

Pravilnik o varstvu osebnih podatkov v Javnem zavodu Ljubljanski grad Na podlagi določil Zakona o varstvu osebnih podatkov (Ur. l. RS, št. 163/2022 - ZVOP-2), Splošne uredbe o varstvu osebnih podatkov (Uredba EU 2016/679 Evropskega parlamenta in sveta z dne 27.3.2016, v nadaljevanju Splošna uredba) in Sklepa o ustanovitvi Javnega zavoda Ljubljanski grad (Ur. l. RS, št. 105/10 in naslednji) je direktorica Javnega zavoda Ljubljanski grad, Grajska planota 1, 1001 Ljubljana, Mateja Avbelj Valentan, sprejela naslednji

PRAVILNIK O VARSTVU OSEBNIH PODATKOV V JAVNEM ZAVODU LJUBLJANSKI GRAD

I. NAMEN PRAVILNIKA

1. člen

S tem pravilnikom se določajo organizacijski, tehnični in logično-tehnični postopki in ukrepi za zavarovanje osebnih podatkov z namenom, da se prepreči slučajno ali namerno nepooblaščen uničevanje podatkov, njihovo spremembo ali izgubo kakor tudi nepooblaščen dostop, obdelava, uporaba ali posredovanje osebnih podatkov.

Varovanje zasebnosti zaposlenih in uporabnikov storitev zavoda izvaja zavod v skladu z zakonom, da se preprečijo nezakoniti in neupravičeni posegi v zasebnost posameznika ter neupravičeni vpogledi ali posredovanje podatkov o posamezni osebi pri obdelavi, varovanju in uporabi le-teh.

2. člen

Zaposleni delavci in zunanji sodelavci, ki pri svojem delu obdelujejo in uporabljajo osebne podatke, morajo biti seznanjeni s Splošno uredbo o varstvu podatkov, z Zakonom o varstvu osebnih podatkov, s področno zakonodajo, ki ureja posamezno področje njihovega dela ter z vsebino tega pravilnika.

Določila tega pravilnika veljajo in se smiselno uporabljajo tudi za vse zunanje sodelavce, štipendiste podjetja in kandidate za sklenitev delovnega razmerja

Osebne podatke o zaposlenih in o uporabnikih storitev zavoda in njihovem poslovanju z zavodom so vsi zaposleni v zavodu zavezani varovati in jih brez njihovega dovoljenja ne smejo izdati ali sporočiti tretji osebi.

3. člen

Opis zbirk osebnih podatkov, katerih upravljavec je Javni zavod Ljubljanski grad, se vodi v evidenci dejavnosti obdelave (katalog osebnih podatkov), ki se vodi v skladu z določbami 30. člena Splošne uredbe. Evidenca dejavnosti obdelave je priloga predmetnega pravilnika.

Evidenca dejavnosti obdelave osebnih podatkov se za vsako zbirko osebnih podatkov zagotovi najkasneje 15 dni pred vzpostavitvijo zbirke osebnih podatkov. Evidenca dejavnosti obdelave se dopolnjuje ob vsaki spremembi vrste osebnih podatkov v posamezni zbirki.

Zaposleni, ki obdelujejo osebne podatke, morajo biti seznanjeni z evidenco dejavnosti obdelave, vpogled v evidenco dejavnosti obdelave pa je potrebno omogočiti tudi vsakomur, ki to zahteva.

Pooblaščen oseba za varstvo osebnih podatkov je dolžna voditi ažuren seznam, iz katerega je za vsako zbirko osebnih podatkov jasno razvidno, katera oseba je odgovorna za posamezno zbirko

Pravilnik o varstvu osebnih podatkov v Javnem zavodu Ljubljanski grad osebnih podatkov ter katere osebe lahko zaradi narave svojega dela obdelujejo osebne podatke, ki se nanašajo na posamezno zbirko osebnih podatkov.

V seznam se vpisujejo sledeči podatki:

- naziv evidence dejavnosti obdelave osebnih podatkov,
- osebno ime in delovno mesto osebe, ki je odgovorna za evidenco dejavnosti ter
- osebno ime in delovno mesto oseb, ki lahko zaradi narave njihovega dela obdelujejo osebne podatke, ki se nanašajo na evidence dejavnosti obdelave.

4. člen

V zavodu oziroma za potrebe zavoda se lahko obdelujejo le tisti osebni podatki, za katere obstaja ustrezna pravna podlaga po določbah ZVOP-2, GDPR ali druge zakonodaje. Če pravna podlaga za obdelavo ne obstaja, je potrebno osebne podatke takoj prenehati aktivno obdelovati in onemogočiti dostop do njih ter o neobstoju podlage obvestiti direktorico zavoda, ki določi nadaljnje ravnanje s takimi podatki.

