**Osnovna šola**
**Franca Rozmana - Staneta**
Kersnikova 10, 2000 MARIBOR
tel.: (02) 2504300, 2504306, fax.: (02) 2504311
info@osfrsmb.si, ***http://www.osfrsmb.si***

Davčna številka.: 25901010
Podračun pri UJP: 01270-6030667458

Štev. zadeve: 6000-1/2022-2
Datum: 17. 2. 2022

# P R A V I L N I K

## O VARSTVU OSEBNIH PODATKOV Z NAVODILI ZA RAVNANJE IN UKREPANJE V PRIMERU KRŠITVE VARSTVA OSEBNIH PODATKOV NA

## OSNOVNI ŠOLA FRANCA ROZMANA – STANETA MARIBOR IN NA PODRUŽNIČNI ŠOLI IVANA CANKARJA KOŠAKI

**Osnovna šola**
**Franca Rozmana - Staneta**
Kersnikova 10, 2000 MARIBOR
tel.: (02) 2504301, fax.: (02) 2504311
info@osfrsmb.si, https://www.osfrsmb.si

Davčna št.: 25901010
Podračun pri UJP: 01270-6030667458

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 veljavnega zakona, ki ureja varstvo osebnih podatkov, izdaja OŠ Franca Rozmana – Staneta, Kersnikova 10, 2000 Maribor (v nadaljevanju: »organizacija«), ki jo zastopa v. d. ravnateljice Katja Pregl (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 organizaciji z namenom, da se prepreči slučajno ali namerno nepooblaščeno uničevanje podatkov, njihovo spremembo ali izgubo, kakor tudi nepooblaščen dostop, obdelava, uporaba ali posredovanje osebnih podatkov.

(2) Odgovorna oseba organizacije, vodstvo, zaposleni, delavci oziroma vse osebe, ki so vključene v delovni proces organizacije na podlagi pogodbe o zaposlitvi ali drugega pogodbenega temelja, ki pri svojem delu v organizaciji obdelujejo in uporabljajo osebne in/ali zaupne podatke in/ali se seznanjajo s poslovno skrivnostjo organizacije, 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. **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;
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;
3. **Nosilec podatkov** pomeni vse vrste sredstev, na katerih so zapisani ali posneti podatki (listine, akti, gradiva, spisi, računalniška oprema vključno s magnetni, optični ali drugi računalniški mediji, fotokopije, zvočno in slikovno gradivo, mikrofilmi, naprave za prenos podatkov, ipd.);
4. **Obdelava** pomeni vsako dejanje ali niz dejanj, ki se izvaja v zvezi z osebnimi podatki ali nizi osebnih podatkov z avtomatiziranimi sredstvi ali brez njih, kot je zbiranje, beleženje, urejanje, strukturiranje, shranjevanje, prilagajanje ali spreminjanje, priklic, vpogled, uporaba, razkritje s posredovanjem, razširjanje ali drugačno omogočanje dostopa, prilagajanje ali kombiniranje, omejevanje, izbris ali uničenje;

5. **Obdelovalec** pomeni fizično ali pravno osebo, javni organ, agencijo ali drugo telo, ki obdeluje osebne podatke v imenu upravljavca;
6. **Osebni podatki** pomeni katero koli informacijo v zvezi z določenim ali določljivim posameznikom (v nadaljnjem besedilu: 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 nanašajo osebni podatki 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 z obdelavo osebnih podatkov, ki se nanašajo nanj;
10. **Tretja oseba** pomeni fizično ali pravno osebo, javni organ, agencijo ali telo, ki ni posameznik, na katerega se nanašajo osebni podatki, upravljavec, obdelovalec in osebe, ki so pooblaščene za obdelavo osebnih podatkov pod neposrednim vodstvom upravljavca ali obdelovalca;
11. **Uporabnik** pomeni fizično ali pravno osebo, javni organ, agencijo ali drugo telo, ki so mu bili osebni podatki razkriti, ne glede na to, ali je tretja oseba ali ne. Vendar pa se 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, 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 organizaciji 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 njegovih osebnih podatkov v enega ali več določenih namenov;
- obdelava je potrebna za izvajanje pogodbe, katere pogodbena 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, 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 členom 13. in 14. 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 organizacije dobiti potrditev, ali se v zvezi z njim obdelujejo osebni podatki, in kadar je temu tako, mu organizacija 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 organizacije je dolžna poskrbeti za to, da so posamezniki na primeren način, ki je skladen z zahtevami Splošne uredbe, obveščeni o pravicah, ki so opredeljene v prejšnjem členu tega pravilnika. Prav tako odgovorna oseba poskrbi za enotno kontaktno točko, na katero se lahko obrnejo in z organizacijo komunicirajo posamezniki pri uveljavljanju svojih pravic.

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

- Zahtevajo lahko informacije o tem, ali ima organizacija 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 organizacije imajo o njih ter preverijo, ali jih organizacija obdeluje zakonito.
- Zahtevajo lahko popravke osebnih podatkov, kot je popravek 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 podatki obdelujejo na podlagi zakonitega interesa (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 organizacija obdeluje njihove osebne podatke za namene neposrednega trženja.

- Zahtevajo lahko omejitev obdelave osebnih podatkov, kar pomeni prekinitev obdelave osebnih podatkov o njih, na primer, če želijo, da organizacija 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 organizacija prenehali obdelovati njihove osebne podatke za namene, ki so jih prvotno sprejeli, razen če organizacija nima druge zakonite pravne podlage za to, da podatke še naprej zakonito obdeluje.

