



Na podlagi določb Uredbe (EU) 2016/679 Evropskega Parlamenta in Sveta z dne 27. aprila 2016 o varstvu posameznikov pri obdelavi osebnih podatkov in o prostem pretoku takih podatkov ter o razveljavitvi Direktive 95/46/ES (v nadaljevanju: »Splošna uredba«) in na podlagi veljavne zakonodaje s področja varstva osebnih podatkov, Javni zavod Športni in mladinski center Piran izdaja (v nadaljevanju: »zavod«), ki ga zastopa direktor Matjaž Ukmar (v nadaljevanju: »odgovorna oseba«)

PRAVILNIK

o varstvu osebnih podatkov

I. SPLOŠNE DOLOČBE

1. člen

- (1) S tem pravilnikom se določajo organizacijski, tehnični in logično-tehnični postopki in ukrepi za zavarovanje osebnih podatkov v zavoda z namenom, da se prepreči slučajno ali namerno nepooblaščen uničevanje podatkov, njihovo spremembo ali izgubo, kakor tudi nepooblaščen dostop, obdelava, uporaba ali posredovanje osebnih podatkov.
- (2) Odgovorna oseba zavoda, vodstvo, zaposleni delavci oziroma vse osebe, ki so vključene v delovni proces zavoda na podlagi pogodbe o zaposlitvi ali drugega pogodbenega temelja, ki pri svojem delu v zavodu obdelujejo in uporabljajo osebne in/ali zaupne podatke in/ali se seznanjajo s poslovno skrivnostjo zavoda, morajo spoštovati določila veljavne zakonodaje, ki ureja področje varstva osebnih podatkov in določila zakonodaje, ki ureja posamezno področje njihovega dela ter vsebino tega pravilnika.

2. člen

V tem pravilniku uporabljeni izrazi imajo naslednji pomen:

1. **Določljivi posameznik** je tisti, ki ga je mogoče neposredno ali posredno določiti, zlasti z navedbo identifikatorja, kot je ime, identifikacijska številka, podatki o lokaciji in spletni identifikator ali z navedbo enega ali več dejavnikov, ki so značilni za fizično, fiziološko, genetsko, duševno, gospodarsko, kulturno ali družbeno identiteto tega posameznika;
2. **Kršitev varstva osebnih podatkov** pomeni kršitev varnosti, ki povzroči nenamerno ali nezakonito uničenje, izgubo, spremembo, nepooblaščen razkritje ali dostop do osebnih podatkov, ki so poslani, shranjeni ali kako drugače obdelani;
3. **Nosilec podatkov** pomeni vse vrste sredstev, na katerih so zapisani ali posneti podatki (listine, akti, gradiva, spisi, računalniška oprema - vključno z magnetnimi, optičnimi ali drugimi računalniškimi mediji - fotokopije, zvočno in slikovno gradivo, mikrofili, naprave za prenos podatkov, ipd.);
4. **Obdelava** pomeni vsako dejanje ali niz dejanj, ki se izvajajo 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;
5. **Obdelovalec** pomeni fizično ali pravno osebo, javni organ, zavod, agencijo ali drugo telo, ki obdeluje osebne podatke v imenu upravljavca;



6. **Osební podatki** pomeni katero koli informacijo v zvezi z določenim ali določljivim posameznikom (v nadaljevanju: »posameznik, na katerega se nanašajo osebni podatki«);
7. **Podatki o zdravstvenem stanju** pomeni osebne podatke, ki se nanašajo na telesno ali duševno zdravje posameznika, vključno z zagotavljanjem zdravstvenih storitev, in razkrivajo informacije o njegovem zdravstvenem stanju;
8. **Posebne vrste osebnih podatkov** so osebni 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;
9. **Privolitev posameznika**, na katerega se osebni podatki nanašajo, pomeni vsako prostovoljno, izrecno, informirano in nedvoumno izjavo volje posameznika, na katerega se nanašajo osebni podatki, s katero z izjavo ali jasnim pritrdilnim dejanjem izrazi soglasje za obdelavo osebnih podatkov, ki se nanašajo nanj;
10. **Tretja oseba** pomeni fizično ali pravno osebo, javni organ, zavod, agencijo ali telo, ki ni posameznik, na katerega se nanašajo osebni podatki, upravljavec, obdelovalec in osebe, ki so pooblaščenice za obdelavo osebnih podatkov pod neposrednim vodstvom upravljavca ali obdelovalca;
11. **Uporabnik** pomeni fizično ali pravno osebo, javni organ, zavod, agencijo ali drugo telo, ki so mu bili osebni podatki razkriti, ne glede na to, ali je tretja oseba ali ne. Vendar pa javni organi, ki lahko prejmejo osebne podatke v okviru posamezne poizvedbe v skladu s pravom Unije ali pravom države članice, ne štejejo za uporabnike; obdelava teh podatkov s strani teh javnih organov poteka v skladu z veljavnimi pravili o varstvu podatkov glede na namene obdelave;
12. **Upravljavec** pomeni fizično ali pravno osebo, javni organ, zavod, agencijo ali drugo telo, ki samo ali skupaj z drugimi določa namene in sredstva obdelave; kadar namene in sredstva obdelave določa pravo Unije ali pravo države članice, se lahko upravljavec ali posebna merila za njegovo imenovanje določijo s pravom Unije ali pravom države članice.