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

Ukrepe za zagotovitev varnosti konkretnih (zbirk) osebnih podatkov, kot so med drugim psevdonimizacija in šifriranje, omejitve roka hrambe in dostopa, omejitve obdelave, omejitve namenov ipd., ter način izvedbe določi direktorica zavoda, skladno z zakonskimi določili.

II. OPREDELITEV POJMOV

5. člen

V tem pravilniku uporabljeni izrazi imajo naslednji pomen:

Osebni podatek - je katerakoli informacija, ki se nanaša na določenega ali določljivega posameznika, ne glede na obliko, v kateri je izražen;

Posameznik - je določena ali določljiva fizična oseba, na katero se nanaša osebni podatek; fizična oseba je določljiva, če se lahko neposredno ali posredno identificira, 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;

Zbirka osebnih podatkov - pomeni vsak strukturiran niz osebnih podatkov, ki so dostopni v skladu s posebnimi merili, niz pa je lahko centraliziran, decentraliziran ali razpršen na funkcionalni ali geografski podlagi;

Obdelava osebnih podatkov - 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;

Upravljevec osebnih podatkov - je zavod;

Obdelovalec - pomeni fizično ali pravno osebo, javni organ, agencijo ali drugo telo, ki obdeluje osebne podatke v imenu upravljavca;

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;

Nosilec podatkov - so 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, mikrofili, naprave za prenos podatkov, ipd.);

Kršitev varstva osebnih podatkov - pomeni kršitev varnosti, ki povzroči nenamerno ali nezakonito uničenje, izgubo, spremembo, nepooblaščen razkritje ali dostop do osebnih podatkov, ki so poslani, shranjeni ali kako drugače obdelani;

Privolitev - pomeni prostovoljen, konkreten, informiran in nedvoumen izraz volje posameznika, na katerega se nanašajo osebni podatki, s katerim je z izjavo ali jasnim pritrdilnim dejanjem izrazil soglasje za obdelavo svojih osebnih podatkov in sestavni del katere je ta pravilnik;

Zaposleni - pomeni osebe, ki imajo z družbo sklenjeno pogodbo o zaposlitvi, osebe, ki opravljajo delo v družbi kot dijaki ali študenti, osebe, ki opravljajo delo v družbi na podlagi pogodbe med družbo in njihovim delodajalcem, ki opravlja dejavnost zagotavljanja dela drugim delodajalcem;

Nadzorni organ pomeni neodvisen javni organ, ki ga ustanovi država članica. V Sloveniji je nadzorni organ Informacijski pooblaščenec.

Izrazi, katerih pomeni v tem pravilniku ni opredeljen, imajo pomen, kot je določen v Zakonu o varstvu osebnih podatkov in Splošni uredbi.

III. VARNOST OSEBNIH PODATKOV

6. člen

Varovanje osebnih podatkov zajema pravne, organizacijske in ustrezne logistično-tehnične postopke in ukrepe, s katerimi se:

- varujejo prostori, aparature in sistemska programska oprema,
- varuje aplikativna programska oprema, s katero se obdelujejo osebni podatki,
- zagotavlja varnost posredovanja in prenosa osebnih podatkov,
- onemogoča nepooblaščenim osebam dostop do naprav, na katerih se obdelujejo osebni podatki in do njihovih zbirk,
- preko vodenja dnevnika obdelave omogoča poznejše ugotavljanje, kdaj so bili posamezni osebni podatki vneseni v zbirko osebnih podatkov, uporabljeni ali drugače obdelani in kdo je osebne podatke vnesel, uporabil ali obdelal.

Dnevnik obdelave mora za dejanja obdelave vsebovati vrsto dejanja obdelave, datum in čas obdelave, identifikacijo osebe, ki je izvedla dejanje obdelave, ter identifikacijo uporabnikov osebnih podatkov, da je mogoče naknadno ugotoviti točno identiteto teh oseb. Dnevnik obdelave se uporablja le za izkazovanje zakonitosti obdelave ter izvajanje notranjega nadzora, izvajanje nadzorov ali drugih zakonsko določenih preverjanj s strani nadzornega organa ali drugih pristojnih

Pravilnik o varstvu osebnih podatkov v Javnem zavodu Ljubljanski grad organov, zagotavljanje celovitosti in varnosti osebnih podatkov ter za odpravljanje napak v delovanju informacijskega sistema ali obdelavi podatkov.

Upravljavca in obdelovalec nadzornemu organu ali drugemu zakonsko določenemu pristojnemu organu na njegovo zahtevo omogočita dostop do dnevnika obdelave.