(3) Če želi posameznik uveljavljati katero koli od prej navedenih pravic, lahko pošlje zahtevek pooblaščeni osebi za varstvo podatkov po elektronski pošti na naslov: dpo@datainfo.si ali z redno pošto na naslov DATAINFO.SI, d.o.o., Tržaška 85, 2000 Maribor. Po prejemu zahteve v zvezi s pravicami posameznika, se posamezniku informacije o ukrepih organizacije zagotovijo brez nepotrebnega odlašanja, v vsakem primeru pa v enem mesecu po prejemu zahteve. Ta rok se lahko po potrebi podaljša za največ dva dodatna meseca ob upoštevanju kompleksnosti in števila zahtev. Organizacija obvesti posameznika, na katerega se nanašajo osebni podatki, o vsakem takem podaljšanju v enem mesecu po prejemu zahteve skupaj z razlogi za zamudo

(4) Dostop do lastnih osebnih podatkov in uveljavljanje pravic je za posameznika brezplačno. Kadar so zahteve posameznika, na katerega se nanašajo osebni podatki, očitno neutemeljene ali pretirane zlasti ker se ponavljajo, lahko upravljavec zaračuna razumno pristojbino, pri čemer upošteva upravne stroške posredovanja informacij ali sporočila ali izvajanja zahtevanega ukrepa, ali zavrne ukrepanje v zvezi z zahtevo.

(5) V primeru uveljavljanja pravic iz tega naslova bo organizacija 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.

**6. člen**

(1) Osebni podatki se na zahtevo uporabnika posredujejo samo tistim uporabnikom, ki se izkažejo z ustrezno zakonsko podlago ali s pisno zahtevo oziroma privolitvijo posameznika, na katerega se podatki nanašajo.

(2) Osebni podatki se po uradni dolžnosti posredujejo samo tistim uporabnikom, ki imajo ustrezno zakonsko podlago.

(3) Posredovanje osebnih podatkov iz prvega odstavka tega člena lahko uporabnik zahteva pisno ali ustno. Ob vložitvi pisne vloge mora uporabnik jasno navesti določbo zakona, ki ga pooblašča za pridobitev osebnih podatkov, ali pa mora k vlogi priložiti pisno zahtevo oziroma privolitev posameznika, na katerega se podatki nanašajo. Če uporabnik zahteva posredovanje osebnih podatkov ustno, sme odgovorna oseba ali pooblaščeni obdelovalec v primeru dvoma o obstoju

pisne zahteve oziroma privolitve posameznika, na katerega se podatki nanašajo, od uporabnika zahtevati, naj predloži pisno zahtevo oziroma privolitev posameznika.

(4) Posredovanje posebnih vrst osebnih podatkov na osnovi prvega odstavka tega člena lahko uporabnik zahteva le pisno. Pisna vloga mora biti po vsebini enaka pisni vlogi iz prejšnjega odstavka.

(5) Osebni podatki, ki se posredujejo uporabniku v fizični obliki, morajo biti posredovani v ovojnici. Ovojnica mora tudi zagotoviti, da odprtja ovojnice in seznanitve z njeno vsebino ni mogoče opraviti brez vidne sledi odpiranja ovojnice.

(6) Osebne podatke je dovoljeno prenašati z informacijskimi, telekomunikacijskimi in drugimi sredstvi le ob izvajanju postopkov in ukrepov, ki nepooblaščenim preprečujejo prilaščanje ali uničenje podatkov ter neupravičeno seznanjanje z njihovo vsebino.

(7) Posebne vrste osebnih podatkov se v fizični obliki pošilja naslovnikom 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. člen**

(1) Delavec, ki je zadolžen za sprejem in evidenco pošte v organizaciji, mora izročiti poštno pošiljko z osebnimi podatki direktno posamezniku ali službi, na katero je ta pošiljka naslovljena. Ravno tako odpira in pregleduje vse poštne pošiljke in pošiljke naslovljene na organizacijo, ki na drug način prispejo v organizacijo (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 organizacijo 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, sme odpirati pošiljke, naslovljene na naslov organizacije in obenem delavca, razen v primerih, ko je iz ovojnice razvidno, da je delavcu treba pismo vročiti osebno.

**8. člen**

(1) Organizacija vodi evidenco dejavnosti obdelave v skladu z določbami 30. člena Splošne uredbe.

(2) Zaposleni, ki obdelujejo osebne podatke, morajo biti seznanjeni z evidenco dejavnosti obdelave. Vpogled v evidenco dejavnosti obdelave je omogočena 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 osebnih podatkov, prenosi osebnih podatkov v tretjo državo, rok hrambe, ter splošen opis tehničnih in organizacijskih varnostnih ukrepov.

**9. 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 organizacije.

(2) V tem primeru se izvede ocena učinka v zvezi z varstvom podatkov, kot jo predvideva 35. člen Splošne uredbe.

**10. člen**

(1) Za namene dokumentiranja aktivnosti in obveščanja javnosti o delu in dogodkih v organizaciji, kot so prireditve, srečanja, tekmovanja, izobraževanja in podobno, lahko organizacija tak dogodek delno ali v celoti snema oziroma fotografira in izdelani material objavi na spletnih straneh, tiskovinah in družabnih omrežjih organizacije.

(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.

**11. člen**

(1) Organizacija redno obvešča zaposlene o pomenu in novostih s področja varstva osebnih podatkov in izvaja izobraževanja s tega področja ter s področja informacijske varnosti.

(1) Organizacija 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 organizacijo 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 organizacije (npr. na prenosnikih, pametnih telefonih, USB ključkih ipd.),
- politiko čiste mize,
- druge prakse, politike in primere s področja varstva osebnih podatkov.

(2) Organizacija redno izvaja varnostne politike na področju informacijske varnosti, ki so opredeljene v internih aktih in jih najmanj enkrat letno preverja.

**12. člen**

(1) Odgovorna oseba organizacije imenuje pooblaščeno osebo za varstvo podatkov s sklepom ali na drug primeren način (npr. s sklenitvijo pogodbe) in poskrbi za objavo informacij o pooblaščeni osebi za varstvo podatkov na spletni strani organizacije.

(2) Pooblaščena oseba za varstvo podatkov se imenuje na podlagi poklicnih odlik in zlasti strokovnega znanja o zakonodaji in praksi na področju varstva osebnih podatkov ter zmožnosti za izpolnjevanje nalog iz 39. člena Splošne uredbe, veljavne zakonodaje s področja varstva osebnih podatkov.

