Ime dokumenta:	Pravilnik o varstvu osebnih podatkov
Ime datoteke:	Pravilnik o varstvu osebnih podatkov podjetja Javno podjetje Kraški vodovod Sežana d.o.o.
Velja od:	01.01.2019

I. SPLOŠNE DOLOČBE 3

II. ZBIRKE OSEBNIH PODATKOV 4

III. VAROVANJE PROSTOROV IN STROJNE OPREME 5

IV. VAROVANJE SISTEMSKE IN APLIKATIVNE PROGRAMSKE OPREME, PODATKOVNIH NOSILCEV TER PRENOS PO TELEKOMUNIKACIJSKIH SREDSTVIH 7

VAROVANJE SISTEMSKE IN APLIKATIVNE PROGRAMSKE OPREME 7

VAROVANJE STREŽNIKOV TER PODATKOVNIH NOSILCEV 8

VAROVANJE PRI PRENOSU PO TELEKOMUNIKACIJSKIH OMREŽJIH 8

V. UKREPI ZA ZAGOTAVLJANJE INTEGRITETE, ZAUPNOSTI IN DOSTOPNOSTI DO OSEBNIH PODATKOV IN SLEDLJIVOSTI OPERACIJ NA NJIH 8

INTEGRITETA PODATKOV 8

ZAUPNOST PODATKOV 9

DOSTOPNOST 9

SLEDLJIVOST OPERACIJ NA PODATKIH IN SLEDLJIVOST POSREDOVANJ PODATKOV 10

VI. ORGANIZACIJA DELOVNIH PROCESOV 10

VII. MANIPULACIJA Z OSEBNIMI PODATKI IN ZBIRKAMI OSEBNIH PODATKOV 11

SPLOŠNE DOLOČBE 11

ZBIRANJE OSEBNIH PODATKOV 12

VZPOSTAVITEV IN DOPOLNITEV ZBIRKE OSEBNIH PODATKOV 13

POSREDOVANJE 13

BRISANJE 13

VIII. OBDELOVALCI OSEBNIH PODATKOV 14

IX. IZNOS OSEBNIH PODATKOV V TRETJE DRŽAVE 15

X. VIDEONADZOR 16

XI. EVIDENCA VSTOPOV IN IZSTOPOV IZ PROSTOROV 17

XII. PRAVICE POSAMEZNIKOV, NA KATERE SE NANAŠAJO OSEBNI PODATKI 17

XIII. IZDELAVA OCENE UČINKA V ZVEZI Z VARSTVOM OSEBNIH PODATKOV TER PREDHODNO POSVETOVANJE 18

XIV. UKREPANJE OB UGOTOVITVI ZLORABE OSEBNIH PODATKOV ALI VDORU V ZBIRKE OSEBNIH PODATKOV 19

XV. ODGOVORNOST DELAVCEV ZA IZVAJANJE UKREPOV ZAVAROVANJA OSEBNIH PODATKOV 20

XVI. VGRAJENO IN PRIVZETO VARSTVO PODATKOV 21

XVII. PREHODNE IN KONČNE DOLOČBE 21

PRILOGA A 22

PRILOGA B 23

PRILOGA C 24
PRILOGA D 25
PRILOGA E 26
PRILOGA F 27
PRILOGA G 29

Pooblastila:	**Ime in priimek/ naziv:**	**Datum:**	**Podpis:**
Pripravil:	Ksenja Fon	01.01.2019	
Pregledal:	Petra Gombač	01.01.2019	
Odobril (velja od):	Primož Turšič	01.01.2019	

Prejemniki Operacijskega predpisa o postopkih in ukrepih za varstvo osebnih podatkov (reverz s številko kopije in žigom »veljavno«):

Št. 1:

Št. 2:

Št. 3:

Št. 4:

Št. 5:

Original je arhiviran v arhivu Javnega podjetja Kraški vodovod Sežana d.o.o.,Bazoviška cesta 6,Sežana

Ostali zaposleni in pogodbeni delavci prejmejo samo na vpogled.

Pregled predhodnih izdaj:				
Izdaja:	**Leto izdaje:**	**Prenehanje veljavnosti:**	**Avtorji sprememb**	**Opis spremembe:**
2018	**2015**	**24.05.2018**	Kristina Terčon Fakin Ksenja Fon	**GDPR**

Na podlagi 25. člena Zakona o varstvu osebnih podatkov ZVOP-1-UPB1 (Uradni list RS, št. 94/2007) je direktor podjetja Javno podjetje Kraški vodovod Sežana d.o.o., Bazoviška cesta 6, 6210 Sežana, matična številka: 5072999, dne 25.05.2018 sprejel naslednji

PRAVILNIK O VARSTVU OSEBNIH PODATKOV

I. SPLOŠNE DOLOČBE

1. člen

Ta pravilnik določa splošne postopke in ukrepe za varovanje osebnih podatkov vodenih v zbirkah osebnih podatkov s katerimi upravlja podjetje Javno podjetje Kraški vodovod Sežana d.o.o., Bazoviška cesta 6, 6210 Sežana, matična številka: 5072999 (v nadaljevanju: upravljavec osebnih podatkov). Pravilnik obsega splošne ukrepe za varovanje zbirk osebnih podatkov pri njihovem zbiranju, obdelovanju, shranjevanju, posredovanju in uporabi. Konkretni postopki in ukrepi za varovanje osebnih podatkov so opisani v operacijskem predpisu o postopkih in ukrepih za varstvo zbirk osebnih podatkov (v nadaljevanju: operacijski predpis za varstvo osebnih podatkov), ki ga upravljavec osebnih podatkov sprejme na podlagi tega pravilnika.

Namen pravilnika je zagotoviti skladnost delovanja upravljavca osebnih podatkov s predpisi s področja varstva osebnih podatkov.

2. člen

Izrazi, ki so uporabljeni v tem pravilniku, imajo naslednji pomen:

Osebni podatek pomeni katerokoli informacijo v zvezi z določenim ali določljivim posameznikom.

Posameznik je določena ali določljiva fizična oseba, na katero se nanaša osebni podatek; fizična oseba je določljiva, če se jo lahko neposredno ali posredno določi, 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, gensko, duševno, gospodarsko, kulturno ali družbeno identiteto tega posameznika.

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.

Zbirka je 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.

Upravljavec je Javno podjetje Kraški vodovod Sežana d.o.o., Bazoviška cesta 6, 6210 Sežana, matična številka: 5072999, ki sam ali skupaj z drugimi določa namene in sredstva obdelave osebnih podatkov.

Obdelovalec je fizična ali pravna oseba, javni organ, agencija ali drugo telo, ki obdeluje osebne podatke v imenu upravljalca.

Podobdelovalec je pravna ali fizična oseba, ki ji obdelovalec poveri določene naloge s področja obdelovanja osebnih podatkov.

Uporabnik osebnih podatkov je fizična ali pravna oseba, javni organ, agencija ali drugo telo, kateremu se razkrijejo osebni podatki.

Posredovanje osebnih podatkov pomeni izmenjavo osebnih podatkov med upravljavcem in uporabnikom ali upravljavcem in upravljavcem ali upravljavcem in obdelovalcem.

Tretja država je država, ki ni država članica Evropske unije ali del Evropskega gospodarskega prostora.

Evidenca dejavnosti obdelave je opis zbirke osebnih podatkov.

Pravilnik o varovanju osebnih podatkov je notranji akt o varovanju osebnih podatkov upravljavca ali obdelovalca osebnih podatkov.

Privolitev posameznika pomeni vsako prostovoljno, konkretno, informirano in nedvoumno ravnanje v obliki izjave ali drugačnega jasnega aktivnega delovanja, iz katerega je mogoče sklepati na želje posameznika, na katerega se nanašajo osebni podatki, s katero izrazi strinjanje z obdelavo osebnih podatkov, ki se nanašajo nanj.

Posebne vrste osebnih podatkov so 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.

Biometrični podatki so osebni podatki, ki so rezultat posebne tehnične obdelave v zvezi s fizičnimi, fiziološkimi ali vedenjskimi značilnostmi posameznika, ki omogočajo ali potrjujejo edinstveno identifikacijo tega posameznika, kot so podobe obraza ali daktiloskopski podatki.

Operacijski predpis o postopkih in ukrepih za varstvo zbirk osebnih podatkov vsebuje opis konkretnih postopkov in ukrepov za varovanje osebnih podatkov v zbirkah osebnih podatkov upravljavca osebnih podatkov.

Psevdonimizacija pomeni obdelavo osebnih podatkov na tak način, da osebnih podatkov brez dodatnih informacij ni več mogoče pripisati specifičnemu posamezniku, na katerega se nanašajo osebni podatki, če se take dodatne informacije hranijo ločeno ter zanje veljajo tehnični in organizacijski ukrepi za zagotavljanje, da se osebni podatki ne pripišejo določenemu ali določljivemu posamezniku.

Oblikovanje profilov pomeni vsako obliko avtomatizirane obdelave osebnih podatkov, ki vključuje uporabo osebnih podatkov za ocenjevanje nekaterih osebnih vidikov v zvezi s posameznikom, zlasti za analizo ali predvidevanje uspešnosti pri delu, ekonomskega položaja, zdravja, osebnega okusa, interesov, zanesljivosti, vedenja, lokacije ali gibanja tega posameznika.

II. ZBIRKE OSEBNIH PODATKOV

3. člen

Upravljavec osebnih podatkov v evidenci obdelav podatkov za vsako zbirko osebnih podatkov navede:

- naziv ali ime in kontaktne podatke upravljavca in, kadar obstajajo, skupnega upravljavca, predstavnika upravljavca in pooblaščene osebe za varstvo podatkov;
- namene obdelave;
- opis kategorij posameznikov, na katere se nanašajo osebni podatki, in vrst osebnih podatkov;
- kategorije uporabnikov, ki so jim bili ali jim bodo razkriti osebni podatki, vključno z uporabniki v tretjih državah ali mednarodnih organizacijah;
- kadar je ustrezno, informacije o prenosih osebnih podatkov v tretjo državo ali mednarodno organizacijo, vključno z identifikacijo te tretje države ali mednarodne organizacije;
- kadar je mogoče, predvidene roke za izbris različnih vrst podatkov;
- kadar je mogoče, splošni opis tehničnih in organizacijskih varnostnih ukrepov.

