Na podlagi določil Uredbe EU 2016/679 Evropskega parlamenta in Sveta z dne 27.04.2016 o varstvu posameznikov pri obdelavi osebnih podatkov in prostem pretoku takih podatkov (GDPR) in 6. člena Zakona o varstvu osebnih podatkov (Uradni list RS št. 163/22, v nadaljevanju ZVOP-2), sprejme v.d. direktor družbe **JP KOMUNALA CERKNICA D.O.O.**, Notranjska cesta 44, 1380 Cerknica, matična številka 5067758000 (v pravilniku družba)

naslednji splošni akt družbe:

PRAVILNIK O VARSTVU OSEBNIH PODATKOV

Vsebina:

SPLOŠNI DEL

1. SPLOŠNE DOLOČBE

1.1 Vsebina in namen pravilnika

1. člen

Ta pravilnik določa načela in pravila ravnanja pri obdelavi osebnih podatkov zaradi zagotavljanja varstva pravic posameznika, na katerega se nanašajo osebni podatki, da se prepreči slučajno ali namerno nedovoljeno ali nezakonito obdelavo ter njihova sprememba, nenamerna izguba, uničenje ali poškodba.

Posebni del pravilnika določa organizacijske, tehnične in logično-tehnične postopke ter ukrepe za zavarovanje osebnih podatkov.

V pravilniku uporabljeni izrazi, zapisani v moški slovnični obliki, so uporabljeni kot nevtralni za ženske in moške.

1.2 Položaj družbe pri obdelavi osebnih podatkov

2. člen

Družba ima pri obdelavi osebnih podatkov položaj upravljavca ter s tem povezane obveznosti in odgovornosti po GDPR, ZVOP-2 in tem pravilniku.

1.3 Opredelitev pojmov in pomen izrazov

3. člen

Za razumevanje določb pravilnika imajo v tem pravilniku uporabljeni izrazi naslednji pomen:

a) „**Osebni podatek**“ (tudi OP) pomeni katero koli informacijo v zvezi z določenim ali določljivim posameznikom, na katerega se nanašajo osebni podatki; določljiv posameznik je tisti, ki ga je mogoče neposredno ali posredno določiti, zlasti z navedbo identifikatorja, kot je ime, identifikacijska številka, podatki o lokaciji, spletni identifikator, ali z navedbo enega ali več dejavnikov, ki so značilni za fizično, fiziološko, gensko, duševno, gospodarsko, kulturno ali družbeno identiteto tega posameznika, zlasti: identifikacijski podatki o posamezniku (rojstni podatki, EMŠO itd.); podatki, ki se nanašajo na rasno poreklo in pripadnost narodu ali narodnosti, na družinska razmerja, na stanovanjske in bivalne pogoje posameznika, podatki o zaposlitvi, o socialnem in ekonomskem stanju posameznika, o izobrazbi in pridobljenih znanjih, o aktivnostih v prostem času, o zdravstvenem stanju posameznika, o ideoloških in verskih prepričanjih, o navadah posameznika itd;

b) „**Občutljivi osebni podatki**“ - so podatki o rasnem, narodnem ali narodnostnem poreklu, političnem, verskem, filozofskem prepričanju, članstvu v sindikatu, zdravstvenem stanju, spolnem življenju, vpisu ali izbrisu v ali iz kazenske evidence ali prekrškovne evidence ter biometrične značilnosti.

c) „**Obdelava**“ pomeni vsako dejanje ali niz dejanj, ki se izvaja v zvezi z osebnimi podatki ali nizi osebnih podatkov z avtomatiziranimi sredstvi ali brez njih, kot je zbiranje, beleženje, urejanje, strukturiranje, shranjevanje, prilagajanje ali spreminjanje, priklic, vpogled, uporaba, razkritje s posredovanjem, razširjanje ali drugačno omogočanje dostopa, prilagajanje ali kombiniranje, omejevanje, izbris ali uničenje;

d) „**Omejitev obdelave**“ pomeni označevanje shranjenih osebnih podatkov zaradi omejevanja njihove obdelave v prihodnosti;

e) „**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;
f) „**Psevdonimizacija**" pomeni obdelavo osebnih podatkov na tak način, da osebnih podatkov brez dodatnih informacij ni več mogoče pripisati specifičnemu posamezniku, na katerega se nanašajo, 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;
g) „**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;
h) „**Upravljavec**" pomeni fizično ali pravno osebo, javni organ, agencijo ali drugo telo, ki samo ali skupaj z drugimi določa namene in sredstva obdelave;
i) „**Obdelovalec**" pomeni fizično ali pravno osebo, javni organ, agencijo ali drugo telo, ki obdeluje osebne podatke v imenu upravljavca;
j) „**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 z zakonom, ne štejejo za uporabnike;
k) „**Tretja oseba**" pomeni fizično ali pravno osebo, javni organ, agencijo ali telo, ki ni posameznik, na katerega se nanašajo osebni podatki, upravljavec, obdelovalec in osebe, ki so pooblaščene za obdelavo osebnih podatkov pod neposrednim vodstvom upravljavca ali obdelovalca;
l) „**Privolitev posameznika, na katerega se nanašajo osebni podatki**" pomeni vsako prostovoljno, konkretno, informirano in nedvoumno izjavo volje posameznika, na katerega se nanašajo osebni podatki, s katero z izjavo ali jasnim pritrdilnim dejanjem izrazi soglasje za obdelavo osebnih podatkov, ki se nanašajo nanj;
m) „**Kršitev varstva osebnih podatkov**" pomeni kršitev varnosti, ki povzroči nenamerno ali nezakonito uničenje, izgubo, spremembo, nepooblaščeno razkritje ali dostop do osebnih podatkov, ki so poslani, shranjeni ali kako drugače obdelani;
n) „**Nosilec podatkov**" Pomenijo vse vrste sredstev, na katerih so zapisani ali posneti podatki (listine, akti, gradiva, spisi, računalniška oprema vključno s magnetni, optični ali drugi računalniški mediji, fotokopije, zvočno in slikovno gradivo, mikrofilmi, naprave za prenos podatkov, ipd.).