II. OBDELAVA OSEBNIH PODATKOV

3. člen

- (1) V zavoda se lahko na osnovi 6. člena Splošne uredbe obdeluje osebne podatke, v kolikor je izpolnjen vsaj eden od naslednjih pogojev:
 - posameznik, na katerega se nanašajo osebni podatki, je privolil v obdelavo svojih osebnih podatkov za enega ali več določenih namenov;
 - obdelava je potrebna za izvajanje pogodbe, katere pogodbená stranka je posameznik, na katerega se nanašajo osebni podatki, ali za izvajanje ukrepov na zahtevo takega posameznika pred sklenitvijo pogodbe;
 - obdelava je potrebna za izpolnitev zakonske obveznosti, ki velja za upravljavca;
 - obdelava je potrebna za zaščito življenjskih interesov posameznika, na katerega se nanašajo osebni podatki, ali druge fizične osebe;



- obdelava je potrebna za opravljanje naloge v javnem interesu ali pri izvajanju javne oblasti, dodeljene upravljavcu;
 - obdelava je potrebna zaradi zakonitih interesov, za katere si prizadeva upravljavec ali tretja oseba, razen kadar nad takimi interesi prevladajo interesi ali temeljne pravice in svoboščine posameznika, na katerega se nanašajo osebni podatki, ki zahtevajo varstvo osebnih podatkov, zlasti kadar je posameznik, na katerega se nanašajo osebni podatki, otrok.
- (2) Osebni podatki se smejo obdelovati samo za določene in zakonite namene ter se ne smejo nadalje obdelovati tako, da bi bila njihova obdelava v neskladju s temi nameni, razen v primerih, če zakon ne določa drugače.
- (3) Pri obdelavi posebnih vrst osebnih podatkov morajo biti zaposleni še posebej vestni in skrbni. Posebne vrste osebnih podatkov morajo biti varovane tako, da se nepooblaščenim osebam prepreči dostop do njih.
- (4) O obdelavi osebnih podatkov mora biti posameznik obveščen v skladu s 13. in 14. členom Splošne uredbe oziroma mu morajo biti predstavljene njegove pravice v skladu s 15. členom Splošne uredbe.

4. člen

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

5. člen

- (1) Odgovorna oseba zavoda je dolžna poskrbeti za to, da so posamezniki na primeren način, ki je skladen z zahtevami Splošne uredbe, obveščeni o pravicah. Prav tako odgovorna oseba poskrbi za enotno kontaktno točko, na katero se lahko posamezniki obrnejo in z zavodom komunicirajo pri uveljavljanju svojih pravic.



6. člen

- (1) Pred nastopom dela v zavoda mora zaposleni podpisati izjavo, ki ga zavezuje k varovanju osebnih podatkov.
- (2) Iz podpisane izjave mora biti razvidno, da je podpisnik seznanjen z določbami tega pravilnika, Splošne uredbe in zakonodaje. Izjava mora vsebovati tudi poduk o posledicah kršitve določb.
- (3) Izjavo iz prvega odstavka tega člena podpišejo tudi zunanji sodelavci zavod, ki se v okviru izvajanja pogodbenih del seznanijo ali bi se lahko seznanili z osebnimi podatki, s katerimi upravlja zavod.
- (4) Izjavo iz prvega odstavka tega člena podpišejo vsi študentje, dijaki, prostovoljci in zunanji pripravniki, ki se seznanijo z osebnimi podatki v okviru sodelovanja z zavodom.

7. člen

- (1) Praviloma imajo posamezniki sledeče pravice iz varstva osebnih podatkov:

- Zahtevajo lahko informacije o tem, ali ima zavod osebne podatke o njih, in če je tako, katere podatke ima ter na kakšni podlagi jih ima in zakaj jih uporablja.
- Zahtevajo lahko dostop do svojih osebnih podatkov, kar jim omogoča, da prejmejo kopijo osebnih podatkov, ki jih imajo o njih ter preverijo, ali jih zavod obdeluje zakonito.
- Zahtevajo lahko popravke osebnih podatkov, kot so popravki nepopolnih ali netočnih osebnih podatkov.
- Zahtevajo lahko izbris osebnih podatkov, kadar ni razloga za nadaljnjo obdelavo oziroma kadar uveljavljajo svojo pravico do ugovora glede nadaljnje obdelave.
- Ugovarjajo lahko nadaljnji obdelavi osebnih podatkov, kjer se zanašamo na zakoniti poslovni interes (tudi v primeru zakonitega interesa tretje osebe), kadar obstajajo razlogi, povezani z njihovim posebnim položajem; ne glede na določilo prejšnjega stavka imajo pravico kadarkoli ugovarjati, če obdeluje zavod njihove osebne podatke za namene neposrednega trženja.
- Zahtevajo lahko omejitev obdelave svojih osebnih podatkov, kar pomeni prekinitev obdelave osebnih podatkov o njih, na primer, če želijo, da zavod ugotovi njihovo točnost ali preveri razloge za njihovo nadaljnjo obdelavo.
- Zahtevajo lahko prenos osebnih podatkov v strukturirani elektronski obliki k drugemu upravljavcu, v kolikor je to mogoče in izvedljivo.
- Prekličejo lahko privolitev oziroma soglasje, ki so ga podali za zbiranje, obdelavo in prenos osebnih podatkov za določen namen; po prejemu obvestila, da so umaknili svojo privolitev, bo zavod prenehala obdelovati njihove osebne podatke za namene, ki so jih prvotno sprejeli, razen če zavod nima druge zakonite pravne podlage za to, da to stori zakonito.

- (2) Če želi posameznik uveljavljati katero koli od prej navedenih pravic, lahko pošlje zahtevek po elektronski pošti na info@simcpiran.si ali z redno pošto na naslov zavod.



- (3) Zavod posameznika, ki z zahtevo uveljavlja svoje pravice, seznanj z odločitvijo in z osebnimi podatki, če je to predmet zahteve, najkasneje v enem mesecu po prejemu zahteve. Ta rok se lahko po potrebi podaljša za največ dva dodatna meseca ob upoštevanju kompleksnosti in števila zahtev. O podaljšanju roka, zavod obvesti posameznika. Odločitev zavod mora vsebovati razloge in informacijo o pravici do pritožbe pri Informacijskem pooblaščenca v roku 15 dni od seznanitve z odločitvijo.
- (4) Dostop do lastnih osebnih podatkov in uveljavljanje pravic je za posameznika brezplačno, vendar lahko zavod zaračuna razumno plačilo, kadar so zahtevki očitno neutemeljeni ali pretirani, zlasti ker se ponavljajo. Če je posameznikova zahteva za dostop očitno neutemeljena ali pretirana, lahko zavod v takšnem primeru zavrne zahtevo.
- (5) V primeru uveljavljanja pravic iz tega naslova bo zavod morda morala od posameznika zahtevati določene informacije, ki ji bodo pomagale pri potrditvi posameznikove identitete, kar je le varnostni ukrep, ki zagotavlja, da se osebni podatki ne razkrijejo nepooblaščenim osebam.
- (6) V primeru, da posameznik meni, da so njegove pravice kršene, se lahko za zaščito ali pomoč obrne na nadzorni organ oz. na Informacijskega pooblaščenca: gp.ip@ip-rs.si ali poišče informacije na spletni strani: www.ip-rs.si.

