)*
   - znanje in izkušnje
   - izobrazba
   - zaposlenost (kaj, kje)
   - neobstoj konflikta interesov *(DPO torej ne sme imeti v rokah odločanja o obdelavah osebnih podatkov)*
   - splošni pogoji (delovna zmožnost, državljanstvo, neobsojenost)

4. **Naloge**

Osnovne naloge po Splošni uredbi:
- obveščanje zavoda in zaposlenih ter pogodbenih delavcev o pravicah in dolžnostih na področju varstva osebnih podatkov
- spremljanje skladnosti poslovanja oziroma obdelav podatkov s predpisi o varstvu osebnih podatkov in internimi politikami o varnosti
- priprava predlogov za izvedbo ukrepov (kaj, kdo, kdaj, kako, kje in zakaj)
- organizacija ali izvedba notranjih uposabljanj po programu, če to narekujejo potrebe (npr. večje spremembe pri obdelavah, zaznani interni problemi, večje spremembe na področju zakonodaje)
- občasne revizije (neposredni pregledi skladnosti ter predlaganje ukrepov za izboljšanje) obdelav in procesov v organizacijskih enotah po programu
- občasno spremljanje izvajanja ocen učinkov po programu
- dajanje mnenj glede ocen učinkov v zvezi z varstvom podatkov
- sodelovanje z nadzornim organom pri nadzorih ali pri posvetovanjih (zagotavljanje stika, notranja koordinacija, zagotavljanje dostopa, skrb za korespondenco ipd.)
- sodelovanje (skrb za stike) s posamezniki, na katere se nanašajo osebni podatki, ki se na zavod obračajo glede vprašanj, povezanih z obdelavo njihovih osebnih podatkov, in uresničevanjem njihovih pravic (npr. seznanitev z lastno zdravstveno dokumentacijo).

Dodatne naloge (primeri):

vodenje evidence dejavnosti obdelave
- aktivno sodelovanje pri pripravi ocen učinkov
- poročanje o kršitvah varstva osebnih podatkov nadzornemu organu
- dokumentiranje zaznanih in sporočenih kršitev
- priprava internih navodil za ravnanje in obvestil za zaposlene

- dajanje pobud za odpravo pomanjkljivosti ali zmanjšanje tveganj na področju varstva osebnih podatkov
- priprava zaprosil za mnenja s področja varstva osebnih podatkov
- sprejemanje prijav domnevnih kršitev in njihova obravnava
- koordinacija dela, vzpodbujanje, usmerjanje in dajanje navodil v zvezi z zgornjimi (…) nalogami ***(pomembno - pooblaščena oseba ni za vse sama! Je centralna oseba za ta vprašanja, toda to še ne pomeni, da je dolžna vse delati sama, pač pa mora imeti možnost, glede na notranjo organizacijo in položaj, da usmerja, koordinira delo, predlaga ali celo (neposredno ali posredno) drugim nalaga posamezna opravila v zvezi z varstvom podatkov)***
- dokumentiranje nalog

<u>Druge določbe v zvezi s položajem pooblaščene osebe</u>

- zavod za potrebe izvajanja tega sklepa v skladu s Splošno uredbo (EU):
  - zagotavlja, da je pooblaščena oseba ustrezno in pravočasno vključena v vse zadeve v zvezi z varstvom osebnih podatkov
  - pooblaščeni osebi pomaga pri opravljanju nalog tako, da zagotovi sredstva, potrebna za opravljanje teh nalog, in dostop do osebnih podatkov in dejanj obdelave, ter ohranjanje njenega strokovnega znanja
  - zagotovi, da pooblaščena oseba pri opravljanju nalog ne prejema nobenih navodil. Pooblaščena oseba ne sme biti razrešena ali kaznovana zaradi opravljanja svojih nalog. Pooblaščena oseba neposredno poroča najvišji upravni ravni upravljavca (…)
- pooblaščena oseba je pri opravljanju svojih nalog zavezana varovati skrivnost ali zaupnost v skladu z zakonodajo s področja varstva osebnih podatkov
- pooblaščena oseba ima za potrebe opravljanja nalog odprete dostopne (uporabniške) pravice do (…)
- pooblaščeni osebi so zaposleni in pogodbeni delavci ter pogodbeni obdelovalci dolžni dajati potrebna pojasnila ter predloge za potrebe izvajanja nalog, ter ji omogočiti dostop do prostorov in sredstev obdelave podatkov

59. 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.

60. 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.

61. 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.

62. 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.

11. Odgovornost za izvajanje ukrepov zavarovanja osebnih podatkov

63. 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. 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 in v skladu z Politiko varovanja v zvezi z osebjem.

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.