1.4 Uporaba pravilnika

4. člen

Določbe tega pravilnika veljajo za:
- zaposlene pri družbi,
- zunanje sodelavce, ki pri družbi opravljajo dela na podlagi pogodbe o delu ali druge pogodbe ter dijake in študente, ki pri družbi opravljajo dela preko napotnic oziroma ali so na praksi in
- zunanje pravne in fizične osebe, s katerimi se družba dogovori za izvedbo vseh ali posameznega opravila v zvezi z obdelavo osebnih podatkov, zlasti za izvajanje specifičnih dejavnosti obdelave (pogodbeni obdelovalec).

Vse te osebe morajo biti seznanjene z določbami GDPR, ZVOP-2, s področno zakonodajo, ki ureja posamezno področje njihovega dela ter z vsebino tega pravilnika.

2. SPLOŠNA NAČELA PRI OBDELAVI OSEBNIH PODATKOV

2.1 Pravna podlaga za obdelavo OP

5. člen

Osebni podatki se lahko obdelujejo le, če je za njihovo obdelavo podana pravna podlaga v GDPR in/ali ZVOP-2 (zakonita obdelava), kar je zlasti, ko:
- posameznik, na katerega se nanašajo osebni podatki, privoli v obdelavo njegovih osebnih podatkov v enega ali več določenih namenov;
- je obdelava potrebna za izvajanje pogodbe, katere pogodbena stranka je posameznik, na katerega se nanašajo osebni podatki, ali za izvajanje ukrepov na zahtevo takega posameznika pred sklenitvijo pogodbe;
- je obdelava potrebna za izpolnitev zakonske obveznosti, ki velja za upravljavca;
- je obdelava potrebna za zaščito življenjskih interesov posameznika, na katerega se nanašajo osebni podatki, ali druge fizične osebe;
- je obdelava potrebna za opravljanje naloge v javnem interesu ali pri izvajanju javne oblasti, dodeljene upravljavcu.

Občutljivi osebni podatki se lahko obdelujejo le na podlagi 23. člena ZVOP-2. Pri obdelavi morajo biti ti podatki posebej označeni (npr. kot ZAUPNO).

2.2 Namen zbiranja in nadaljnja obdelava

6. člen

Osebni podatki se lahko zbirajo le za določene, izrecne 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 („omejitev namena").

2.3 Obseg zbiranja

7. člen

Osebni podatki se lahko zbirajo le v ustreznem obsegu, njihovo zbiranje je omejeno na to, kar je potrebno za namene, za katere se obdelujejo („najmanjši obseg podatkov").

2.4 Točnost osebnih podatkov

8. člen

Osebni podatki, ki se obdelujejo morajo biti točni in, kadar je to potrebno, posodobljeni. Sprejeti je treba vse razumne ukrepe za zagotovitev, da se netočni osebni podatki brez odlašanja izbrišejo ali popravijo ob upoštevanju namenov, za katere se obdelujejo („točnost").

2.5 Čas hrambe osebnih podatkov

9. člen

Hramba osebnih podatkov v obliki, ki dopušča identifikacijo posameznika je dopustno le toliko časa, kolikor je potrebno za namene, za katere se osebni podatki obdelujejo, za daljše obdobje pa le za namene arhiviranja v javnem interesu, za znanstveno ali zgodovinsko raziskovalne namene ali

statistične namene („omejitev hrambe"). Upravljavec v posamezni zbirki osebnih podatkov določi rok njihove hrambe.

Po izpolnitvi namena obdelave se osebni podatki zbrišejo, uničijo, blokirajo ali anonimizirajo, če niso na podlagi zakona opredeljeni kot arhivsko gradivo. Upravljavec osebnih podatkov po poteku roka hrambe obvesti obdelovalce osebnih podatkov, da izbrišejo vse povezave do osebnih podatkov, kopij ali drugih ponovitev.

2.6 Varstvo osebnih podatkov

10. člen

Osebni podatki se obdelujejo na način, ki zagotavlja ustrezno varnost, da se zaščitijo pred nedovoljeno ali nezakonito obdelavo ter pred nenamerno izgubo, uničenjem ali poškodbo. Varovanje osebnih podatkov zajema pravne, organizacijske in logistično-tehnične postopke in ukrepe, s katerimi se:
(1) varujejo prostori, aparature in sistemska programska oprema,
(2) varuje aplikativna programska oprema, s katero se obdelujejo osebni podatki,
(3) zagotavlja varnost posredovanja in prenosa osebnih podatkov,
(4) onemogoča nepooblaščenim osebam dostop do naprav, na katerih se obdelujejo osebni podatki in do njihovih zbirk.

2.7 Odgovornost upravljavca/obdelovalca

11. člen

Upravljavec je odgovoren za zakonitost obdelave osebnih podatkov in skladnost s splošnimi načeli ter je to skladnost tudi zmožen dokazati („odgovornost").

Obdelovalec je odgovoren za obdelavo in škodo, ki jo povzroči obdelava le, kadar ne izpolnjuje obveznosti iz GDPR in/ali ZVOP-2, ki so posebej naslovljene na obdelovalca, ali kadar je prekoračil zakonita navodila upravljavca ali ravnal v nasprotju z njimi.

3. UPRAVLJAVEC OSEBNIH PODATKOV

3.1 Privolitev posameznika

12. člen

Upravljavec podatkov jamči za pravno podlago za obdelavo osebnih podatkov.

Kadar je pravna podlaga privolitev posameznika, jo pridobi v obliki, da je zmožen dokazati, da je posameznik zanesljivo izrazil strinjanje z obdelavo podatkov, ki se nanašajo nanj v obliki izjave ali jasnega pritrdilnega ravnanja (npr. posebna pisna izjava).

Privolitev je lahko podana v posebnem dokumentu, ločeno od ostalih dogovorov, oblikovana mora biti v preprostem jeziku, na jasen in razumljiv način mora vsebovati, kateri osebni podatki se bodo zbirali in namen zbiranja, če je namenov več, mora posameznik podati strinjanje k vsakemu od njih posebej. (Obrazec 1).