(3) Organizacija zagotavlja, da je pooblaščena oseba za varstvo podatkov ustrezno in pravočasno vključena v vse zadeve v zvezi z varstvom osebnih podatkov, ter da so ji zagotovljena ustrezna sredstva, potrebna za kvalitetno opravljanje svojih nalog, ter da ji je omogočen dostop do osebnih podatkov in dejanj obdelave.

(4) Organizacija zagotovi, da pooblaščena oseba za varstvo podatkov pri opravljanju svojih nalog ne prejema nobenih navodil. Pooblaščena oseba za varstvo podatkov ne sme biti razrešena ali kaznovana zaradi opravljanja svojih nalog. Pooblaščena oseba za varstvo podatkov neposredno poroča odgovorni osebi organizacije.

**13. člen**

(1) Posamezniki, na katere se nanašajo osebni podatki, lahko s pooblaščeno osebo za varstvo podatkov stopijo v stik glede vseh vprašanj, povezanih z obdelavo njihovih osebnih podatkov, in uresničevanjem njihovih pravic na podlagi Splošne uredbe.

**14. člen**

(1) Pooblaščena oseba za varstvo podatkov je pri opravljanju svojih nalog dolžna varovati kot skrivnost vse podatke s katerimi se seznani pri opravljanju svojih nalog v skladu z veljavno nacionalno zakonodajo.

**15. člen**

(1) Pooblaščena oseba za varstvo podatkov ima vsaj naslednje naloge:
- obveščanje organizacije, 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 organizacije s Splošno uredbo in nacionalnim pravom, vključno z dodeljevanjem nalog v zvezi z varstvom osebnih podatkov, osveščanjem in usposabljanjem zaposlenih v organizaciji, 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 členom 35 Splošne uredbe;
- sodelovanje z nadzornim organom;
- delovanje kot kontaktna točka za nadzorni organ pri vprašanjih v zvezi z obdelavo, vključno s predhodnim posvetovanjem iz člena 36 Splošne uredbe, in, kjer je ustrezno, posvetovanje glede katere koli druge zadeve.

(2) Pooblaščena oseba za varstvo podatkov pri opravljanju svojih nalog upošteva tveganje, povezano z dejanji obdelave, ter naravo, obseg, okoliščine in namene obdelave.

## III. POGODBENA OBDELAVA OSEBNIH PODATKOV

### 16. člen

(1) Z vsako zunanjo pravno ali fizično osebo, ki opravlja posamezna opravila v zvezi z obdelavo osebnih podatkov za organizacijo, se sklene pisna pogodba ali drug pravni akt v skladu s pravom Unije ali pravom države članice, ki določa obveznosti obdelovalca do upravljavca, v katerem so določeni vsebina in trajanje obdelave, narava in namen obdelave, vrsta osebnih podatkov, kategorije posameznikov, na katere se nanašajo osebni podatki, ter obveznosti in pravice upravljavca. Vsebino takšne pogodbe natančneje določa člen 28 Splošne uredbe.

(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 organizacije in osebnih podatkov ne smejo obdelovati ali drugače uporabljati za noben drug namen.

(4) Pooblaščena pravna ali fizična oseba, ki za organizacijo opravlja dogovorjene storitve izven prostorov upravljavca, mora imeti vsaj enako strog način zagotavljanja varnosti osebnih podatkov, kakor ga določa ta pravilnik.

## IV. BRISANJE PODATKOV

### 17. člen

(1) Osebni podatki se lahko obdelujejo le toliko časa, kolikor je določen rok hrambe oziroma dokler obstaja pravna podlaga iz člena 6 Splošne uredbe. Po preteku roka hranjenja se osebni podatki zbrišejo, uničijo, blokirajo ali anonimizirajo, razen če zakon ali drug akt ne določa drugače.

(2) Osebne podatke, ki jih organizacija obdeluje na osnovi pogodbenega odnosa s posameznikom, organizacija hrani za obdobje, ki je potrebno za izvršitev pogodbe in še 6 let po njenem prenehanju, razen v primerih, ko pride med posameznikom in organizacijo do spora v zvezi s pogodbo. V takem primeru hrani organizacija podatke še 6 let po pravnomočnosti sodne odločbe, arbitraže ali poravnave ali, če sodnega spora ni bilo, pa 6 let od dneva mirne razrešitve spora.

(3) Tiste osebne podatke, ki jih organizacija obdeluje na podlagi osebne privolite posameznika ali zakonitega interesa, bo organizacija hranila do preklica te privolitve oziroma do zahteve do izbrisa. Po prejemu preklica ali zahteve za izbris se podatki izbrišejo brez nepotrebnega odlašanja, v vsakem primeru pa 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 čemer se obvesti posameznika. Organizacija lahko te podatke izbriše tudi pred preklicem, kadar je bil dosežen namen obdelave osebnih podatkov ali če tako določa zakon.

(4) Izjemoma lahko organizacija 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 zgodovinskoraziskovalni nameni ali statistični nameni,

- izvajanje ali obramba pravnih zahtevkov.

**18. 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 (npr. matrice, izračune in grafikone, skice, poskusne oziroma neuspešne izpise ipd.).

(3) Prepovedano je odmetavati odpadne nosilce podatkov z osebnimi 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.

## V. INFORMACIJSKO VARNOSTNA POLITIKA

**19. člen**

(1) Zaposleni uporabljajo različno informacijsko tehnologijo (računalnik, telefon, tablica in druge elektronske naprave) ter različne elektronske storitve (dostop do interneta, elektronska pošta, dostop do oblaka, skupni imeniki in mape ter drugo programsko opremo oziroma storitve), ki jim jo dodeli delodajalec, izključno za službene namene.