Vsebina dnevnika obdelave se hrani dve leti od zaključka koledarskega leta, v katerem so bila zabeležena dejanja obdelave, če zakon ne določa drugače. Kadar je z oceno učinka ali analizo upoštevni tveganj ugotovljeno tveganje, ki ga je mogoče učinkovito upravljati s podaljšanjem roka hrambe, se sme dnevnik obdelave hraniti največ pet let od zaključka koledarskega leta, v katerem so bila zabeležena dejanja obdelave.

Zavod bo v času določanja sredstev obdelave kot tudi v času same obdelave izvajal ustrezne tehnične in organizacijske ukrepe, ki so oblikovani za učinkovito izvajanje načel varstva podatkov, ter v obdelavo vključil potrebne zaščitne ukrepe, da se izpolnijo zahteve te uredbe in zaščitijo pravice posameznikov, na katere se nanašajo osebni podatki.

Zavod bo izvedel ustrezne tehnične in organizacijske ukrepe, s katerimi bo zagotovil, da se privzeto obdelujejo samo osebni podatki, ki so potrebni za vsak poseben namen obdelave.

7. člen

Obdelava in varovanje občutljivih osebnih podatkov, med katere sodijo podatki o rasnem, narodnem ali narodnostnem poreklu, političnem, verskem ali filozofskem prepričanju, članstvu v sindikatu, zdravstvenem stanju, spolnem življenju, vpisu ali izbrisu v ali iz kazenske evidence ali evidenc in biometrične značilnosti, mora biti izvajana posebno vestno in skrbno.

IV. POOBLAŠČENA OSEBA ZA VARSTVO OSEBNIH PODATKOV

8. člen

Nadzor nad izvajanjem postopkov in ukrepov, določenih s tem pravilnikom, opravlja pooblaščenca oseba za varstvo osebnih podatkov, ki jo imenuje direktorica zavoda.

Naloge pooblaščenca osebe so:

- obveščanje in svetovanje zaposlenim glede izvajanja predmetnega pravilnika in veljavne zakonodaje s področja varstva osebnih podatkov,
- svetovanje direktorici družbe glede obveznosti in odgovornosti v skladu s predpisi s področja varstva osebnih podatkov ter glede ukrepov varovanja osebnih podatkov ter tveganjih in neskladnostih,
- spremljanje izvajanja tega pravilnika in njegove skladnosti z veljavno zakonodajo s področja varstva osebnih podatkov,
- sodelovanje z Informacijskim pooblaščencom,
- obveščanje Informacijskega pooblaščenca in posameznika glede kršitev varstva osebnih podatkov,
- delovanje kot kontaktna točka za posameznike, na katere se nanašajo osebni podatki,
- odločanje o zahtevah posameznikov glede njihovih pravic v zvezi z varstvom osebnih podatkov,
- vodenje evidenc dejavnosti obdelave,
- vodenje seznama odgovornih oseb za posamezno zbirko osebnih podatkov,
- vodenje evidence o vloženi zahtevi za uresničevanje pravic posameznika,
- vodenje evidence kršitev varstva osebnih podatkov,
- vodenje evidence posredovanja osebnih podatkov.

Pravilnik o varstvu osebnih podatkov v Javnem zavodu Ljubljanski grad
Kontaktne podatke pooblaščenih oseb za varstvo osebnih podatkov so objavljeni na spletni strani zavoda in v evidencah obdelave.

V. VAROVANJE SISTEMSKÉ IN APLIKATIVNE PROGRAMSKE RAČUNALNIŠKE OPREME TER PODATKOV, KI SE OBDELUJEJO Z RAČUNALNIŠKO OPREMO

9. člen

Prostori, kjer se nahajajo nosilci osebnih podatkov - vsak dokument, računalniški medij ali drug elektronski nosilec podatka na katerem so zapisani osebni podatki, morajo biti varovani z organizacijskimi, fizičnimi in tehničnimi ukrepi, ki onemogočajo nepooblaščenim osebam dostop do osebnih podatkov (v nadaljevanju: varovani prostori).

Ključni varovanih prostorov se uporabljajo in hranijo v skladu s hišnim redom. Ključni 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. Občutljivi osebni podatki se ne smejo hraniti izven varovanih prostorov.

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

Nosilci osebnih podatkov, ki se nahajajo izven zavarovanih prostorov (hodniki, skupni prostori) morajo biti stalno zaklenjeni.

Izven delovnega časa morajo biti nosilci osebnih podatkov shranjeni v ognjevarnih omarah. Računalniki in druga strojna oprema, na kateri se obdelujejo ali hranijo osebni podatki, morajo biti izven delovnega časa izklopljeni in fizično ali programsko zaklenjeni.

V delovnem času, ko delavci niso prisotni pri delovni mizi, morajo biti računalniki zaklenjeni z geslom, omare in predalniki z nosilci osebnih podatkov pa zaklenjeni.