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

64. člen

Delavci zavoda so dolžni izvajati ukrepe za preprečevanje zlorabe osebnih podatkov in morajo z osebnimi podatki, s katerimi se seznanijo pri svojem delu, ravnati vestno in skrbno na način in po postopkih, ki jih določa ta pravilnik.

Delavec, 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 direktorja ali pooblaščenega delavca, ki vodi in ureja zbirko osebnih podatkov, ki so bili zlorabljeni ali v katero se je vdrlo, v skladu s Politiko upravljanja varnostnih incidentov in Politiko revizijskih sledi.

65. člen

Direktor mora zoper tistega, ki je zlorabil osebne podatke ali je nepooblaščeno vdrl v zbirko osebnih podatkov, ustrezno ukrepati v skladu s Pravilnikom u disciplinski in odškodninski odgovornosti zaposlenih.

Če obstaja sum pri vdoru v zbirko osebnih podatkov, da je ta storjen z naklepom in namenom zlorabiti osebne podatke ali jih uporabiti v nasprotju z nameni, za katere so zbrani, ali če je do zlorabe osebnih podatkov že prišlo, mora direktor poleg uvedbe disciplinskega postopka zoper storilca, če je ta delavec zavoda, vdor ali zlorabo prijaviti organom pregona.

O zlorabi ali dvomu o zlorabi osebnih podatkov vodenih v zbirkah osebnih podatkov zavoda s strani oseb, ki niso delavci zavoda, se obvesti organe pooblaščene za pregon

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

66. 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.

67. 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.

POSEBNE UREDITVE ZA ZBIRKE OSEBNIH PODATKOV VODENIH PRI IZVAJALCU

68. 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).

69. 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 obdelave in shranjevanja podatkov,
- seznanitev z možnostjo preklica soglasja,
- datum podpisa izjave in podpis osebe.

70. 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.

71. 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 (lahko se obvestilo objavi tudi na spletni strani).

Obvestilo iz prejšnjega odstavka mora vsebovati naslednje informacije (poleg navedenih informacij iz prvega odstavka 13. člena Splošne uredbe):
- pisno ali nedvoumno grafično opisano dejstvo, da se izvaja videonadzor;
- namen obdelave, navedbo upravljavca videonadzornega sistema, telefonsko številko ali naslov elektronske pošte ali spletni naslov za potrebe uveljavljanja pravic posameznika s področja varstva osebnih podatkov;
- informacije o posebnih vplivih obdelave, zlasti nadaljnje obdelave;
- kontaktne podatke pooblaščene osebe (telefonska številka ali naslov e-pošte) in
- neobičajne nadaljnje obdelave, ko so prenosi subjektom v tretje države, spremljanje dogajanja v živo, možnost zvočne intervencije v primeru spremljanja dogajanja v živo.

O izvajanju videonadzora in o vsebinah iz prvega odstavka tega člena je dolžan izvajalec psino obvestiti vse zaposlene, ki opravljajo delo v nadzorovanem prostoru.

Zbirka posnetkov videonadzornega sistema vsebuje posnetek posameznika (slika), podatek o lokaciji, datum in čas posnetka, izjemoma tudi zvok. Zbirka osebnih podatkov lahko vsebuje tudi: datum in čas vstopa in izstopa v uradni službeni prostor, osebno ime posameznika, naslov njegovega stalnega ali začasnega prebivališča, zaposlitev, številko in podatke o vrsti njegovega osebnega dokumenta ter razlog vstopa, če se navedeni osebni podatki zbirajo skupaj s posnetkom videonadzornega sistema.

Videonadzora ni dovoljeno izvajati v dvigalih, sanitarijah, prostorih za preoblačenje, hotelskih sobah in drugih podobnih prostorih, v katerih posameznik utemeljeno pričakuje višjo stopnjo zasebnosti.

Video nadzorni sistem, s katerim se izvaja videonadzor, mora biti zavarovan z ustreznimi tehničnimi in organizacijskimi ukrepi, da se preprečijo tveganja nenamernega ali nezakonitega uničenja, izgube, spremembe, nepooblaščenega razkritja ali dostopa osebnih podatkov, ki so poslani, shranjeni ali kako drugače obdelani.

Vpogled, uporaba ali posredovanje posnetkov videonadzornega sistema so dopustni samo za namene, ki so zakonito obstajali ali so navedeni na obvestilu v času zajema posnetka. Upravljalec videonadzornega sistema pa je dolžan za vsak vpogled ali uporabo posnetkov zagotoviti možnost naknadnega ugotavljanja, kateri posnetki so bili obdelani, kdaj in kako so bili uporabljeni ali komu so bili posredovani, kdo je izvedel ta dejanja obdelave, kdaj in s kakšnim namenom in na kateri pravni podlagi. Te podatke je izvajalec dolžan hraniti v dnevniku obdelave, kot ga določa 22. člen ZVOP-2, dve leti po koncu leta, kot so podatki nastali.