(2) V omejenem obsegu in razumnih mejah se s strani organizacije dodeljena informacijska tehnologija in elektronske storitve lahko uporabljajo tudi v zasebne namene. Pri tem morajo delavci varovati ugled organizacije, tehnologij in storitev pa se ne sme uporabljati za neprimerne ali žaljive namene. Vodstvo lahko po lastni presoji delavcu kadarkoli prepove uporabo v zasebne namene.

**20. člen**

(1) Dostop do svetovnega spleta je omogočen zaposlenim za njihovo delo, izobraževanje in informiranje.

(2) Zaposleni v organizaciji 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 organa javnega zavoda (IP naslov).

(3) Posredovanje službenih elektronskih naslovov na zunanje spletne strežnike za namene prijave določene storitve (npr. pošte, prijava na izobraževanja ipd.) ni dovoljeno, razen če je povezano s poslovnim procesom organizacije.

(4) V omrežju organizacije se na zahtevo odgovorne osebe lahko izdeluje statistika obiskanih spletnih strani, ki mora biti anonimizirana in ni za javno objavo. Statistika se lahko uporablja izključno za načrtovanje in varovanje informacijskega sistema.

(5) Vodstvo organizacije lahko zaradi zagotavljanja informacijske varnosti in razpoložljivosti informacijskih virov ter zaradi preprečevanja kršitev s posebno odredbo odredi blokado določenih spletnih strani. Blokado dostopa do določenih spletnih strani izvede oseba, zadolžena za delovanje

računalniškega informacijskega sistema, na podlagi pisne odredbe odgovorne osebe. O blokadi se obvesti vse zaposlene po elektronski pošti.

**21. člen**

(1) Službena elektronska pošta se v organizaciji lahko uporablja kot orodje za komunikacijo s starši, učenci/dijaki , strankami, zaposlenimi in zunanjimi izvajalci. Pri tem se morajo delavci držati ne le etičnih in moralnih norm, temveč tudi bontona. Pošiljatelj se mora zavedati, da se vsako sporočilo s službenega elektronskega naslova pri prejemniku lahko šteje kot mnenje organizacije, v katerem je pošiljatelj zaposlen.

(2) Zaposleni po elektronski pošti ne smejo pošiljati verižnih pisem in obsežnih datotek (glasba, filmi, predstve, zagonske datoteke in skripte ipd.), v kolikor niso namenjene delu.

(3) Zaposleni svojega službenega elektronskega naslova ne smejo uporabljati v trženjske namene in z 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 organizacije, razen če to ni povezano s potrebami delovnega mesta.

(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 izključno za namene komuniciranja med zaposlenimi na osnovi dovoljenja odgovorne osebe dovoljeno uporabljati zasebno elektronsko pošto.

(7) Mobilnim telefonom, ki so v lasti organizacije in v uporabi posameznega delavca, se ne sme slediti. V mobilne naprave se ne sme namestiti naprav oziroma aplikacije za sledenje.

**22. člen**

(1) Oddaljeni dostop do informacijskega sistema organizacije je dovoljen le na podlagi odobrene metode z ustrezno ravnjo 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 delovnem mestu.

(2) Za uveljavitev oddaljenega varnega dostopa je na strojni opremi zagotovljena prepoznava ustrezne programske opreme, ki omogoča zaščito končne točke pred internetnimi grožnjami. Za zagotavljanje zaupnosti se ves promet iz končne točke oddaljenega omrežja do omrežja organizacije šifrira.

**23. člen**

(1) Oseba, zadolžena za delovanje informacijskega sistema v organizaciji, lahko na posebej utemeljeno pisno zahtevo pooblaščene osebe v prisotnosti tri članske 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 v podobnih izrednih primerih) vpogleda v informacijsko tehnologije (npr. v računalnik) ali druge elektronske storitve (npr. v elektronsko pošto) delavca le, če je to nujno potrebno za izpolnjevanje zakonskih obvez organizacije oziroma za vodenje delovnega procesa.

(2) Vpogled opravi 3 članska komisija, ki jo vsakokrat imenuje pooblaščena oseba organizacije. 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) 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 organizacija, lahko organizacija zahteva od operaterjev telekomunikacijskih storitev ali vzdrževalca hišne centrale le takrat, kadar pride med organizacijo in zaposlenim do kakršnegakoli 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 e-pošti.

**24. člen**

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

**25. člen**

(1) Delavec lahko za namene opravljanja dela poleg službene opreme uporablja svojo zasebno opremo in druge tehnične naprave (predvsem mobilni telefon), 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 z 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.

## VI. VAROVANJE PROSTOROV IN RAČUNALNIŠKE OPREME

### 26. 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 nepooblaščene 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 organizacije.

(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 nepooblaščene 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, učilnice, predavalnice, jedilnice) morajo biti stalno zaklenjeni v omarah. Posebne vrste osebnih podatkov se ne sme hraniti izven varovanih prostorov.

**27. 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 nepooblaščene osebe seznanile z osebnim podatki posameznika za katere organizacija nima pravne podlage za njihovo objavo.

**28. člen**

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

**29. 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).

## VII. VAROVANJE SISTEMSKE IN APLIKATIVNO PROGRAMSKE RAČUNALNIŠKE OPREME

**30. člen**

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

**31. člen**

(1) Popravljanje, spreminjanje in dopolnjevanje sistemske in aplikativne programske opreme je dovoljeno samo na podlagi odobritve odgovorne osebe ali od nje pooblaščene osebe. Izvajajo ga lahko samo pooblaščeni servis ali vzdrževalec, ki ima z organizacijo sklenjeno ustrezno pogodbo. Izvajalci morajo izvedene spremembe in dopolnitve sistemske 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.

**32. člen**

(1) Vsebine na nosilcih podatkov na mrežnih strežnikih in lokalnih delovnih postajah, kjer se nahajajo osebni podatki, se mora 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 organizacijo na medijih za prenos računalniških podatkov ali preko telekomunikacijskih kanalov, morajo biti pred uporabo preverjeni glede prisotnosti računalniških virusov.

