Na podlagi 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 (Splošna uredba o varstvu podatkov, v nadaljevanju: GDPR), in Zakona o varstvu osebnih podatkov (Uradni list RS, v nadaljevanju: ZVOP-2) izdaja predsednica uprave ustanove **Ustanova Zdenke Gustinčič, fundacija za dobro ljudi in narave (v nadaljevanju UZG), Gradnikove brigade 53, Nova Gorica**

PRAVILNIK O VARSTVU OSEBNIH PODATKOV

UVODNE DOLOČBE

1 člen
(Namen in pravna narava pravilnika)

S tem pravilnikom se opredeljujejo tehnični in organizacijski ukrepi, s katerimi ustanova UZG, Gradnikove brigade 53, Nova Gorica (v nadaljnjem besedilu: ustanova) varuje osebne podatke.

Ukrepi iz prejšnjega odstavka se izvajajo z namenom, da:

- so osebni podatki obdelani zakonito, pošteno in na pregleden način;
- so osebni podatki zbrani za določene, izrecne in zakonite namene, in se ne obdelujejo na način, ki ni združljiv s temi nameni;
- se privzeto obdelajo samo osebni podatki, ki so potrebni za vsak poseben namen obdelave; ta obveznost velja za količino zbranih osebnih podatkov, obseg njihove obdelave, obdobje njihove hrambe in njihovo dostopnost;
- se spoštujejo in zaščitijo pravice in svoboščine posameznikov, na katere se nanašajo osebni podatki;
- se zagotovi varnost osebnih podatkov, vključno z zaščito pred nedovoljeno ali nezakonito obdelavo ter pred nenamerno izgubo, uničenjem ali poškodbo;
- lahko ustanova dokaže skladnost z zakonodajo s področja varstva osebnih podatkov.

Ta pravilnik je splošni akt v smislu zakonodaje s področja delovnih razmerij in določa obveznosti, ki jih morajo delavci poznati zaradi izpolnjevanja svojih pogodbenih in drugih obveznosti.

Ta pravilnik velja tudi za osebe, ki v ustanovi ali za ustanovo opravljajo delo na podlagi pogodb, ki niso pogodbe o zaposlitvi, vključno z dijaki in študenti.

Katerakoli od oseb, navedenih v 3. ali 4. odstavku tega člena, je dolžna ob kakršnemkoli dvomu glede pomena določb tega pravilnika poiskati strokovno razlago oziroma pomoč pri predsednici uprave Lilijana Reljič (v nadaljnjem besedilu: predsednik uprave).

2 člen
(Opredelitev pojmov)

V tem pravilniku imajo izrazi »osebni podatek«, »posebne vrste osebnih podatkov«, »zbirka«, »obdelava«, »posameznik«, upravljavec«, »obdelovalec«, »uporabnik«, »tretja oseba« in »privolitev posameznika, na katerega se nanašajo osebni podatki« enak pomen kot v GDPR.

»Nosilec podatkov« pomeni vse vrste sredstev, na katerih so zapisani ali posneti osebni podatki (listine, akti, gradiva, spisi, računalniška oprema, fotokopije, zvočno in slikovno gradivo, itd.).

»Zaposleni« pomeni osebe, ki imajo z ustanovo sklenjeno pogodbo o zaposlitvi, osebe, ki opravljajo delo v ustanovi kot dijaki ali študenti, osebe, ki opravljajo delo v ustanovi na podlagi pogodbe med ustanovo in njihovim delodajalcem, ki opravlja dejavnost zagotavljanja dela drugim delodajalcem, ter osebe, ki opravljajo delo za ustanovo na podlagi pogodb civilnega prava.

»Varnostni incident« pomeni kršitev varnosti, ki povzroči nenamerno ali nezakonito uničenje, izgubo, spremembo, nepooblaščeno razkritje ali dostop do osebnih podatkov, ki so poslani, shranjeni ali kako drugače obdelani.

3 člen
(Evidenca dejavnosti obdelave osebnih podatkov)[1]

Ustanova vodi in vzdržuje evidenco dejavnosti obdelave osebnih podatkov s predpisani sestavinami, skladno z določbo 30. člena GDPR, in sicer za vsako zbirko posebej.