Zaposleni morajo geslo na računalniku menjati redno in upoštevati dobro prakso za oblikovanje varnega gesla.

10. člen

Osebe, ki niso zaposlene v zavodu in osebe, ki ne delajo v prostorih zavoda, v varovane prostore ne smejo vstopati brez spremstva ali prisotnosti zaposlenega delavca. Delavec, ki dela v varovanih prostorih, mora vestno in skrbno nadzorovati prostor in ob zapustitvi prostora zakleniti prostor.

Dostop do računalniške programske opreme mora biti varovan na način, ki omogoča dostop samo določenim pooblaščenim delavcem in delavcem, ki za zavod po pogodbi opravljajo servisiranje računalniške in programske opreme. Določbe o varovanju osebnih podatkov so obvezna sestavina pogodb o servisiranju računalniške in programske opreme.

11. člen

Popravljanje, spreminjanje, dopolnjevanje varovanje in shranjevanje systemske in aplikativne programske opreme je dovoljeno samo na podlagi odobritve osebe zadolžene za naročanje servisiranja računalniške in programske opreme, izvajajo pa ga lahko samo pooblaščenih servis in organizacije oziroma njihovi delavci, ki imajo z zavodom sklenjeno ustrezno pogodbo.

Pravilnik o varstvu osebnih podatkov v Javnem zavodu Ljubljanski grad
Izvajalci morajo spremembe in dopolnitve systemske in aplikativne programske opreme ustrezno dokumentirati.

12. člen

Delavec, pooblaščen za obdelavo in ravnanje z osebnimi podatki na računalniku, mora biti v času servisiranja računalnika in programske opreme ves čas prisoten in mora nadzirati, da ne pride do nedopustnega ravnanja z osebnimi podatki ter da se ob morebitnem kopiranju osebnih podatkov, po prenehanju potrebe po kopiji, kopija uniči.

13. člen

Vsebina diskov mrežnega strežnika in lokalnih delovnih postaj, kjer se nahajajo osebni podatki, se preverja na prisotnost računalniških virusov v skladu z načrtom preverjanja, prav tako se za prisotnost računalniških virusov preverijo vsi v zavod prispeli računalniški zapisi.

14. člen

Dostop do podatkov prek aplikativne programske opreme mora biti varovan s sistemom gesel za avtorizacijo in identifikacijo uporabnikov programov in podatkov.

15. člen

Za potrebe restavriranja osebnih podatkov oziroma računalniškega sistema po okvarah ali izgubi podatkov iz drugih razlogov, mora delavec, ki vodi zbirke osebnih podatkov, redno izdelovati kopije vsebine zbirk osebnih podatkov, ki jih vodi.

Računalniške kopije vsebin zbirk osebnih podatkov na različnih drugih medijih se hranijo v zavarovanih zaklenjenih omarah odpornih proti ognju, poplavam in elektromagnetnim motnjam in v predpisanih klimatskih razmerah.

VI. STORITVE, KI JIH OPRAVLJAJO ZUNANJE PRAVNE ALI FIZIČNE OSEBE

16. člen

Zavod z vsako zunanjo pravno ali fizično osebo, ki opravlja posamezna opravila, ki so povezane ali se nanašajo na zbiranje, obdelavo, shranjevanje ali posredovanje osebnih podatkov (v nadaljevanju obdelovalec) sklene pisno pogodbo. Obvezna sestavina tovrstnih pogodb so pogoji in ukrepi za zagotovitev varstva osebnih podatkov ter njihovega zavarovanja, prav tako pa tudi vsebina in trajanje obdelave, narava in namen obdelave, vrsta osebnih podatkov, kategorije posameznikov, na katere se nanašajo osebni, ter obveznosti in pravice upravljavca.

Obdelovalci morajo biti pred obdelavo osebnih podatkov seznanjeni z določbami Zakona o varstvu osebnih podatkov, Splošne uredbe ter z vsebino tega pravilnika, kot tudi ostalimi pravilniki in akti zavoda, ki se nanašajo na varstvo osebnih podatkov, o čemer so dolžni podpisati izjavo kot dodatek k pogodbi za izvajanje del in nalog.

Obveznosti obdelovalca so, da:

- obdeluje podatke po dokumentiranih navodilih zavoda,
- zagotoviti, da so osebe, ki so pri njem pooblašcene za obdelavo osebnih podatkov, zavezane k zaupnosti ali jih k zaupnosti zavezuje ustrezen zakon,
- sprejme vse potrebne ukrepe za varnost obdelave,

- zavodu z ustreznimi tehničnimi in organizacijskimi ukrepi pomaga pri izpolnjevanju njegovih obveznosti glede uresničevanja pravic posameznika,
- zavodu pomaga pri izpolnjevanju obveznosti glede varstva osebnih podatkov.