**33. 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 organizacije brez odobritve odgovorne osebe organizacije ali vodje organizacijske enote in vednosti osebe, zadolžene za delovanje računalniškega informacijskega sistema.

**34. 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 biti dolžine minimalno 8 znakov ali ustrezno daljša, v kolikor je to določeno za posamezno uporabniško rešitev;
- gesla ne smejo vsebovati smiselnih alfanumeričnih zaporedij znakov (npr. 123456, abcdefg...);
- gesla morajo biti kvalitetna (ustrezne dolžine, velike in male črke, številke, lahko tudi posebni znaki);
- gesla naj ne bodo ciklična in naj se ne ponavljajo iz predhodnih obdobij;
- uveljavljeno mora biti obvezno redno spreminjanje gesel (najmanj na 6 mesecev);
- začetna gesla se ob prvi prijavi spremenijo;
- gesla, ki jih je generiral 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 napotke:
- pooblaščena 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;
- gesla se ne smejo lepiti na monitor ali shranjevati pod tipkovnico;
- 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 pooblaščeni 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 organizacije. Po vsaki takšni uporabi se določi nova vsebina gesel.

**35. 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.

## VIII. UKREPANJE OB SUMU NEPOOBLAŠČENEGA DOSTOPA

**36. člen**

(1) Zaposleni so dolžni o aktivnostih, ki so povezane z odkrivanjem, nepooblaščenim dostopom ali uničenjem podatkov, zlonamerni ali nepooblaščeni uporabi, prilaščanju, spreminjanju ali poškodovanju 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 ta 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 tem pravilnikom ustrezno ravnati.

**37. člen**

(1) Nemudoma, ko zaposleni zasledijo, da se je v organizaciji zgodil varnostni incident, morajo nujno o tem obvestiti nadrejenega delavca oziroma vodstvo organizacije.

(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 posameznikov posvetuje s pooblaščeno osebo za varstvo podatkov.

(3) V primeru, da vodstvo organizacije oceni, da bo zaradi incidenta nastalo tveganje za pravice in svoboščine posameznikov, mora o tem obvestiti Informacijskega pooblaščenca brez odlašanja, najkasneje pa v 72 urah po zaznani kršitvi. V primeru, da se je incident zgodil v zvezi s podatki, pri katerih je organizacija v vlogi obdelovalca, mora o kršitvi obvestiti upravljavca v najkrajšem možnem času po zaznani kršitvi.

(4) Za prijavo se uporabi obrazec, ki ga priporoča Informacijski pooblaščenec in predstavlja del dokumentacije organizacije. Ob prijavi mora Informacijski pooblaščenec pridobiti 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 pooblaščene 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.

**38. člen**

(1) Za obveščanje Informacijskega poblaščenca o kršitvah varstva osebnih podatkov po 33. členu Splošne uredbe je odgovorna odgovorna oseba organizacije.

(2) Podrobneje so ukrepi ob sumu nepooblaščenega dostopa do osebnih podatkov urejeni v dokumentu: Navodila za ravnanje in ukrepanje v primeru kršitve varstva osebnih podatkov.

## IX. ODGOVORNOST ZA IZVAJANJE VARNOSTNIH UKREPOV IN POSTOPKOV

**39. člen**

(1) Za izvajanje postopkov in ukrepov za zavarovanje osebnih podatkov so odgovorni vsi zaposleni v organizaciji, kot tudi zunanji izvajalci, ki imajo s podjetjem podpisan dogovor o sodelovanju.

(2) Nadzor nad izvajanjem postopkov in ukrepov, določenih s tem pravilnikom, opravlja odgovorna oseba organizacije, ali iz njene strani pooblaščena oseba.

**40. člen**

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

**41. člen**

(1) V primeru kršitev določil tega pravilnika, je zaposleni odškodninsko odgovoren organizaciji za škodo, ki bi nastala organizaciji oziroma fizičnim ali pravnim osebam, s katerimi organizacija sodeluje.

(2) Kršitev določil pravilnika predstavlja hujšo kršitev delovnih obveznosti po pogodbi o zaposlitvi oziroma bistveno kršitev druge pogodbe, zaradi katere lahko organizacija odpove pogodbo o zaposlitvi oziroma drugo pogodbo, ki je podlaga za opravljanje dela pri za ali pri organizaciji.

(3) Kršitev določil pravilnika ima lahko za posledico kazensko, prekrškovno in/ali odškodninsko odgovornost zaposlenega oziroma osebe, ki krši ta pravilnik.

## X. KONČNE DOLOČBE

### 42. člen

(1) S pravilnikom so seznanjeni zaposleni v organizaciji, tako da se pravilnik objavi na oglasni deski in/ali na intranetu organizacije ter se pošlje vsem zaposlenim preko elektronske pošte. S vsebino pravilnika se lahko zaposleni v organizaciji kadarkoli seznanijo z zahtevo, ki jo podajo odgovorni osebi organizacije.

(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 23. 2. 2022

V Mariboru, dne 16. 2. 2022

Podpis odgovorne osebe:

OSNOVNA ŠOLA FRANCA ROZMANA - STANETA
Maribor, Kersnikova ulica 10
2
Maribor

Katja Pregl,
v. d. ravnateljice

**Osnovna šola**
**Franca Rozmana - Staneta**
Kersnikova 10, 2000 MARIBOR
tel.: (02) 2504300, 2504306, fax.: (02) 2504311
info@osfrsmb.si, *http://www.osfrsmb.si*

Davčna številka.: 25901010
Podračun pri UJP: 01270-6030667458

# Navodila za ravnanje in ukrepanje v primeru kršitve varstva osebnih podatkov

V skladu s Pravilnikom o varstvu osebnih podatkov organizacije in v smislu izvajanja 33. in 34. člena Splošne Uredbe (GDPR) pripravljamo navodila za ravnanje in ukrepanje v primeru kršitve varstva osebnih podatkov.[1]

Kot upravljavec ali obdelovalec mora organizacija za dokazovanje skladnosti s Splošno Uredbo (GDPR) imeti vzpostavljen učinkovit sistem za zaznavanje in sporočanje v primeru kršitev. Ta navodila predstavljajo del omenjenega sistema. Najpomembnejša obveza iz Splošne Uredbe (GDPR)nalaga, da je organizacija dolžna obvestiti nadzorni organ (Informacijskega pooblaščenca) o zaznanih kršitvah varstva osebnih podatkov, če je (vsaj) verjetno, da bi bile s kršitvijo ogrožene pravice in svoboščine posameznikov. **Obvestilo je treba podati takoj po zaznani kršitvi, najkasneje pa v 72 urah**.