Evidenca dejavnosti obdelave se vodi v papirni obliki, in sicer na upravi UZG.

Za vodenje evidence dejavnosti obdelave je pristojen vsak vodja enote, v okviru katerega se vodi posamezna zbirka, nadzor pa izvaja predsednik uprave.

4 člen
(Obdelava osebnih podatkov, varnost in obveščanje posameznikov)

V ustanovi oziroma za potrebe ustanove (s pomočjo obdelovalcev: računovodstvo) se lahko obdelujejo le tisti osebni podatki, za katere obstaja ustrezna pravna podlaga po določbah GDPR ali druge zakonodaje. Če pravna podlaga za obdelavo ne obstaja, je potrebno osebne podatke takoj prenehati aktivno obdelovati in onemogočiti dostop do njih ter o neobstoju podlage obvestiti predsednika uprave ustanove, ki določi nadaljnje ravnanje s takimi podatki.

Osebni podatki se smejo zbirati samo za določene in zakonite namene ter se ne smejo nadalje obdelovati tako, da bi bila njihova obdelava v neskladju s temi nameni, če zakon ne določa drugače. Kadar namerava ustanova nadalje obdelovati osebne podatke za namen, ki ni namen, za katerega so bili osebni podatki zbrani, je potrebno predhodno preveriti, ali je nov namen združljiv s prvotnim in izdelati o tem pisno poročilo.

Ukrepe za zagotovitev varnosti konkretnih (zbirk) osebnih podatkov, kot so med drugim psevdonimizacija in šifriranje, omejitev roka hrambe in dostopa, omejitev obdelave, omejitev namenov ipd., ter način izvedbe določi predsednik uprave na predlog vodje enote.

Posebne vrste osebnih podatkov se lahko obdelujejo le v skladu z določbami GDPR in druge zakonodaje. Pri obdelavi morajo biti ti podatki posebej označeni in zavarovani tako, da se nepooblaščenim osebam onemogoči dostop do njih.

O obdelavi osebnih podatkov mora biti posameznik obveščen v skladu z določbami 12., 13. in 14. člena GDPR. Za izvedbo obvestil je pristojen vsak vodja enote, v okviru katerega se vodi posamezna zbirka.
Vsak vodja enote, v okviru katerega se vodi posamezna zbirka, je dolžan (za vsako posamezno zbirko) določiti in voditi pisen seznam oseb, ki lahko zaradi narave svojega dela

[1]

in/ali funkcije v ustanovi obdelujejo določene osebne podatke oziroma imajo dostop do zbirk (v nadaljevanju »pooblaščeni obdelovalci«). Vodje enot so dolžni pisne sezname pooblaščenih obdelovalcev posredovati predsedniku uprave ustanove.

Pooblaščeni obdelovalci morajo biti pred obdelavo osebnih podatkov seznanjeni z določbami GDPR ter z vsebino tega pravilnika, o čemer so dolžni podpisati posebno izjavo (dokument - GDPR izjava delavca).

5 člen
(Zagotavljanje in uresničevanje pravic posameznikov)

Posameznik ima pravico od ustanove dobiti potrditev, ali se obdelujejo njegovi osebni podatki, in če se, pravico dobiti dostop do osebnih podatkov (vpogled) in informacije iz 1. odstavka 15. člena GDPR.

Posameznik ima pravico doseči, da ustanova brez nepotrebnega odlašanja popravi netočne oziroma dopolni nepopolne osebne podatke v zvezi z njim.