8. člen

- (1) Zavod posreduje osebne podatke drugim osebam javnega sektorja ali drugim fizičnim ali pravnim osebam, če je za posredovanje dana ustrezna pravna podlaga v skladu z zakonodajo, razen če drug zakon določa drugače. Prejemnik podatkov sme osebne podatke obdelovati samo za namen, za uresničevanje katerega se mu posredujejo.
- (2) Posredovanje osebnih podatkov mora vlagatelj zahtevati pisno. Zahteva mora vsebovati:
 - podatke o vlagatelju zahteve (za fizično osebo: osebno ime, naslov stalnega ali začasnega prebivališča; za samostojnega podjetnika posameznika, posameznika, ki samostojno opravlja dejavnost, ter za pravno osebo: naziv oziroma firmo in naslov oziroma sedež in matično številko) ter podpis vlagatelja oziroma pooblaščenih oseb;
 - pravno podlago za pridobitev zahtevanih osebnih podatkov;
 - namen obdelave osebnih podatkov oziroma razloge, ki izkazujejo potrebnost in primernost osebnih podatkov za doseg namena pridobitve;
 - identifikacijo zadeve, v zvezi s katero so osebni podatki potrebni, ter navedbo organa ali drugega subjekta, ki obravnava zadevo;
 - vrste osebnih podatkov, ki naj se mu posredujejo;
 - obliko in način pridobitve zahtevanih osebnih podatkov.
- (3) Zavod vlagatelju, če drug zakon ne določa drugače, zahtevane osebne podatke posreduje najpozneje v 15 dneh od prejema popolne zahteve ali pa ga v tem roku pisno obvesti o razlogih, zaradi katerih mu zahtevanih osebnih podatkov ne bo posredovala. Zavod in vlagatelj se v roku lahko dogovorita za njegovo podaljšanje. Če zavod v roku 15 dni ne posreduje podatkov oz. se rok ne podaljša, se šteje, da je zahteva zavrnjena.



- (4) Osební podatki, ki se posredujejo uporabniku v fizični obliki, morajo biti posredovani v ovojnici. Ovojница mora zagotoviti, da odprtja ovojnice in seznanitve z njeno vsebino ni mogoče opraviti brez vidne sledi odpiranja ovojnice.
- (5) Osebné 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.
- (6) Posebne vrste osebnih podatkov se v fizični obliki pošilja naslovníkom v zaprtih ovojnicah proti podpisu v dostavni knjigi ali z vročilnico. V primeru, da se posebne vrste osebnih podatkov pošilja v elektronski obliki, mora biti med prenosom zagotovljena njihova nečitljivost, tako da so šifrirani in zavarovani z geslom.
- (7) Zaposleni, ki obdeluje osebné podatke, je dolžan evidentirati vsako posredovanje osebnih podatkov izven zavoda. V evidenco posredovanja podatkov se vpisuje, kateri osebni podatki so bili posredovani, komu, kdaj in na kateri pravni podlagi ter za kateri namen oz. za potrebe katerega postopka.

9. člen

- (1) Delavec, ki je zadolžen za sprejem in evidenco pošte v zavoda, odpira in pregleduje vse poštné pošiljke in pošiljke, naslovljene na zavod, ki na drug način prispejo v zavod (npr. prinesejo jih stranke ali kurirji), razen pošiljk iz drugega in tretjega odstavka tega člena.
- (2) Delavec, ki je zadolžen za sprejem in evidenco pošte, ne odpira tistih pošiljk, ki so naslovljene na drug organ ali zavod in so pomotoma dostavljena ter pošiljk, ki so označene kot osebni podatki ali za katere iz označb na ovojnici izhaja, da se nanašajo na natečaj ali razpis.
- (3) Delavec, ki je zadolžen za sprejem in evidenco pošte v zavoda, pošiljke z osebnimi podatki ne odpira in jo mora izročiti direktno posamezniku ali službi oz. oddelku zavoda, na katero je ta pošiljka naslovljena, kadar je to razvidno iz ovojnice pošiljke. Delavec, ki je zadolžen za sprejem in evidenco pošte, ne sme odpirati pošiljke, naslovljene na naslov zavoda in obenem posameznika, v primerih, ko je iz ovojnice razvidno, da je posamezniku treba pošiljko vročiti osebno (npr. z oznako v roke, osebno itd.).

10. člen

- (1) Zavod vodi evidenco dejavnosti obdelave v skladu z določbami člena 30 Splošne uredbe.
- (2) Zaposleni, ki obdelujejo osebné podatke, morajo biti seznanjeni z evidenco dejavnosti obdelave. Vpogled v evidenco dejavnosti obdelave je omogočen vsakemu zaposlenemu na zahtevo.
- (3) V evidenco dejavnosti se vpisuje, v kolikor je to možno: naziv zbirke osebnih podatkov, namen obdelave, pravna podlaga, kategorije posameznikov, na katere se podatki nanašajo, vrste osebnih podatkov, kategorije uporabnikov, ki so jim bili ali jim bodo razkriti osebni podatki, prenos osebnih podatkov v tretjo državo, rok hrambe in splošen opis tehničnih in organizacijskih varnostnih ukrepov.



11. člen

- (1) Kadar je možno, da bi lahko načrtovana obdelava osebnih podatkov, zlasti z uporabo novih tehnologij, ob upoštevanju narave, obsega, okoliščin in namenov obdelave osebnih podatkov, povzročila veliko tveganje za pravice in svoboščine posameznikov, se na to opozori vodstvo zavoda.
- (2) V tem primeru se opravi presoja glede izvedbe, ocena učinka v zvezi z varstvom podatkov, kot jo predvideva člen 35 Splošne uredbe in veljavna zakonodaja s področja varstva osebnih podatkov.