## Kaj je kršitev varstva osebnih podatkov?

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 ta kršitev **pomeni varnostni incident**, ki ogroža zaupnost, celovitost in dostopnost osebnih podatkov.

Primeri, ki se obravnavajo kot varnostni incident, kot jih navaja Informacijski pooblaščenec, so npr.:

- dostop do osebnih podatkov s strani nepooblaščene osebe;
- posredovanje osebnih podatkov napačnemu naslovniku;
- izguba ali kraja računalniške opreme (prenosni računalnik, USB ključek, itd., …), ki vsebuje osebne podatke;
- nepooblaščeno uničenje baz z osebnimi podatki;
- sprememba osebnih podatkov brez potrebnega dovoljenja;
- izguba dostopa do osebnih podatkov (izguba gesla; izguba opreme, ki omogoča dešifriranje; nepooblaščena namestitev šifrirnega programa, ki onemogoča dostop do podatkov, t.i. »izsiljevalski virus«) idr.

Zaposleni so dolžni pri svojem delu spremljati in biti pozorni na morebitne varnostne incidente in v skladu z pravilnikom in temi navodili ustrezno ravnati.

## Obveščanje vodstva organizacije

Nemudoma, ko zaposleni zasledijo, da se je v organizaciji zgodil varnostni incident, morajo nujno o tem **obvestiti nadrejenega delavca oziroma vodstvo organizacije**.

Priporočamo, da ima organizacija s strani vodstva določeno **kontaktno osebo**, ki bo v primeru varnostnega incidenta najprej dokumentirala kršitev varstva osebnih podatkov, nato skupaj z vodstvom evidentirala nadaljnje nujne ukrepe, obvestila ali se posvetovala s Pooblaščeno osebo za

[1] Pri pripravi navodil smo upoštevali informacije Informacijskega pooblaščenca RS na spletni strani: https://www.ip-rs.si/zakonodaja/reforma-evropskega-zakonodajnega-okvira-za-varstvo-osebnih-podatkov/kljucna-podrocja-uredbe/prijava-krsitev/

Osnovna šola
Franca Rozmana - Staneta
Kersnikova 10, 2000 MARIBOR
tel.: (02) 2504300, 2504306, fax.: (02) 2504311
info@osfrsmb.si, *http://www.osfrsmb.si*

Davčna številka.: 25901010
Podračun pri UJP: 01270-6030667458

varstvo podatkov če je ta imenovana, ter izvajala nadaljnje korake vključno s prijavo kršitve Informacijskemu pooblaščenca.

Kontaktna oseba za vse primere kršitve varstva osebnih podatkov v organizaciji je: Katja Pregl, v. d. ravnateljice

### Obveščanje Pooblaščene osebe za varstvo podatkov

V primeru, da je organizacija imenovala Pooblaščeno osebo za varstvo podatkov (v nadaljevanju: » pooblaščena oseba«), jo mora vodstvo o zaznani kršitvi nemudoma obvestiti na dpo@datainfo.si Vodstvo v primeru, da mora organizacija imeti imenovano Pooblaščeno osebo za varstvo podatkov, nemudoma **Pooblaščeni osebi pošlje obvestilo o zaznani kršitvi** . V skladu s Splošno Uredbo (GDPR) pooblaščena oseba namreč sodeluje z nadzornim organom (Informacijskim pooblaščencem) ter deluje kot kontaktna točka za nadzorni organ pri vprašanjih v zvezi z obdelavo.

### POMEMBNO: Kako pravilno obvestiti pooblaščeno osebo o domnevni kršitvi varstva podatkov?

Informacijski pooblaščenec predlaga dve možnosti:

- prva možnost je, da pooblaščeno osebo obvestite priporočeno po pošti.
- druga možnost pa je obvestitev preko elektronske pošte. V tem primeru je potrebno vsebino/priponko elektronskega sporočila šifrirati in nato posredovati geslo v ločenem elektronskem sporočilu.

Pooblaščena oseba organizaciji pomaga izdelati **oceno verjetnosti in resnosti** posledic za pravice in svoboščine posameznikov. Verjetnost je povezana z možnostjo nastanka posledic, resnost pa s škodo, ki jo kršitev lahko povzroči posameznikom.

V primeru, da organizacija nima imenovane Pooblaščene osebe, vseeno priporočamo, da se vodstvo organizacije obrne po strokovno pomoč, predvsem zaradi ustrezne priprave ocene verjetnosti in resnosti posledic za pravice in svoboščine posameznikov, npr. tako da na dpo@datainfo.si pošlje sporočilo o zaznani kršitvi.

Od ocene je odvisno, ali bo treba o kršitvi obvestiti Informacijskega pooblaščenca. Če je verjetno, da bo nastalo tveganje za pravice in svoboščine posameznikov, mora organizacija o tem obvestiti Informacijskega pooblaščenca. Če ni verjetno, da bo nastalo tveganje za pravice in svoboščine posameznikov, obveščanje ni potrebno.

Za **pripravo ocene mora** upravljavec 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.

### Obvestilo Informacijskemu pooblaščencu

Upravljavec mora o kršitvi obvestiti Informacijskega pooblaščenca **brez odlašanja, najkasneje pa v 72 urah** po zaznani kršitvi. V primeru, da ste v organizaciji v vlogi obdelovalca, morate o kršitvi obvestiti upravljavca v najkrajšem možnem času po zaznani kršitvi.