Zagotavljanje kakšne storitve ne sme biti pogojeno s privolitvijo posameznika v obdelavo osebnih podatkov.

Posameznika je potrebno v privolitvi obvestiti o pravici, da lahko privolitev kadarkoli prekliče, preklic privolitve mu mora biti zagotovljeno na enako enostaven način, kot je urejena privolitev. Preklic privolitve ne vpliva na zakonitost obdelave pred preklicem.

Privolitev za osebo, mlajšo od 18. let, mora podati njen zakoniti zastopnik.

3.2 Zbirke osebnih podatkov

13. člen

Družba vodi seznam zbirk osebnih podatkov, ki jih kot upravljavec obdeluje v svojem imenu (Obrazec 2).

3.3 Katalog zbirke osebnih podatkov

14. člen

Zakoniti zastopnik družbe za vsako zbirko osebnih podatkov vzpostavi katalog zbirke osebnih podatkov, za katere veljajo v celoti ta pravila ravnanja z osebnimi podatki.

3.4 Obveščanje posameznika o obdelavi osebnih podatkov (Pravila ravnanja z osebnimi podatki)

15. člen

Upravljavec mora posameznika obvestiti o obdelavi osebnih podatkov, seznaniti ga mora o osebi upravljavca, namenu obdelave, uporabnikih njegovih osebnih podatkov, ali se bodo prenašali v tretjo državo, obdobje hrambe, o njegovih pravicah (do vpogleda, prepisa, kopiranja, dopolnitve, popravka, blokiranja in izbrisa osebnih podatkov, ki se nanašajo nanj).

Če se osebni podatki pridobivajo od posameznika neposredno, se mu te informacije zagotovijo takrat, ko se od njega pridobivajo osebni podatki, sicer pa v razumnem roku, ki ne sme biti daljši od enega meseca.

3.5 Odgovorna oseba in pooblaščene osebe

16. člen

Zakoniti zastopnik družbe je odgovorna oseba za zbirke osebnih podatkov (v nadaljevanju: odgovorna oseba). Odgovorna oseba pooblasti osebe, ki v družbi lahko zaradi narave njihovega dela obdelujejo osebne podatke (v nadaljevanju: pooblaščene osebe) (Obrazec 3).

Odgovorna oseba ter pooblaščene osebe morajo biti pred obdelavo osebnih podatkov seznanjeni z določbami GDPR, ZVOP-2 in tega pravilnika ter morajo podpisati Izjavo o varovanju osebnih podatkov (Obrazec 4 in 5).

4. POGODBENI OBDELOVALEC OSEBNIH PODATKOV

4.1 Pogoji za pogodbenega obdelovalca osebnih podatkov

17. člen

Družba sodeluje zgolj s pogodbenimi obdelovalci, ki zagotovijo zadostna jamstva za izvedbo ustreznih tehničnih in organizacijskih ukrepov, da obdelava izpolnjuje zahteve iz GDPR, ZVOP-2 in tega pravilnika ter zagotavlja varstvo pravic posameznika, na katerega se nanašajo osebni podatki.

Pogodbeni obdelovalci ne smejo zaposliti drugega obdelovalca brez predhodnega posebnega ali splošnega pisnega dovoljenja družbe.

4.2 Odgovornost pogodbenega obdelovalca

18. člen

Pogodbeni obdelovalec lahko opravlja storitve obdelave osebnih podatkov samo v okviru pooblastil iz sklenjene pogodbe in podatkov ne sme obdelovati ali drugače uporabljati za noben drug namen.

Pogodbeni obdelovalec je odgovoren za obdelavo in škodo, ki jo povzroči z obdelavo le, kadar ne izpolnjuje obveznosti iz GDPR in/ali ZVOP-2, ki so posebej naslovljene na obdelovalca, ali kadar prekorači zakonita navodila upravljavca ali ravna v nasprotju z njimi.

Kadar v soglasju z družbo delo pogodbenega obdelovalca opravi drugi obdelovalec, pogodbeni obdelovalec še naprej v celoti odgovarja za izpolnjevanje obveznosti drugega obdelovalca.

4.3 Tehnični in organizacijski ukrepi

19. člen

Pogodbeni obdelovalci, ki za družbo opravljajo pogodbeno dogovorjene storitve izven prostorov družbe, morajo imeti vsaj enako stopnjo tehničnega varovanja osebnih podatkov, kakor ga predvideva posebni del tega pravilnika ter izvajati organizacijske in logistično-tehnične postopke in ukrepe iz posebnega dela tega pravilnika.

POSEBNI DEL

5. ORGANIZACIJSKI POSTOPKI

5.1 Evidenca dejavnosti obdelave

20. člen

Evidenco dejavnosti obdelave vodita upravljavec in pogodbeni obdelovalec, vsak za vrsto dejavnosti obdelave, ki jih izvajata. Evidenca je v pisni obliki, vključno v elektronski obliki in vsebuje informacije iz 30. člena GDPR.

5.2 Posredovanje osebnih podatkov

21. člen

Osebni podatki se posredujejo samo tistim uporabnikom, o katerih je bil posameznik obveščen in je zanje podal privolitev pred pridobivanjem osebnih podatkov oziroma imajo njegovo kasnejšo pisno privolitev ali, ki se izkažejo z ustrezno zakonsko podlago.

Uporabnik poda zahtevo za posredovanje osebnih podatkov s pisno vlogo, v kateri mora jasno navesti določbo zakona, ki ga pooblašča za pridobitev osebnih podatkov, ali pa mora k zahtevi priložiti pisno privolitev posameznika, na katerega se podatki nanašajo.

5.3 Način posredovanja / prenašanja osebnih podatkov

22. člen

Osebne podatke je dovoljeno posredovati v fizični obliki, z informacijskimi, telekomunikacijskimi in drugimi sredstvi pa le ob izvajanju postopkov in ukrepov, ki nepooblaščenim osebam preprečujejo prilaščanje ali uničenje podatkov ter neupravičeno seznanjanje z njihovo vsebino.