12. člen

- (1) Za namene dokumentiranja aktivnosti in obveščanja javnosti o delu in dogodkih v zavoda, kot so prireditve, srečanja, tekmovanja, izobraževanja in podobno, lahko zavod tak dogodek delno ali v celoti snema oziroma fotografira in izdelani material objavi na spletnih straneh, tiskovinah in družabnih omrežjih zavoda.
- (2) Obvestilo o tem, da bo dogodek sneman oziroma fotografiran, se zapiše na vabilo oziroma na obvestilo o dogodku. Navede se tudi namen snemanja oziroma fotografiranja. Na ta način se šteje, da so udeleženci oziroma obiskovalci obveščeni o snemanju oziroma fotografiranju javnega dogodka.
- (3) Kadar je to bolj primerno (ob dogodkih z manjšim številom udeleženih, dogodkih, ki niso odprti za javnost, udeleženci pa utemeljeno pričakujejo večjo stopnjo zasebnosti), se snemanje oziroma fotografiranje ustno napove in udeležencem pusti možnost, da izrazijo svojo voljo glede zajema njihove podobe s kamero.

13. člen

- (1) Zavod redno obvešča zaposlene o pomenu in novostih s področja varstva osebnih podatkov in izvaja izobraževanja s tega področja ter s področja informacijske varnosti.
- (2) Zavod praviloma enkrat letno zaposlenim predstavi sledeče:
 - pravice in dolžnosti zaposlenih glede varovanja osebnih podatkov;
 - nevarnosti in najpogostejša tveganja za varovanje osebnih podatkov;
 - možne posledice za zavod in zaposlene v primeru kršitve varstva podatkov;
 - varovanje gesel in upravljanje z gesli;
 - varovanje opreme in prostorov;
 - varno ravnanje v primeru iznosa podatkov izven prostorov zavoda (npr. na prenosnikih, pametnih telefonih, USB-ključkih ipd.);
 - politiko čiste mize;
 - druge prakse, politike in primere s področja varstva osebnih podatkov.
- (3) Zavod redno izvaja varnostne politike na področju informacijske varnosti, ki so opredeljene v internih aktih in jih najmanj enkrat letno preverja.



III. POOBLAŠČENA OSEBA ZA VARSTVO PODATKOV

14. člen

- (1) Odgovorna oseba zavoda imenuje pooblaščen osebno za varstvo podatkov s sklepom ali na drug primeren način (npr. s sklenitvijo pogodbe) in poskrbi za objavo informacij o pooblaščen osebni na spletni strani zavoda.
- (2) Za pooblaščen osebno za varstvo podatkov in njenega namestnika je lahko določen posameznik, ki je poslovno sposoben, ima znanja oziroma praktične izkušnje s področja varstva osebnih podatkov in ni bil pravnomočno obsojen na kazen zapora najmanj šestih mesecev oz. ni bil pravnomočno obsojen za kaznivo dejanje glede zlorabe osebnih podatkov ter je zmožen izpolnjevanja nalog iz 39. člena Splošne uredbe.
- (3) Zavod zagotavlja, da je pooblaščen osebno za varstvo podatkov ustrezno in pravočasno vključena v vse zadeve v zvezi z varstvom osebnih podatkov, ter da so ji zagotovljena vsa ustrezna sredstva, potrebna za kvalitetno opravljanje svojih nalog, ter da ji je omogočen dostop do osebnih podatkov in dejanj obdelave.
- (4) Zavod zagotovi, da pooblaščen osebno za varstvo podatkov pri opravljanju svojih nalog ne prejema nobenih navodil. Pooblaščen osebno za varstvo podatkov ne sme biti razrešena ali kaznovana zaradi opravljanja svojih nalog. Pooblaščen osebno za varstvo podatkov neposredno poroča odgovorni osebni zavoda.

15. člen

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

16. člen

- (1) Pooblaščen osebno za varstvo podatkov je pri opravljanju svojih nalog dolžna varovati kot skrivnost vse podatke, s katerimi se seznanijo pri opravljanju svojih nalog v skladu z veljavno nacionalno zakonodajo.

17. člen

- (1) Pooblaščen osebno za varstvo podatkov ima vsaj naslednje naloge:
 - obveščanje zavoda, njenih pogodbenih obdelovalcev in zaposlenih, ki izvajajo obdelavo, ter svetovanje navedenim o njihovih obveznostih v skladu s Splošno uredbo in drugimi zakonskimi določbami o varstvu osebnih podatkov;
 - spremljanje skladnosti zavoda s Splošno uredbo in nacionalnim pravom, vključno z dodeljevanjem nalog v zvezi z varstvom osebnih podatkov, osveščanjem in usposabljanjem zaposlenih v zavoda, ki pri svojem delu obdelujejo osebne podatke;
 - svetovanje, kadar je to zahtevano, glede ocene učinka v zvezi z varstvom podatkov in spremljanje njenega izvajanja v skladu s 35. členom Splošne uredbe;
 - sodelovanje z nadzornim organom;



ŠPORTNI IN MLADINSKI CENTER PIRAN CENTRO SPORTIVO E GIOVANILE DI PIRANO

- delovanje kot kontaktna točka za nadzorni organ pri vprašanjih v zvezi z obdelavo, vključno s predhodnim posvetovanjem iz 36. člena Splošne uredbe in, kjer je ustrezno, posvetovanje glede katere koli druge zadeve.
- (2) Pooblaščen osebja za varstvo podatkov pri opravljanju svojih nalog upošteva tveganje, povezano z dejanji obdelave ter naravo, obseg, okoliščine in namene obdelave.

IV. POGODBENA OBDELAVA OSEBNIH PODATKOV

18. člen

- (1) Z vsako zunanjo pravno ali fizično osebo, ki opravlja posamezna opravila v zvezi z obdelavo osebnih podatkov za zavod, se sklene pisna pogodba o opravljanju storitev, katera vsebuje tudi določila o predmetu obdelave (zlasti vsebino in trajanje obdelave, naravo in namen obdelave, vrste osebnih podatkov in kategorije posameznikov), pravicah in obveznostih pogodbenega obdelovalca in upravljavca ter postopke in ukrepe za zavarovanje osebnih podatkov skladno s Splošno uredbo in zakonom, ki ureja varstvo osebnih podatkov.
- (2) Obdelovalci so tudi zunanji sodelavci, ki vzdržujejo strojno in programsko opremo ter izdelujejo in nameščajo novo strojno ali programsko opremo, v kolikor imajo pri svojem delu dostop do osebnih podatkov.
- (3) Zunanje pravne ali fizične osebe smejo opravljati storitve obdelave osebnih podatkov samo v okviru pooblastil zavoda in osebnih podatkov ne smejo obdelovati ali drugače uporabljati za noben drug namen.
- (4) Pooblaščen pravna ali fizična oseba, ki za zavod opravlja dogovorjene storitve izven prostorov upravljavca, mora imeti vsaj enako strog način zagotavljanja varnosti osebnih podatkov, kakor ga določa ta pravilnik.