Posameznik ima pravico doseči, da ustanova brez nepotrebnega odlašanja izbriše osebne podatke v zvezi z njim, kadar velja eden od naslednjih razlogov:

- osebni podatki niso več potrebni v namene, za katere so bili zbrani ali kako drugače obdelani;
- posameznik prekliče privolitev, na podlagi katere poteka obdelava in za obdelavo ne obstaja nobena druga pravna podlaga;
- posameznik obdelavi ugovarja, za njihovo obdelavo pa ne obstajajo nobeni prevladujoči zakoniti razlogi;
- osebni podatki so bili obdelani nezakonito;
- osebne podatke je treba izbrisati za izpolnitev pravne obveznosti zaradi izpolnitve zakonskih obveznosti;
- osebni podatki so bili zbrani v zvezi s ponudbo storitev informacijske ustanove od mladoletnega posameznika.
- Posameznik ima pravico doseči, da ustanova omeji obdelavo, kadar velja en od naslednjih primerov:
- posameznik oporeka točnosti podatkov, in sicer za obdobje, ki ustanovi omogoča preveriti točnost osebnih podatkov;
- je obdelava nezakonita in posameznik nasprotuje izbrisu osebnih podatkov ter namesto tega zahteva omejitev njihove uporabe;
- ustanova osebnih podatkov ne potrebuje več za namene obdelave, temveč jih posameznik potrebuje za uveljavljanje, izvajanje ali obrambo pravnih zahtevkov;
- je posameznik vložil ugovor v zvezi z obdelavo, dokler se ne preveri, ali zakoniti razlogi upravljavca prevladajo nad razlogi posameznika, na katerega se nanašajo osebni podatki.
- Posameznik ima pravico, da prejme osebne podatke ki jih je posredoval ustanovi, v strukturirani, splošno uporabljani in strojno berljivi obliki, in pravico, da te podatke posreduje drugemu upravljavcu, ne da bi ga ustanova pri tem ovirala, kadar:
- obdelava temelji na privolitvi in
- se obdelava izvaja z avtomatiziranimi sredstvi.

Predsednik uprave ustanove je dolžan poskrbeti za to, da so posamezniki na primeren način, ki je skladen z zahtevami GDPR, obveščeni o pravicah iz prejšnjih odstavkov tega člena. Predsednik uprave tudi poskrbi za enotno kontaktno točko, na katero se lahko obrnejo posamezniki pri uveljavljanju svojih pravic.

Za uveljavitev pravic posameznikov in za komunikacijo z njimi je zadolžen vodja enot, v okviru katerega se vodi zbirka, v kateri so osebni podatki posameznika. Če se osebni podatki posameznika nahajajo v več zbirkah, predsednik uprave ustanove določi pristojnega vodjo enot.

6 člen
(Ocena učinka v zvezi z varstvom podatkov)

Vodja enote ali druga oseba, ki to zazna, je dolžna predsednika uprave opozoriti na dejstvo, da bi lahko načrtovana obdelava osebnih podatkov, zlasti (toda ne izključno) z uporabo novih tehnologij, ob upoštevanju narave, obsega, okoliščin in namenov obdelave osebnih podatkov, povzročila veliko tveganje za pravice in svoboščine posameznikov.

V tem primeru predsednik uprave odloči, ali je potrebno izvesti oceno učinka predvidenih dejanj obdelave na varstvo osebnih podatkov. Za samo izvedbo ocene učinka je odgovoren vodja enote, ali druga od predsednika uprave pooblaščena oseba. Vsi zaposleni, ki lahko dajo na razpolago potrebne podatke in ocene, so dolžni sodelovati.

Ocena učinka se izvede v pisni obliki in obsega vsaj:

- sistematičen opis predvidenih dejanj obdelave in namenov obdelave, kadar je ustrezno pa tudi zakonitih interesov, za katere si prizadeva ustanova;
- oceno potrebnosti in sorazmernosti dejanj obdelave glede na njihov namen;
- oceno tveganj za pravice in svoboščine posameznikov, na katere se nanašajo osebni podatki;
- ukrepe za obravnavanje tveganj, vključno z zaščitnimi ukrepi, varnostne ukrepe ter mehanizme za zagotavljanje varstva osebnih podatkov in za dokazovanje skladnosti z GDPR, ob upoštevanju pravic in zakonitih interesov posameznikov, na katere se nanašajo osebni podatki, ter drugih oseb, ki jih to zadeva.

Če vodja enote ali druga oseba, ki je izdelala oceno učinka, ugotovi, da bi predvidena obdelava povzročila veliko tveganje, če ustanova ne bi sprejela ukrepov za ublažitev tveganja, je dolžan o tem obvestiti predsednika uprave ustanove, da presodi, ali je potrebno posvetovanje z nadzornim organom.