Občutljive osebne podatke je dovoljeno posredovati preko komunikacijskih omrežij le, če so posebej zavarovani s kriptografskimi metodami in elektronskim podpisom tako, da je zagotovljena nečitljivost podatkov med njihovim prenosom.

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

Nikoli se ne posreduje originalen dokument, ki vsebuje osebne podatke, razen v primeru pisne odredbe sodišča, ki mora biti v času odsotnosti nadomeščen s fizično (fotokopijo) ali elektronsko (skenirano) kopijo.

5.4 Evidenca posredovanj osebnih podatkov

23. člen

Vsako posredovanje osebnih podatkov se zaznamuje v Evidenci posredovanj osebnih podatkov (Obrazec 6), z navedbo naslednjih podatkov:

- osebno ime/firmo/ime in naslov/sedež osebe, ki so ji bili posredovani osebni podatki,
- datum in ura posredovanja osebnih podatkov,
- kateri osebni podatki so bili posredovani,
- podlaga, na kateri so bili posredovani osebni podatki.

Zaznamek o tem se v pisni ali elektronski obliki, odvisno od nosilca podatkov, ki vsebuje posredovani osebni podatek, evidentira tudi v samo zbirko osebnih podatkov, ki ji pripada posredovani osebni podatek, v posebno rubriko "Evidenca posredovanj osebnih podatkov".

5.5 Sprejem poštne pošiljke z osebnimi podatki

24. člen

Delavec, ki je zadolžen za sprejem in evidenco pošte, odpira in pregleduje vse poštne pošiljke in pošiljke, ki na drug način prispejo v družbo (prinesejo jih stranke ali kurirji itd.) in so naslovljene na družbo, ne odpira pa tistih pošiljk, ki so naslovljene na drug organ ali organizacijo in so pomotoma dostavljena ter pošiljk, ki so naslovljene direktno na posameznika ali za katere iz označb na ovojnici izhaja, da se nanašajo na osebne podatke.

Delavec, ki je zadolžen za sprejem in evidenco pošte, ne sme odpirati pošiljk, ki so naslovljene na delavca, na katerih je na ovojnici navedeno, da se vročijo osebno naslovniku, ter pošiljk, na katerih je najprej navedeno osebno ime delavca brez označbe njegovega delovnega položaja v družbi in šele nato naslov družbe.

5.6 Uporaba osebnih podatkov s strani zaposlenih/zunanjih sodelavcev v družbi

25. člen

Zaposleni v družbi in zunanji sodelavci, ki pri izvajanju svojih delovnih nalog kopirajo, tiskajo in na drug tehničen način razmnožujejo dokumente, ki vsebujejo osebne podatke na napravah, ki jih uporablja večje število zaposlenih, po končanem kopiranju ali tiskanju dokumentov ne smejo puščati v, na ali ob napravah.

5.7 Hramba in uničenje osebnih podatkov

26. člen

Osebni podatki se lahko hranijo le toliko časa, kolikor je potrebno za dosego namena, zaradi katerega so se zbirali ali nadalje obdelovali. Čas hrambe določi upravljavec osebnih podatkov.

27. člen

Po preteku roka hrambe se osebni podatki zbrišejo, uničijo, blokirajo ali anonimizirajo, razen če zakon ali drug predpis za posamezne vrste osebnih podatkov ne določa drugače.

Za brisanje osebnih podatkov v elektronski obliki se uporabi takšna metoda brisanja, tako da je nemogoča rekonstrukcija vseh ali dela brisanih podatkov.

Osebni podatki v fizični obliki, vsebovani na klasičnih nosilcih (listine, kartoteke, register, seznam) se brišejo z uničenjem nosilcev tako, da se zagotovi, da postane osebni podatek nerazpoznaven in neobnovljiv (npr. rezalnik papirja).

Na enak način se mora brisati in uničevati tudi pomožna dokumentacija ali računalniški produkti oziroma predloge, ki vsebujejo posamezne osebne podatke.

Osebni podatki se izbrišejo tako, da se izbrišejo vse povezave do osebnih podatkov, kopije ali druge ponovitve osebnih podatkov.

Prepovedano je odmetavati odpadne nosilce podatkov, ki vsebujejo osebne podatke, na način, ki omogoča obnovitev ali razpoznavnost osebnih podatkov (npr. v koš za smeti).

Pri prenosu nosilcev osebnih podatkov na mesto uničenja je potrebno zagotoviti ustrezno zavarovanje tudi v času prenosa, zlasti tako, da je onemogočena razpoznavnost ali obnovitev osebnih podatkov.

Prenos nosilcev podatkov, ki vsebujejo občutljive osebne podatke, na mesto uničenja ter uničevanje takih nosilcev podatkov nadzoruje posebna tričlanska komisija, ki jo imenuje odgovorna oseba. Komisijo sestavljajo zaposleni v družbi, en član komisije je odgovorna oseba. O uničenju se sestavi ustrezen zapisnik.

6. TEHNIČNI IN LOGIČNO-TEHNIČNI POSTOPKI

6.1 Varovanje prostorov

28. člen

Prostori, v katerih se nahajajo nosilci podatkov, ki vsebujejo osebne podatke, strojna in programska oprema (v nadaljevanju: varovani prostori), morajo biti varovani z organizacijskimi in/ali tehničnimi ukrepi iz tega pravilnika, ki onemogočajo nepooblaščenim osebam dostop do podatkov.

Varovani prostori, v katerih se nahajajo nosilci podatkov, ki vsebujejo občutljive osebne podatke, morajo biti varovani tako, da je zagotovljen popolni nadzor nad delom in gibanjem v teh prostorih.

Pisarne morajo biti stalno pod nadzorom zaposlenih, ki v njih delajo. Ob odsotnosti mora zaposleni pisarno zakleniti. Ključi se ne smejo puščati v ključavnici v vratih.

V varovanih prostorih morajo biti po zaključku delovnega časa oziroma po končanem delu izven delovnega časa omare in pisalne mize z nosilci podatkov, ki vsebujejo osebne podatke, zaklenjene, računalniki in druga strojna oprema pa izklopljeni in fizično ali programsko zaklenjeni.