V. BRISANJE PODATKOV

19. člen

- (1) Osebnih podatki se lahko obdelujejo le toliko časa, kolikor je določen rok hrambe oziroma dokler obstaja pravna podlaga iz 6. člena Splošne uredbe. Rok hrambe osebnih podatkov zavod omeji na najkrajše možno obdobje in le, dokler je hramba potrebna za doseg namena obdelave, zaradi katerega so se podatki zbrali ali nadalje obdelovali. Po preteku roka hranjenja se osebni podatki zbršejo, uničijo, blokirajo ali anonimizirajo oz. se izvede drug postopek, ki onemogoča identifikacijo posameznika, razen če zakon ali drug akt ne določata drugače.
- (2) Osebnih podatke, ki jih zavod obdeluje na osnovi pogodbenega odnosa s posameznikom, zavod hrani za obdobje, ki je potrebno za izvršitev pogodbe in še **6 let po njenem prenehanju**, razen v primerih, ko pride med posameznikom in zavod do spora v zvezi s pogodbo. **V primeru spora** hrani zavod podatke **še 10 let po pravomočnosti sodne odločbe**, arbitraže ali poravnave. V primeru, če pa ne pride do sodnega spora, pa **6 let od dneva mirne razrešitve spora**.



- (3) Tiste osebne podatke, ki jih zavod obdeluje na podlagi osebne privolitve posameznika ali zakonitega interesa, zavod hrani do preklica te privolitve oziroma do zahteve za izbris. V primeru prejemu preklica ali utemeljene zahteve za izbris se podatki izbrišejo brez nepotrebnega odlašanja, po tem ko zavod odloči o zahtevku posameznika. Zavod lahko te podatke izbriše tudi pred preklicem, kadar je bil dosežen namen obdelave osebnih podatkov ali če tako določa zakon.
- (4) V primeru ko zavod prejme zahtevo posameznika v zvezi z njegovimi pravicami iz 15. do 22. člena Splošne uredbe, zavod 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 ravna skladno s pravnomočno odločitvijo v zadevi.
- (5) Izjemoma lahko zavod zavrne zahtevo za izbris iz razlogov iz Splošne uredbe, kot jih našteva:
 - uresničevanje pravice do svobode izražanja in obveščanja;
 - izpolnjevanje pravne obveznosti obdelave;
 - razlogi javnega interesa na področju javnega zdravja;
 - nameni arhiviranja v javnem interesu;
 - znanstveno ali zgodovinsko raziskovalni nameni ali statistični nameni;
 - izvajanje ali obramba pravnih zahtevkov.

20. člen

- (1) Za brisanje podatkov iz nosilcev podatkov se uporabi takšna metoda brisanja, da je nemogoča restavracija vseh ali dela brisanih podatkov.
- (2) Podatki na klasičnih medijih (listine, kartoteke, register, seznam ...) se uničijo na način, ki onemogoča branje vseh ali dela uničenih podatkov. Na enak način se uničuje pomožno gradivo (matrice, izračune in grafikone, skice, poskusne oziroma neuspešne izpise ...).
- (3) Prepovedano je odmetavati odpadne nosilce podatkov z osebni podatki v koše za smeti.
- (4) Pri prenosu nosilcev osebnih podatkov na mesto uničenja je potrebno zagotoviti ustrezno zavarovanje tudi v času prenosa. Prenos nosilcev podatkov na mesto uničenja ter uničevanje nosilcev osebnih podatkov nadzoruje posebna komisija, ki o uničenju sestavi tudi ustrezen zapisnik oziroma se uničenje preda ustrezni zunanji službi na osnovi sklenjene pogodbe.

VI. INFORMACIJSKO VARNOSTNA POLITIKA

21. člen

- (1) Zaposleni uporabljajo različno informacijsko tehnologijo (računalnik, telefon, tablica in druge elektronske naprave) in različne elektronske storitve (dostop do interneta, elektronska pošta, dostop do oblaka, skupni imeniki in mape ter drugo programsko opremo oziroma storitve), ki jim jih dodeli delodajalec izključno za službene namene.
- (2) V omejenem obsegu in razumnih mejah se s strani zavoda dodeljena informacijska tehnologija in elektronske storitve lahko uporabljajo tudi v zasebne namene. Pri tem morajo delavci varovati ugled zavoda, tehnologij in storitev pa ne smejo uporabljati za neprimerne ali žaljive namene. Vodstvo lahko po lastni presoji delavcu kadarkoli prepove uporabo službenih informacijskih tehnologij v zasebne namene.



22. člen

- (1) Dostop do svetovnega spleta je omogočen zaposlenim za njihovo delo, izobraževanje in informiranje.
- (2) Zaposleni v zavodu morajo uporabljati svetovni splet v skladu z etičnimi in moralnimi normami. Vsi uporabniki informacijskih sistemov se morajo zavedati, da se v medmrežju izkazujejo z mrežnim naslovom zavoda (IP naslov).
- (3) Posredovanje službenih elektronskih naslovov na zunanje spletne strežnike za namene prijave določene storitve (npr. pošte, prijav na izobraževanja ipd.) ni dovoljeno, razen če je povezano s poslovnim procesom dela zavoda.
- (4) V omrežju zavoda se na zahtevo odgovorne osebe lahko izdeluje statistika obiskanih spletnih strani, ki mora biti anonimizirana in se je ne sme javno objaviti. Statistika se lahko uporablja izključno za načrtovanje in varovanje informacijskega sistema.
- (5) Vodstvo zavoda lahko zaradi zagotavljanja informacijske varnosti in razpoložljivosti informacijskih virov ter zaradi preprečevanja kršitev s posebno odredbo ali sklepom odredi blokado uporabe določenih spletnih strani. Blokado dostopa do določenih spletnih strani izvede oseba, zadolžena za delovanje računalniškega informacijskega sistema, na podlagi pisne odredbe ali pisnega sklepa odgovorne osebe zavoda. O blokadi se obvesti vse zaposlene po elektronski pošti.