4. člen

Posamezna zbirka osebnih podatkov je lahko sestavljena iz ene ali več fizičnih zbirk osebnih podatkov.

5. člen

Fizična zbirka lahko obstaja v:

- papirni obliki (knjiga, fascikel, datotečna omara, itd.),
- elektronski obliki (magnetni diski, CD-ROMi in drugi nosilci elektronskih zapisov),
- obliki mikrofilma itd.

6. člen

Upravljavec osebnih podatkov v operacijskem predpisu za varstvo osebnih podatkov popiše fizične zbirke podatkov, ki vsebujejo osebne podatke in jih razvrsti po evidencah.

7. člen

Varovanje osebnih podatkov zajema organizacijske, tehnične in ustrezne logično-tehnične postopke in ukrepe, s katerimi se preprečuje slučajno ali namerno nepooblaščeno uničevanje podatkov, njihova sprememba, izguba ali nepooblaščena obdelava, tako da se:
- varujejo prostori in strojna oprema v katerih oz. s pomočjo katere se obdelujejo osebni podatki;
- varuje aplikativna in sistemska 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;
- omogoča naknadno ugotavljanje kdaj so bili posamezni podatki vneseni, uporabljeni ali preneseni v zbirko podatkov in kdo je to storil, in sicer za obdobje, za katero se posamezni podatki shranjujejo - evidenca sledljivosti notranjih obdelovanj osebnih podatkov se vodi na obrazcu (Priloga A);
- zagotavlja učinkovit način blokiranja, uničenja, izbrisa ali anonimiziranja osebnih podatkov.

III. VAROVANJE PROSTOROV IN STROJNE OPREME

8. člen

Upravljavec osebnih podatkov v operacijskem predpisu za varstvo osebnih podatkov za vsako fizično zbirko osebnih podatkov določi, v katerem prostoru se zbirka nahaja oz. v katerih prostorih je preko telekomunikacijskih sredstev možen dostop do te zbirke.

9. člen

Upravljavec osebnih podatkov za fizične zbirke, ki jih zanj vodijo obdelovalci osebnih podatkov ne določi ukrepov varovanja v pravilniku o varstvu osebnih podatkov, ampak v pogodbi z obdelovalcem, upoštevajoč zakon in pravilnik upravljavca osebnih podatkov ter dobro poslovno prakso pri varovanju podatkov.

10. člen

Prostori, v katerih se nahajajo zbirke osebnih podatkov in strojna ter programska oprema, ki omogoča dostop do teh podatkov, so varovani z organizacijskimi ter fizičnimi in tehničnimi ukrepi, ki onemogočajo nepooblaščenim osebam dostop do podatkov (v nadaljevanju: varovani prostori).

11. člen

Upravljavec osebnih podatkov v operacijskem predpisu za varstvo osebnih podatkov popiše ukrepe za varovanje prostorov, v katerih se nahajajo fizične zbirke oz. je možen dostop do njih.

12. člen

Upravljavec osebnih podatkov v operacijskem predpisu za varstvo osebnih podatkov določi osebe oz. delovna mesta, ki imajo pravico do vstopa v posamezen prostor v in izven delovnega časa, kjer se nahajajo zbirke osebnih podatkov. Dostop v varovane prostore je dovoljen le tistim delavcem, katerih pravica do vstopa v posamezni prostor izhaja iz operacijskega predpisa za varstvo osebnih podatkov.

Vstop v varovane prostore upravljavca osebnih podatkov je dovoljen tudi tistim pogodbenim sodelavcem, ki imajo z upravljavcem osebnih podatkov sklenjene ustrezne pogodbe o sodelovanju, ki vključujejo tudi dolžnost varovanja osebnih podatkov (obdelovalci osebnih podatkov).

Pod pogoji, ki jih določa ta pravilnik je vstop v varovane prostore upravljavca osebnih podatkov dovoljen tudi nezaposlenim osebam, poslovnim partnerjem in drugim obiskovalcem (tretje osebe).

13. člen

Delavcem je vstop v varovane prostore dopusten v delovnem času, izven delovnega časa pa le na podlagi izrecnega dovoljenja vodje sektorjev oz. odgovorne osebe podjetja. Izven delovnega časa je mogoč le zaposlenim, ki imajo ključe za vstop v prostore.

14. člen

Obdelovalci osebnih podatkov v varovane prostore upravljavca osebnih podatkov v delovnem času ne smejo vstopati ali se zadrževati brez prisotnosti odgovornega delavca, razen če jih veže dolžnost varovanja osebnih podatkov, ki je določena v pogodbi z upravljavcem osebnih podatkov.

Oseba, ki dela v varovanih prostorih, mora vestno in skrbno nadzorovati prostor in ob koncu delovnega časa vključiti alarm.

Obdelovalci osebnih podatkov se lahko gibljejo v varovanih prostorih upravljavca osebnih podatkov izven delovnega časa in brez prisotnosti odgovornega delavca le, če so nosilci podatkov shranjeni na način, ki ga določa ta pravilnik za čas izven delovnega časa.

15. člen

Oseba, ki pri svojem delu uporablja osebne podatke ali jih kakorkoli obdeluje (pooblaščena oseba za obdelavo osebnih podatkov), ne sme med delovnim časom brez nadzora puščati nosilcev osebnih podatkov na pisalnih mizah ali jih kako drugače izpostavljati nevarnosti vpogleda s strani nepooblaščenih oseb.

Če ima v varovane prostore pravico vstopiti oseba, ki ni zaposlena pri upravljavcu osebnih podatkov, morajo biti nosilci podatkov in računalniški prikazovalniki nameščeni v času obdelave ali dela na njih tako, da tem osebam ni omogočen vpogled vanje.

16. člen

Tretje osebe v varovane prostore upravljavca osebnih podatkov, kjer se nahajajo osebni podatki, ki niso posebej zaščiteni, ne smejo vstopati ali se zadrževati brez prisotnosti odgovornega delavca.

17. člen

Strojno opremo za zajemanje, obdelavo, izdelavo, kopiranje, prikazovanje, tiskanje, skeniranje, prenašanje in hranjenje podatkov se uporablja v skladu s tehničnimi navodili izdelovalca opreme, določili tega pravilnika ter standardi in navodili za posamezna področja dela.

Strojna oprema se lahko nahaja in uporablja samo v prostorih, ki ustrezajo predpisanim pogojem za delo s to opremo.

S strojno opremo lahko upravljajo samo pooblaščeni delavci pri upravljavcu osebnih podatkov. Vsak delavec, ki ima pooblastilo za delo z opremo, je odgovoren za svoje geslo in odgovarja za vsak izveden postopek ali transakcijo.

Omrežna gesla za prijavo v mrežo osebnih računalnikov podeljuje pooblaščenim osebam za obdelavo osebnih podatkov pooblaščena oseba za IT.

Ob prvi prijavi v sistem je uporabnik dolžan zamenjati dostopno geslo. V nadaljevanju je uporabnik dolžan periodično menjati dostopno geslo.

IV. VAROVANJE SISTEMSKE IN APLIKATIVNE PROGRAMSKE OPREME, PODATKOVNIH NOSILCEV TER PRENOS PO TELEKOMUNIKACIJSKIH SREDSTVIH

18. člen

Upravljavec osebnih podatkov v tem poglavju predpiše ukrepe in postopke za varovanje sistemske in aplikativne programske opreme, postopke in ukrepe za varovanje podatkovnih nosilcev ter prenos po telekomunikacijskih omrežjih.

19. člen

Izven delovnega časa morajo biti računalniki ali druga strojna oprema, na kateri se obdelujejo ali hranijo osebni podatki, izklopljeni in fizično ali programsko zaklenjeni, dostop do osebnih podatkov, hranjenih na disku računalnika, pa mora biti zaščiten z geslom.

20. člen

Vzdrževanje in popravilo strojne računalniške in druge opreme, s katero se obdelujejo osebni podatki, lahko izvajajo samo pooblaščeni servisi in njihovi vzdrževalci, ki imajo z upravljavcem sklenjeno pogodbo o servisiranju računalniške oziroma strojne opreme.

Vsak delavec, ki na svojem računalniku (namiznem, prenosnem, itd.) hrani osebne podatke, je dolžan v primeru servisiranja računalnika, pred predajo računalnika servisu poskrbeti, da se osebni podatki na njem ustrezno zaščitijo (anonimizirati, šifrirati ali trajno izbrisati).

VAROVANJE SISTEMSKE IN APLIKATIVNE PROGRAMSKE OPREME

21. člen

Dostop do sistemske in aplikativne programske opreme mora biti varovan s sistemom gesel za avtorizacijo in identifikacijo pooblaščenih oseb za obdelavo osebnih podatkov (posebej na ravni sistemske programske opreme in aplikativne programske opreme), ki omogoča dostop samo določenim pooblaščenim delavcem in osebam, ki za upravljavca osebnih podatkov po pogodbi opravljajo servisiranje računalniške in programske opreme.

Program oziroma aplikacija mora biti sestavljena tako, da je obdelava podatkov ponovljiva, ter da ob prekinitvi obdelav ne pride do izgube, uničenja ali sprememb podatkov.

Vsak nov program ali spremembo pri obstoječih programih je treba pred redno uporabo testirati na testnem sistemu. Razvojni programi in testne podatkovne zbirke morajo biti ločene od produkcijskega okolja.

22. člen

Če je za servisiranje, popravilo, spreminjanje ali dopolnjevanje sistemske ali aplikativne programske opreme potrebno kopiranje osebnih podatkov, mora delavec, ki je pooblaščen za obdelavo osebnih podatkov in manipulacijo z osebnimi podatki na računalniku po prenehanju potrebe po kopiji poskrbeti, da se le-ta uniči.

