

Na podlagi določb Uredbe (EU) 2016/679 Evropskega parlamenta in Sveta z dne 27. aprila 2016 o varstvu posameznikov pri obdelavi osebnih podatkov in o prostem pretoku takih podatkov ter o razveljavitvi Direktive 95/46/ES (»GDPR«) in na podlagi veljavnega zakona, ki ureja varstvo osebnih podatkov, izdaja Javni zavod Kranjski vrtci, Ulica Nikole Tesle 2, Kranj, ki ga zastopa ravnateljica Dolinar Tea (v nadaljevanju ravnateljica)

PRAVILNIK **o zbiranju in varstvu osebnih podatkov**

I. UVODNE DOLOČBE

1. člen

Pravilnik o zbiranju in varstvu osebnih podatkov (v nadaljevanju: pravilnik) določa organizacijske, tehnične in logistično-tehnične postopke in ukrepe za zavarovanje osebnih podatkov v javnem zavodu Kranjski vrtci (v nadaljevanju zavod) z namenom, da se prepreči slučajno ali namerno nepooblaščen uničevanje, spreminjanje in izguba podatkov, kakor tudi nepooblaščen dostop, uporaba, obdelava in/ali posredovanje osebnih podatkov.

Zavarovanje varovanih podatkov obsega organizacijske in ustrezne logično-tehnične postopke in ukrepe, s katerimi se:

- varujejo prostori, oprema in sistemsko programska oprema ter vhodno-izhodne enote,
- varuje aplikativna programska oprema, s katero se obdelujejo osebni podatki,
- zagotavlja varnost posredovanja in prenosa varovanih podatkov,
- preprečuje nepooblaščenim osebam dostop do osebnih podatkov, dostop do naprav, na katerih se obdelujejo osebni podatki in njihovih evidenc,
- omogoča poznejše ugotavljanje, kdaj so bili posamezni osebni podatki uporabljeni ali vneseni v evidenco in kdo je to storil in sicer za obdobje, ko je mogoče zakonsko varstvo pravice posameznika zaradi nedopustnega posredovanja osebnih podatkov,
- preprečuje nepooblaščen dostop do varovanih podatkov pri njihovem prenosu, vključno s prenosom po telekomunikacijskih omrežjih.

Zaposleni in zunanji sodelavci, ki pri svojem delu uporabljajo, obdelujejo ali se seznanjajo z osebnimi podatki, morajo biti seznanjeni z določili tega pravilnika in z zakonodajo s tega področja. Smiselno enako velja za študente, dijake in zunanje pogodbene izvajalce. Zavod lahko zbira, vodi in vzdržuje zbirke osebnih podatkov samo na podlagi Zakona o organizaciji in financiranju vzgoje in izobraževanja, Zakona o vrtcih, Pravilnika o zbiranju in varstvu podatkov s področja predšolske vzgoje in ostalih predpisov, ki urejajo področje vzgoje in izobraževanja ali če je za obdelavo določenih osebnih podatkov podana osebna privolitev staršev oziroma zakonitega zastopnika otroka (v nadaljevanju: starši) oz. če kak drug zakonski predpis to dovoljuje.

2. člen

V tem pravilniku uporabljeni pojmi imajo naslednji pomen:

- Zakon - vsakokrat veljavni zakon, ki v Republiki Sloveniji ureja varstvo osebnih podatkov;

- osebni podatek - je katerikoli podatek, ki se nanaša na posameznika, ne glede na obliko, v kateri je izražen; 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, genetsko, duševno, gospodarsko, kulturno ali družbeno identiteto tega posameznika;
- posameznik - je določena ali določljiva fizična oseba, na katero se nanaša osebni podatek;
- posebne vrste osebnih podatkov - so podatki, ki razkrivajo rasno ali etnično poreklo, politično mnenje, versko ali filozofsko prepričanje ali članstvo v sindikatu, in obdelava genetskih podatkov, biometričnih podatkov za namene edinstvene identifikacije posameznika, podatkov v zvezi z zdravjem ali podatkov v zvezi s posameznikovim spolnim življenjem ali spolno usmerjenostjo;
- zbirka osebnih podatkov - je vsak strukturiran niz podatkov, ki vsebuje vsaj en osebni podatek, ki je dostopen na podlagi meril, ki omogočajo uporabo ali združevanje podatkov, ne glede na to, ali je niz centraliziran, decentraliziran ali razpršen na funkcionalni ali geografski podlagi; strukturiran niz podatkov je niz podatkov, ki je organiziran na takšen način, da določi ali omogoči določljivost posameznika;
- obdelava osebnih podatkov - pomeni kakršnokoli delovanje ali niz delovanj, ki se izvaja v zvezi z osebnimi podatki, ki so avtomatizirano obdelani ali ki so pri ročni obdelavi del zbirke osebnih podatkov ali so namenjeni vključitvi v zbirko osebnih podatkov, zlasti zbiranje, pridobivanje, vpis, urejanje, shranjevanje, prilagajanje ali spreminjanje, priklicanje, vpogled, uporaba, razkritje s prenosom, sporočanje, širjenje ali drugo dajanje na razpolago, razvrstitev ali povezovanje, blokiranje, anonimiziranje, izbris ali uničenje; obdelava je lahko ročna ali avtomatizirana;
- upravljavec osebnih podatkov - je fizična ali pravna oseba ali druga oseba javnega ali zasebnega sektorja, ki sama ali skupaj z drugimi določa namene in sredstva obdelave osebnih podatkov oziroma oseba, določena z zakonom, ki določa tudi namene in sredstva obdelave;
- obdelovalec osebnih podatkov - je fizična ali pravna oseba, javni organ, agencija ali drugo telo, ki obdeluje osebne podatke v imenu upravljavca;
- uporabnik osebnih podatkov - je fizična ali pravna oseba ali druga oseba javnega ali zasebnega sektorja, ki se ji razkrijejo osebni podatki, ne glede na to, ali je tretja oseba ali ne;
- nosilec osebnih podatkov - so vse vrste sredstev, na katerih so zapisani ali posneti podatki (listine, akti, optični ali drugi računalniški mediji, zvočna in slikovna gradiva itd.) ne glede na to, ali so v trenutku pričetka veljavnosti tega pravilnika znani;
- pogodbeni obdelovalec - je fizična ali pravna oseba, ki obdeluje osebne podatke v imenu in na račun upravljavca osebnih podatkov;
- posredovanje osebnih podatkov - je posedovanje ali razkritje osebnih podatkov;
- blokiranje - je takšna označitev osebnih podatkov, da se omeji ali prepreči njihova nadaljnja obdelava;
- anonimiziranje - je takšna sprememba oblike osebnih podatkov, da jih ni mogoče povezati s posameznikom ali je to mogoče le z nesorazmerno velikimi napori, stroški ali porabo časa.