23. člen

- (1) Službena elektronska pošta se v zavodu lahko uporablja kot orodje za komunikacijo z državljanji, strankami, zaposlenimi in zunanjimi izvajalci. Pri tem se morajo zaposleni delavci zavoda držati ne le etičnih in moralnih norm, temveč tudi bontona. Pošiljatelj se mora zavedati, da se vsako sporočilo iz službenega elektronskega naslova pri prejemniku lahko šteje kot mnenje zavoda, v katerem je pošiljatelj zaposlen.
- (2) Zaposleni po elektronski pošti ne smejo pošiljati verižnih pisem in obsežnih datotek (glasba, filmi, predstave, zagonske datoteke in skripte ipd.), v kolikor niso namenjene delu.
- (3) Zaposleni svojega službenega elektronskega naslova ne smejo uporabljati v trženske namene in iz njega ne smejo pošiljati oglasne pošte na znane in/ali neznane naslove. Prav tako se zaposleni ne smejo prijavljati na oglasno pošto ali novice z elektronskimi naslovi zavoda, razen če to ni povezano s potrebami posameznega delovnega mesta zaposlenega.
- (4) Zaposleni morajo biti previdni pri odpiranju elektronske pošte s priponkami neznanih pošiljateljev. Ob sumu, da gre za nezaželeno pošto, ki bi lahko bila škodljiva, se te ne sme odpirati, temveč se o tem obvesti pristojno osebo, zadolženo za delovanje računalniškega informacijskega sistema.
- (5) Zaposleni nikakor ne smejo pošiljati posebnih vrst osebnih podatkov ali gesel po elektronski pošti, razen v ustrezno akreditiranih sistemih, oziroma mora biti med prenosom podatkov zagotovljena njihova nečitljivost, tako da so šifrirani in zavarovani z geslom.



- (6) Uporaba zasebne elektronske pošte (npr. Gmail., Yahoo., ipd.) za službene namene je prepovedana, saj potencialno predstavlja neupravičeno obdelavo osebnih podatkov. Izjemoma je dovoljena uporaba zasebne elektronske pošte izključno za namene komuniciranja med zaposlenimi na osnovi dovoljenja odgovorne osebe. Zaposlenim je dovoljeno uporabljati zasebno elektronsko pošto po izpolnjeni in podpisani izjavi.
- (7) Mobilnim telefonom, ki so v lasti zavoda in v uporabi posameznega delavca, se ne sme slediti. V mobilne naprave se ne sme namestiti naprav oziroma aplikacije za sledenje.

24. člen

- (1) Oddaljeni dostop do informacijskega sistema zavoda je dovoljen le na podlagi odobrene metode z ustrežno ravno varnosti, in sicer za tiste delavce, ki dostop potrebujejo zaradi opravljanja delovnih nalog, vendar le v omejenem obsegu. Treba je upoštevati tudi načelo čistega (praznega) zaslona. Po končanem delu se je treba obvezno odjaviti iz sistema in zagotoviti, da katerikoli podatki in sledi ne ostanejo na delovni postaji.
- (2) Za uveljavitev oddaljenega varnega dostopa je na strojni opremi zagotovljena prepoznavna ustrezne programske opreme, ki omogoča zaščito končne točke pred internetnimi grožnjami. Za zagotavljanje zaupnosti se ves promet iz končne točke oddaljenega omrežja do omrežja zavoda šifrira.

25. člen

- (1) Oseba, zadolžena za delovanje informacijskega sistema zavoda, lahko na posebej utemeljeno pisno zahtevo pooblaščenice osebe v prisotnosti tričlanske komisije v izrednih primerih (nenadna odpoved delavca, smrt delavca, nepričakovane, nenadne in dalj časa trajajoče ali trajne odsotnosti delavca, odpoved delovnega razmerja s strani zaposlenega brez odpovednega roka, odpoved delovnega razmerja iz krivdnih razlogov zaradi neopravičene odsotnosti in podobni izredni primeri) vpogleda v informacijsko tehnologije (npr. v računalnik) ali druge elektronske storitve (npr. v elektronsko pošto) delavca le, v primeru, če je to nujno potrebno za izpolnjevanje zakonskih obvez zavoda oziroma za vodenje delovnega procesa.
- (2) Vpogled opravi tričlanska komisija, ki jo vsakokrat imenuje pooblaščenica oseba zavoda. V njej mora biti vsaj en predstavnik zaposlenih, ki ni vodstveni delavec. O vpogledu mora komisija napisati zapisnik, ki vsebuje:
 - obrazložitev razloga vpogleda;
 - zapisnik o vstopu z morebitnimi pripombami delavca, če je ta navzoč;
 - navedbe prisotnih oseb;
 - seznam oziroma izpis pridobljenih podatkov.
- (3) V primeru, če se pojavi utemeljen sum, da zaposleni ne spoštujejo določil informacijsko-varnostne politike tega pravilnika, lahko oseba, zadolžena za delovanje računalniškega informacijskega sistema, na posebej utemeljeno pisno zahtevo odgovorne osebe opravi nadzor uporabe elektronskih storitev, a zgolj z vidika pregleda dnevniških zapisov o količini prometa in shranjenih podatkov, ki obremenjujejo strežnik. Pri tem se ne sme pregledovati vsebin.
- (4) Vpogled v telefonske prometne podatke priključkov, katerih lastnik je zavod, lahko zavod zahteva od operaterjev telekomunikacijskih storitev ali od vzdrževalca hišne centrale le takrat, kadar pride med zavod in zaposlenim do kakršnega koli spora glede višine stroškov porabe konkretnega telefonskega priključka.