Posnetki videonadzora se lahko hranijo največ eno leto od trenutka nastanka posnetka.

72. 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 zaposlenih. Pri tem mora paziti, da se videonadzor izvaja brez snemanja delov stanovanjskih stavb, ki niso službeni ali poslovni prostori.

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 delov prostorov in v obsegu, kjer je treba varovati takšne interese. Prepovedano je snemati delovna mesta, kjer delavec po navadi dela, razen če je to nujno za varnost ljudi ali premoženja oziroma varovanje tajnih podatkov in poslovnih skrivnosti. V primeru izvajanja videonadzora delovnih prostorov je neposredno spremljanje dogajanje pred kamerami dopustno le, če ga izvaja izrecno pooblaščeno osebje pri izvajalcu.

Videonadzor na javnih površinah (praviloma odprta prostorska ureditev, namenjena splošni rabi, naravna ali ustvarjena z gradbenimi ali drugimi posegi v prosto, kot so cesta, ulica, pasaža, trg, tržnica, atrij, parkirišče, pokopališče, park, zelenica, otroško igrišče, športno igrišče ter druga površina za rekreacijo in prosti čas; javna površina je grajena ali zelena; v lasti države, občine ali v zasebni lasti,…) je dovoljen le, kadar je to potrebno zaradi obstoja resne in utemeljene nevarnosti za življenje, osebno svobodo, telo in zdravje ljudi, varnost premoženja upravljavca ali varovanje tajnih podatkov upravljavca ali obdelovalca v prenosu in teh namenov ni mogoče doseči z drugi sredstvi. Videonadzor pa se lahko izvaja le glede tistih bližnjih ali povezanih delov javne površine in v obsegu, kjer je treba varovati interese. Videonadzor na javnih površinah lahko pri izvajalcu, ki je uvrščen v zasebni sektor, izvaja pooblaščeno varnostno osebje (oseba mora biti izrecno pooblaščena za izvajanje videonadzora).

Izvajalec kot upravljalec videonadzornega sistema, ki izvaja videonadzor javnih površin, mora v primeru, ko videonadzorni sistem posname dogodek, ki ogroža zdravje ali življenje posameznika, o tem nemudoma obvestiti policijo ali drug pristojni subjekt.
Posnetki videonadzora na javnih površinah se lahko hranijo največ šest mesecev od trenutka nastanka posnetka.

73. člen

Zbirka osebnih podatkov iz identifikacijskega dokumenta

Izvajalec lahko za zagotavljanje varnosti ljudi in premoženja, varovanja tajnih podatkov ter reda v poslovnih prostorih ali prostorih, ki jim ima v uporabi, od posameznika, ki namerava vstopiti ali izstopiti iz tega prostora, zahteva razlog vstopa ali izstopa ter navedbo vseh ali nekaterih osebnih podatkov: osebno ime, številka in vrsta uradnega identifikacijskega dokumenta, naslov prebivališča, zaposlitev, vrsta in registrska številka vozila ter datum, ura in razlog vstopa ali izstopa v prostore ali izstopa iz njih. Izvajalec lahko osebne dokumente posameznika po potrebi preveri tudi z vpogledom v uradni identifikacijski dokument.

Tako pridobljeni osebni podatki se lahko hranijo največ dve leti do konca koledarskega leta po vnosu osebnih podatkov v zbirko, nato se izbrišejo ali na drug način uničijo.

74. člen

Zbirka biometričnih osebnih podatkov

Obdelava biometričnih osebnih podatkov pri izvajalcu se lahko izvaja, če je to nujno potrebno za opravljanje dejavnosti, za varnost ljudi, varstvo premoženja, varovanje tajnih podatkov ali poslovnih skrivnosti in ob pogoju, da je predhodno odobrena s strani nadzornega organa.
Obdelava biometričnih podatkov zaradi varstva točnosti identitete svojih pacientov (posameznikov) je dopustna, če to določa zakon ali pogodba ali na podlagi izrecne privolitve posameznika.

Pred začetkom obdelave biometričnih osebnih podatkov morajo biti posamezniki o tem pisno obveščeni, kadar gre za zaposlene, pa mora izvajalec z zaposlenimi izvesti predhodni posvetovanje o sorazmernosti obdelave.

PRAVICE IZVEDENCA DO PODATKOV IZ MEDICINSKE DOKUMENTACIJE

75. 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.

76. 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.

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

77. 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 ter opredeliti rok, do katerega izvedence ali sodišče original medicinsko dokumentacijo izvajalcu vrne.

III. PREHODNE IN KONČNE DOLOČBE

12. Skrbništvo, odgovornost in nadzor

78. člen

Skrbnik tega dokumenta je strokovni sodelavec. Za izvajanje postopkov in ukrepov za zavarovanje osebnih podatkov so odgovorni vsi zaposleni.