Obdelovalec, ki za zavod opravlja dogovorjene storitve izven prostorov zavoda, mora imeti vsaj enako strog način varovanja osebnih podatkov, kakor ga predvideva ta pravilnik.

Obdelovalec mora po zaključku storitev v zvezi z obdelavo v skladu z odločitvijo zavoda izbrisati ali vrniti vse osebne podatke zavodu ter uničiti obstoječe kopije. Obdelovalec mora dati zavodu vse informacije, potrebne za dokazovanje izpolnjevanja obveznosti, omogočiti izvajanje revizij in pregledov ter ostalih zahtev v skladu s Splošno uredbo in Zakonom o varstvu osebnih podatkov.

VII. RAVNANJE Z OSEBNIMI PODATKI

17. člen

Delavec, ki je zadolžen za sprejem in vodenje evidence pošte, odpira in pregleduje poštno in druge pošiljke (v nadaljevanju: pošiljke), ki prispejo na zavod ne glede na način dostave. Pošiljke z osebnimi podatki se izročijo direktno posamezniku ali notranji organizacijski enoti, na katero je pošiljka naslovljena.

Delavec, ki je zadolžen za sprejem in vodenje evidence pošte, ne odpira pošiljk, kjer je označeno, da pošiljka vsebuje osebne podatke, pošiljk, na katerih je na ovojnici navedeno, da se vročijo osebno naslovniku, pošiljk, na katerih je navedeno osebno ime delavca brez označbe njegovega uradnega položaja in šele nato naslov zavoda, in tistih pošiljk, kjer iz označb na ovojnici izhaja, da se nanašajo na javni natečaj ali javni razpis.

18. člen

Pisemske pošiljke, ki vsebujejo osebne podatke, se pošiljajo naslovniku priporočeno ali po kurirju z oznako »zaupno« na pisemski ovojnici.

Ovojnica, v kateri se posredujejo osebni podatki, mora biti izdelana na takšen način, da odprtje ovojnice in seznanitve z njeno vsebino ni mogoče opraviti brez vidne sledi odpiranja ovojnice.

Obdelava občutljivih osebnih podatkov mora biti posebej označena in zavarovana.

Prenos osebnih podatkov prek telekomunikacijskih sredstev, elektronske pošte ali drugih elektronskih medijev izven prostorov zavoda mora biti zavarovan s postopki in ukrepi na način, ki nepooblaščenim osebam preprečuje prilaščanje, uničenje ali nedovoljeno seznanjanje z njihovo vsebino. Za zavarovanje osebnih podatkov prek telekomunikacijskih omrežij se uporabijo kriptografske metode in elektronski podpisi tako, da je zagotovljena nečitljivost podatkov med njihovim prenosom.

19. člen

Za vsako posredovanje osebnih podatkov mora upravičenec vložiti pisno vlogo, v kateri mora biti jasno navedena določba zakona, ki uporabnika pooblašča za pridobitev osebnih podatkov, ali mora biti k vlogi priložena pisna zahteva oziroma privolitev posameznika, na katerega se podatki nanašajo.

Pravilnik o varstvu osebnih podatkov v Javnem zavodu Ljubljanski grad
Nikoli se ne posredujejo originali dokumentov, razen v primeru pisne odredbe sodišča. Originalni dokument se mora v času odsotnosti nadomestiti s kopijo.

Pooblašcene osebe zunanjih institucij, katerim so bili posredovani osebni podatki, smejo take podatke uporabiti samo za namene, za katere so jim bili dani, in jih ne smejo razkriti tretjim osebam.

Zunanje institucije, katerim so bili osebni podatki posredovani, morajo zagotoviti enake ukrepe in postopke za varovanje osebnih podatkov kot veljajo v zavodu. Osebne podatke hranijo le do konca postopka, zaradi katerega so bili zbrani, po prenehanju razlogov pa se morajo podatki (uradno, komisijsko) uničiti.

Vsako posredovanje osebnih podatkov se v roku treh dni od dneva posredovanja sporoči osebi, na katero so se posredovani podatki nanašali, in se zabeleži v evidenco posredovanj, iz katere mora biti razvidno, kateri osebni podatki so bili posredovani, komu, kdaj in na kakšni podlagi.

VIII. PRAVICE POSAMEZNIKA

20. člen

Zavod s predmetnim pravilnikom vsem posameznikom, na katere se nanašajo osebni podatki, ki jih zavod obdeluje, zagotavlja uresničevanje njihovih pravic iz Uredbe.