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

26. člen

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

27. člen

- (1) Delavec lahko za namene opravljanja dela poleg službene opreme uporablja svojo zasebno opremo in druge tehnične naprave (predvsem mobilni telefon in e-poštni naslov), če takšno uporabo odobri odgovorna oseba in delavec poda prostovoljno pisno soglasje, da lahko delodajalec za namene izvajanja delovnega procesa pri tem obdeluje njegovo zasebno telefonsko številko oziroma zasebni elektronski naslov.
- (2) V primeru prenehanja delovnega razmerja je delavec dolžan iz zasebne opreme ali drugih naprav in njihovih nosilcev podatkov, ki jih je v soglasju z delodajalcem uporabljal za službene namene, izbrisati vse osebne podatke, ki so bili preneseni v okviru opravljanja delovnega procesa, in vse datoteke, ki jih je zaposleni uporabljal v službene namene, ne glede na to, ali vsebujejo osebne podatke.

VII. VAROVANJE PROSTOROV IN RAČUNALNIŠKE OPREME

28. člen

- (1) Prostori, v katerih se nahajajo nosilci osebnih podatkov, strojna in programska oprema (varovani prostori), morajo biti varovani z organizacijskimi ter fizičnimi in/ali tehničnimi ukrepi, ki onemogočajo nepooblaščenim osebam dostop do podatkov.
- (2) Kot varovani prostori so opredeljeni prostori vodstva oziroma uprave, tajništva, strežniške sobe, prostori programerske in servisne službe, pisarne, kabineti in drugi prostori, v katere nepooblaščen osebe nimajo vstopa.
- (3) Dostop do varovanih prostorov je mogoč le v rednem delovnem času, izven tega časa pa samo na podlagi dovoljenja odgovorne osebe zavoda.
- (4) Ključi varovanih prostorov se uporabljajo in hranijo v skladu s hišnim redom. Ključi se ne puščajo v ključavnici v vratih od zunanje strani.
- (5) Varovani prostori ne smejo ostajati nenadzorovani, oziroma se morajo zaklepati ob odsotnosti delavcev, ki jih nadzorujejo.
- (6) Zaposleni svojega delovnega mesta ne smejo pustiti nenadzorovanega oziroma morajo poskrbeti, da so takrat originalne listine in nosilci osebnih podatkov shranjeni tako, da nepooblaščen osebe do njih nimajo dostopa. Izven delovnega časa morajo biti omare in pisalne mize z nosilci osebnih podatkov zaklenjene (politika čiste mize).



- (7) Računalniki in druga informacijska tehnologija oziroma oprema, ki omogoča dostop do osebnih podatkov morajo biti v času odsotnosti zaposlenega bodisi izklopljeni bodisi fizično ali programsko zaklenjeni (politika čistega zaslona).
- (8) Zaposleni ne smejo puščati nosilcev osebnih podatkov na mizah v prisotnosti oseb, ki nimajo pravice vpogleda vanje.
- (9) Nosilci osebnih podatkov, ki se nahajajo izven varovanih prostorov (npr. avla, hodniki, skupni prostori, predavalnice, jedilnice), morajo biti stalno zaklenjeni v omarah. Posebne vrste osebnih podatkov se ne sme hraniti izven varovanih prostorov.

29. člen

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

30. člen

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

31. člen

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

VIII. VAROVANJE SISTEMSKÉ IN APLIKATIVNO PROGRAMSKÉ RAČUNALNIŠKE OPREME

32. člen

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

33. člen

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



34. člen

- (1) Vsebine na nosilcih podatkov na mrežnih strežnikih in lokalnih delovnih postajah, kjer se nahajajo osebni podatki, se morajo redno preverjati zaradi potencialne prisotnosti računalniških virusov in drugih oblik zlonamerne kode. V primeru odkritja virusa se ta odpravi s strani ustrezne strokovne službe oziroma pristojne osebe, zadolžene za delovanje računalniškega informacijskega sistema, obenem pa se skuša ugotovi tudi vzrok pojava virusa.
- (2) Vsi osebni podatki in programska oprema, ki so namenjeni uporabi v računalniškem informacijskem sistemu in prispejo v zavod na medijih za prenos računalniških podatkov ali preko telekomunikacijskih kanalov, morajo biti pred uporabo preverjeni glede prisotnosti računalniških virusov.

35. člen

- (1) Zaposleni ne smejo inštalirati programske opreme brez odobritve osebe, zadolžene za delovanje računalniškega informacijskega sistema. Prav tako ne smejo odnašati programske opreme iz zavoda brez odobritve odgovorne osebe zavoda ali vodje organizacijske enote in vednosti osebe, zadolžene za delovanje računalniškega informacijskega sistema.

36. člen

- (1) Dostop do podatkov in uporaba sistemske in aplikativno programske opreme se varuje s sistemom gesel za avtorizacijo in identifikacijo uporabnikov programske opreme in podatkov. Vsak uporabnik ima svoje geslo za dostopanje do posameznih elektronskih storitev. Posojanje gesel in uporaba skupinskih gesel je prepovedana.
- (2) Pri generiranju oziroma določanju gesel je treba spoštovati naslednja pravila:
 - gesla morajo imeti minimalno 8 znakov ali več, v kolikor je to določeno za posamezno uporabniško rešitev;
 - gesla ne smejo vsebovati smiselnih alfanumeričnih zaporedij znakov;
 - gesla morajo biti kvalitetna (ustrezne dolžine, velike in male črke, številke, lahko tudi vsebujejo posebne znake);
 - gesla naj ne bodo ciklična in naj se ne ponavljajo iz predhodnih obdobj;
 - dobro je uveljaviti redno spreminjanje gesel (vsaj na 6 mesecev);
 - začetna gesla je dobro ob prvi prijavi spremeniti;
 - gesla, ki jih je general zunanji dobavitelj, je potrebno takoj spremeniti ob prvi uporabi v produkcijskem okolju;
 - uporabniško ime ne sme kazati posebnih pooblastil uporabnika.
- (3) Pri ravnanju z gesli je treba obvezno spoštovati sledeče napotke:
 - pooblaščen oseba, ki dodeljuje gesla, jih mora obravnavati zaupno, preprečiti mora možnost nepooblaščenega vpogleda in jih posredovati na varen način;
 - uporabnikom mora biti omogočeno, da kadarkoli spremenijo svoje uporabniško geslo;
 - geslo ne sme biti nikdar prikazano na zaslonu;
 - gesla morajo biti obvezno shranjena v šifrirani obliki;
 - vsak uporabnik mora imeti svoje uporabniško ime in geslo izključno za osebno rabo;
 - geslo je potrebno hraniti na način, ki drugi osebi popolnoma onemogoči možnost vpogleda;
 - vsak uporabnik je odgovoren za zaupnost gesla in ga ne sme v nobenem primeru zaupati drugi osebi;
 - v nobenem primeru uporabnik ne sme izdati gesla nadrejenemu, podrejenemu ali osebi, ki ga nadomešča, ali IT osebju;
 - v primeru razkritja gesla ali suma razkritja gesla mora to nemudoma sporočiti pooblaščen osebi za dodeljevanje gesel.