Omare, mize in drugo pohištvo z nosilci podatkov, ki vsebujejo osebne podatke, ki se nahajajo izven varovanih prostorov (hodniki, skupni prostori) mora biti stalno zaklenjeno.

Osebe, ki niso zaposlene v družbi (npr. vzdrževalci prostorov, strojne in programske opreme, obiskovalci, poslovni partnerji) se smejo gibati v varovanih prostorih samo z vednostjo zaposlenega, ki nadzoruje varovani prostor, kjer se oseba giba.

Zaposleni, kot so čistilke, varnostniki idr., se lahko izven delovnega časa gibljejo samo v tistih varovanih prostorih, kjer je onemogočen vpogled v osebne podatke (nosilci podatkov so shranjeni v zaklenjenih

omarah in pisalnih mizah, računalniki in druga strojna oprema so izklopljeni ali kako drugače fizično ali programsko zaklenjeni).

6.2 Varovanje nosilcev podatkov, ki vsebujejo osebne podatke

29. člen

Zaposleni pri družbi ne smejo puščati nosilcev podatkov, ki vsebujejo osebne podatke, na vidnem mestu (npr. na mizah) v prisotnosti oseb, ki nimajo pravice vpogleda vanje.

Nosilci podatkov, ki vsebujejo občutljive osebne podatke, se ne smejo hraniti izven varovanih prostorov.

Nosilce podatkov, ki vsebujejo osebne podatke, lahko zaposleni pri družbi odnašajo izven prostorov družbe samo z dovoljenjem direktorja družbe ali s strani direktorja družbe pooblaščene osebe.

Nosilcev podatkov, ki vsebujejo občutljive osebne podatke, zaposleni pri družbi ne smejo odnašati izven prostorov družbe, razen izjemoma z dovoljenjem direktorja družbe ali s strani direktorja družbe pooblaščene osebe, če je to nujno potrebno za reševanje zadeve, ki vsebuje te občutljive osebne podatke.

V prostorih, ki so namenjeni poslovanju s strankami, morajo biti nosilci podatkov, ki vsebujejo osebne podatke, in računalniški prikazovalniki nameščeni tako, da stranke nimajo vpogleda vanje.

6.3 Varovanje strojne in programske opreme

30. člen

Vzdrževanje in popravila strojne računalniške in druge opreme je dovoljeno samo z odobritvijo osebe, zadolžene za delovanje računalniškega informacijskega sistema, izvajajo pa ga lahko samo pooblaščeni servisi in vzdrževalci, ki imajo z družbo sklenjeno ustrezno pogodbo.

Dostop do programske opreme mora biti varovan tako, da dovoljuje dostop samo zaposlenim pri družbi, ali pravnim ali fizičnim osebam, ki v skladu s pogodbo opravljajo dogovorjene storitve.

Popravljanje, spreminjanje in dopolnjevanje sistemske in aplikativne programske opreme je dovoljeno samo na podlagi odobritve osebe, zadolžene za delovanje računalniškega informacijskega sistema, izvajajo pa ga lahko samo pooblaščeni servisi in organizacije ter posamezniki, ki imajo z družbo sklenjeno ustrezno pogodbo. Izvajalci morajo spremembe in dopolnitve sistemske in aplikativne programske opreme ustrezno dokumentirati.

Za shranjevanje in varovanje aplikativne programske opreme veljajo enaka določila kot za ostale podatke iz tega pravilnika.

Vsebina diskov mrežnega strežnika in lokalnih delovnih postaj, kjer se nahajajo osebni podatki, se vsakodnevno preveri z vidika prisotnosti računalniških virusov. Ob pojavu računalniškega virusa se tega čim prej odpravi s pomočjo ustrezne strokovne službe, obenem pa se ugotovi vzrok pojava virusa v računalniškem informacijskem sistemu upravljavca osebnih podatkov.

Vsi podatki in programska oprema, ki so namenjeni uporabi v računalniškem informacijskem sistemu in prispejo v družbo na medijih za prenos računalniških podatkov ali preko komunikacijskih kanalov, morajo biti pred uporabo preverjeni z vidika prisotnosti računalniških virusov.

Zaposleni pri družbi ne smejo inštalirati programske opreme in odnašati programske opreme iz prostorov družbe brez vednosti osebe, zadolžene za delovanje računalniškega informacijskega sistema.

Pristop do podatkov preko aplikativne programske opreme se varuje s sistemom gesel za avtorizacijo in identifikacijo uporabnikov programov in podatkov. Sistem gesel mora omogočati tudi možnost naknadnega ugotavljanja, kdaj so bili posamezni osebni podatki vneseni v zbirko podatkov, uporabljeni ali drugače obdelani ter kdo je to storil.

Oseba, zadolžena za delovanje računalniškega informacijskega sistema, določi način dodeljevanja, hranjenja in spreminjanja gesel in o tem seznani vse zaposlene pri družbi.

Vsa gesla in postopki, ki se uporabljajo za vstop in administriranje mreže osebnih računalnikov (nadzorniška gesla), administriranje elektronske pošte in administriranje aplikativnih programov se hranijo v zapečatenih ovojnicah in se jih varuje pred dostopom nepooblaščenih oseb. Uporabi se jih samo v izrednih okoliščinah oziroma ob nujnih primerih. Vsaka uporaba vsebine zapečatenih ovojnic se dokumentira. Po vsaki takšni uporabi se določi nova vsebina gesel.

Za potrebe restavriranja računalniškega sistema ob okvarah in ob drugih izjemnih situacijah se zagotavlja redna izdelava kopij vsebine mrežnega strežnika in lokalnih postaj, če se podatki nahajajo tam.

Kopije iz prejšnjega odstavka se hranijo na za to določenih mestih, ki morajo biti ognjevarna, zavarovana proti poplavam in elektromagnetnim motnjam, v okviru predpisanih klimatskih pogojev ter zaklenjena.

7. ODGOVORNOST ZA IZVAJANJE UKREPOV ZAVAROVANJA OSEBNIH PODATKOV

7.1 Izvajanje postopkov in ukrepov

31. člen

Vsak, ki obdeluje osebne podatke, je dolžan varovati osebne podatke, s katerimi se seznani pri opravljanju svojega dela, z njimi ravnati skrbno in vestno ter na način in po postopkih, ki jih določa ta pravilnik, da se preprečijo zlorabe osebnih podatkov.