Te pravice so:

- pravica do dostopa do osebnih podatkov,
- pravica do popravka,
- pravica do izbrisa (pravica do pozabe),
- pravica do omejitve obdelave,
- pravica do ugovora,
- pravica prenosljivosti podatkov,
- pravica do vložitve pritožbe pri Informacijskem pooblaščenču.

V primeru, ko se osebni podatki posameznika obdelujejo na podlagi njegovega izrecnega soglasja, lahko posameznik soglasje kadarkoli preklic. Preklic soglasja posameznik uveljavi pri pooblaščenca osebi za varstvo osebnih podatkov zavoda.

Posameznik lahko poda vlogo z zahtevo za uresničevanje pravic, navedenih v prvem odstavku tega člena, pisno na elektronski naslov kadrovska-služba@ljubljangrad.si, ali jo pošlje na naslov Grajska planota 1, 1001 Ljubljana ali jo poda ustno preko telefona na številki 01 306 42 40.

Pooblaščenca oseba za varstvo osebnih podatkov vzame v obravnavo vlogo posameznika iz tretjega odstavka tega člena brez nepotrebnega odlašanja, vendar najkasneje v roku 1 meseca od prejema vloge. Pooblaščenca oseba za varstvo osebnih podatkov posameznika obvesti ali je zahtevi ugodila oziroma v kolikor ji ni ugodila, razloge za zavrnitev. Prav tako pa mu sporoči sprejete ukrepe in ga informira o vseh pomembnih dejstvih, ki so vplivala na odločitev.

Rok iz prejšnjega odstavka se lahko po potrebi podaljša za največ dva dodatna meseca ob upoštevanju kompleksnosti in števila zahtev. Pooblaščenca oseba za varstvo osebnih podatkov bo obvestila posameznika o vsakem takem podaljšanju v enem mesecu po prejemu zahteve skupaj z razlogi za zamudo.

Kadar posameznik zahtevo iz drugega odstavka tega člena poda z elektronskimi sredstvi, se informacije zagotovijo z elektronskimi sredstvi, razen če posameznik ne zahteva drugače.

Če pooblaščenca oseba za varstvo osebnih podatkov presodi, da zahteva posameznika ni primerna za ukrepanje, bo posameznika brez odlašanja, najpozneje pa v enem mesecu po prejemu zahteve, obvestila o razlogih za neukrepanje ter o možnosti vložitve pritožbe pri nadzornem organu in možnosti uveljavljanja pravnih sredstev.

Šteje se, da je zahteva očitno neutemeljena ali pretirana, kadar posameznik, na katerega se nanašajo osebni podatki, zahtevo z bistveno enako vsebino naslovi na zavod več kot dvakrat v obdobju šestih mesecev.

Pooblaščenca oseba za varstvo osebnih podatkov vodi evidenco o vloženi zahtevah za uresničevanje pravic posameznika (v nadaljevanju evidenca o vloženi zahtevah), v katero vpisuje:

- ime in priimek posameznika,
- dan prejema vloge oziroma zahteve,
- vsebino zahteve,
- dan obvestitve posameznika o odločitvi in sprejetih ukrepih,
- v primeru zavrnitve oziroma neukrepanja razloge za tako odločitev,
- izvod zahteve in obvestila, ki je bilo poslano posamezniku,
- v primeru podaljšanja roka za odločitev, obvestilo, nov rok in razlogi za podaljšanje roka.

Do evidence o vloženi zahtevah ima dostop samo pooblaščenca oseba za varstvo osebnih podatkov. Pooblaščenca oseba za varstvo osebnih podatkov mora zagotoviti varno hranjenje evidence iz prejšnjega odstavka tega člena. Podatki v evidenci o vloženi zahtevah se hranijo do izpolnitve namena oziroma najdalj 5 let od vpisa v evidenco.

IX. HRAMBA IN ROK HRAMBE OSEBNIH PODATKOV

21. člen

Za hrambo zbirk osebnih podatkov so odgovorni zaposleni, ki so pooblaščenca za obdelavo zbirk osebnih podatkov.

Zbirke osebnih podatkov zaposlenih v zavodu (kadrovske evidence), se hranijo v zaklenjeni, vodotesni in ognjevarni omari v arhivskih prostorih službe za kadrovske in splošne zadeve. Druge zbirke osebnih podatkov, vodene v zavodu, se hranijo v arhivskih prostorih posameznih služb zavoda (organizacijskih enot zavoda).

Roki hranjenja zbirk osebnih podatkov se določijo za vsako zbirko osebnih podatkov v evidenci dejavnosti obdelave za vsako posamezno zbirko osebnih podatkov.

Zavod zbira in hrani osebne podatke le toliko časa, kolikor je potrebno, da se doseže namen, za katerega so se zbirali. Obdobje hrambe osebnih podatkov je odvisno od podlage obdelave in namena obdelave posamezne kategorije osebnih podatkov.