UKREPI ZA VAROVANJE OSEBNIH PODATKOV

7 člen
(Varovanje prostorov in nosilcev podatkov)

Prostori, v katerih se nahajajo nosilci podatkov in strojna ter programska oprema (v nadaljnjem besedilu: varovani prostori), so varovani z organizacijskimi ter tehničnimi ukrepi, ki onemogočajo nepooblaščenim osebam dostop do podatkov.

Dostop v varovane prostore je mogoč in dopusten le v delovnem času, izven delovnega časa pa samo na podlagi dovoljenja predsednika uprave. V primeru, da posamezni zaposleni redno opravljajo delo tudi izven delovnega časa, v obliki nadur ali na drug način, lahko ti dostopajo v varovane prostore brez posebnega dovoljenja tudi izven rednega delovnega časa.

Varovani prostori ne smejo ostajati nenadzorovani oziroma jih je treba zaklepati ob odsotnosti zaposlenih, ki jih nadzorujejo.

V varovane prostore ne smejo brez spremstva ali prisotnosti zaposlenega, ki te prostore nadzoruje, vstopati osebe, ki niso zaposlene v ustanovi. Zaposleni, ki dela v varovanih prostorih, mora vestno in skrbno nadzorovati prostor in ga ob zapustitvi zakleniti.

Vzdrževalci, čistilci, varnostniki, serviserji, obiskovalci, poslovni partnerji se smejo zadrževati v varovanih prostorih samo z vednostjo zaposlenih. Izven delovnega časa se lahko delavci, kot so čistilci ali varnostniki, če je to nujno potrebno, gibljejo samo v tistih varovanih prostorih, kjer je onemogočen vpogled v osebne podatke (nosilci podatkov so shranjeni v zaklenjenih omarah in pisalnih mizah, računalniki in druga strojna oprema so izklopljeni ali kako drugače fizično ali programsko zaklenjeni).

Nosilci osebnih podatkov, hranjeni izven aktivnih delovnih prostorov oz. izven varovanih prostorov (hodniki, skupni prostori ipd.), morajo biti stalno zaklenjeni, razen kadar so neposredno v uporabi.

Posebnih vrst osebnih podatkov v nobenem primeru ni dovoljeno hraniti izven varovanih prostorov.

Zaposleni, ki pri svojem delu uporablja osebne podatke ali jih kakorkoli obdeluje, ne sme med delovnim časom nenadzorovano puščati nosilcev osebnih podatkov na pisalni mizi ali jih kako drugače izpostavljati nevarnosti, da bi nepooblaščene osebe dobile vpogled v osebne podatke.

Ključe, kartice, gesla in ostala sredstva, ki omogočajo dostop do varovanih prostorov, je treba varovati, upravljati in hraniti vestno in skrbno. Vsako izgubo ali odtujitev ali sum o zlorabi, mora zaposleni takoj sporočiti predsedniku uprave, ki morata sprejeti ustrezne ukrepe.

Vzdrževanje in popravilo strojne računalniške in druge opreme, s katero se obdelujejo osebni podatki, je dovoljeno samo z vednostjo in odobritvijo vodje enote, ki obdeluje te podatke, ali predsednika uprave, izvajajo pa ga lahko samo pooblaščeni servisi, ki imajo z ustanovo sklenjeno pogodbo o servisiranju te opreme, ki vključuje ustrezne določbe o pogodbeni obdelavi osebnih podatkov.

8 člen
(Obdelava osebnih podatkov)

Obdelava osebnih podatkov je dovoljena le v prostorih ustanove. Izjemoma je v primerih kadar delavec dela na domu ali ob uporabi tehnologije dostopa na daljavo dovoljena obdelava osebnih podatkov izven ustanove, pri tem pa morajo biti zagotovljeni vsi potrebni ukrepi za zavarovanje osebnih podatkov, ki jih v posameznih (izjemnih) primerih pisno dogovorijo z predsednikom uprave.