Če pogodba o obdelovanju osebnih podatkov z upravljavcem osebnih podatkov ni sklenjena, se morajo podatki z diska računalnika izbrisati na način, ki onemogoča restavracijo.

23. člen

Glede vsebine diskov mrežnega strežnika in lokalnih delovnih postaj, kjer se nahajajo osebni podatki, se preverja prisotnost računalniških virusov.

Ob pojavu računalniškega virusa je potrebno storiti vse, da se s pomočjo strokovnjakov virus odpravi.

Vsi podatki in programska oprema, ki so namenjeni uporabi v računalniškem informacijskem sistemu pri upravljavcu osebnih podatkov in prispejo k upravljavcu osebnih podatkov na medijih za prenos računalniških podatkov ali prek telekomunikacijskih kanalov, morajo biti pred uporabo preverjeni glede prisotnosti računalniških virusov.

VAROVANJE STREŽNIKOV TER PODATKOVNIH NOSILCEV

24. člen

Nosilci osebnih podatkov, hranjeni izven varovanih prostorov (hodniki, skupni prostori ipd.) morajo biti vedno zaklenjeni v omarah.

25. člen

Zaposleni delavci smejo odnašati nosilce osebnih podatkov izven poslovnih prostorov upravljavca osebnih podatkov le na podlagi predhodne poučitve glede varovanja nosilcev podatkov.

Posredovanje osebnih podatkov pooblaščenim zunanjim institucijam in drugim, ki izkažejo zakonsko podlago za pridobitev osebnih podatkov, dovoli pristojna oseba v posameznem oddelku, izvršeno posredovanje pa se vpiše v obrazec manipulacij z osebnimi podatki (Priloga A) ali evidentira na kakšen drug način.

26. člen

Strežniki, na katerih se nahajajo podatki morajo biti fizično, organizacijsko in tehnično varovani. Neposreden dostop do podatkov v zbirkah podatkov na strežnikih mora biti zavarovan na enak način, kot je zavarovan aplikativni dostop do teh podatkov.

VAROVANJE PRI PRENOSU PO TELEKOMUNIKACIJSKIH OMREŽJIH

27. člen

Osebni podatki morajo biti pri prenosu po telekomunikacijskih sredstvih in omrežjih zaščiteni.

28. člen

Posebne vrste osebnih podatkov morajo biti pri prenosu po telekomunikacijskih sredstvih in omrežjih zaščiteni z uporabo kriptografskih metod in elektronskega podpisa tako, da je zagotovljena njihova nečitljivost oziroma neprepoznavnost.

V. UKREPI ZA ZAGOTAVLJANJE INTEGRITETE, ZAUPNOSTI IN DOSTOPNOSTI DO OSEBNIH PODATKOV IN SLEDLJIVOSTI OPERACIJ NA NJIH

INTEGRITETA PODATKOV

29. člen

Upravljavec osebnih podatkov mora zagotoviti integriteto obdelovanih podatkov.

Integriteta (nespremenljivost podatkov) se zagotavlja z uporabo sistemov in aplikacij, ki onemogočajo spreminjanje zajetih podatkov ter z različnimi logično-tehničnimi postopki kot so uporaba uporabniških imen in gesel, elektronskega podpisa itd.

Organizacijsko se integriteta podatkov zagotavlja s tem, da imajo dostop do posameznega podatka le pooblaščene osebe za obdelavo osebnih podatkov v obsegu dodeljenih uporabniških pravic, veže pa jih dolžnost varovanja integritete podatkov.

Integriteta podatkov se zagotavlja tudi s fizičnim varovanjem prostorov, programske opreme in podatkovnih nosilcev.

ZAUPNOST PODATKOV

30. člen

Upravljavec osebnih podatkov mora zagotoviti zaupnost obdelovanih podatkov.

Zaupnost podatkov se logično-tehnično zagotavlja z uporabniškimi imeni in gesli na ravni sistemske in aplikativne programske opreme, s katero se obdelujejo podatki. Podatki so lahko kodirani ali šifrirani ali pa mora sistem za upravljanje s podatki zagotavljati, da do njih ne dostopajo nepooblaščene osebe. Zaupnost podatkov se lahko zagotavlja tudi s kriptografijo (šifriranjem) podatkov, kjer sam zapis podatkov onemogoča njihovo branje s strani nepooblaščenih oseb.

Organizacijsko se zaupnost podatkov lahko zagotavlja v aktu o sistemizaciji delovnih mest, kjer se za vsako delovno mesto opredelijo pravice in pooblastila na posamezni podatkovni zbirki. Če to v sistemizaciji delovnih mest ni podrobneje opredeljeno, omenjene pravice in pooblastila izhajajo iz operacijskega predpisa o varstvu osebnih podatkov. Za vsako delovno mesto se v notranjih aktih upravljavca lahko opredeli tudi dolžnost varovanja zaupnosti osebnih podatkov.

Zaupnost podatkov se zagotavlja tudi s fizičnim varovanjem prostorov, sistemske in aplikativne programske opreme ter podatkovnih nosilcev.

31. člen

Dostop do podatkov prek aplikativne programske opreme je varovan s sistemom gesel za avtorizacijo in identifikacijo uporabnikov programov in podatkov. Sistem gesel vsakemu subjektu priredi skupino pravic in pooblastil na posamezni sistemski in aplikativni programski opremi.

32. člen

Vsa gesla, ki se uporabljajo za vstop in za administriranje v mreži osebnih računalnikov, administriranje z elektronsko pošto in administriranje prek aplikativnih programov, se hranijo v zapečatenih ovojnicah in varujejo v zaklenjeni omari.

Varovana gesla, hranjena v zapečatenih ovojnicah, se smejo uporabiti samo v izjemnih in nujnih primerih. Vsaka uporaba vsebine zapečatenih ovojnic se dokumentira.

Po uporabi zapečatenih gesel iz ovojnic pooblaščena oseba za IT določi nova gesla ter zagotovi, da se ta gesla še naprej hranijo na zgoraj opredeljen način.

DOSTOPNOST

33. člen

Upravljavec osebnih podatkov mora zagotoviti dostopnost obdelovanih podatkov.

Dostopnost podatkov se zagotavlja z ukrepi, ki omogočajo neprekinjen in trajen (do izbrisa) dostop do podatkov: izdelava varnostnih kopij podatkov (back-up), arhiviranje podatkov, vzporedne evidence,

izdelava izvedenih evidenc itd. Varnostna kopija podatkov lahko obstaja v isti obliki kot izvirni podatki (npr. kopirani papirni arhiv), lahko je njihova varnostna kopija v drugem formatu (npr. skenirani dokumenti, shranjeni v sistemu za elektronsko upravljanje z dokumenti), lahko pa gre za povzetek podatkov v drugem formatu (npr. vpis podatkov iz papirnih vlog v elektronsko zbirko podatkov).

Vsi postopki izdelovanja varnostnih kopij morajo biti ustrezno dokumentirani in morajo zagotavljati natančen zajem, transformacijo in shranjevanje podatkov.

34. člen

Upravljavec osebnih podatkov mora za potrebe restavriranja osebnih podatkov oziroma računalniškega sistema po okvarah ali izgubi podatkov iz drugih razlogov redno izdelovati kopije vsebine osebnih podatkov.

Vse izdelane papirne kopije vsebin zbirk osebnih podatkov se morajo vpisati v obrazec manipulacij z osebnimi podatki (Priloga A) in se hranijo v zaklenjeni omari.

Informacije o izdelavi elektronskih kopij vsebin zbirk osebnih podatkov se vodijo v dnevniških datotekah (log files) aplikacij za kopiranje.

SLEDLJIVOST OPERACIJ NA PODATKIH IN SLEDLJIVOST POSREDOVANJ PODATKOV

35. člen

Sledljivost operacij (vnos, uporaba, sprememba, posredovanje, brisanje) na osebnih podatkih se dosega z vodenjem evidenc o operacijah na podatkih oz. zbirkah podatkov. Take evidence so lahko elektronske ali papirne, njihovo vodenje pa je lahko ročno ali avtomatsko. Vodenje je ročno, če se vsaka obdelava podatkov ročno zavede. Vodenje je avtomatsko, če se vsaka obdelava avtomatsko zavede. Primer avtomatskega vodenja je vodenje dnevnikov v posameznih aplikacijah (log files), iz katerih se da razbrati dejanja posameznih oseb v zvezi s posameznimi osebnimi podatki.

36. člen

Sledljivost posredovanj osebnih podatkov uporabnikom, se dosega z vodenjem evidenc o posredovanju osebnih podatkov. Take evidence so lahko pisne (npr. obrazec posredovanj) ali elektronske (npr. preglednica ali zbirka podatkov o posredovanjih), njihovo vodenje pa je lahko ročno (ročen vpis v posamezno evidenco) ali pa avtomatsko (kjer je posredovanje izvršeno preko aplikacije, ki vodi dnevnik operacij). Omenjene evidence se vodijo na obrazcu manipulacij z osebnimi podatki (Priloga A).

37. člen

Upravljavec osebnih podatkov v operacijskem predpisu za varstvo osebnih podatkov podrobneje določi načine zagotavljanja integritete, zaupnosti in dostopnosti podatkov ter sledljivosti operacij na njih.

VI. ORGANIZACIJA DELOVNIH PROCESOV

38. člen

Upravljavec zbirk osebnih podatkov v operacijskem predpisu za varstvo osebnih podatkov določi tipične pravice v zvezi z obdelavo osebnih podatkov (dostop, pregledovanje, spreminjanje, brisanje, posredovanje). Za vsako evidenco določi: katere pravice na tej evidenci obstajajo in katera delovna mesta iz sistemizacije delovnih mest imajo te pravice pri posamezni evidenci.