3. člen

Za varovane osebne podatke štejejo tisti podatki o fizični osebi, ki kažejo na lastnosti, stanja ali razmerja posameznika, ne glede na obliko, v kateri so izraženi.

V smislu določbe 1. odstavka tega člena štejejo za osebne podatke o fizični osebi 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
- 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

Varovanje osebnih podatkov zajema pravne, organizacijske in ustrezne logistično-tehnične postopke in ukrepe, 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 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 in kdo je to storil, in sicer za obdobje, za katero se posamezni podatki shranjujejo;
- omogoča posamezniku uresničevanje pravic do popravka, izbrisa, omejitve obdelave, do obveščanja v zvezi s popravkom, izbrisom ali omejitvijo obdelave, do prenosljivosti, do ugovora ter do drugih pravic, ki jih določata GDPR ali Zakon.

Posebne vrste osebnih podatkov morajo biti pri obdelavi posebej označene in zavarovane tako, da se nepooblaščenim osebam onemogoči dostop do njih, razen v primeru izjeme, ki jo določa GDPR ali Zakon.

II. ZBIRANJE OSEBNIH PODATKOV

4. člen

Zavod lahko zbira, obdeluje, shranjuje, posreduje, varuje in uporablja osebne podatke, vsebovane v evidencah, v skladu s predpisi o varstvu osebnih podatkov.

Kadar veljavni predpisi s področja vzgoje in izobraževanja določajo, da se posamezni osebni podatki zbirajo v soglasju s starši, jih lahko zavod zbira samo ob predhodni pridobitvi pisnega soglasja.

5. člen

Za izvajanje predšolske vzgoje, spremljanje dejavnosti in statistične namene zavod vodi naslednje zbirke oz. evidence podatkov:

- Evidenca vpisanih in vključenih otrok
- Evidenca plačil staršev
- Evidenca otrok, ki potrebujejo svetovanje oziroma pomoč
- Evidenca upravičencev do sofinanciranja plačil staršev iz državnega proračuna.

Zavod vodi na podlagi zakona in za namene poslovanja zavoda tudi druge zbirke oz. evidence podatkov, in sicer:

- Evidenca zaposlenih,
- Evidenca o stroških dela,
- Evidenca o izrabi delovnega časa.

Vse evidence zavod vzpostavi na podlagi Zakona oz. predpisa, ki dovoljuje vzpostavitev evidence in v njej zbira izključno tiste podatke za katere predpis določa, da je to dovoljeno. Evidence vodi zavod na način, ki ga določa predpis, podatke iz evidenc pa lahko obdelujejo samo osebe, ki jih za to pooblasti ravnateljica. Podatki se v evidencah hranijo toliko časa, kot to predpis določa. Če predpis roka hrambe ne določa, se podatkov hranijo le toliko časa, kolikor je potrebno za dosego namena, zaradi katerega se podatki sploh zbirajo.

V primeru vzpostavitve nove evidence v skladu s tem pravilnikom, sprememba predmetnega Pravilnika ni potrebna, je pa Zavod dolžan pri vzpostavitvi nove evidence upoštevati Zakon in vse predpise, ki se nanašajo na varstvo osebnih podatkov, kot tudi določbe tega pravilnika, v zvezi z vzpostavitvijo, zbiranjem, obdelavo in hrambo osebnih podatkov v evidenci.

III. ODGOVORNOST ZA VAROVANJE OSEBNIH PODATKOV

6. člen

Osebnne podatke, ki jih zbira zavod lahko obdelujejo samo delavci, ki jih za to pooblasti ravnateljica.

Nadzor nad izvajanjem postopkov in ukrepov, določenih v tem pravilniku, opravlja ravnateljica.

Delavci, ki so pooblaščen za obdelovanje osebnih podatkov, so dolžni:

- poskrbeti, da se pri zbiranju, uporabi, spreminjanju, prenosu, shranjevanju in uničenju osebnih podatkov ne more z osebnimi podatki seznaniti nepooblaščen oseba,
- po končani izdelavi dokumentov z osebnimi podatki uničiti pomožno gradivo, ki je nastalo pri izdelavi dokumenta,
- v primeru nepravilne, zlonamerne in nepooblaščen uporabe, prilaščanja, odstopanja, prikrivanja, spreminjanja ali poškodovanja osebnih podatkov iz zbirk podatkov oziroma o poskusu takšnega ravnanja takoj obvestiti ravnateljico,
- zaklepati pisalne mize, omare, blagajne in prostore, v katerih hranijo osebnne podatke, kadar zapuščajo delovne prostore med delovnim časom in po končanem delovnem času.