Predsednik uprave ali vodja enote dovoli iznos nosilcev osebnih podatkov iz ustanove, pri čemer je potrebno zabeležiti razlog za iznos nosilcev iz ustanove. Za več iznosov oziroma za ponavljajoče iznašanje se lahko da eno dovoljenje.

Posredovanje osebnih podatkov uporabnikom dovoli predsednik uprave ustanove. Posredovanje osebnih podatkov iz prejšnjega odstavka tega člena se ustrezno evidentira na Upravi ustanove.

VAROVANJE PROGRAMSKE OPREME ZA OBDELAVO OSEBNIH PODATKOV

9 člen
(Splošno)

Dostop do programske opreme, s katero ali s pomočjo katere se obdelujejo osebni podatki, mora biti varovan na način, ki dovoljuje dostop samo za to vnaprej določenim zaposlenim in osebam, ki za ustanovo po pogodbi opravljajo servisiranje ali vzdrževanje strojne ali programske opreme, pri čemer si zaposleni med seboj ali s tretjimi osebami ne smejo izmenjevati ali razkrivati podatkov za dostop (ne glede na nivo pravic, ki jim je dodeljen).

Za dodeljevanje dostopa do programske opreme za zaposlene in vodenje evidence o tem je pristojen vodja enote ali predsednik uprave.

Popravljanje, spreminjanje in dopolnjevanje (posodabljanje) programske opreme oziroma sestava navodil v zvezi s tem so v pristojnosti predsednika uprave.

Zaposleni ne smejo brez odobritve predsednika uprave na strojno opremo in druge naprave, ki so v lasti ali uporabi ustanove, namestiti nobene programske opreme.

Popravljanje, spreminjanje in dopolnjevanje (posodabljanje) programske opreme s strani zunanjih izvajalcev je dovoljeno samo na podlagi odobritve predsednika uprave, izvajajo pa ga lahko samo pooblaščeni servisi in organizacije in posamezniki, ki imajo z ustanovo sklenjeno pogodbo, ki vključuje ustrezne določbe o pogodbeni obdelavi osebnih podatkov.

Vse spremembe in dopolnitve programske opreme, je potrebno dokumentirati na način, ki omogoča sledljivost sprememb ali dopolnitev.

Zaposleni, ki v okviru svojih delovnih nalog ustvari ali dovoli ustvariti kopijo (baze) osebnih podatkov za namene servisiranja, popravila, spreminjanja ali dopolnjevanja programske opreme ali za nudenje podpore, je dolžan poskrbeti, da se, ko preneha potreba, kopija učinkovito uniči ali izbriše.

Predsednik uprave ustanove podrobneje določi oziroma predpiše izdelavo kopij (baz) osebnih podatkov, tako da je mogoča restavracija osebnih podatkov v primeru neželenega izbrisa, spremembe ali uničenja osebnih podatkov ali nosilca, na katerem se nahajajo osebni podatki.

10 člen
(Omejevanje in nadzor dostopa do osebnih podatkov)

Dostop do osebnih podatkov preko programske opreme mora biti varovan z enotnim in centraliziranim sistemom gesel ali drugih varnih sredstev za avtorizacijo in identifikacijo uporabnikov. Pri programski opremi mora biti spremljanje dogodkov v posamezni aplikaciji, ki omogoča možnost naknadnega ugotavljanja, kdaj so bili posamezni osebni podatki vneseni v zbirko podatkov, uporabljeni ali drugače obdelovani ter kdo je to storil, in sicer za obdobje 5 let od zadnje obdelave osebnih podatkov.

Za določitev režima sistema oziroma načina dodeljevanja, hranjenja in spreminjanja gesel je pristojen predsednik uprave ustanove.

11 člen
(Hramba podatkov izven baz)

Osebni podatki se lahko zgolj izjemoma, kadar je to glede na naravo dela nujno potrebno, shranjujejo in obdelujejo lokalno (na lokalnih računalnikih in drugih podobnih napravah). Po prenehanju potrebe po takem shranjevanju in obdelavi osebnih podatkov, se morajo osebni podatki prenesti v centralizirane baze podatkov ali pa se trajno izbrisati.