X. BRISANJE PODATKOV OZ. UNIČENJE NOSILCEV PODATKOV

22. člen

Po izpolnitvi namena obdelave ali po preteku roka hranjenja se osebni podatki zbršejo, uničijo, blokirajo ali anonimizirajo, če niso na podlagi zakona, ki ureja arhivsko gradivo in arhive, opredeljeni kot arhivsko gradivo, oziroma če zakon za posamezne vrste osebnih podatkov ne določa drugače.

Osebni podatki, ki se zbirajo na podlagi soglasja posameznika, se zбриšejo ali uničijo na podlagi njegovega izrecnega preklica soglasja.

Roki, po katerih se osebni podatki izbrišejo iz zbirke podatkov, so razvidni iz 7. točke kataloga zbirke osebnih podatkov.

Osebni podatki, vsebovani na klasičnih nosilcih (listine, kartoteke, seznam) se uničijo z uničenjem nosilcev. Nosilci se fizično uničijo (razrežejo) v prostorih zavoda pod nadzorom v ta namen imenovane komisije, ki o uničenju sestavi tudi ustrezen zapisnik.

Na enak način se uničuje pomožno gradivo (npr. matrice, izračune in grafikone, skice, poskusne oziroma neuspešne izpise).

Pri prenosu nosilcev osebnih podatkov na mesto uničenja je potrebno zagotoviti ustrezno zavarovanje tudi v času prenosa. Prepovedano je odmetavati odpadne nosilce podatkov z osebnimi podatki v koše za smeti.

Brisanje osebnih podatkov na računalniških medijih opravi za to pooblaščen oseba na način, po postopku in metodi, ki onemogoča restavriranje vseh ali dela brisanih podatkov.

Uničenje nosilcev in brisanje podatkov se mora izvajati tekoče in ažurno.

XI. UKREPANJE OB SUMU NEPOOBLAŠČENEGA DOSTOPA

23. člen

Zaposleni so dolžni o aktivnostih, ki so povezane z odkrivanjem ali nepooblaščenim uničenjem zaupnih podatkov, zlonamerni ali nepooblaščen uporabi, prilaščanju, spreminjanju ali poškodovanju takoj obvestiti pooblaščen osebo za varstvo osebnih podatkov ali direktorico, sami pa poskušajo takšno aktivnost preprečiti.

V primeru kršitve varstva osebnih podatkov bo zavod oziroma pooblaščen oseba za varstvo osebnih podatkov brez nepotrebnega odlašanja oziroma najpozneje v 72 urah po seznanitvi s kršitvijo, o kršitvi obvestil Informacijskega pooblaščenca, razen če ni verjetno, da bi bile s kršitvijo varstva osebnih podatkov ogrožene pravice in svoboščine posameznikov.

V primeru verjetnosti, da bo kršitev varstva osebnih podatkov povzročila veliko tveganje za pravice in svoboščine posameznikov, na katere se osebni podatki nanašajo, bo zavod oziroma pooblaščen oseba za varstvo osebnih podatkov brez nepotrebnega odlašanja sporočila posamezniku, da je prišlo do kršitve varstva osebnih podatkov in mu podala vse potrebne informacije skladno s 34. členom Uredbe.

Pooblaščen oseba za varstvo osebnih podatkov bo vsak primer kršitve varstva osebnih podatkov zabeležila v evidenco kršitev varstva osebnih podatkov.

Pooblaščen oseba za varstvo osebnih podatkov vodi evidenco kršitev varstva osebnih podatkov, v katero vpisuje:

- dan zaznave kršitve,
- opis kršitve in kršitelja, če je znan,
- opis verjetnih posledic kršitve varstva osebnih podatkov
- sprejeti ukrepi za ublažitev škodljivih učinkov kršitve,

- dan obvestitve Informacijskega pooblaščenca,
- dan obvestitve posameznika.

Do evidence kršitev varstva osebnih podatkov ima dostop pooblaščen osebna oseba za varstvo osebnih podatkov in direktorica zavoda. Pooblaščen osebna oseba za varstvo osebnih podatkov mora zagotoviti varno hranjenje evidence iz prejšnjega odstavka tega člena. Podatki v evidenci o vloženih zahtevah se hranijo do izpolnitve namena.

XII. ODGOVORNOST ZA IZVAJANJE VARNOSTNIH UKREPOV IN POSTOPKOV

24. člen

Delavec, ki bo nastopil delo na delovnem mestu, kjer se zbirajo, urejajo, obdelujejo, spreminjajo, shranjujejo, posredujejo ali uporabljajo osebni podatki ali nosilci osebnih podatkov, mora podpisati izjavo, ki ga zavezuje k varovanju osebnih podatkov kot poklicne skrivnosti in ga opozarja na posledice kršitve zaveze.