39. člen

Upravljavec osebnih podatkov določi odgovorno osebo za vsako zbirko osebnih podatkov v operacijskem predpisu za varstvo osebnih podatkov.

Vsi ostali delavci (pooblaščene osebe za obdelavo osebnih podatkov) morajo za obdelavo osebnih podatkov pridobiti ustrezno pooblastilo odgovorne osebe za posamezno zbirko osebnih podatkov (Priloga B).

40. člen

Upravljavec osebnih podatkov je za pooblaščeno osebo za varstvo osebnih podatkov v organizaciji imenoval Jerneja Dolenca.

41. člen

Pooblaščena oseba za varstvo podatkov ima vsaj naslednje naloge:

- obveščanje upravljavca in zaposlenih, ki izvajajo obdelavo, ter svetovanje navedenim o njihovih obveznostih v skladu s določbami prava Evropske unije ali zakonskih določil na področju varstva osebnih podatkov;
- spremljanje skladnosti s pravom Evropske unije ali pravom Republike Slovenije in politikami upravljavca osebnih podatkov ali obdelovalca v zvezi z varstvom osebnih podatkov, vključno z dodeljevanjem nalog, ozaveščanjem in usposabljanjem osebja, vključenega v dejanja obdelave, ter s tem povezanimi revizijami;
- svetovanje, kadar je to zahtevano, glede ocene učinka v zvezi z varstvom podatkov in spremljanje njenega izvajanja v skladu z 71. členom tega Pravilnika;
- sodelovanje z nadzornim organom (Informacijskim pooblaščencem);
- delovanje kot kontaktna točka za nadzorni organ pri vprašanjih v zvezi z obdelavo, vključno s predhodnim posvetovanjem iz 72. člena tega Pravilnika in, kjer je to ustrezno, posvetovanje glede katere koli druge zadeve.

Pooblaščena oseba za varstvo podatkov se imenuje na podlagi poklicnih odlik in zlasti strokovnega znanja o zakonodaji in praksi na področju varstva podatkov ter zmožnosti za izpolnjevanje nalog iz prejšnjega odstavka.

Pooblaščena oseba za varstvo podatkov je lahko član osebja upravljavca ali obdelovalca ali pa naloge opravlja na podlagi pogodbe o storitvah.

Upravljavec osebnih podatkov objavi kontaktne podatke pooblaščene osebe za varstvo osebnih podatkov in jih sporoči Informacijskemu pooblaščencu.

VII. MANIPULACIJA Z OSEBNIMI PODATKI IN ZBIRKAMI OSEBNIH PODATKOV

SPLOŠNE DOLOČBE

42. člen

Upravljavec osebnih podatkov za vsako operacijo na osebnih podatkih zagotovi možnost poznejšega ugotavljanja, kdaj so bili posamezni osebni podatki vneseni v zbirko osebnih podatkov, uporabljeni ali drugače obdelani in kdo je to storil, in sicer za obdobje, ko je mogoče zakonsko varstvo pravice posameznika zaradi nedopustnega posredovanja ali obdelave osebnih podatkov.

43. člen

Upravljavec osebnih podatkov v operacijskem predpisu za varstvo osebnih podatkov podrobneje razčleni operacije v zvezi s posameznimi zbirkami osebnih podatkov.

ZBIRANJE OSEBNIH PODATKOV

44. člen

Pravna podlaga za zbiranje osebnih podatkov je bodisi zakon, ki dovoljuje obdelovanje določene vrste osebnih podatkov, bodisi osebna privolitev posameznika za obdelovanje osebnih podatkov (1. odstavek 10. člena ZVOP-1). Osebna privolitev posameznika naj bo praviloma pisna, zlasti pa kadar se obdelujejo posebne vrste osebnih podatkov. Pisna privolitev posameznika naj bo praviloma v obliki podpisane izjave posameznika (Priloga C ali D).

Izjemoma se lahko obdelujejo tudi osebni podatki, za katere ni eksplicitnega zakonskega pooblastila ali privolitve posameznika, če gre za osebne podatke posameznikov, ki so z upravljavcem osebnih podatkov sklenili pogodbo ali pa so z njim v fazi pogajanj za sklenitev pogodbe, če je obdelava osebnih podatkov potrebna za izvedbo pogajanj ali izpolnitev pogodbe (2. odstavek 10. člena ZVOP-1).

45. člen

Upravljavec osebnih podatkov mora zagotoviti, da je posameznik katerega osebni podatki se vnašajo v zbirki osebnih podatkov obveščen o obdelavi njegovih osebnih podatkov in da je podana osebna privolitev posameznika v skladu z veljavno zakonodajo s področja varstva osebnih podatkov.

Če se osebni podatki zbirajo neposredno od posameznika, upravljavec osebnih podatkov posamezniku sporoči naslednje informacije, če z njimi posameznik še ni seznanjen:

- podatke o upravljavcu osebnih podatkov (firma in sedež) ter
- kontaktne podatke pooblaščene osebe za varstvo podatkov, kadar ta obstaja; ter
- namen obdelave osebnih podatkov;
- kadar je obdelava potrebna zaradi uveljavljanja zakonitih interesov, zakonite interese, za uveljavljanje katerih si prizadeva upravljavec ali tretja oseba;
- uporabnike ali kategorije uporabnikov osebnih podatkov, če obstajajo;
- kadar je ustrezno, dejstvo, da upravljavec namerava prenesti osebne podatke v tretjo državo ali mednarodno organizacijo, ter obstoj ali neobstoj sklepa Komisije o ustreznosti ali v primeru prenosov pri katerih sta upravljavec osebnih podatkov ter obdelovalec predvidela ustrezne zaščitne ukrepe, na podlagi zavezujočih poslovnih pravil ali druge ustrezne pravne podlage za iznos osebnih podatkov v tretjo državo ali mednarodno organizacijo, sklic na ustrezne ali primerne zaščitne ukrepe in sredstva za pridobitev njihove kopije ali kje so na voljo.

Če je glede na posebne okoliščine zbiranja teh osebnih podatkov potrebno, da se zagotovi zakonita in poštena obdelava osebnih podatkov posameznika, upravljavec osebnih podatkov sporoči tudi dodatne informacije, če posameznik z njimi še ni seznanjen, zlasti:

- obdobje hrambe osebnih podatkov ali, kadar to ni mogoče, merila, ki se uporabijo za določitev tega obdobja;
- obstoj pravice, da se od upravljavca zahtevajo dostop do osebnih podatkov in popravek ali izbris osebnih podatkov ali omejitev obdelave v zvezi s posameznikom, na katerega se nanašajo osebni podatki, ali obstoj pravice do ugovora obdelavi in pravice do prenosljivosti podatkov;
- kadar obdelava temelji na privolitvi posameznika, obstoj pravice, da se lahko privolitev kadar koli prekliče, ne da bi to vplivalo na zakonitost obdelave podatkov, ki se je na podlagi privolitve izvajala do njenega preklica;
- pravico do vložitve pritožbe pri nadzornem organu;
- ali je zagotovitev osebnih podatkov statutarna ali pogodbena obveznost ali pa obveznost, ki je potrebna za sklenitev pogodbe, ter ali mora posameznik, na katerega se nanašajo osebni podatki, zagotoviti osebne podatke ter kakšne so morebitne posledice, če se taki podatki ne zagotovijo, in
- obstoj avtomatiziranega sprejemanja odločitev, vključno z oblikovanjem profilov ter vsaj v takih primerih smiselne informacije o razlogih zanj, kot tudi pomen in predvidene posledice take obdelave za posameznika, na katerega se nanašajo osebni podatki.

VZPOSTAVITEV IN DOPOLNITEV ZBIRKE OSEBNIH PODATKOV

46. člen

Osebni podatki se vpisujejo v zbirke osebnih podatkov samo na podlagi ustrezne pravne podlage iz 44. člena tega pravilnika.

47. člen

Evidenca dejavnosti obdelave vsebuje naslednje podatke:

- naziv ali ime in kontaktne podatke upravljavca in, kadar obstajajo, skupnega upravljavca, predstavnika upravljavca in pooblaščene osebe za varstvo podatkov;
- namene obdelave;
- opis kategorij posameznikov, na katere se nanašajo osebni podatki, in vrst osebnih podatkov;
- kategorije uporabnikov, ki so jim bili ali jim bodo razkriti osebni podatki, vključno z uporabniki v tretjih državah ali mednarodnih organizacijah;
- kadar je ustrezno, informacije o prenosih osebnih podatkov v tretjo državo ali mednarodno organizacijo, vključno z identifikacijo te tretje države ali mednarodne organizacije;
- kadar je mogoče, predvidene roke za izbris različnih vrst podatkov;
- kadar je mogoče, splošni opis tehničnih in organizacijskih varnostnih ukrepov.

Vsak obdelovalec in predstavnik obdelovalca, kadar ta obstaja, mora voditi evidenco vseh vrst dejavnosti obdelave, ki jih izvajata v imenu upravljavca, ki vsebuje:

- naziv ali ime in kontaktne podatke obdelovalca ali obdelovalcev in vsakega upravljavca, v imenu katerega deluje obdelovalec, ter, kadar obstajajo, predstavnika upravljavca ali obdelovalca, in pooblaščene osebe za varstvo podatkov;
- vrste obdelave, ki se izvaja v imenu posameznega upravljavca;
- kadar je ustrezno, prenose osebnih podatkov v tretjo državo ali mednarodno organizacijo, vključno z identifikacijo te tretje države ali mednarodne organizacije.

Upravljavec osebnih podatkov mora skrbeti za točnost in ažurnost vsebine evidence dejavnosti obdelave.

POSREDOVANJE

48. člen

Osebni podatki, vodeni v zbirki osebnih podatkov pri upravljavcu osebnih podatkov, se lahko posredujejo drugim uporabnikom samo, če so za njihovo pridobitev in uporabo pooblaščeni z zakonom ali na podlagi pisne zahteve ali privolitve osebe, na katero se osebni podatki nanašajo.