Morebitne kopije vsebin zbirk osebnih podatkov na lokalnih nosilcih (zunanji diski, USB-ključi in drugo) se hranijo v zaklenjenih omarah.

POGODBENA OBDELAVA OSEBNIH PODATKOV

12 člen
(Splošno)

Z vsako zunanjo pravno ali fizično osebo, ki opravlja posamezna opravila v zvezi z zbiranjem, obdelovanjem, shranjevanjem ali posredovanjem osebnih podatkov (obdelovalec), se sklene pisna pogodba, predvidena v 28. členu Splošne uredbe o varstvu podatkov. V takšni pogodbi morajo biti obvezno predpisani tudi pogoji in ukrepi za zagotovitev varstva osebnih podatkov in njihovega zavarovanja. Pred sklenitvijo pogodbe z obdelovalcem je odgovorna oseba (praviloma vodja enote) dolžna od njega pridobiti podatke, ki omogočajo preveritev, ali obdelovalec izpolnjuje zahteve zakonodaje s področja varstva osebnih podatkov; to vključuje tudi razkritje vseh podpogodbenih obdelovalcev, vključno z njihovimi nazivi in sedeži.

Že zgolj možnost dostopa do podatkov, četudi na izrecno zahtevo ustanove (npr. v okviru servisnega posega na strojni opremi ipd.), se šteje za pogodbeno obdelavo v smislu 1. odstavka tega člena.

Obdelovalci smejo opravljati storitve obdelave osebnih podatkov samo v okviru naročnikovih pooblastil in podatkov ne smejo obdelovati ali drugače uporabljati za noben drug namen, k čemur se jih zaveže s pogodbo.

Obdelovalec mora imeti vsaj enako strog način varovanja osebnih podatkov, kakor ga predvideva ta pravilnik.

Poleg drugih zahtev si mora ustanova v pogodbah z obdelovalci zagotoviti pravico, da najmanj enkrat letno pri pogodbenem obdelovalcu izvede pregled ali revizijo na področju varstva osebnih podatkov. Pregled ali revizijo je potrebno izvesti ob vsakem sumu ali indicu, da obdelovalec krši sklenjeno pogodbo ali da ne zagotavlja zadostne ravni varstva osebnih podatkov. Revizija se izvede na stroške ustanove, pri čemer obdelovalec morebitnega angažmaja svojih ljudi in/ali podpogodbenih obdelovalcev ustanovi ne sme zaračunati.

BRISANJE, UNIČENJE IN ANONIMIZACIJA PODATKOV

13 člen
(Splošno)

Osebni podatki se lahko shranjujejo le toliko časa, kolikor je rok hrambe, razviden iz evidence dejavnosti obdelave, če tega roka ni, pa toliko časa, kolikor določa zakon ali dokler traja pogodba s posameznikom, čigar podatki se obdelujejo, in še 5 let po njenem prenehanju, ali za čas, za katerega je posameznik privolil v obdelavo svojih osebnih

podatkov ali dokler ni dosežen namen obdelave. Rok hrambe za konkretne (baze) osebnih podatkov določi predsednik uprave ustanove.

Po preteku roka hrambe se osebni podatki učinkovito izbrišejo, uničijo ali anonimizirajo, razen če zakon ali drug akt določa drugače. Uničenje, izbris ali anonimizacijo osebnih podatkov odredi vodja enote. O uničenju, izbrisu ali anonimizaciji osebnih podatkov se napravi zapisnik, ki ne sme vsebovati osebnih podatkov posameznikov, katerih podatki so se izbrisali, uničili ali anonimizirali.

Za brisanje podatkov z računalnikov, strežnikov in podobnih naprav se uporabi takšna metoda brisanja, da je nemogoča rekonstrukcija brisanih podatkov.

Podatki na fizičnih nosilcih, ki jih ni mogoče izbrisati, se uničijo na način, ki zagotovi, da postane osebni podatek nerazpoznaven in neobnovljiv. Točen način uničenja za posamezne tipe osebnih podatkov ali nosilcev določi predsednik uprave ustanove.