7. člen

Vsak, ki obdeluje osebne podatke, s katerimi se seznani pri opravljanju svojega dela, je dolžan izvajati predpisane postopke in ukrepe, določene v tem pravilniku.

Obveznost varovanja osebnih podatkov, s katerimi se zaposleni seznani pri svojem delu, velja za čas trajanja delovnega razmerja in tudi po prenehanju delovnega razmerja v zavodu.

Pred nastopom dela na delovnem mestu, kjer se zbirajo, urejajo obdelujejo, spreminjajo, shranjujejo, posredujejo ali uporabljajo osebni podatki ali nosilci osebnih podatkov, mora zaposleni podpisati izjavo, ki ga zavezuje k varovanju osebnih podatkov. Iz izjave mora biti razvidno, da je podpisnik seznanjen z določbami tega pravilnika ter določbami veljavnega Zakona in drugih predpisov, ki se nanašajo na varovanje osebnih podatkov.

8. člen

Za kršitev določil iz prejšnjega člena so zaposleni odgovorni na podlagi določil zakona, ki ureja delovna razmerja, ostali pa na temelju pogodbenih obveznosti.

IV. SPLOŠNI VARNOSTNI UKREPI

9. člen

Za zagotovitev varovanja zaupnih in osebnih podatkov morajo delavci zavoda in ostali pogodbeni ali zunanji sodelavci izvajati naslednje splošne varovalne ukrepe:

- Zakleniti pisalne mize, omare, blagajne in prostore, v katerih se hranijo varovani podatki, ob vsaki zapustitvi prostora;
- Uničiti pomožno gradivo, ki so ga uporabili oziroma katero je nastalo pri izdelavi dokumenta z varovanimi podatki;
- Dosledno izvajati postopek prijave oziroma odjave s svojim osebnim geslom na začetku oziroma ob zaključku dostopa do varovanih podatkov, ki se obdelujejo s pomočjo aplikativne programske opreme;
- Hraniti navodilo za uporabo računalniških evidenc tako, da ni dostopno nepooblaščenim osebam;
- Takoj obvestiti pooblaščenega računalničarja ali vodstvo zavoda o vsaki opaženi nepooblaščen uporabi varovanih podatkov, prilaščanju, spreminjanju ali poškodovanju in v okviru svojih zmožnosti takšno dejanje tudi preprečiti;
- V evidenčno knjigo oziroma v druge nosilce osebnih podatkov vpisati, kdaj so bili posamezni osebni podatki uporabljeni ali vneseni v zbirko podatkov in kdo je to storil;
- Shraniti pečat zavoda, papir z že natisnjenimi podatki zavoda in druge predmete, s katerimi bi bilo mogoče ponarediti dokumente, v zaklenjenih omarah oziroma predalih in z njimi ravnati kot z zaupnim gradivom;
- Ves čas ravnati v skladu z veljavnimi predpisi s področja varstva osebnih podatkov in v skladu s tem pravilnikom.

V. VAROVANJE PROSTOROV IN RAČUNALNIŠKE OPREME

10. člen

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

Dostop v varovane prostore je mogoč in dopusten le v delovnem času, izven delovnega časa pa le na podlagi dovoljenja ravnateljice.

Ključke prostorov in omar, v katerih so shranjeni varovani podatki in nosilci varovanih podatkov ter kjer je shranjena dokumentacija z osebnimi podatki izven rednega delovnega časa hranijo pooblaščen delavci vrta. Delavci, ki hranijo ključke so odgovorni ravnateljici. Ključki zavarovanih prostorov in omar morajo biti označeni in hranjeni ločeno od ključev za ostale prostore. Posebej se označijo in hranijo tudi rezervni ključki.

Delavec odgovoren za vzdrževanje prostorov mora poskrbeti za takojšnjo menjavo ključavnice, če se za določen prostor, v katerem so shranjeni varovani podatki, izgubi eden od ključev za vrata tega prostora.

Delavci, katerim so izročeni ključki posameznih prostorov in/ali od vhodnih vrat zavoda, morajo ob vsaki daljši odsotnosti, kot je letni dopust, odsotnost zaradi bolezni, izobraževanje ipd. ključke izročiti ravnateljici ali z njene strani pooblaščenim osebam.

Nosilci osebnih podatkov, hranjeni izven aktivnih delovnih prostorov oziroma izven varovanih prostorov (hodniki, skupni prostori, aktivni arhivi, ipd.), morajo biti stalno zaklenjeni v ognjevarni in protivlomno zaščiteni omari.

11. člen

Varovani prostori, v katerih se nahajajo nosilci podatkov, ki vsebujejo posebne vrste osebnih podatkov, morajo biti varovani tako, da je zagotovljen popoln nadzor nad delom in gibanjem v teh prostorih.

Prostori, v katere imajo vstop obiskovalci, poslovni partnerji, druge osebe, ki niso zaposlene v zavodu, ali nepooblaščen osebe morajo biti pod stalnim nadzorom zaposlenih. Nosilci podatkov in računalniški prikazovalniki morajo biti v teh prostorih v času obdelave nameščeni tako, da je strankam onemogočen vpogled vanje. Ob vsakršni odsotnosti iz teh prostorov morajo zaposleni prostore zakleniti, pri čemer se ključki prostorov ne smejo puščati v ključavnici v vratih ali na drugih vidnih mestih.

Zaposleni, ki pri svojem delu uporablja osebne podatke ali jih kakorkoli obdeluje, ne sme med delovnim časom puščati nosilcev osebnih podatkov na pisalnih mizah ali drugih vidnih mestih ali jih kakorkoli drugače izpostavljati nevarnosti odtujitve, kopiranja ali vpogleda vanje nepooblaščenim osebam, tudi nepooblaščenim sodelavcem.