49. člen

Upravljavec osebnih podatkov za vsako posredovanje osebnih podatkov zagotovi, da je mogoče pozneje ugotoviti, kateri osebni podatki so bili posredovani, komu, kdaj in na kakšni podlagi in sicer za obdobje, ko je mogoče zakonsko varstvo pravice posameznika zaradi nedopustnega posredovanja osebnih podatkov.

BRISANJE

50. člen

Upravljavec osebnih podatkov shranjuje osebne podatke le toliko časa, dokler je to potrebno za dosego namena, zaradi katerega so se zbirali ali nadalje obdelovali. Rok hrambe osebnih podatkov je opredeljen v evidenci obdelav podatkov. Po izpolnitvi tega namena obdelave se osebni podatki zbrišejo, 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.

51. člen

Brisanje osebnih podatkov na računalniških medijih se opravi na način, ki onemogoča restavriranje brisanih podatkov, kar lahko vključuje tudi uničenje računalniških medijev na način opredeljen v drugem odstavku tega člena.

Osebni podatki, vsebovani na klasičnih nosilcih (listine, kartoteke, register, seznam) se brišejo z uničenjem nosilcev. Nosilci se fizično uničijo (zažgejo, razrežejo) v prostorih upravljavca osebnih podatkov, lahko pa tudi pri drugi organizaciji, ki se ukvarja z uničevanjem zaupne dokumentacije, v obeh primerih pa mora postopek potekati pod nadzorom pooblaščenega delavca upravljavca osebnih podatkov.

52. člen

Z vestnostjo in skrbnostjo določeno s tem pravilnikom za uničevanje osebnih podatkov, vodenih v zbirkah oziroma na posameznih nosilcih podatkov, se mora brisati in uničevati tudi pomožna dokumentacija ali računalniški produkti oziroma predloge, ki vsebujejo posamezne osebne podatke.

Uničevanje osebnih podatkov na nosilcih iz predhodnega odstavka se mora izvajati tekoče in ažurno.

VIII. OBDELOVALCI OSEBNIH PODATKOV

53. člen

Upravljavec osebnih podatkov lahko poveri posamezna opravila v zvezi z obdelavo osebnih podatkov obdelovalcu osebnih podatkov, ki je registriran za opravljanje takšne dejavnosti in zagotavlja ustrezne postopke in ukrepe za varovanje osebnih podatkov.

Upravljavec osebnih podatkov v operacijskem predpisu za varstvo osebnih podatkov določi seznam obdelovalcev osebnih podatkov za posamezno zbirko osebnih podatkov.

54. člen

Za vsakega obdelovalca osebnih podatkov določi upravljavec osebnih podatkov v pogodbi o obdelovanju osebnih podatkov do katerih zbirk oz. do katerih vrst osebnih podatkov v posamezni zbirki osebnih podatkov ima obdelovalec osebnih podatkov dostop, kakšna pooblastila ima obdelovalec osebnih podatkov na teh zbirkah oz. vrstah podatkov (dostop, pregledovanje, spreminjanje, brisanje, posredovanje) ter kakšne ukrepe in postopke mora obdelovalec osebnih podatkov sprejeti oz. izvajati za varstvo teh podatkov.

55. člen

Upravljavec osebnih podatkov v operacijskem predpisu za varstvo osebnih podatkov evidentira do katerih zbirk oz. do katerih vrst osebnih podatkov znotraj posamezne zbirke osebnih podatkov imajo obdelovalci osebnih podatkov dostop in kakšna so njihova pooblastila za obdelavo teh podatkov.

56. člen

Obdelovalec osebnih podatkov sme opravljati posamezna opravila v zvezi z obdelavo osebnih podatkov v okviru pooblastil upravljavca osebnih podatkov in osebnih podatkov ne sme obdelovati za drug namen.

Pogodba o obdelovanju osebnih podatkov ali drug pravni akt mora določati, da obdelovalec:

(a) osebne podatke lahko obdeluje samo po dokumentiranih navodilih upravljavca, vključno glede prenosov osebnih podatkov v tretjo državo ali mednarodno organizacijo, razen če to od njega zahteva pravo Unije ali pravo države članice, ki velja za obdelovalca; v slednjem primeru obdelovalec o tej

pravni zahtevi pred obdelavo podatkov obvesti upravljavca, razen če zadevno pravo prepoveduje takšno obvestilo na podlagi pomembnih razlogov v javnem interesu;

(b) zagotovi, da so osebe, ki so pooblaščene za obdelavo osebnih podatkov, zavezane k zaupnosti ali jih k zaupnosti zavezuje ustrezen zakon;

(c) sprejme vse ukrepe, potrebne za zagotavljanje varnosti obdelave osebnih podatkov;

(d) spoštuje pogoje da brez predhodnega pisnega dovoljenja upravljavca, obdelovalec ne more prenesti posamezne obdelave osebnih podatkov na podobdelovalca;

(e) ob upoštevanju narave obdelave pomaga upravljavcu z ustreznimi tehničnimi in organizacijskimi ukrepi, kolikor je to mogoče, pri izpolnjevanju njegovih obveznosti, da odgovori na zahteve za uresničevanje pravic posameznika, na katerega se nanašajo osebni podatki;

(f) upravljavcu pomaga pri izpolnjevanju obveznosti varovanja osebnih podatkov ob upoštevanju narave obdelave in informacij, ki so dostopne obdelovalcu;

(g) v skladu z odločitvijo upravljavca izbriše ali vrne vse osebne podatke upravljavcu po zaključku storitev v zvezi z obdelavo ter uniči obstoječe kopije, razen če pravo Evropske Unije ali pravo države članice predpisuje shranjevanje osebnih podatkov;

(h) da upravljavcu na voljo vse informacije, potrebne za dokazovanje izpolnjevanja obveznosti iz tega člena, ter upravljavcu ali drugemu revizorju, ki ga pooblasti upravljavec, omogoči izvajanje revizij, tudi pregledov, in pri njih sodeluje.

57. člen

V primeru spora med upravljavcem osebnih podatkov in obdelovalcem osebnih podatkov je dolžan obdelovalec osebnih podatkov na podlagi zahteve upravljavca osebnih podatkov osebne podatke, ki jih je pogodbeno obdeloval, nemudoma vrniti upravljavcu osebnih podatkov. Morebitne kopije teh podatkov mora takoj uničiti ali jih posredovati državnemu organu, ki je v skladu z zakonom pristojen za odkrivanje ali pregon kaznivih dejanj, sodišču ali drugemu državnemu organu, če tako določa zakon.

58. člen

V primeru prenehanja obdelovalca osebnih podatkov se osebni podatki brez nepotrebnega odlašanja vrnejo upravljavcu osebnih podatkov.

IX. IZNOS OSEBNIH PODATKOV V TRETJE DRŽAVE

59. člen

Prenos osebnih podatkov v tretjo državo ali mednarodno organizacijo se lahko izvede, če Komisija odloči, da zadevna tretja država, ozemlje, eden ali več določenih sektorjev v tej tretji državi ali mednarodna organizacija zagotavlja ustrezno raven varstva podatkov. Za tak prenos ni potrebno posebno dovoljenje.

60. člen

Kadar sklep v skladu s prejšnjim členom ni sprejet, lahko upravljavec ali obdelovalec osebne podatke prenese v tretjo državo ali mednarodno organizacijo le, če je upravljavec ali obdelovalec predvidel ustrezne zaščitne ukrepe, in pod pogojem, da imajo posamezniki, na katere se nanašajo osebni podatki, na voljo izvršljive pravice in učinkovita pravna sredstva.

Ustrezni zaščitni ukrepi iz prejšnjega odstavka se lahko, ne da bi bilo potrebno posebno dovoljenje nadzornih organov, zagotovijo s:

(a) pravno zavezujočim in izvršljivim instrumentom, ki ga sprejmejo javni organi ali telesa;
(b) zavezujočimi poslovnimi pravili;
(c) standardnimi določili o varstvu podatkov, ki jih sprejme Komisija;

(d) standardnimi določili o varstvu podatkov, ki jih sprejme Informacijski pooblaščenec in odobri Komisija;
(e) odobrenim kodeksom ravnanja, skupaj z zavezujočimi in izvršljivimi zavezami upravljavca ali obdelovalca v tretji državi, da bo uporabljal ustrezne zaščitne ukrepe, tudi glede pravic posameznikov, na katere se nanašajo osebni podatki, ali
(f) odobrenim mehanizmom potrjevanja iz EU Uredbe, skupaj z zavezujočimi in izvršljivimi zavezami upravljavca ali obdelovalca v tretji državi, da bo uporabljal ustrezne zaščitne ukrepe, tudi glede pravic posameznikov, na katere se nanašajo osebni podatki.

61. člen

Ustrezni zaščitni ukrepi iz 1. odstavka prejšnjega člena se lahko z dovoljenjem ustreznega nadzornega organa zagotovijo tudi zlasti s:
(a) pogodbenimi določili med upravljavcem ali obdelovalcem in upravljavcem, obdelovalcem ali uporabnikom osebnih podatkov v tretji državi ali mednarodni organizaciji, ali
(b) določbami, ki se vstavijo v upravne dogovore med javnimi organi ali telesi in v katere so vključene izvršljive in učinkovite pravice za posameznike, na katere se nanašajo podatki.

X. VIDEONADZOR

62. člen

Upravljavec osebnih podatkov mora o izvajanju videonadzora objaviti obvestilo. Obvestilo mora biti vidno in razločno objavljeno na način, ki omogoča posamezniku, da se seznani z njegovim izvajanjem najkasneje, ko se nad njim začne izvajati videonadzor.

Obvestilo iz prejšnjega odstavka mora vsebovati naslednje informacije:
- da se izvaja videonadzor;
- naziv upravljavca osebnih podatkov ter
- telefonsko številko za pridobitev informacije, kje in koliko časa se shranjujejo posnetki iz videonadzornega sistema.

Videonadzorni sistem, s katerim se izvaja videonadzor, mora biti zavarovan pred dostopom nepooblaščenih oseb.