Prepovedano je odmetavati nosilce podatkov na način, ki omogoča obnovitev ali razpoznavnost osebnih podatkov (npr. v koš za smeti).

UKREPANJE OB VARNOSTNIH INCIDENTIH V ZVEZI Z OSEBNIMI PODATKI

14 člen
(Splošno)

Zaposleni 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.

Zaposleni so dolžni o aktivnostih, ki so povezane z odkrivanjem ali nepooblaščenim uničenjem osebnih podatkov, zlonamerni ali nepooblaščeni uporabi, prilaščanju, spreminjanju ali poškodovanju osebnih podatkov takoj obvestiti vodjo svoje enote ali predsednika uprave ustanove, sami pa morajo poskusiti z zakonitimi ukrepi takšno aktivnost preprečiti.

Predsednik uprave ustanove mora ob vsakem sumu kršitve varstva osebnih podatkov takšno kršitev sporočiti Informacijskemu pooblaščencu v 72 urah. Kadar je verjetno, da kršitev varstva osebnih podatkov povzroči veliko tveganje za pravice in svoboščine posameznikov, mora predsednik uprave ustanove poskrbeti za to, da so prizadeti posamezniki brez nepotrebnega odlašanja obveščeni o tem, da je prišlo do kršitve varstva osebnih podatkov.

15 člen
(Interni ukrepi)

Predsednik uprave ustanove je dolžan poskrbeti za to, da se po varnostnem incidentu opravi analiza vzrokov in predlog ukrepov, ki naj zmanjšajo ali izničijo tveganje za take in bodoče varnostne incidente, ter da se, če je to smiselno in mogoče, predlagani ukrepi tudi izvedejo.

Če se izkaže, da je varnostni incident povzročil ali bil pri njem udeležen zaposleni ali je do varnostnega incidenta prišlo zaradi malomarnosti s strani zaposlenega, predsednik uprave ustanove, ne glede na ostale določbe tega pravilnika, sprejme ustrezne delovnopravne ukrepe zoper zaposlenega.

ODGOVORNOST ZA IZVAJANJE UKREPOV ZAVAROVANJA OSEBNIH PODATKOV

16 člen
(Splošno)

Za nadzor nad izvajanjem postopkov in ukrepov za zavarovanje osebnih podatkov je odgovoren predsednik uprave ustanove, ki lahko za posamezne naloge pooblasti druge osebe, ki niso zaposlene pri ustanovi.

Nadzor iz 1. odstavka tega člena vključuje tudi postopke rednega testiranja, ocenjevanja in vrednotenja učinkovitosti tehničnih in organizacijskih ukrepov za zagotavljanje varnosti obdelave. Pri tem so dolžni sodelovati vsi zaposleni in druge osebe v ustanovi.

Vsak, ki obdeluje osebne podatke, je dolžan izvajati predpisane postopke in ukrepe za zavarovanje podatkov in varovati podatke, s katerimi je bil seznanjen pri opravljanju svojega dela. Obveza varovanja podatkov ne preneha s prenehanjem delovnega razmerja.

Pred nastopom dela na delovnem mestu, kjer se obdelujejo osebni podatki, mora zaposleni podpisati posebno izjavo, ki ga zavezuje k varovanju osebnih podatkov. Izjava je lahko tudi del pogodbe o zaposlitvi.

Iz podpisane izjave mora biti razvidno, da je podpisnik seznanjen z določbami tega pravilnika ter določbami GDPR, izjava pa mora vsebovati tudi pouk o posledicah kršitve.

KONČNE DOLOČBE

17 člen
(Datum uveljavitve)

Ta pravilnik velja in se uporablja od 25.5.2018 naprej.

18 člen
(Objava, dostopnost)

Ta pravilnik se objavi na oglasni deski, vsem zaposlenim in uporabnikom pa je na vpogled tudi na sedežu UZG.

Pripravil: Lilijana Reljič

Zadnja sprememba: 26.6.2018

USTANOVA ZDENKE GUSTINČIČ • FUNDACIJA ZA DOBRO LJUDI IN NARAVE •