V varovanih prostorih morajo biti izven delovnega časa omare in pisalne mize, v katerih so shranjeni osebni podatki, in drugi nosilci osebnih podatkov, zaklenjene, računalniki in druga strojna oprema pa izklopljeni in fizično ali programsko zaklenjeni.

Omare, mize in drugo pohištvo z nosilci podatkov, ki vsebujejo osebne podatke, ki se nahajajo izven varovanih prostorov (hodniki, skupni prostori) morajo biti stalno zaklenjeni.

Osebe, ki niso zaposlene pri upravljavcu osebnih podatkov (npr. vzdrževalci prostorov, strojne in programske opreme, obiskovalci, poslovni partnerji), se smejo gibati v varovanih prostorih samo z vednostjo zaposlenega, ki nadzoruje varovani prostor, kjer se oseba giba.

12. člen

Nosilci podatkov, ki vsebujejo posebne vrste osebnih podatkov, se ne smejo hraniti izven varovanih prostorov.

Nosilce podatkov, ki vsebujejo osebne podatke, lahko zaposleni pri upravljavcu osebnih podatkov odnašajo izven prostorov upravljavca osebnih podatkov samo z dovoljenjem ravnateljice oziroma s strani ravnateljice pooblaščen osebe.

Nosilcev podatkov, ki vsebujejo posebne vrste osebnih podatkov, zaposleni pri upravljavcu ne smejo odnašati izven prostorov upravljavca osebnih podatkov, razen izjemoma z dovoljenjem ravnateljice oziroma s strani ravnateljice pooblaščen osebe, če je to nujno potrebno za reševanje zadeve, ki vsebuje te posebne vrste osebnih podatkov.

Zaposleni ne smejo uporabljati zasebnih nosilcev podatkov ali druge zasebne strojne opreme, ne da bi pred tem pridobili soglasje ravnateljice ali s strani ravnateljice pooblaščen osebe, zadolžene za delovanje informacijskega sistema.

13. člen

Vzdrževanje in popravilo strojne računalniške in druge opreme, ne glede na to, ali se s takšno opremo obdelujejo osebni podatki, je dovoljeno samo z vednostjo in odobritvijo pooblaščen osebe, zadolžene za delovanje informacijskega sistema, izvajajo pa ga lahko samo pooblaščen servisi in njihovi vzdrževalci, ki imajo z zavodom sklenjeno ustrezno pogodbo.

Vzdrževalna dela se praviloma opravljajo na samem mestu, kjer se oprema nahaja. V primeru, da je potrebno popravilo računalnika izven zavoda in brez kontrole pooblaščen osebe, zadolžene za delovanje informacijskega sistema, se morajo nosilci podatkov odstraniti in varno hraniti oziroma z diska računalnika izbrisati na način, ki onemogoča restavriranje. Če to ni mogoče, se mora popravilo opraviti v poslovnih prostorih zavoda v prisotnosti pooblaščen osebe, zadolžene za delovanje informacijskega sistema.

14. člen

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

Ravnateljica lahko dovoli iznos nosilcev osebnih podatkov iz zavoda le izjemoma in pod pogojem, da zaposleni ravna v skladu z določbami GDPR, Zakona in tega pravilnika.

15. člen

Za potrebe restavriranja računalniškega sistema ob okvarah ali ob drugih izjemnih situacijah se zagotavlja redna izdelava kopij vsebine mrežnega strežnika in lokalnih postaj, če se osebni podatki tam hranijo.

Te kopije se hranijo v zaklenjeni omari, ki je ognjevarna, zavarovana proti poplavam in elektromagnetnim motnjam, vse v skladu s predpisanimi klimatskimi razmerami.

VI. VAROVANJE SISTEMSKE IN APLIKATIVNE RAČUNALNIŠKE OPREME TER PODATKOV, KI SE OBDELUJEJO Z RAČUNALNIŠKO OPREMO

16. člen

Dostop do računalniške programske opreme mora biti varovan na način, da omogoča dostop samo zaposlenim, ki so pooblaščen in delavcem, ki v skladu s pogodbo opravljajo dogovorjene storitve.

17. člen

Popravljanje, spreminjanje in dopolnjevanje systemske in aplikativne programske opreme je dovoljeno samo na podlagi odobritve pooblaščen osebe, zadolžene za delovanje informacijskega sistema, izvajajo pa ga lahko samo pooblaščen servis in organizacije in posamezniki, ki imajo z zavodom sklenjeno ustrezno pogodbo.

Izvajalci morajo spremembe in dopolnitve systemske in aplikativne programske opreme ustrezno dokumentirati.

18. člen

Za shranjevanje in varovanje aplikativne programske opreme veljajo enaka določila kot za ostale podatke iz tega pravilnika.

Zaposleni, pooblaščen za obdelavo osebnih podatkov na računalniku, mora skrbeti, da se v primeru servisiranja, popravila, spreminjanja ali dopolnjevanja systemske ali aplikativne programske opreme (v nadaljevanju: vzdrževanje računalnika) ob morebitnem kopiranju osebnih podatkov, po prenehanju potrebe po kopiji, kopija uniči.

19. člen

Vsebina diskov mrežnega strežnika in lokalnih delovnih postaj, kjer se nahajajo osebni podatki, se redno preverja glede prisotnosti računalniških virusov.

Ob pojavu računalniškega virusa je potrebno storiti vse, da se virus čim prej odpravi in da se ugotovi vzrok pojava virusa.

Vsi osebni podatki in programska oprema, ki so namenjeni uporabi v računalniškem informacijskem sistemu zavoda, in prispejo v zavod na medijih za prenos računalniških

podatkov ali prek telekomunikacijskih kanalov, morajo biti pred uporabo preverjeni glede prisotnosti računalniških virusov.