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

37. člen

- (1) Za potrebe restavriranja računalniškega sistema ob okvarah in ob drugih izjemnih situacijah se redno izdelujejo varnostne kopije podatkov.
- (2) Varnostne kopije podatkov se hranijo zaklenjene v zavarovanih ognjevarnih omarah, zaščitene pred poplavami in elektromagnetnimi motnjami.

IX. UKREPANJE OB SUMU KRŠITVE VARSTVA OSEBNIH PODATKOV

38. člen

- (1) Zaposleni so dolžni o aktivnostih, ki so povezane z odkrivanjem, nepooblaščenih dostopov ali uničenjem podatkov, zlonamerni ali nepooblaščeni uporabi, prilaščanju, spreminjanju ali poškodovanju naprav takoj obvestiti pooblaščeno osebo, sami pa poskušajo takšno aktivnost preprečiti.
- (2) Kršitev varstva osebnih podatkov pomeni kršitev varnosti, ki povzroči nenamerno ali nezakonito uničenje, izgubo, spremembo, nepooblaščeno razkritje ali dostop do osebnih podatkov, ki so poslani, shranjeni ali kako drugače obdelani. Kršitev je lahko storjena nehote (npr. iz malomarnosti) ali pa je načrtovana oziroma naklepna. Na splošno taka kršitev pomeni varnostni incident, ki ogroža zaupnost, celovitost in dostopnost osebnih podatkov.
- (3) Zaposleni so dolžni pri svojem delu spremljati in biti pozorni na morebitne varnostne incidente ter v skladu s tem pravilnikom ustrezno ravnati.

39. člen

- (1) Nemudoma, ko zaposleni zasledijo, da se je v zavodu zgodil varnostni incident, morajo nujno o tem obvestiti nadrejenega delavca oziroma vodstvo zavoda.
- (2) Vodstvo mora najprej izvedeti, kaj se je zgodilo, oceniti, kakšne so potencialne škodljive posledice za pravice in svoboščine posameznikov in sprejeti ustrezne ukrepe za odpravo posledic ali vsaj zmanjšanje tveganj. Priporočljivo je, da se vodstvo za pripravo ocene verjetnosti in resnosti posledic za pravice in svoboščine posameznih zaposlenih posvetuje s pooblaščenim osebo za varstvo podatkov.
- (3) V primeru, da vodstvo zavoda oceni, da bo zaradi incidenta nastalo tveganje za pravice in svoboščine posameznikov, mora informacijskega pooblaščenca o tem obvestiti brez odlašanja, najkasneje pa v 72 urah po zaznani kršitvi. V primeru, da se je incident zgodil v zvezi s podatki, pri katerih je zavod v vlogi obdelovalca, mora o kršitvi obvestiti upravljavca v najkrajšem možnem času po zaznani kršitvi.



- (4) Za prijavo se uporabi obrazec, ki vsebuje vsaj naslednje informacije, kot to zahteva Splošna uredba:
- opis vrste kršitve, kategorije in približno število posameznikov, na katere se nanašajo osebni podatki, vrste in približno število evidenc osebnih podatkov;
 - kontaktne podatke pooblaščenice osebe za varstvo podatkov;
 - opis verjetnih posledic kršitve varstva osebnih podatkov;
 - opis ukrepov, ki jih je upravljavec sprejel ali pa predvidenih ukrepov za ublažitev tveganj za kršitve.

40. člen

- (1) Za obveščanje Informacijskega pooblaščenca o kršitvah varstva osebnih podatkov po 33. členu Splošne uredbe je pristojna odgovorna oseba zavoda.
- (2) Zavod lahko s posebnim aktom podrobneje predpiše ravnanje in ukrepe v primerih kršitve varstva osebnih podatkov.

X. ODGOVORNOST ZA IZVAJANJE VARNOSTNIH UKREPOV IN POSTOPKOV

41. člen

- (1) Za izvajanje postopkov in ukrepov za zavarovanje osebnih podatkov so odgovorni vsi zaposleni v zavodu kot tudi zunanji izvajalci, ki imajo s podjetjem podpisan dogovor o sodelovanju.
- (2) Nadzor nad izvajanjem postopkov in ukrepov, določenih s tem pravilnikom, opravlja pooblaščenica oseba zavoda.

42. člen

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

43. člen

- (1) V primeru kršitev določil tega pravilnika, je zaposleni odškodninsko odgovoren zavodu za škodo, ki bi nastala zavodu oziroma fizičnim ali pravnim osebam, s katerimi zavod sodeluje.
- (2) Kršitev določil pravilnika predstavlja hujšo kršitev delovnih obveznosti po pogodbi o zaposlitvi oziroma bistveno kršitev druge pogodbe, zaradi katere lahko zavod odpove pogodbo o zaposlitvi oziroma drugo pogodbo, ki je podlaga za opravljanje dela v zavodu.
- (3) Kršitev določil pravilnika ima lahko za posledico kazensko, prekrškovno in/ali odškodninsko odgovornost zaposlenega oziroma osebe, ki krši ta pravilnik.



XI. KONČNE DOLOČBE

44. člen

- (1) S pravilnikom se seznanijo vsi zaposleni v zavodu. Pravilnik se objavi na oglasni deski in na intranetu / internetni strani zavoda ter se pošlje vsem zaposlenim preko elektronske pošte.
- (2) Z dnem, ko je sprejet ta pravilnik, preneha veljati obstoječi Pravilnik o varstvu osebnih podatkov.
- (3) Ta pravilnik prične veljati in se začne uporabljati z dnem objave na oglasni deski.

V Luciji, dne 10. 10. 2023

JZ ŠPORTNI IN MLADINSKI EPI CENTER PIRAN
Direktor : Matjaž Ukmar