Obveza varovanja podatkov ne preneha s prenehanjem delovnega razmerja oziroma z razvezo druge pogodbe.

7.2 Izjava o varovanju osebnih podatkov

32. člen

Pred izvajanjem dela, ki zajema tudi obdelavo osebni podatki, mora zaposleni / pogodbeni izvajalec podpisati izjavo, ki ga zavezuje k varovanju osebnih podatkov.

Iz podpisane izjave mora biti razvidno, da je podpisnik seznanjen z določbami tega pravilnika ter določbami GDPR in ZVOP-2, izjava pa mora vsebovati tudi pouk o posledicah kršitve teh pravil.
Za izjavo iz prejšnjega odstavka se šteje tudi ustrezna določba (člen) v pogodbi o zaposlitvi /pogodbi o izvajanju storitev.

7.3 Redno testiranje, ocenjevanje in vrednotenje ukrepov in nadzor nad izvajanjem ukrepov

33. člen

Družba bo redno testirala, ocenjevala in vrednotila učinkovitost tehničnih in organizacijskih ukrepov za zagotavljanje varnosti obdelave osebnih podatkov. V ta namen se bo enkrat letno preverila zakonitost obdelave osebnih podatkov, opravila notranja kontrola seznamov, evidenc, posvet s strokovnjaki za informacijsko varnost itd..

Nadzor nad izvajanjem postopkov in ukrepov za zavarovanje osebnih podatkov izvaja direktor družbe oziroma po njemu pooblaščena oseba.

7.4 Odgovornost za kršitev

34. člen

Zaposleni v družbi so za kršitev določil tega pravilnika disciplinsko odgovorni, ostali pa na temelju pogodbenih obveznosti.

Za hujšo kršitev delovne dolžnosti se šteje zlasti če zaposleni:
- nepooblaščeno sporoča osebne podatke, s katerimi se je seznanil pri svojem delu, sodelavcem ali drugim osebam,
- opusti skrb in nadzor nad nosilci osebnih podatkov med delovnim časom in tako dopusti možnost vpogleda vanje nepooblaščenim osebam,
- nepooblaščeno izdela kopije nosilcev osebnih podatkov,
- brez izrecnega dovoljenja odgovorne osebe družbe ali od nje pooblaščene osebe odnaša iz družbe nosilce osebnih podatkov,
- ne vpiše v knjigo evidenc o ravnanju z osebnimi podatki dejstva o posredovanju osebnih podatkov,
- nepooblaščeno popravlja, spreminja ali dopolnjuje zbrane osebne podatke,
- inštalira ali odnese programsko opremo iz družbe brez izrecnega dovoljenja odgovorne osebe družbe ali od nje pooblaščene osebe.

Odgovornost iz prejšnjih odstavkov ne izključuje prekrškovne, kazenske ali odškodninske odgovornosti.

8. PRAVICE POSAMEZNIKOV

8.1. Politika varstva osebnih podatkov

35. člen

Družba ima sprejete ustrezne ukrepe, s katerimi zagotavlja posamezniku, na katerega se nanašajo osebni podatki, uresničevanje njegovih pravic.

Družba z namenom zagotavljanja informacij ter z namenom učinkovitega uresničevanja pravic posameznika, na katerega se nanašajo osebni podatki, sprejme in na spletni strani Javnega podjetja Komunala Cerknica d.o.o. in povezanih spletnih straneh javno objavi Politiko varstva osebnih podatkov, v kateri v jedrnati, pregledni, razumljivi in lahko dostopni obliki ter jasnem in preprostem jeziku da na voljo informacije, skladno z zahtevami Uredbe GDPR.

Posamezniki lahko s pisno zahtevo od družbe zahtevajo dostop do svojih osebnih podatkov, ki so bili zbrani v povezavi z njimi; popravek netočnih podatkov, zbranih v povezavi z njimi; omejitev obdelave osebnih podatkov; izbris vseh podatkov, če so izpolnjeni pogoji iz 17. člena Uredbe GDPR, ali obdelavi ugovarjajo. Posameznik lahko dane privolitve v obdelavo osebnih podatkov kadarkoli trajno ali začasno, v celoti ali delno prekliče pod pogoji, navedenimi v nadaljevanju.

36. člen

Posameznik, na katerega se nanašajo osebni podatki, ima pravico od družbe dobiti potrditev, ali se v zvezi z njim obdelujejo osebni podatki. Pravico do dostopa družba uresničuje tako, da posamezniku na njegovo zahtevo omogoči dostop do osebnih podatkov in naslednje informacije:

- namene obdelave;
- vrste zadevnih osebnih podatkov;
- uporabnike ali kategorije uporabnika, ki so jim bili ali jim bodo razkriti osebni podatki;
- kadar je mogoče, predvideno obdobje hrambe osebnih podatkov ali, če to ni mogoče, merila, ki se uporabijo za določitev tega obdobja;
- obstoj pravice, da od družbe zahteva popravek ali izbris osebnih podatkov ali omejitev obdelave osebnih podatkov oz. obstoj pravice do ugovora taki obdelavi;
- pravico do vložitve pritožbe pri nadzornem organu;
- kadar osebni podatki niso zbrani pri posamezniku, na katerega se ti nanašajo, vse razpoložljive informacije v zvezi z njihovim virom;
- obstoj avtomatiziranega sprejemanja odločitev, vključno z oblikovanjem profilov.

Odgovor družba posamezniku posreduje v obliki kopije na naslov ali e-naslov, ki ga družbi posameznik sporoči ob vložitvi zahteve.

8.2. Popravek netočnih podatkov

37. člen

Posameznik, na katerega se nanašajo osebni podatki, ima pravico doseči, da družba brez nepotrebnega odlašanja popravi netočne osebne podatke v zvezi z njim. Posameznik, na katerega se nanašajo osebni

podatki, ima ob upoštevanju namenov obdelave, pravico do dopolnitve nepopolnih osebnih podatkov, vključno s predložitvijo dopolnilne izjave.