20. člen

Zaposleni ne smejo inštalirati kakršnekoli programske opreme, brez vednosti osebe, ki je zadolžena za delovanje informacijskega sistema.

Zaposleni smejo odnašati programsko opremo iz prostorov zavoda samo z vednostjo zgoraj navedene osebe in z odobritvijo ravnateljice.

21. člen

Pristop do podatkov prek aplikativne programske opreme mora biti varovan s sistemom gesel za avtorizacijo in identifikacijo uporabnikov programov in podatkov. Sistem gesel mora omogočati tudi možnost naknadnega ugotavljanja, kdaj so bili posamezni osebni podatki vneseni v zbirko podatkov, uporabljeni ali drugače obdelani ter kdo je to storil.

Oseba, zadolžena za delovanje računalniškega informacijskega sistema (informatik), zaposlenemu, ki pri delu uporablja delovno postajo, ob sklenitvi delovnega razmerja pripravi in preda lokalno delovno postajo.

Vsakemu uporabniku informatik dodeli unikatno uporabniško ime, ki ga lahko uporablja samo lastnik. Posojanje uporabniškega imena ni dovoljeno. Prav tako ni dovoljena uporaba skupinskih uporabniških imen. Uporabniške pravice morajo biti skladne z nalogami in deli, ki jih opravlja posamezni zaposleni.

Informatik je zadolžen za varnostno kopiranje podatkov v informacijskem sistemu zavoda.

Zaposleni, ki pri delu uporabljajo delovne postaje morajo uporabljati gesla, ki so sestavljena iz kombinacije najmanj 8 črk, števil ali posebnih znakov. Geslo ne sme vsebovati besed, ki imajo posebno povezavo s posameznikom (kot so npr. posameznikovo ali partnerjevo ime, ime hišnega ljubljence, rojstni datumi in podobno) ter delov ali celote uporabniškega imena.

Informatik daje zaposlenim pomoč pri izbiri in spreminjanju gesel.

Zaposleni morajo delovne postaje ob izhodu iz pisarne zaradi preprečitve dostopa nepooblaščenih oseb zakleniti (politika čistega zaslona) s pomočjo tipke WIN+L. Informatik na delovne postaje namesti samodejno zaklepanje zaslona po 10 minutah neaktivnosti. Vstop v računalnik po zaklepanju je možen samo z vnosom gesla. Ob koncu delovnega dne morajo zaposleni fizično ugasniti svoje delovne postaje.

Ob prekinitvi delovnega razmerja se zaposlenemu ukinejo vse dostopne pravice v informacijskem okolju. Zaposlenemu mora biti dana možnost, da lahko pred prekinitvijo delovnega razmerja s službenih sredstev, ki so mu bila dodeljena v uporabo, pobriše ali skopira osebne podatke in zasebno korespondenco, ki je nastala ob uporabi službenih sredstev v izključno osebne namene.

22. člen

Vsa gesla in postopki, ki se uporabljajo za vstop in administriranje mreže osebnih računalnikov (supervisorska gesla), administriranje elektronske pošte in administriranje aplikativnih programov, se hranijo v zapečatenih ovojnica in se jih varuje pred dostopom nepooblaščenih oseb. Uporabi se jih samo v izrednih okoliščinah oziroma ob nujnih primerih. Vsaka uporaba vsebine zapečatenih ovojnic se dokumentira. Po vsaki takšni uporabi se določi nova vsebina gesel. Zaposleni na svojih delovnih postajah ne smejo imeti administratorskih pravic.

VII. STORITVE ZUNANJIH PRAVNIH ALI FIZIČNIH OSEB (ZUNANJI IZVAJALCI)

23. člen

Z vsako fizično ali pravno osebo, ki kot zunanji izvajalec opravlja posamezna opravila v zvezi z obdelovanjem osebnih podatkov, in je registrirana za opravljanje takšne dejavnosti (pogodbeni obdelovalec), se sklene pogodba v pisni obliki.

S pogodbo se določi vsebina in trajanje obdelave, narava in namen obdelave, vrsta osebnih podatkov, kategorije posameznikov, na katere se nanašajo osebni podatki, ter obveznosti in pravice upravljalca kot to izhaja iz Uredbe in Zakona. V takšni pogodbi morajo biti obvezno določeni tudi postopki in ukrepi za zagotovitev varstva osebnih podatkov, kot jih zahtevata GDPR in Zakon.

Obdelovalec brez predhodnega posebnega ali splošnega pisnega dovoljenja upravljalca v obdelavo ne sme vključiti drugih obdelovalcev, pri čemer upravljalec posebej presodi, ali lahko vključitev dodatnega obdelovalca vpliva na tveganost obdelave osebnih podatkov.

Zgoraj navedeno pogodbo je treba skleniti tudi z zunanjimi izvajalci, ki izdelujejo, nadgrajujejo, instalirajo ali vzdržujejo strojno ali programsko računalniško opremo.

24. člen

Zunanji izvajalci smejo opravljati storitve obdelave osebnih podatkov samo v okviru naročnikovih pooblastil. Podatkov ne smejo uporabljati ali obdelovati za noben drug namen.

25. člen

Zunanji izvajalci morajo imeti vsaj enako strog način varovanja osebnih podatkov, kot je določen v tem pravilniku.

Obdelovalec je dolžan voditi evidenco dejavnosti obdelav v skladu s 30. členom Splošne uredbe o varstvu podatkov.

VIII. SPREJEM IN POSREDOVANJE OSEBNIH PODATKOV

26. člen

Zaposleni, ki je zadolžen za sprejem in evidenco pošte, mora izročiti poštno pošiljko z osebni podatki neposredno posamezniku, na katerega je pošiljka naslovljena ali mu jo poslati priporočeno s povratnico ali po kurirju z oznako »zaupno« na kuverti.