**Osnovna šola**
**Franca Rozmana - Staneta**
Kersnikova 10, 2000 MARIBOR
tel.: (02) 2504300, 2504306, fax.: (02) 2504311
info@osfrsmb.si, *http://www.osfrsmb.si*

Davčna številka.: 25901010
Podračun pri UJP: 01270-6030667458

V predvidenem času 72 ur včasih ni mogoče zagotoviti vseh potrebnih informacij o incidentu, kot to zahteva Splošna Uredba (GDPR), zato lahko upravljavec Informacijskemu pooblaščencu obvestilo o kršitvah posreduje po fazah, vendar brez odlašanja. Od upravljavca se pričakuje, da bo svoje obveznosti v zvezi s preiskovanjem varnostnih incidentov izvedel prioritetno in hitro. Ne glede na to, je treba v roku 72 ur podati vsaj informacijo o zaznani kršitvi, izsledki notranje preiskave pa se lahko posredujejo kasneje. Upravljavci naj razlog za zamudo pri podaji popolnega obvestila o kršitvah posebej obrazložijo.

Pri Informacijskem pooblaščencu so pripravili **neobvezen obrazec za podajo obvestila o kršitvi**, ki je dostopen na naslednji povezavi: https://www.ip-rs.si/zakonodaja/reforma-evropskega-zakonodajnega-okvira-za-varstvo-osebnih-podatkov/kljucna-podrocja-uredbe/prijava-krsitev-varnosti/#c1955 Omenjen obrazec pa je priložen tudi kot priloga temu navodilu.

Obrazec izpolnite v največji možni meri, pomembno je, da ob prijavi Informacijski pooblaščenec pridobi vsaj naslednje informacije, kot to zahteva Splošna Uredba (GDPR):

- opis vrste kršitve, kategorije in približno število posameznikov, na katere se nanašajo osebni podatki, vrste in približno število evidenc osebnih podatkov.
- kontaktne podatke pooblaščene 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.

**Obvestilo posameznikom**

Kadar je verjetno, da kršitev varstva osebnih podatkov povzroči **veliko tveganje za pravice in svoboščine posameznikov**, Splošna Uredba (GDPR) zahteva, da upravljavec o kršitvi neposredno obvesti zadevne posameznike in da to stori brez odlašanja.

Za obveščanje posameznikov Splošna Uredba (GDPR) postavlja standard **'veliko tveganje'**, ki je višja stopnja ogroženosti pravic in svoboščin posameznikov, kot velja za uradno obvestilo nadzornemu organu. Kot je že bilo poudarjeno je treba stopnjo tveganja ocenjevati v vsakem primeru posebej, upoštevaje verjetnost nastanka posledic in resnost teh posledic. Treba je zlasti upoštevati, da je potreba po obveščanju večja, če obstaja velika verjetnost neugodnih posledic, pri tem pa lahko **ukrep obveščanja zmanjša tveganje** za nastanek teh posledic. Cilj in smoter zahteve po obveščanju posameznikov o kršitvi je prav v možnosti zmanjševanja tveganj za nastanek neugodnih posledic. Na ta način se torej pomaga posameznikom preprečiti neugodne posledice, ki bi sicer lahko pomenile tudi premoženjsko ali nepremoženjsko škodo (upravljavec je lahko odškodninsko odgovoren poleg sankcij, ki jih lahko izreče nadzorni organ).

Informacijski pooblaščenec navaja kot primer, nepooblaščen dostop do zdravstvenih podatkov pacientov določene **bolnišnice,** kjer je že zaradi **narave podatkov** tveganje za pravice in svoboščine pacientov visoko in bo verjetno treba posameznike o kršitvi obvestiti.

V vsakem primeru je smiselno, da se o ukrepu obveščanja posameznikov posvetujete s pooblaščeno osebo.

**Osnovna šola**
**Franca Rozmana - Staneta**
Kersnikova 10, 2000 MARIBOR
tel.: (02) 2504300, 2504306, fax.: (02) 2504311
info@osfrsmb.si, ***http://www.osfrsmb.si***

Davčna številka.: 25901010
Podračun pri UJP: 01270-6030667458

Samo **obvestilo posameznikom** mora v jasnem in preprostem jeziku vsebovati vsaj:

- kontaktne podatke pooblaščene osebe za varstvo osebnih podatkov (ali druge kontaktne osebe), pri kateri lahko posameznik prejme več informacij oziroma pojasnil o kršitvi,
- informacijo o posledicah,
- informacijo o sprejetih ali predlaganih ukrepih in kjer je to mogoče, dodatna pojasnila posameznikom, kako lahko sami zmanjšajo tveganje za nastanek posledic.

### Vpis v seznam obvestil o kršitvah

Priporoča se, da organizacija vodi seznam obvestil o kršitvah. Pri Informacijskem pooblaščencu priporočajo vodenje dokumentacije tudi o tistih zaznanih kršitvah, ki niso bile sporočene nadzornemu organu ali posameznikom.

Seznam obvestil o kršitvah naj vsebuje vsaj naslednje podatke:

- datum kršitve
- datum seznanitve s kršitvijo
- datum obvestila Informacijskemu pooblaščencu (v kolikor je bilo uradno obvestilo potrebno)
- interna številka dokumenta / obvestila
- kratek opis kršitve
- opis ukrepov

### Neukrepanje ob zaznani kršitvi

Informacijski pooblaščenec navaja, da neukrepanje ob zaznavi kršitev varstva osebnih podatkov in neobveščanje nadzornega organa, ko je to potrebno, predstavlja samostojno kršitev po Splošni Uredbi (GDPR), za katero je predpisana globa do 10 milijonov evrov oz. do 2% letnega prometa. Upravljavca lahko doleti kazen za kršitev in kazen, če ni izpolnil zahteve po obveščanju. Temu se dodajo tudi popravljalni ukrepi, ki jih lahko nadzorni organ naloži upravljavcu skladno s členom 58 Splošne Uredbe (GDPR). Zato morate zagotoviti učinkovit interni postopek javljanja kršitev, ki bo omogočil pravočasno zaznavo in sporočanje kršitev z vsemi potrebnimi informacijami o varnostnem incidentu.