Ob prejemu zahteve direktor oziroma pooblaščena oseba osebni podatek posameznika popravi skladno z zahtevo posameznika v roku 30 dni.

8.3. Izbris osebnih podatkov

38. člen

Posameznik, na katerega se nanašajo osebni podatki, ima pravico doseči, da družba brez nepotrebnega odlašanja izbriše osebne podatke v zvezi z njim, družba pa ima obveznost osebne podatke brez nepotrebnega odlašanja izbrisati kadar osebni podatki niso več potrebni v namene, za katere so bili zbrani ali kako drugače obdelani:

- če posameznik, na katerega se nanašajo osebni podatki, prekliče privolitev, na podlagi katere poteka obdelava in kadar za obdelavo ne obstaja nobena druga pravna podlaga;
- kadar posameznik, na katerega se nanašajo osebni podatki, obdelavi ugovarja, za njihovo obdelavo pa ne obstajajo nobeni prevladujoči zakoniti razlogi;
- kadar so bili osebni podatki obdelani nezakonito;
- kadar je treba osebne podatke izbrisati za izpolnitev pravne obveznosti v skladu z veljavnimi predpisi;
- ali če so bili osebni podatki zbrani v zvezi s ponudbo storitev informacijske družbe.

Presojo, ali so izpolnjeni pogoji za izbris, opravi direktor oziroma skrbnik posamezne evidence dejavnosti obdelave.

V primeru utemeljene zahteve za izbris osebnih podatkov je družba dolžna ob upoštevanju razpoložljive tehnologije in stroškov izvajanja upravljavce, ki obdelujejo osebne podatke, obvestiti da posameznik, na katerega se nanašajo osebni podatki, od njih zahteva, naj izbrišejo morebitne povezave do teh osebnih podatkov ali njihove kopije.

Družba ni dolžna zagotoviti izbrisa osebnih podatkov v zvezi s posameznikom, če je obdelava potrebna:

- za uresničevanje pravice do svobode izražanja in obveščanja;
- za izpolnjevanje pravne obveznosti obdelave na podlagi veljavnih predpisov ali za izvajanje naloge v javnem interesu ali pri izvajanju javne oblasti;
- ali za namene arhiviranja v javnem interesu,
- za znanstveno- ali zgodovinsko-raziskovalne namene ali statistične namene,

v kolikor bi pravica do izbrisa lahko onemogočila ali resno ovirala uresničevanje namenov te obdelave, ali za uveljavljanje, izvajanje ali obrambo pravnih zahtevkov.

8.4. Omejitev obdelave

39. člen

Družba na zahtevo posameznika omeji obdelavo osebnih podatkov posameznika, kadar:

- posameznik, na katerega se nanašajo osebni podatki, oporeka točnosti podatkov, in sicer za obdobje, ki družbi omogoča preveriti točnost osebnih podatkov;
- je obdelava nezakonita in posameznik, na katerega se nanašajo osebni podatki, nasprotuje izbrisu osebnih podatkov ter namesto tega zahteva omejitev njihove uporabe;
- družba osebnih podatkov ne potrebuje več za namene obdelave, temveč jih posameznik, na katerega se nanašajo osebni podatki, potrebuje za uveljavljanje, izvajanje ali obrambo pravnih zahtevkov;
- je posameznik, na katerega se nanašajo osebni podatki, vložil ugovor v zvezi z obdelavo, dokler se ne preveri, ali zakoniti razlogi upravljavca prevladajo nad razlogi posameznika, na katerega se nanašajo osebni podatki.

Kadar je bila obdelava osebnih podatkov omejena, se taki osebni podatki z izjemo njihovega shranjevanja obdelujejo le s privolitvijo posameznika, na katerega se ti nanašajo, ali za uveljavljanje, izvajanje ali obrambo pravnih zahtevkov ali zaradi varstva pravic druge fizične ali pravne osebe ali zaradi pomembnega javnega interesa Unije ali države članice.

Pred preklicem omejitve obdelave družba o tem obvesti posameznika, na katerega se nanašajo osebni podatki po elektronski pošti ali na drug primeren način.

8.4. Pravice posameznikov

40. člen

Družba vsakemu uporabniku, ki so mu bili osebni podatki razkriti, sporoči vse popravke ali izbrise osebnih podatkov ali omejitve obdelave, razen če se to izkaže za nemogoče ali vključuje nesorazmeren napor. Na zahtevo posameznika družba o teh uporabnikih obvesti posameznika, na katerega se nanašajo osebni podatki.

41. člen

Kadar obdelava osebnih podatkov temelji na privolitvi ali na pogodbi in se obdelava izvaja z avtomatiziranimi sredstvi, ima posameznik, na katerega se nanašajo osebni podatki, pravico, da prejme osebne podatke v zvezi z njim v strukturirani, splošno uporabljani in strojno berljivi obliki, in pravico, da te podatke posreduje drugemu upravljavcu, ne da bi ga družba, ki so ji bili osebni podatki zagotovljeni, pri tem ovirala. Kadar je to tehnično izvedljivo družba na zahtevo posameznika osebne podatke neposredno prenese k drugemu upravljavcu.

42. člen

Posameznik, na katerega se nanašajo osebni podatki, ima na podlagi razlogov, povezanih z njegovim posebnim položajem, pravico, da kadar koli ugovarja obdelavi osebnih podatkov v zvezi z njim, če obdelava temelji na zakonitih interesih, za katere si prizadeva družba ali tretja oseba. V primeru ugovora družba:

- dokaže nujne legitimne razloge za obdelavo;
- dokaže, da je obdelava potrebna za uveljavljanje, izvajanje ali obrambo pravnih zahtevkov; ali
- preneha obdelovati osebne podatke.

Ce se osebni podatki obdelujejo za namene neposrednega trženja, ima posameznik, na katerega se nanašajo osebni podatki, pravico, da kadar koli ugovarja obdelavi osebnih podatkov v zvezi z njim za namene takega trženja, vključno z oblikovanjem profilov, kolikor je povezano s takim neposrednim trženjem. Kadar posameznik, na katerega se nanašajo osebni podatki, ugovarja obdelavi za namene neposrednega trženja, se osebni podatki ne obdelujejo več v te namene.