Zaposleni, ki je zadolžen za sprejem in evidenco pošte, odpira in pregleduje vse poštno pošiljke in pošiljke, ki na drug način prispejo v zavod (prinesejo kurirji, stranke), razen pošiljk iz naslednjega odstavka.

Zaposleni, ki je zadolžen za sprejem in evidenco pošte, ne sme:

- odpirati pošiljk, ki so naslovljene na drug organ, organizacijo ali družbo in so pomotoma dostavljene;
- odpirati pošiljk, naslovljenih na zaposlenega, na katerih je na ovojnici navedeno, da se vročijo osebno naslovniku;
- odpirati pošiljk, na katerih je najprej navedeno osebno ime zaposlenega brez označbe njegovega naziva v zavodu in šele nato naslov zavoda;
- odpirati pošiljk, ki so naslovljene na neznano osebo, organ ali drugo entiteto, ki naj bi obstajala v zavodu;

27. člen

Prenašanje osebnih podatkov s telekomunikacijskimi sredstvi, z elektronsko pošto ali drugimi računalniškimi mediji izven prostorov zavoda mora biti zavarovano s postopki in ukrepi na način, ki nepooblaščenim preprečuje prilaščanje, uničenje ali neupravičeno seznanjanje z njihovo vsebino.

Prenos osebnih podatkov po elektronski pošti mora biti zavarovan z geslom za identifikacijo.

Pri vsebini zbirk podatkov, ki se prenašajo s telekomunikacijskimi sredstvi, z elektronsko pošto ali fizično na računalniških medijih izven prostorov zavoda, se med prenosom poskrbi za nečitljivost vsebine z ustreznimi standardnimi kriptografskimi metodami.

28. člen

Osebni podatki se pošiljajo priporočeno.

Ovojnica, v kateri se posredujejo osebni podatki, mora biti izdelana na takšen način, da je ob normalni svetlobi ali pri osvetlitvi ovojnice z običajno lučjo onemogočena čitljivost vsebine. Prav tako mora ovojnica zagotoviti, da odprta ovojnice in seznanitve z njeno vsebino ni mogoče opraviti brez vidne sledi odpiranja.

Občutljivi osebni podatki se pošiljajo naslovniku v zaprtih ovojnicah proti podpisu v knjigi evidenc ali z vročilnico ter z navedbo v knjigi evidenc.

29. člen

Osební podatki se posredujejo samo tistim uporabnikom, ki izkažejo ustrezno zakonsko podlago za pridobitev podatkov ali s pisno privolitvijo oziroma zahtevo posameznika, na katerega se ti podatki nanašajo.

Za vsako posredovanje osebnih podatkov mora upravičenec vložiti pisno vlogo z navedbo zakonske podlage za pridobitev podatkov ali pa mora biti k vlogi priložena pisna zahteva ali privolitev posameznika, na katerega se osebni podatki nanašajo. Podatki se morajo vlagatelju posredovati v čim krajšem roku.

Dejstva o posredovanih osebnih podatkih se morajo v treh dneh od dneva posredovanja sporočiti osebi, o kateri so bili posredovani podatki. Na zahtevo te osebe mora zaposleni, ki je osebne podatke posredoval, izročiti osebi seznam subjektov, katerim so bili v določenem obdobju posredovani podatki, ki so vsebovani v zbirki podatkov zavoda, in se nanašajo nanj.

Vsako posredovanje osebnih podatkov iz zbirk osebnih podatkov drugim upravičencem se vpiše v knjigo evidenc z navedbo, kateri podatki so bili posredovani, komu, kdaj in na kakšni podlagi.

Nikoli se ne posredujejo originali dokumentov, razen v primeru pisne odredbe sodišča. Originalni dokument se mora v času odsotnosti nadomestiti s kopijo.

O vlogah, privolitvah in zahtevah mora biti ravnateljica seznanjena.

IX. BRISANJE OSEBNIH PODATKOV

30. člen

Osebni podatki se vodijo v zbirki osebnih podatkov le toliko časa, kolikor je potrebno, da se doseže namen, za katerega se zbirajo in vodijo. Roki, po katerih se osebni podatki izbrišejo iz zbirke podatkov, so razvidni iz kataloga zbirke osebnih podatkov.

Po preteku roka hranjenja se osebni podatki zbršejo, uničijo, blokirajo ali anonimizirajo, razen če GDPR ali Zakon ali drug akt ne določa drugače.

31. člen

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

Osebni podatki, vsebovani na klasičnih nosilcih (listine, kartoteke, registri, sezname, spisi, itd.) se uničijo na način, ki onemogoča restavriranje vseh ali določenih delov brisanih podatkov. Nosilci se fizično uničijo (pokurijo, razrežejo) v prostorih zavoda ali pod nadzorom pooblaščenega delavca zavoda pri organizaciji, ki se ukvarja z uničevanjem zaupne dokumentacije.

Na enak način se uničijo ali brišejo podatki v pomožni dokumentaciji v računalniški ali papirnati obliki (matrice, skice, pomožni izračuni, delovno gradivo, osnutki ipd.).

Prepovedano je odmetavanje nosilcev osebnih podatkov v koše za smeti, ne glede na to, kje se koš nahaja.

32. člen

Uničevanje in brisanje osebnih podatkov se opravi komisijsko, v sestavi najmanj dveh oseb, ki ju določi ravnateljica. Člana oz. člani komisije so osebe, ki so vredne zaupanja.

Komisija o vsakem uničenju in/ali brisanju sestavi zapisnik, ki ga podpišejo vsi člani.

Komisija prisostvuje tudi pri prenosu nosilcev osebnih podatkov na mesto uničenja oziroma brisanja.

Uničevanje osebnih podatkov na nosilcih iz predhodnega odstavka se mora izvajati tekoče in ažurno.