63. člen

Videonadzor dostopa v uradne službene oziroma poslovne prostore se lahko izvaja, če je to potrebno za varnost ljudi in premoženja, zaradi zagotavljanja nadzora vstopa ali izstopa v ali iz službenih oziroma poslovnih prostorov ali če zaradi narave dela obstaja možnost ogrožanja delavcev.

Odločitev o uvedbi videonadzora dostopa v uradne službene oziroma poslovne prostore sprejme direktor. V pisni odločitvi morajo biti obrazloženi razlogi za uvedbo videonadzora.

O izvajanju videonadzora je potrebno pisno obvestiti vse delavce, ki opravljajo delo v nadzorovanem prostoru.

Zbirka osebnih podatkov po tem členu vsebuje posnetek posameznika (slika oziroma glas), datum in čas vstopa in izstopa iz prostora, lahko pa tudi osebno ime posnetega posameznika, naslov njegovega stalnega ali začasnega prebivališča, zaposlitev, številko in podatke o vrsti njegovega osebnega dokumenta ter razlogu vstopa, če se navedeni osebni podatki zbirajo poleg ali s posnetkom videonadzornega sistema.

64. člen

Videonadzor znotraj delovnih prostorov se lahko izvaja le v izjemnih primerih, kadar je to nujno potrebno za varnost ljudi in premoženja ali za varovanje tajnih podatkov ter poslovne skrivnosti, tega namena pa ni možno doseči z milejšimi sredstvi.

Videonadzor se lahko izvaja le glede tistih delovnih prostorov, kjer je potrebno varovati interese iz prejšnjega odstavka.

Prepovedano je izvajati videonadzor v delovnih prostorih izven delovnega mesta, zlasti v garderobah, dvigalih in sanitarnih prostorih.

Delavci morajo biti pred začetkom izvajanja videonadzora po tem členu vnaprej pisno obveščeni o njegovem izvajanju.

Pred uvedbo videonadzora se mora upravljavec osebnih podatkov posvetovati z reprezentativnim sindikatom upravljavca osebnih podatkov.

XI. EVIDENCA VSTOPOV IN IZSTOPOV IZ PROSTOROV

65. člen

Upravljavec osebnih podatkov lahko za namene varovanja premoženja, življenja ali telesa posameznika ter reda v njegovih prostorih od posameznika, ki namerava vstopiti ali izstopiti iz tega prostora, zahteva, da navede vse ali nekatere osebne podatke iz drugega odstavka tega člena ter razlog vstopa ali izstopa. Po potrebi lahko osebne podatke preveri tudi z vpogledom v osebni dokument.

V evidenci vstopov in izstopov se lahko o posamezniku vodijo samo naslednji osebni podatki: osebno ime, številka in vrsta osebnega dokumenta, naslov stalnega ali začasnega prebivališča, zaposlitev ter datum, ura in razlog vstopa ali izstopa v ali iz prostorov družbe.

XII. PRAVICE POSAMEZNIKOV, NA KATERE SE NANAŠAJO OSEBNI PODATKI

66. člen

Posameznik, na katerega se nanašajo osebni podatki, ima pravico od upravljavca dobiti potrditev, ali se v zvezi z njim obdelujejo osebni podatki, in kadar je temu tako, dostop do osebnih podatkov in naslednje informacije:

(a) namene obdelave;
(b) vrste zadevnih osebnih podatkov;
(c) uporabnike ali kategorije uporabnika, ki so jim bili ali jim bodo razkriti osebni podatki, zlasti uporabnike v tretjih državah ali mednarodnih organizacijah;
(d) kadar je mogoče, predvideno obdobje hrambe osebnih podatkov ali, če to ni mogoče, merila, ki se uporabijo za določitev tega obdobja;
(e) obstoj pravice, da se od upravljavca zahteva popravek ali izbris osebnih podatkov ali omejitev obdelave osebnih podatkov v zvezi s posameznikom, na katerega se nanašajo osebni podatki, ali obstoj pravice do ugovora taki obdelavi;
(f) pravico do vložitve pritožbe pri nadzornem organu;
(g) kadar osebni podatki niso zbrani pri posamezniku, na katerega se ti nanašajo, vse razpoložljive informacije v zvezi z njihovim virom;
(h) obstoj avtomatiziranega sprejemanja odločitev, vključno z oblikovanjem profilov, ter vsaj v takih primerih smiselne informacije o razlogih zanj, kot tudi pomen in predvidene posledice take obdelave za posameznika, na katerega se nanašajo osebni podatki.

67. člen

Poleg pravice do posredovanja osebnih podatkov ima posameznik prav tako:

- pravico do popravka,
- pravico do izbrisa (pravico do pozabe),
- pravico do omejitve obdelave,

- pravico do obveščanja drugih uporabnikov v zvezi s popravkom ali izbrisom osebnih podatkov ali omejitvijo obdelave,
- pravico do prenosljivosti podatkov.

68. člen

Upravljavec zagotovi kopijo osebnih podatkov, ki se obdelujejo. Za dodatne kopije, ki jih zahteva posameznik, na katerega se nanašajo osebni podatki, lahko upravljavec zaračuna razumno pristojbino ob upoštevanju upravnih stroškov. Kadar posameznik, na katerega se nanašajo osebni podatki, zahtevo predloži z elektronskimi sredstvi, in če posameznik, na katerega se nanašajo osebni podatki, ne zahteva drugače, se informacije zagotovijo v elektronski obliki, ki je splošno uporabljana.

69. člen

Posameznik lahko kadarkoli pisno ali na drug dogovorjen način zahteva, da upravljavec osebnih podatkov trajno ali začasno preneha uporabljati njegove osebne podatke za namen neposrednega trženja. Upravljavec osebnih podatkov je dolžan v petnajstih (15) dneh ustrezno preprečiti uporabo osebnih podatkov za namen neposrednega trženja ter o tem v nadaljnjih petih (5) dneh pisno ali na drug dogovorjen način obvestiti posameznika, ki je to zahteval.

70. člen

Interne postopke v zvezi s pravicami posameznika vodi Ksenja Fon, tajnica direktorja in referent za splošne in kadrovske zadeve.

XIII. IZDELAVA OCENE UČINKA V ZVEZI Z VARSTVOM OSEBNIH PODATKOV TER PREDHODNO POSVETOVANJE

71. člen

Kadar je možno, da bi lahko vrsta obdelave, zlasti z uporabo novih tehnologij, ob upoštevanju narave, obsega, okoliščin in namenov obdelave povzročila veliko tveganje za pravice in svoboščine posameznikov, upravljavec pred obdelavo opravi oceno učinka predvidenih dejanj obdelave na varstvo osebnih podatkov. V eni oceni je lahko obravnavan niz podobnih dejanj obdelave, ki predstavljajo podobna velika tveganja.

Ocena učinka v zvezi z varstvom podatkov iz 1. odstavka se zahteva zlasti v primeru:
(a) sistematičnega in obsežnega vrednotenja osebnih vidikov v zvezi s posamezniki, ki temelji na avtomatizirani obdelavi, vključno z oblikovanjem profilov, in je osnova za odločitve, ki imajo pravne učinke v zvezi s posameznikom ali nanj na podoben način znatno vplivajo;
(b) obsežne obdelave posebnih vrst podatkov ali osebnih podatkov v zvezi s kazenskimi obsodbami in prekrški ali
(c) obsežnega sistematičnega spremljanja javno dostopnega območja.

Upravljavec pri izvedbi ocene učinka v zvezi z varstvom podatkov za mnenje zaprosi pooblaščeno osebo za varstvo podatkov.

Ocena zajema vsaj:
(a) sistematičen opis predvidenih dejanj obdelave in namenov obdelave, kadar je ustrezno pa tudi zakonitih interesov, za katere si prizadeva upravljavec;
(b) oceno potrebnosti in sorazmernosti dejanj obdelave glede na njihov namen;
(c) oceno tveganj za pravice in svoboščine posameznikov, na katere se nanašajo osebni podatki, iz odstavka 1, ter
(d) ukrepe za obravnavanje tveganj, vključno z zaščitnimi ukrepi, varnostne ukrepe ter mehanizme za zagotavljanje varstva osebnih podatkov in za dokazovanje skladnosti s to uredbo, ob

upoštevanju pravic in zakonitih interesov posameznikov, na katere se nanašajo osebni podatki, ter drugih oseb, ki jih to zadeva.

72. člen

Upravljavec se pred obdelavo posvetuje z Informacijskim pooblaščencem, kadar je iz ocene učinka v zvezi z varstvom podatkov iz prejšnjega člena razvidno, da bi obdelava povzročila veliko tveganje, če upravljavec ne bi sprejel ukrepov za ublažitev tveganja.

Pri posvetovanju z nadzornim organom v skladu s 1. odstavkom upravljavec Informacijskemu pooblaščencu predloži:
(a) kadar je ustrezno, dolžnosti upravljavca, skupnih upravljavcev in obdelovalcev, vključenih v obdelavo, zlasti pri obdelavi v povezani družbi;
(b) namene in sredstva predvidene obdelave;
(c) ukrepe in zaščitne ukrepe za zaščito pravic in svoboščin posameznikov, na katere se nanašajo osebni podatki, v skladu s to uredbo;
(d) kadar je ustrezno, kontaktne podatke pooblaščene osebe za varstvo podatkov;
(e) oceno učinka v zvezi z varstvom podatkov iz prejšnjega člena in
(f) vsakršne druge informacije, ki jih zahteva nadzorni organ.

XIV. UKREPANJE OB UGOTOVITVI ZLORABE OSEBNIH PODATKOV ALI VDORU V ZBIRKE OSEBNIH PODATKOV

73. člen

Delavci upravljavca osebnih podatkov, ki pridejo v stik z osebnimi podatki, so dolžni izvajati ukrepe za preprečevanje zlorabe osebnih podatkov in morajo z osebnimi podatki, s katerimi se seznanijo pri svojem delu, ravnati vestno in skrbno na način in po postopkih, ki jih določata ta pravilnik in operacijski predpis.