43. člen

Posameznik, na katerega se nanašajo osebni podatki, ima pravico, da zanj ne velja odločitev, ki temelji zgolj na avtomatizirani obdelavi, vključno z oblikovanjem profilov, ki ima pravne učinke v zvezi z njim ali na podoben način nanj znatno vpliva. Izjeme opredeljuje Uredba GDPR.

44. člen

Posameznik zahtevo, vezano na uresničevanje njegovih pravic, posreduje na naslov: Javno podjetje Komunala Cerknica d.o.o., Notranjska cesta 44, 1380 Cerknica, s pripisom: »osebni podatki« ali po elektronski pošti na naslov dpo@komunala-cerknica.si s pripisom »osebni podatki«.

Družba informacije posamezniku, na katerega se nanašajo osebni podatki, zagotovi brez nepotrebnega odlašanja in v vsakem primeru v enem mesecu po prejemu zahteve. Ta rok se lahko po potrebi podaljša za največ dva dodatna meseca ob upoštevanju kompleksnosti in števila zahtev. Družba obvesti posameznika, na katerega se nanašajo osebni podatki, o vsakem takem podaljšanju v enem mesecu po prejemu zahteve skupaj z razlogi za zamudo. Kadar posameznik, na katerega se nanašajo osebni podatki, zahtevo predloži z elektronskimi sredstvi, se informacije, kadar je mogoče, zagotovijo z elektronskimi sredstvi, razen če posameznik, na katerega se nanašajo osebni podatki, ne zahteva drugače.

Če družba ne ukrepa na zahtevo posameznika, na katerega se nanašajo osebni podatki, takega posameznika brez odlašanja, najpozneje pa v enem mesecu po prejemu zahteve, obvesti o razlogih za neukrepanje ter o možnosti vložitve pritožbe pri nadzornem organu in možnosti uveljavljanja pravnih sredstev.

Informacije ter vsa sporočila in ukrepi se posamezniku zagotovijo brezplačno. Kadar so zahteve posameznika, na katerega se nanašajo osebni podatki, očitno neutemeljene ali pretirane, zlasti ker se ponavljajo, lahko družba zavrne ukrepanje v zvezi z zahtevo. Šteje se, da je zahteva očitno neutemeljena ali pretirana, kadar posameznik zahtevo z bistveno enako vsebino naslovi na družbo več kot trikrat v obdobju šestih mesecev.

Kadar družba upravičeno dvomi v identiteto posameznika, lahko od njega zahteva zagotovitev dodatnih informacij, ki so potrebne za potrditev njegove identitete.

9. UKREPANJE OB SUMU ZLORABE OSEBNIH PODATKOV

9.1 Evidentiranje varnostnih incidentov

45. člen

Družba zagotavlja dosleden in učinkovit sistem za ravnanje z varnostnimi incidenti, z dokumentiranjem in z obveščanjem o varnostnih dogodkih.

Zagotovi se informacijski sistem, ki je sposoben izvajati nadzor nad prepoznavanjem dogodkov (npr. požarni zid, zaznavanje vdorov itd.) in omogoča njihovo dokumentiranje.

Družba vodi evidenco varnostnih incidentov, v katero se varnostni incidenti vpisujejo po kronološkem vrstnem redu, ne glede na stopnjo in vrsto tveganja (Obrazec 7).

Direktor družbe za vodenje evidence pooblasti odgovorno osebo, ki se določi tudi kot oseba za poročanje nadzornemu organu v primeru varnostnega incidenca (Obrazec 8).

Zaposleni pri družbi, ki izve ali opazi, da je prišlo do zlorabe osebnih podatkov (odkrivanje osebnih podatkov, nepooblaščeno uničenje, nepooblaščeno spreminjanje, poškodovanje zbirke osebnih podatkov, prilaščanje osebni podatkov) ali do vdora v zbirko osebnih podatkov, mora o tem takoj obvestiti odgovorno osebo družbe ali nadrejenega delavca, sam pa mora poskusiti z zakonitimi ukrepi takšno aktivnost preprečiti. Enako mora ravnati tudi oseba, ki ni zaposlena v družbi, pa pri svojem delu zazna te aktivnosti.

9.2 Poročanje v primeru varnostnega incidenta

46. člen

V primeru kršitve varstva osebnih podatkov mora upravljavec o kršitvi nemudoma, najkasneje pa v roku 72 ur po seznanitvi s kršitvijo uradno obvestiti pristojni nadzorni organ (Informacijskega pooblaščenca).

Kadar kršitev nastane pri obdelovalcu osebnih podatkov, mora ta o kršitvi obvestiti upravljavca.

Kadar je verjetno, da kršitev varstva osebnih podatkov povzroči veliko tveganje za pravice posameznikov, se mora upravljavec o kršitvi obvestiti tudi posameznika.

Direktor družbe mora zoper tistega, ki je zlorabil osebne podatke ali je nepooblaščeno vdrl v zbirko osebnih podatkov, ustrezno ukrepati v skladu z delovnopravno zakonodajo/pogodbenimi zavezami. Če obstaja sum, da je bilo z zlorabo osebnih podatkov ali vdorom v zbirko osebnih podatkov oziroma z njunim poskusom storjeno kaznivo dejanje, mora ta dejanja prijaviti organom pregona.

10. KONČNA DOLOČBA

47. člen

Direktor družbe lahko ta pravilnik kadarkoli spremeni in dopolni, če to narekujejo zahteve poslovanja podjetja.

Sprememba je veljavna, če jo direktor družbe sprejme v pisni obliki kot spremembo tega pravilnika.

Ta pravilnik velja z dnem sprejema.

S sprejemom tega pravilnika preneha veljati Pravilnik o varstvu osebnih podatkov z dne 01.06.2021.

Cerknica, marec 2026

JP KOMUNALA CERKNICA d.o.o.
Klemen ŽAGAR, v.d. direktor

2 KOMUNALA CERKNICA