Nadzor nad izvajanjem procesa izvaja Pooblaščena osebo za varstvo osebnih podatkov, ki o izvajanju nadzora vodi zapise, ki so podlaga za izvajanje korektivnih, korekcijskih in preventivnih ukrepov.
O izvajanju teh ukrepov se vodijo ustrezni zapisi.

13. Dostop

79. člen

Prejemniki tega dokumenta so vsi zaposleni, ki imajo dostop do intraneta.
Skrbnik procesa/dokumenta o sprejetih dokumentih ustrezno obvesti vodje služb in enot, ki so dolžni seznaniti svoje sodelavce z vsebinami sprejetih dokumentov.

14. Arhiviranje

80. člen

Arhiviranje se izvaja skladno z zahtevami, opredeljenimi v PR Arhiviranje dokumentacije in OP Proces vrednotenja in izboljševanja.

81. člen

Kazalnik kakovosti procesa je naslednji:

- **število ugotovljenih varnostnih incidentov.**

Merjenja kakovosti se izvajajo najmanj 1-krat letno. Strokovni sodelavec na osnovi doseženih rezultatov izvaja ustrezne ukrepe (korekcijski, korektivni, preventivni).

15. Izvedbeni dokumenti

Številka dokumenta	NAZIV DOKUMENTA
Ni številke	Politika dostopa do omrežja
Ni številke	Politika fizične zaščite in fizičnega dostopa
Ni številke	Politika izdelave in hrambe arhivskih kopij
Ni številke	Politika nadzora dostopa
Ni številke	Politika nadzora sprememb informacijskega sistema
Ni številke	Politika o navodilih za klasifikacijo
Ni številke	Politika oddaljenega nadzora dostopa do informacij, aplikacij in sistemov
Ni številke	Politika razvoja, spreminjanja in vzdrževanja programske opreme
Ni številke	Politika revizijskih sledi
Ni številke	Politika uporabe storitev interneta
Ni številke	Politika upravljanja in varovanja gesel
Ni številke	Politika upravljanja kakovosti in varnosti storitev tretjih strank
Ni številke	Politika upravljanja varnostnih incidentov
Ni številke	Politika varnostnega kopiranja
Ni številke	Politika varovanja v zvezi z osebjem
Ni številke	Politika zagotavljanja kakovosti infrastrukture
Ni številke	Politika zaščite pred zlonamerno programsko opremo

17. Povezave z drugimi dokumenti

Številka dokumenta	NAZIV DOKUMENTA
PR FKS 01	Pravilnik o arhiviranju dokumentacije
PR SKS 05	Notranja pravila za zajem in hrambo dokumentarnega gradiva v digitalni obliki
OP FKS 01	Obvladovanje dokumentacije
OP FKS 02	Proces vrednotenja in izboljševanja
Ni številke	EKN
Ni številke	ZVOP-2
Ni številke	Uredba (EU) 2016/679 Evropskega parlamenta in Sveta z dne 26. aprila 2016 o varstvu posameznikov pri obdelavi osebnih podatkov (GDPR)
Ni številke	Pravilnik o disciplinski in odškodninski odgovornosti zaposlenih

18. Priloge

Številka dokumenta	NAZIV DOKUMENTA
OB PRFKS03 01	Evidenca posredovanih osebnih podatkov (ambulanta, uprava)
OB PRFKS03 02	Evidenca dejavnosti obdelave
OB PRFKS03 03	Izjava o varovanju osebnih podatkov in drugih podatkov zavoda
OB PRFKS03 04	Privolitvena izjava posameznika
OB PRFKS03 05	Potrdilo o izročitvi medicinske dokumentacije izvedencu
OB PRFKS03 06	Obvestilo posamezniku o posredovanju osebnih podatkov
OB PRFKS03 07	Evidenca o spremembah in dopolnitvah sistemske in aplikativne programske opreme
OB PRFKS03 08	Evidenca gesel za uporabo računalniške opreme
OB PRFKS03 09	Sklep o imenovanju pooblaščene osebe za varstvo osebnih podatkov
Ni številke / OB PRFKS03 10	Pogodba z zunanjim izvajalcem o obdelavi osebnih podatkov
OB PRFKS03 11	Uradno obvestilo nadzornemu organu
OB PRFKS03 12	Seznam obdelovalcev osebnih podatkov
OB PRFKS03 13	Evidenca oddaljenega dostopa
OB PRFKS03 14	Zahteva za posredovanje medicinske dokumentacije
OB PRFKS03 15	Izjava dijakov/študentov na obvezni praksi

19. Prenehanje veljavnosti

Številka dokumenta	NAZIV DOKUMENTA
PR SKS 03	Pravilnik varstvo osebnih in drugih podatkov zavoda