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 Avditorij Portorož-Portorose (v nadaljevanju: organizacija), ki jo zastopa direktorica Dragica Petrovič (v nadaljevanju: odgovorna oseba)

PRAVILNIK
o varstvu osebnih podatkov

I. SPLOŠNE DOLOČBE

1. člen

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.

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 z 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

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.

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.

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.

O obdelavi osebnih podatkov mora biti posameznik obveščen v skladu z določbo 13. in 14. člena oziroma mu morajo biti predstavljene pravice iz 15. in nasldnjih členov Splošne uredbe.

4. člen

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

Odgovorna oseba organizacije 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 obrnejo in z organizacijo komunicirajo posamezniki pri uveljavljanju svojih pravic.

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 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 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 organizacija njihove osebne podatke za namene neposrednega trženja.
- Zahtevajo lahko omejitev obdelave vaših 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 to stori zakonito.

Če želi posameznik uveljavljati katero koli od prej navedenih pravic, lahko pošlje zahtevek po elektronski pošti na info@avditorij ali z redno pošto na naslov Avditorij Portorož, senčna pot 8A, 6320 PORTOROŽ .

Dostop do lastnih osebnih podatkov in uveljavljene pravic je za posameznika brezplačno, vendar lahko organizacija zaračuna razumno plačilo. Če je posameznikova zahteva za dostop očitno neutemeljena ali pretirana, lahko v takšnem primeru tudi zavrne zahtevo.

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.

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

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.

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

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 jih predloži.

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.

Osebni podatki, ki se posredujejo uporabniku v fizični obliki, morajo biti posredovani v ovojnici, ki ne omogoča, da bi bila ob normalni svetlobi ali pri osvetlitvi ovojnice z običajno lučjo vidna vsebina ovojnice. Ovojnica mora tudi zagotoviti, da odprtja ovojnice in seznanitve z njeno vsebino ni mogoče opraviti brez vidne sledi odpiranja ovojnice.

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.

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

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.

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.

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

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

Zaposleni, ki obdelujejo osebne podatke, morajo biti seznanjeni evidenco dejavnosti obdelave, vpogled v evidenco dejavnosti obdelave je omogočana vsakemu zaposlenemu na zahtevo.

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, prenosi osebnih podatkov v tretjo državo, rok hrambe, splošen opis tehničnih in organizacijskih varnostnih ukrepov, podatek o lokaciji, obliki podatka, in dostop do evidence – informacijska podpora.

9. člen

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.

V tem primeru se izvede ocena učinka v zvezi z varstvom podatkov, kot jo predvideva 35. člen GDPR.

10. člen

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.

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.

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

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

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.

Organizacija 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

12. člen

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 na spletni strani organizacije.

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.

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.

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

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

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

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.

Pooblaščena oseba 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

16. člen

Z vsako zunanjo pravno ali fizično osebo, ki opravlja posamezna opravila v zvezi z obdelavo osebnih podatkov za organizacijo, 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.

Obdelovalci so tudi zunanji sodelavci, ki vzdržujejo strojno in programsko opremo ter izdelujejo in instalirajo novo strojno ali programsko opremo, v kolikor imajo pri svojem delu dostop do osebnih podatkov.

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.

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.

V. BRISANJE PODATKOV

17. člen

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

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 organizcija podatke še 6 let po pravnomočnosti sodne odločbe, arbitraže ali poravnave ali, če sodnega spora ni bilo, 6 let od dneva mirne razrešrešitve spora.

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 najkasneje v 15 dneh. Organizacija lahko te podatke izbriše tudi pred preklicem, kadar je bil dosežen namen obdelave osebnih podatkov ali če tako določa zakon.

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 zgodovinskoraziskovalne nameni ali statistični nameni, izvajanje ali obramba pravnih zahtevkov.

18. člen

Za brisanje podatkov iz nosilcev podatkov se uporabi takšna metoda brisanja, da je nemogoča restavracija vseh ali dela brisanih podatkov.

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.).

Prepovedano je odmetavati odpadne nosilce podatkov z osebnimi podatki v koše za smeti.

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

19. člen

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 druga programska oprema oziroma storitve), ki jim jo dodeli delodajalec, izključno za službene namene.

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, tehnologije 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

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

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).

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

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.

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

Službena elektronska pošta se v organizaciji lahko uporablja kot orodje za komunikacijo s posamezniki, 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 razloži kot mnenje organizacije, v katerem je pošiljatelj zaposlen.

Zaposleni po elektronski pošti ne smejo pošiljati verižnih pisem in obsežnih datotek (glasba, filmi, predstve, zagonske datoteke in skripte ipd.), razen, če so namenjene delu.

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.

Zaposleni morajo biti previdni pri odpiranju elektronske pošte s priponkami neznanih pošiljateljev. Če sumijo, da gre za nezaželeno pošto, ki bi lahko bila škodljiva, naj je ne odpirajo, temveč naj o tem obvestijo pristojno osebo, zadolženo za delovanje računalniškega informacijskega sistema.

Zaposleni nikakor ne smejo pošiljati posebnih vrst osebnih podatkov ali gesel po elektronski pošti razen v ustrezno akreditiranih sistemih, oziroma mora biti podatkom med prenosom zagotovljena njihova nečitljivost, tako da so šifrirani in zavarovani z geslom.

Uporaba zasebne elektronske pošte (npr. Gmail, Yahoo, ipd.) za službene namene je prepovedana, saj potencialno predstavlja neupravičeno obdelavo osebnh podatkov. Izjemoma je izključno za namene komuniciranja med zaposlenimi na osnovi dovoljenja odgovorne osebe dovoljeno uporabljati zasebno elektronsko pošto.

Mobilnim telefonom, ki so v lasti organizacije in v uporabi posameznega delavca, se ne sme slediti in v ta namen v te mobilne naprave ne sme namestiti naprav oziroma aplikacije za sledenje.

22. člen

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 praznega zaslona. Po končanem delu se je treba obvezno odjaviti iz sistema in zagotoviti, da katerikoli podatki in sledi ne ostanejo na delovni postaji.

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

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 podobni izredni primeri) 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.

Vpogled opravi tri 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.

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.

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.

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

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

25. člen

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.

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.

VII. VAROVANJE PROSTOROV IN RAČUNALNIŠKE OPREME

26. člen

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.

Kot varovani prostor 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.

Dostop do varovanih prostorov je mogoč le v rednem delovnem času, izven tega časa pa samo na podlagi dovoljenja odgovorne osebe organizacije.

Ključi varovanih prostorov se uporabljajo in hranijo v skladu s hišnim redom. Ključi se ne puščajo v ključavnici v vratih od zunanje strani.

Varovani prostori ne smejo ostajati nenadzorovani, oziroma se morajo zaklepati ob odsotnosti delavcev, ki jih nadzorujejo.

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).

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).

Zaposleni ne smejo puščati nosilcev osebnih podatkov na mizah v prisotnosti oseb, ki nimajo pravice vpogleda vanje.

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

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 in za katere organizacija nima pravne podlage za njihovo objavo oziroma obdelavo.

28. člen

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

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 SISTEMSKE IN APLIKATIVNO PROGRAMSKE RAČUNALNIŠKE OPREME

30. člen

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

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