X. UKREPANJE V PRIMERU ZLORAB ALI SUMA O ZLORABI

33. člen

Zaposleni so dolžni izvajati ukrepe za preprečevanje zlorab osebnih podatkov.

Zaposleni 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.

Zaposleni, ki izve ali opazi, da je prišlo do zlorabe osebnih podatkov (odkrivanje osebnih podatkov, nepooblaščen uničenje, nepooblaščen spreminjanje, poškodovanje zbirke, prilaščanje osebnih podatkov ipd.) ali do vdora v zbirko osebnih podatkov, mora takoj o tem obvestiti ravnateljico ali neposrednega vodjo.

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.

34. člen

Ravnateljica mora zoper tistega, ki je zlorabil osebne podatke ali je nepooblaščen vdrl v zbirko osebnih podatkov, ustrezno ukrepati.

Če obstaja sum, da je zaposleni vdrl v zbirko osebnih z naklepom in namenom zlorabiti te podatke ali uporabiti v nasprotju z nameni, za katere so zbrani, ali če je do zlorabe osebnih podatkov že prišlo, mora ravnateljica ali od nje pooblaščen oseba (v nadaljevanju ravnateljica) poleg ukrepov na podlagi Zakona o delovnih razmerjih, vdor ali zlorabo oziroma poskus zlorabe prijaviti organom pregona.

O zlorabi ali sumu zlorabe osebnih podatkov ali o vdoru ali poskusu vdora v zbirko osebnih podatkov osebe, se takšna zloraba prijavijo organom pregona.

Kadar zavod nastopa kot upravljavec osebnih podatkov je ravnateljica v primeru kršitve varstva osebnih podatkov brez nepotrebnega odlašanja, po možnosti pa najpozneje v 72 urah po seznaitvi s kršitvijo, dolžna o kršitvi uradno obvestiti Informacijskega pooblaščenca. Tega ni dolžna storiti, če ni verjetno, da bi bile s kršitvijo varstva osebnih podatkov ogrožene pravice in svoboščine posameznikov. Kadar uradno obvestilo Informacijskemu pooblaščenču ni podano v 72 urah, se mu priloži navedbo razlogov za zamudo.

Obdelovalec po seznaitvi s kršitvijo varstva osebnih podatkov brez nepotrebnega odlašanja uradno obvesti upravljavca, pri čemer mu posreduje:

- opis vrste kršitve in po možnosti približno število prizadetih posameznikov ter vrsto in število prizadetih evidenc osebnih podatkov;
- ime in kontaktne podatke pooblaščenih oseb za varstvo podatkov v zavodu ali drugo kontaktno točko, pri kateri je mogoče pridobiti več informacij;
- opis verjetnih posledic kršitve varstva osebnih podatkov;
- opis ukrepov, sprejetih za obravnavanje kršitve ter za ublažitev morebitnih škodljivih učinkov kršitve.

Kadar in kolikor informacij ni mogoče zagotoviti istočasno, se informacije lahko zagotovijo postopoma brez nepotrebnega dodatnega odlašanja.

Upravljavec dokumentira vsako kršitev varstva osebnih podatkov, vključno z dejstvi v zvezi s kršitvijo varstva osebnih podatkov, njene učinke in sprejete popravne ukrepe.

35. člen

Kadar je verjetno, da kršitev varstva osebnih podatkov povzroči veliko tveganje za pravice in svoboščine posameznikov, ravnateljica, če zavod nastopa kot upravljavec, brez nepotrebnega odlašanja sporoči posamezniku, da je prišlo do kršitve varstva osebnih podatkov.

Sporočilo posamezniku iz tega člena ni potrebno, če so za to izpolnjeni pogoji iz GDPR

XI. PRAVICE POSAMEZNIKA

36. člen

Pravica do popravka je pravica posameznika, da upravljavec brez nepotrebnega odlašanja popravi netočne osebne podatke v zvezi z njim in da upravljavec dopolni nepopolne osebne podatke, ki se nanašajo nanj.

Pravica do izbrisa je pravica, s katero ima posameznik pravico doseči, da upravljavec brez nepotrebnega odlašanja izbriše osebne podatke v zvezi z njim, upravljavec pa ima obveznost osebne podatke brez nepotrebnega odlašanja izbrisati. Upravljavec ima pravico zavrniti izbris, če tako izhaja iz določb GDPR ali Zakona.

Pravica do omejitve obdelave je pravica posameznika, da upravljavec omeji obdelavo v primeru (i) netočnosti podatkov, (ii) nezakonite obdelave, če posameznik nasprotuje izbrisu osebnih podatkov, (iii) če upravljavec podatkov ne potrebuje več za namene obdelave posameznik pa jih potrebuje zaradi pravnih zahtevkov, (iv) če je posameznik vložil ugovor za

obdelavo osebnih podatkov, in sicer za čas odločitve o ugovoru, ali iz drugih razlogov kot določata GDPR in Zakon.

Pravica do obveščanja v zvezi s popravkom, izbrisom ali omejitvijo obdelave je pravica posameznika, da ga upravljavec na njegovo zahtevo obvesti o vseh uporabnikih, katerim so bili razkriti njegovi osebni podatki, sporočeni popravki, izbrisi ali omejitve obdelave.

Pravica do prenosljivosti je pravica posameznika, da od upravljavca prejme osebne podatke v zvezi z njim v strukturirani, splošno uporabljani in strojno berljivi obliki, ter pravico, da te podatke posreduje drugemu upravljavcu, če obdelava temelji na soglasju posameznika, če je obdelava potrebna za izvajanje pogodbe, katere pogodbeni stranka je tudi posameznik ali če gre za obdelavo posebnih vrst osebnih podatkov.