Delavec, ki izve ali opazi, da je prišlo do zlorabe osebnih podatkov (razkritje osebnih podatkov, nepooblaščeno uničenje, nepooblaščeno spreminjanje, poškodovanje zbirke, prilaščanje osebnih podatkov) ali do vdora v zbirko osebnih podatkov, mora o tem takoj obvestiti direktorja in pooblaščenega delavca, ki vodi in ureja zbirko osebnih podatkov, ki so bili zlorabljeni ali v katero se je nepooblaščeno poseglo.

74. člen

Upravljavec lahko zoper tistega, za katerega obstaja sum, da je zlorabil osebne podatke ali je nepooblaščeno posegel v zbirko osebnih podatkov, ukrepa v skladu z zakonodajo.

Če pri nepooblaščenem posegu v zbirko osebnih podatkov obstaja sum, da je ta storjen z naklepom in namenom zlorabiti osebne podatke ali jih uporabiti v nasprotju z nameni, za katere so zbrani ali če je do zlorabe osebnih podatkov že prišlo, lahko upravljavec osebnih podatkov poleg uvedbe disciplinskega postopka oz. postopka odpovedi pogodbe zoper storilca, če je ta delavec družbe, nepooblaščeni poseg ali drugo zlorabo prijavi organom pregona.

Za zlorabo osebnih podatkov se šteje vsaka uporaba osebnih podatkov v namene, ki niso v skladu z nameni zbiranja, določenimi v zakonu na podlagi katerega se zbirajo ali nameni, določenimi v evidenci obdelav podatkov.

75. člen

V primeru kršitve varstva osebnih podatkov upravljavec brez nepotrebnega odlašanja, po možnosti pa najpozneje v 72 urah po seznanitvi s kršitvijo, o njej uradno obvesti Informacijskega pooblaščenca, razen če ni verjetno, da bi bile s kršitvijo varstva osebnih podatkov ogrožene pravice in svoboščine

posameznikov. Kadar uradno obvestilo Informacijskemu pooblaščencu ni podano v 72 urah, se mu priloži navedbo razlogov za zamudo.

Uradno obvestilo iz prejšnjega odstavka vsebuje vsaj (Priloga F):

a) opis vrste kršitve varstva osebnih podatkov, po možnosti tudi kategorije in približno število zadevnih posameznikov, na katere se nanašajo osebni podatki, ter vrste in približno število zadevnih evidenc osebnih podatkov;

b) sporočilo o imenu in kontaktnih podatkih pooblaščene osebe za varstvo podatkov ali druge kontaktne točke, pri kateri je mogoče pridobiti več informacij;

c) opis verjetnih posledic kršitve varstva osebnih podatkov;

d) opis ukrepov, ki jih upravljavec osebnih podatkov sprejel ali katerih sprejetje predlaga za obravnavanje kršitve varstva osebnih podatkov, pa tudi ukrepov za ublažitev morebitnih škodljivih učinkov kršitve, če je to ustrezno.

Upravljavec osebnih podatkov je dolžan dokumentirati vsako kršitev varstva osebnih podatkov, vključno z dejstvi v zvezi s kršitvijo varstva osebnih podatkov, njene učinke in sprejete popravne ukrepe. Ta dokumentacija Informacijskemu pooblaščencu omogoči, da preveri skladnost s tem členom.

76. člen

Kadar je verjetno, da kršitev varstva osebnih podatkov lahko povzroči veliko tveganje za pravice in svoboščine posameznikov, upravljavec osebnih podatkov brez nepotrebnega odlašanja sporoči posamezniku, na katerega se nanašajo osebni podatki, da je prišlo do kršitve varstva osebnih podatkov.

V sporočilo posamezniku, na katerega se nanašajo osebni podatki, mora biti v jasnem in preprostem jeziku opisana vrsta kršitve varstva osebnih podatkov tet vsebovane vsaj naslednje informacije:

- sporočilo o imenu in kontaktnih podatkih pooblaščene osebe za varstvo podatkov ali druge kontaktne točke, pri kateri je mogoče pridobiti več informacij;
- opis verjetnih posledic kršitve varstva osebnih podatkov;
- opis ukrepov, ki jih je upravljavec osebnih podatkov sprejel ali katerih sprejetje predlaga za obravnavanje kršitve varstva osebnih podatkov, pa tudi ukrepov za ublažitev morebitnih škodljivih učinkov kršitve, če je to ustrezno.

Sporočilo posamezniku, na katerega se nanašajo osebni podatki, iz prvega odstavka tega člena ni potrebno, če je izpolnjen kateri koli izmed naslednjih pogojev:

- upravljavec osebnih podatkov je izvedel ustrezne tehnične in organizacijske zaščitne ukrepe in so bili ti ukrepi uporabljeni za osebne podatke, v zvezi s katerimi je bila storjena kršitev varstva, zlasti ukrepe, na podlagi katerih postanejo osebni podatki nerazumljivi vsem, ki niso pooblaščeni za dostop do njih, kot je šifriranje;
- upravljavec osebnih podatkov je sprejel naknadne ukrepe za zagotovitev, da se veliko tveganje za pravice in svoboščine posameznikov, na katere se nanašajo osebni podatki, iz prvega odstavka tega člena verjetno ne bo več udejanjilo;
- to bi zahtevalo nesorazmeren napor. V takšnem primeru se namesto tega objavi javno sporočilo ali izvede podoben ukrep, s katerim so posamezniki, na katere se nanašajo osebni podatki, enako učinkovito obveščeni.

XV. ODGOVORNOST DELAVCEV ZA IZVAJANJE UKREPOV ZAVAROVANJA OSEBNIH PODATKOV

77. člen

Pred nastopom dela delavca na delovnem mestu, kjer se zbirajo, urejajo, obdelujejo, spreminjajo, shranjujejo, posredujejo ali uporabljajo osebni podatki ali nosilci osebnih podatkov, mora delavec

podpisati izjavo, ki ga zavezuje k varovanju osebnih podatkov kot poklicne skrivnosti in v kateri je opozorjen na posledice kršitve te dolžnosti (Priloga E).

Dolžnost varovanja osebnih podatkov, s katerimi se je delavec seznanil pri svojem delu, velja tudi po prenehanju delovnega razmerja pri upravljavcu osebnih podatkov.

XVI. VGRAJENO IN PRIVZETO VARSTVO PODATKOV

78. člen

Upravljavec mora tako v času določanja sredstev obdelave kot tudi v času same obdelave izvajati ustrezne tehnične in organizacijske ukrepe, ki so oblikovani za učinkovito izvajanje načel varstva podatkov, ter v obdelavo vključiti potrebne zaščitne ukrepe, da se izpolnijo zahteve tega pravilnika in zaščitijo pravice posameznikov, na katere se nanašajo osebni podatki.

79. člen

Odgovorne osebe upravljavca morajo izvesti ustrezne tehnične in organizacijske ukrepe, s katerimi zagotovijo, da se privzeto obdelajo samo osebni podatki, ki so potrebni za vsak poseben namen obdelave. Ta obveznost velja za količino zbranih osebnih podatkov, obseg njihove obdelave, obdobje njihove hrambe in njihovo dostopnost. S takšnimi ukrepi se zagotovi zlasti, da osebni podatki niso samodejno dostopni nedoločenemu številu posameznikov brez posredovanja zadevnega posameznika (Priloga G).

XVII. PREHODNE IN KONČNE DOLOČBE

80. člen

Spremembe in dopolnitve tega pravilnika sprejme direktor podjetja po postopku in na način kot velja za sprejem tega pravilnika.

Direktor v roku enega (1) meseca po sprejetju tega pravilnika, sprejme operacijski predpis o varstvu osebnih podatkov, v katerem konkretizira postopke in ukrepe za varstvo zbirk osebnih podatkov iz tega pravilnika.

81. člen

Z določbami tega pravilnika morajo biti seznanjeni vsi delavci pri upravljavcu osebnih podatkov, ki pridejo v stik z osebnimi podatki.

Vsi zaposleni pri upravljavcu morajo podpisati izjavo iz 77. člena tega pravilnika v roku 30 dni od dneva sprejema tega pravilnika.

82. člen

Ta pravilnik prične veljati v roku osmih (8) dni od dneva objave.

Direktor Javnega podjetja Kraški vodovod Sežana d.o.o.

PRIMOŽ TURŠIČ

KRAŠKI VODOVOD SEŽANA
JAVNO PODJETJE d.o.o.