V Mariboru, 16. 2. 2022

v. d. ravnateljice:
Katja Pregl

OSNOVNA ŠOLA FRANCA ROZMANA - STANETA Maribor, Kersnikova ulica 10 2 Maribor

**Osnovna šola**
**Franca Rozmana - Staneta**
Kersnikova 10, 2000 MARIBOR
tel.: (02) 2504301, fax.: (02) 2504311
info@osfrsmb.si, https://www.osfrsmb.si

Davčna št.: 25901010
Podračun pri UJP: 01270-6030667458

# OBVESTILO ZAPOSLENIM GLEDE OBDELAVE OSEBNIH PODATKOV V KADROVSKIH EVIDENCAH DELODAJALCA

Obvestilo je izdano na podlagi določb prvega odstavka 13. člena Splošne uredba (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 (Splošna uredba o varstvu podatkov; GDPR).

**Upravljavec zbirke osebnih podatkov:**
OSNOVNA ŠOLA FRANCA ROZMANA – STANETA, Kersnikova 10, 2000 MARIBOR

**Za pooblaščeno osebo za varstvo podatkov (ang. DPO) smo imenovali:**
V skladu z določilom 37. člena Splošne uredbe smo za pooblaščeno osebo za varstvo podatkov imenovali družbo:

*DATAINFO.SI, d.o.o.*
*Tržaška cesta 85, SI-2000 Maribor*
*www.datainfo.si*
*e-pošta: dpo@datainfo.si*
*telefon: +386 (0) 2 620 4 300*

**Namen obdelave osebnih podatkov:** Vaše osebne podatke bomo kot delodajalec obdelovali za namene izvrševanje pravic in obveznosti pogodbenih strank iz delovnega razmerja, obračun in izplačilo plače, prijav v obvezna socialna in druga zavarovanja, vodenja obveznih evidenc po veljavni zakonodaji in druge zakonite namene iz delovnega razmerja. Vaše osebne podatke v omejenem obsegu prav tako obdelujemo v skladu z vašimi podanimi privolitvami.

Kadar uporabljate delovna sredstva delodajalca (internet, elektronska pošta, mrežni tiskalniki, stacionarna in mobilna telefonija, magnetne/RFID kartice za odpiranje vrat in druga elektronska oprema in storitve …) se prav tako obdelujejo vaši osebni podatki, kot so: čas tiskanja in število strani tiskanja, IP številka, čas prijave, število klicev, prihod na delo ipd. Naštete navedene osebne podatke namreč obdelujemo za namen izvajanja pravic in obveznosti iz delovnega razmerja na podlagi veljavne zakonodaje.
**Pravna podlaga za obdelavo osebnih podatkov:**

Vaše osebne podatke obdelujemo:

- na podlagi zakonodaje, ki ureja delovna razmerja in druge relevantne zakonodaje,
- na podlagi sklenjene pogodbe o zaposlitvi in
- na podlagi vaše privolitve, v kolikor ste takšno privolitev podali.

**Uporabniki ali kategorije uporabnikov osebnih podatkov:**
Podatke lahko posredujemo tretjim osebam, katerim smo to dolžni posredovati po veljavni zakonodaji, kot je Zavod za pokojninsko in invalidsko zavarovanje Slovenije, Finančna uprava RS, Zavod za zdravstveno zavarovanje Slovenije, banka za nakazilo plače, inšpekcijske službe RS v primeru nadzora,

policija ipd. Podatke lahko posredujemo tudi tretjim osebam, s katerimi smo sklenili ustrezno pogodbo o pogodbeni obdelavi in varovanju podatkov in zaupnosti, kot so računovodski servisi, dobavitelji programske opreme, vzdrževalci informacijske tehnologije, kadrovske agencije, pravni, davčni in poslovni svetovalci ipd. Več informacij o tem lahko dobite pri vodstvu delodajalca.

**Informacije o prenosih osebnih podatkov v tretjo državo ali mednarodno organizacijo:**
Podatki se ne prenašajo v tretje države ali mednarodne organizacije.

Pravice zaposlenega pri delodajalcu:
V skladu z zakonodajo lahko zahtevate dostop do lastnih osebnih podatkov, popravek ali izbris osebnih podatkov, omejitev obdelave, imate pravico do ugovora o obdelavi ter pravico do prenosljivosti podatkov. Za vsa vprašanja v zvezi z obdelavo in varstvom osebnih podatkov se lahko obrnete na vodstvo delodajalca. Vsa pojasnila boste prejeli brezplačno.

Dodatne informacije o obdelavi osebnih podatkov najdete v Evidenci dejavnosti obdelave in Politiki varstva osebnih podatkov, objavljeni na spletni strani: info@osfrsmb.si. Če imate kakršnakoli vprašanja v zvezi z obdelavo vaših osebnih podatkov, se lahko vedno obrnete na nas preko elektronske pošte na naslov info@osfrsmb.si, preko telefonske številke 02 250 43 01 ali osebno pri tajnici VIZ. Lahko se obrnete tudi na pooblaščeno osebo za varstvo podatkov na naslovu: dpo@datainfo.si

V primeru, da menite, da so vaše pravice kršene, se lahko za zaščito ali pomoč obrnete na nadzorni organ oz. na informacijskega pooblaščenca. Povezava na: https://www.ip-rs.si/zakonodaja/reforma-evropskega-zakonodajnega-okvira-za-varstvo-osebnih-podatkov/kljucna-podrocja-uredbe/prijava-krsitev-varnosti/

Kraj, datum:
Maribor, 16. 2. 2022

OSNOVNA ŠOLA FRANCA ROZMANA - STANETA Maribor, Kersnikova ulica 10 1 Maribor

Katja Pregl,
v. d. ravnateljice