Pravica do ugovora je pravica posameznika, da kadar koli ugovarja obdelavi osebnih podatkov v zvezi z njim, ki temelji na obdelavi potrebni za opravljanje nalog v javnem interesu ali pri izvajanju javne oblasti, dodeljene upravljavcu ali če je obdelava potrebna zaradi zakonitih interesov, vključno z oblikovanjem profilov na podlagi teh določb. Kadar se osebni podatki obdelujejo za namene neposrednega trženja, ima posameznik, pravico, da kadar koli ugovarja obdelavi osebnih podatkov v zvezi z njim za namene takega trženja, vključno z oblikovanjem profilov, kolikor je povezano s takim neposrednim trženjem

Posameznik ni dolžan določiti ali poimenovati, katero pravico uresničuje. Posameznik je upravičen do vseh pravic na podlagi GDPR, Zakona in druge zakonodaje, ne glede na to, ali so pravice opredeljene v tem pravilniku.

37. člen

Če zaposleni prejme zahtevo posameznika, s katero ta uveljavlja katero od pravic iz prvega odstavka tega člena ali uveljavlja katerokoli drugo zahtevo iz naslova pravic varstva osebnih podatkov, mora o tem še isti delovni dan o tem pisno obvestiti ravnateljico ter ravnati skladno z njegovimi navodili. Zaposleni, ki prejme zahtevo posameznika ne sme sam reševati zahteve posameznika, niti posredovati posamezniku kakršnekoli informacije v zvezi s tem, razen kontaktnih podatkov ravnateljice, na katero se lahko posameznik vedno neposredno obrne.

Ravnateljica je dolžna pravočasno odgovoriti na poziv posameznika, ki se nanaša na uveljavljanje njegovih pravic v zvezi z varstvom osebnih podatkov ter pripraviti vse potrebno za uveljavitev pravice posameznika, če je ta utemeljena. Ravnateljica lahko za uveljavitev pravic posameznikom zaposlenim daje navodila, vendar z vednostjo zaposlenemu neposredno nadrejenega.

X. ODGOVORNI (POOBlašČENI) ZAPOSLENI

38. člen

(1) Opis zbirk oz. eviden osebni podatkov, ki se vodijo v zavodu, se vodi v katalogu zbirk oz. evidenc osebnih podatkov, vse v skladu z GDPR ali vsakokrat veljavnim Zakonom (v nadaljevanju: katalog).

(2) Zbirke osebnih podatkov zaposlenih se vzpostavijo ob sklenitvi delovnega razmerja z zaposlenim in se ažurirajo ob vsaki spremembi, ki jo sporoči zaposleni.

(3) Vrste zbirk oz. evidenc osebnih podatkov so določene v skladu z Internim seznamom katalogov zbirk oz. evidenc osebnih podatkov, ki je priloga tega pravilnika. Interni seznam sprejme ravnateljica.

(4) Pooblaščen osebo, ki vodi katalog, imenuje oziroma pooblasti ravnateljica.

39. člen

(1) Ravnateljica je dolžna voditi ažuren seznam, iz katerega je za vsako zbirko oz. evidenco osebnih podatkov jasno razvidno, katera oseba je odgovorna za posamezno zbirko oz. evidenco ter katere osebe lahko zaradi narave svojega dela obdelujejo osebne podatke, ki se nanašajo na posamezno zbirko oz. evidenco osebnih podatkov.

(2) Pooblaščen oseba, ki vodi katalog, je odgovorna tudi za hrambo zbirk oz. evidenc osebnih podatkov.

40. člen

Ravnateljica je pooblaščen za potrebe svojega dela obdelovati osebne podatke, vsebovane v vseh zbirkah osebnih podatkov vodenih v zavodu.

41. člen

(1) Za vzpostavitev in vodenje zbirke osebnih podatkov ali osebnega podatka, ki jo ali ga želi zavod voditi, pa vodenje takšne zbirke ali osebnega podatka nima zakonske podlage, mora pridobiti pisno soglasje zaposlenega, katerega podatki se vodijo.

(2) Pisno soglasje zaposlenega mora vsebovati:

- prostovoljno, izrecno, informirano in nedvoumno pisno izjavo zaposlenega, da se strinja z vodenjem ali vzpostavitvijo njegovih osebnih podatkov, in sicer za vsak osebni podatek in namen posebej;
- navedbo osebnih podatkov, ki se vodijo;
- vse namene zbiranja podatkov;
- vse dejavnosti obdelave;
- seznanitev z možnostjo uveljavitve pravice do popravka, izbrisa, omejitve obdelave, do obveščanja v zvezi s popravkom, izbrisom ali omejitvijo obdelave, do prenosljivosti in do ugovora;
- čas vodenja in shranjevanja podatkov;
- datum podpisa soglasja in podpis zaposlenega;
- izrecno soglasje za obdelavo posebnih vrst osebnih podatkov, če je to relevantno.

Zavod mora voditi osebne podatke samo v skladu z namenom, za katere je zbral takšne podatke.

XI. KONČNE DOLOČBE

42. člen

Pravilnik sprejme ravnateljica.

Vse spremembe in dopolnitve tega pravilnika sprejme ravnateljica po postopku in na način kot velja za sprejem pravilnika.

43. člen

Za vprašanja in razmerja, ki niso urejena s tem pravilnikom, se uporabljajo določbe GDPR in veljavnega Zakona.

44. člen

Pravilnik stopi v veljavo 21. 02. 2020.

Priloga tega pravilnika je interni seznam katalogov zbirk osebnih podatkov.

Z dnem uveljavitve tega pravilnika prenehajo veljati določbe Pravilnika o zavarovanju osebnih podatkov z dne 21. 01. 2019.

V Kranju, dne 20. 02. 2020



Ravnateljica
Tea Dolinar