Iz podpisane izjave mora biti razvidno, da je podpisnik seznanjen z določbami tega pravilnika ter določbami Uredbe in Zakona o varstvu osebnih podatkov, izjava pa mora vsebovati tudi pouk o posledicah kršitve.

Dostop do osebnih podatkov imajo pooblaščen osebe, ki so podpisale izjavo iz 1. odstavka tega člena, vendar le v obsegu, ki je potreben za opravljanje njihovih delovnih nalog. Nihče ne sme dobiti osebnega podatka prej in v večjem obsegu, kot je to potrebno za opravljanje njegovih delovnih nalog.

Pooblaščen delavci in druge osebe, ki sodelujejo ali so sodelovale pri ravnanju z osebnimi podatki, in vse druge osebe, ki so zaradi narave svojega dela prišle v stik z osebnimi podatki, teh podatkov ne smejo sporočiti tretjim osebam, razen v primerih, določenih z zakonskimi predpisi, na podlagi katerih so zbrani, ali s soglasjem delavca, na katerega se nanašajo osebni podatki, niti jih ne smejo same uporabljati ali omogočiti, da bi jih uporabljale tretje osebe.

Obveza varovanja osebnih podatkov, s katerimi se delavec seznanja pri svojem delu v zavodu, traja tudi po prenehanju delovnega razmerja v zavodu.

25. člen

Nadzor nad izvajanjem postopkov in ukrepov, določenih s tem pravilnikom, opravlja pooblaščen osebna oseba za varstvo osebnih podatkov.

26. člen

Za kršitev določil iz prejšnjega člena so zaposleni disciplinsko odgovorni, ostali pa na temelju pogodbenih obveznosti.

Delavec stori lažjo kršitev delovne dolžnosti:

- če opusti vestno in skrbno nadzorovanje varovanih prostorov,
- če opusti ravnanja za preprečitev vpogleda v ali na nosilce osebnih podatkov,
- če ne uniči kopije osebnih podatkov,
- če ne vodi evidence kopij vsebin zbirk osebnih podatkov v knjigi evidenc o ravnanju z osebnimi podatki in
- če ne obvesti pooblaščenega delavca ali direktorja v primeru zlorabe osebnih podatkov ali vdora v zbirko osebnih podatkov.

Delavec stori hujšo kršitev delovne dolžnosti:

- če sporoča osebne podatke, s katerimi se je seznanil pri svojem delu, sodelavcem ali drugim osebam,
- če opusti skrb in nadzor nad nosilci osebnih podatkov med delovnim časom in tako dopusti možnost vpogleda vanje nepooblaščenim osebam,
- če nepooblaščenoma izdela kopije nosilce osebnih podatkov,
- če brez izrecnega dovoljenja odnaša iz zavoda nosilce osebnih podatkov,
- če posreduje osebne podatke, pooblaščenim zunanjim institucijam brez dovoljenja pooblaščenih oseb ali direktorja,
- če ne vpiše v knjigo evidenc o ravnanju z osebnimi podatki dejstva o posredovanju osebnih podatkov eksternim institucijam,
- če popravlja, spreminja ali dopolnjuje sistemsko ali aplikativno programsko opremo,
- če inštalira ali odnese programsko opremo iz zavoda brez izrecnega dovoljenja pooblaščenih oseb ali direktorja,
- če ne izdeluje redno kopije vsebine osebnih podatkov in
- če ne hrani računalniških kopij vsebin zbirk osebnih podatkov v zavarovanih zaklenjenih omarah.

XIII. KONČNE DOLOČBE:

28. člen

Z določbami tega pravilnika morajo biti seznanjeni vsi zaposleni zavoda, obdelovalci osebnih podatkov in zunanji sodelavci zavoda.

Zaposleni, ki delajo na delovnih mestih, kjer se zbirajo, urejajo, obdelujejo, spreminjajo, shranjujejo, posredujejo ali uporabljajo osebni podatki ali nosilci osebnih podatkov, morajo podpisati izjavo o varstvu osebnih podatkov v roku 30 dni od dneva sprejema tega pravilnika.

29. člen

Z dnem, ko prične veljati ta pravilnik, preneha veljati Pravilnik o varstvu osebnih podatkov z dne 22. 5. 2018, ta Pravilnik pa ga v celoti nadomesti.

30. člen

Ta pravilnik prične veljati naslednji dan po objavi na intranetu zavoda in obvestilu zaposlenim.

Številka: 01-05/2023
Datum: 16. 5. 2023

Javni zavod Ljubljanski grad
direktorica
Mateja Avbelj Valentan