PRILOGA A

OBRAZEC MANIPULACIJ Z OSEBNIMI PODATKI

SLEDLJIVOST NOTRANJIH OBDELOVANJ

Zap.št.	Opredelitev posameznega osebnega podatka (oseba na katero se osebni podatek nanaša in vrsta osebnega podatka)	Datum vnosa posameznega osebnega podatka v zbirko, uporabe ali druge obdelave	Izvedena obdelava na posameznem osebnem podatku (vnos, uporaba, sprememba, kopiranje ipd.)	Oseba, ki je posamezni osebni podatek vnesla v zbirko, uporabila ali kako drugače obdelala

OBRAZEC POSREDOVANJ OSEBNIH PODATKOV

Zap.št.	Datum posredovanja	Uporabnik	Pravna podlaga	Vrste osebnih podatkov	Namen posredovanja

PRILOGA B

POOBLASTILO DELAVCU ZA DELO Z OSEBNIMI PODATKI

Na podlagi 39. člena Pravilnika o varstvu osebnih podatkov, sprejetega dne _____, spodaj podpisani/a _____ *(ime in priimek odgovorne osebe za posamezno zbirko osebnih podatkov)*
pooblaščam _____ *(ime in priimek pooblaščenega delavca za obdelavo osebnih podatkov),* zaposlenega v podjetju Javno podjetje Kraški vodovod Sežana d.o.o., za delo z osebnimi podatki v evidenci osebnih podatkov _____ *(navedite naslov evidence osebnih podatkov).*

Datum: __ . __ . _____ Podpis odgovorne osebe: _____

PRILOGA C

PRIVOLITEV POSAMEZNIKA ZA ZBIRANJE OSEBNIH PODATKOV

Če ste posameznika, od katerega pridobivate soglasje za obdelavo osebnih podatkov, že seznanili z informacijami iz 13. člena Uredbe EU, lahko uporabite naslednji obrazec za soglasje:

Spodaj podpisani/a _____ *(ime in priimek),* _____ *(naslov stalnega oz. začasnega prebivališča),* _____ (datum rojstva), dovoljujem, da podjetje Javno podjetje Kraški vodovod Sežana d.o.o., (»upravljavec«) sledeče osebne podatke*(navedite osebne podatke)*

_____

_____

obdeluje za naslednje namene (prosimo, označite ali se strinjate z obdelovanjem vaših osebnih podatkov za zapisan namen):

1. namen (vpišite namen) DA NE
2. namen (vpišite namen) DA NE

Datum: Podpis:

Dne _____, preklicujem obdelavo svojih osebnih podatkov za naslednji namen:

1. namen (vpišite namen) PREKLICUJUEM
2. namen (vpišite namen) PREKLICUJUEM

Podpis: _____

PRILOGA D

INFORMACIJE, KI SE ZAGOTOVIJO, KADAR SE OSEBNI PODATKI PRIDOBIJO OD POSAMEZNIKA, NA KATEREGA SE NANAŠAJO OSEBNI PODATKI

Če posamezniku na drug način niso bile zagotovljene informacije iz 13. člena Uredbe EU, jih vključite v soglasje za obdelavo osebnih podatkov.

Spodaj podpisani/a _____ (ime in priimek), _____ (naslov stalnega oz. začasnega prebivališča), _____ (datum rojstva), dovoljujem, da podjetje Javno podjetje Kraški vodovod Sežana d.o.o., (»upravljavec osebnih podatkov«) obdeluje moje kontaktne podatke (kot so na primer _____, ipd.), za spodaj opredeljene namene:

Prosimo označite, ali se strinjate z obdelovanjem vaših osebnih podatkov za zapisan namen:

1. namen (vpišite namen) DA NE

2. namen (vpišite namen) DA NE

Upravljavec zagotavlja, da bodo Vaši osebni podatki predmet obdelave zgolj za namene, s katerimi izrecno soglašate. Privolitev v posredovanje osebnih podatkov je prostovoljna, soglasje pa lahko na isti način, kot ste ga podali, tudi kadarkoli prekličete. V primeru, da osebnih podatkov ne posredujete ali oz. v kolikor soglasje prekličete, upravljavec ne more izpolniti namena, za katerega se podatki zbirajo. Poleg tega imate pravico do dostopa do podatkov, pravico do popravka, pravico do izbrisa (»pravica do pozabe«), pravico do omejitve obdelave, pravico do ugovora ter pravico do prenosljivosti podatkov. Za uveljavljanje prej omenjenih pravic oz. morebitnih pritožb Vas prosimo, da se obrnete na _____. Pooblaščena oseba za varstvo osebnih podatkov v podjetju Javno podjetje Kraški vodovod Sežana d.o.o. je _____.

Če menite, da obdelava osebnih podatkov krši določila na področju varstva osebnih podatkov, imate pravico vložiti pritožbo tudi pri Informacijskemu pooblaščencu.

Podatki se hranijo _____ /do vašega preklica oz. dokler je potrebno, da se doseže namen, zaradi katerega so podatki zbrani ter se po preteku roka zbrišejo, uničijo, blokirajo oz. anonimizirajo.

Upravljavec, podjetje Javno podjetje Kraški vodovod Sežana d.o.o., se obvezuje, da bo podatke obdeloval in varoval v skladu z Zakonom o varstvu osebnih podatkov ter določili Uredbe (EU) 2016/679 Evropskega parlamenta in Sveta.

Datum: Podpis:

Dne _____, preklicujem obdelavo svojih osebnih podatkov v zvezi s spodaj opredeljenimi nameni:

1. namen (vpišite namen) PREKLICUJUEM
2. namen (vpišite namen) PREKLICUJUEM

Podpis: _____

PRILOGA E

IZJAVA

IME IN PRIIMEK: _____

NASLOV PREBIVALIŠČA: _____

Datum: _____

Na podlagi 77. in 81. člena Pravilnika o varstvu osebnih podatkov, sprejetega dne _____, podpisani

_____

IZJAVLJAM,

I.

da sem bil/a dne _____, pred pričetkom dela na delovnem mestu poučen/a o postopkih in ukrepih za zavarovanje osebnih podatkov v podjetju Javno podjetje Kraški vodovod Sežana d.o.o., Bazoviška cesta 6, 6210 Sežana, matična številka: 5072999 in da sem bil seznanjen s Pravilnikom o varstvu osebnih podatkov ter Operacijskim predpisom za varstvo osebnih podatkov.

II.

da sem bil/a istega dne kot pod točko I. opozorjen/a na dolžnost varovanja osebnih podatkov, s katerimi sem se ali se bom seznanil/a pri svojem delu kot poklicno tajnost, ter da sem bil/a opozorjen, da sem zavezan/a varovati osebne podatke, s katerimi sem se ali se bom seznanil/a pri svojem delu v podjetju, tudi po prenehanju delovnega razmerja.

III.

da sem bil/a istega dne kot pod točko I. poučen/a, da lahko kršitev dolžnosti iz točke II. predstavlja podlago za disciplinsko odgovornost, odpoved pogodbe oz. uvedbo kazenskega postopka.

Podpis:

_____

PRILOGA F

Obvestilo o kršitvi varstva osebnih podatkov

1. Podatki o prijavitelju

Ime in priimek ali naziv pravne osebe	
Naslov	
Telefon	
E-pošta	

2. Kontaktni podatki pooblaščene osebe za varstvo osebnih podatkov, ali druge kontaktne točke, kjer je mogoče pridobiti več informacij

Ime in priimek	
Naslov	
Telefon	
E-pošta	

3. Podrobnejši podatki o kršitvi

Opišite vrste kršitve varstva osebnih podatkov	
Kategorije in približno število zadevnih posameznikov, na katere se nanašajo osebni podatki	
Vrste in približno število zadevnih evidenc osebnih podatkov	

4. Verjetne posledice kršitve varstva osebnih podatkov

Opišite verjetne posledice kršitve varstva osebnih podatkov

5. Sprejeti/predlagani ukrepi za obravnavanje kršitve

Opišite ukrepe, ki ste jih sprejeli ali ukrepe, ki jih predlagate za obravnavanje kršitve ter ukrepe za ublažitev morebitnih škodljivih učinkov kršitve, če je to ustrezno

PRILOGA G

Privzeto in vgrajeno varstvo osebnih podatkov

	DA	NE
APLIKACIJE		
Razvojno, testno in produkcijsko okolje je ločeno.	☐	☐
Tesni podatki so skrbno izbrani, varovani in nadzorovani.	☐	☐
GESLA		
Dolžina uporabniških gesel je predpisana na min. 8 znakov.	☐	☐
Geslo mora biti predpisano na način, da je sestavljeni iz minimalno 3 različnih znakov ter brez šumnikov.	☐	☐
Pet zaporednih gesel je neponovljivih.	☐	☐
Sistem samodejno opozarja na potek veljavnosti gesel ter samodejno zahteva menjavo gesla po preteku veljavnosti.	☐	☐
SLEDLJIVOST DOSTOPA DO PODATKOV		
Beležijo se uporabniški dostopi do podatkov.	☐	☐
Beležijo se administratorski dostopi do podatkov.	☐	☐
Omogočena je sledljivost sprememb podatkov.	☐	☐
Omogočena je sledljivost dostopov do podatkov.	☐	☐
Zagotovljena je celovitost in avtentičnost revizijskih sledi.	☐	☐
VAROVANJE PODATKOV		
Uporablja se sistem za zaznavo nepooblaščenega dostopa.	☐	☐
Občutljivi osebni podatki so posebej označeni.	☐	☐
Občutljivi osebni podatki se pri prenosu telekomunikacijskih omrežij kriptirajo ali pa so elektronsko podpisani.	☐	☐
Sistemsko je omogočeno, da se podatki obdelujejo/ne obdelujejo za posamezne namene.	☐	☐
Tehnično je izvedljiv izvoz in prenos osebnih podatkov za vsakega posameznika .	☐	☐
Beležijo se izvozi podatkov.	☐	☐
Aplikacija omogoča popravek oz. izbris osebnih podatkov.	☐	☐
Predvideni so ukrepi za preprečitev nepooblaščenega dostopa in obdelave podatkov v celotnem procesu obdelave.	☐	☐
Zagotovljen je minimalni rok hrambe vhodnih podatkov.	☐	☐

Zbirajo se samo potrebni osebni podatki (upoštevano je načelo sorazmernosti).	☐	☐
Pri rezultatih iskanja se prikazujejo samo podatki, ki uporabnika zanimajo.	☐	☐
SPLETNE STRANI		
Uporabniku je na voljo izbira, ali se strinja z uporabo piškotkov ali ne.	☐	☐
Uporabnik je bil, še preden je bil piškotek naložen, jasno in izčrpno obveščen o upravljavcu, kateri piškotki se uporabljajo in za kakšen namen bodo uporabljeni podatki, ki se s pomočjo piškotka obdelujejo.	☐	☐
Ob začetnem obisku vhodne strani ni naložen noben piškotek, za katerega je potrebna privolitev.	☐	☐
Uporabniku je ponujena možnost, da naknadno spremeni nastavitve piškotkov.	☐	☐
Potrditvena polja, s katerimi posameznik potrdi strinjanje z obdelavo svojih podatkov so privzeto prazna – strinjanje lahko posameznik z izpolnitvijo aktivno poda.	☐	☐