JAVNO PODJETJE ZA KOMUNALNE STORITVE ROGAŠKA SLATINA d.o.o.
3250 Rogaška Slatina, Celjska cesta 12, Tel.: (03) 81-21-400, ID za DDV: SI43438806, Matična št.: 5111501000
TRR: Delavska hranilnica d.d., SI56 6100 0002 0825 374, BIC: HDELSI22, e-mail: tajnistvo@okp.si, www.okp.si

Na podlagi 24.in 25.člena Zakona o varstvu osebnih podatkov (ZVOP-1, UPB-1; Ur.l. RS, št.94/07) in skladno z novo ureditvijo, ki jo prinaša Uredba EU 2016/679, Evropskega parlamenta in Sveta o varstvu posameznikov pri obdelavi osebnih podatkov (GDPR), izdaja direktor javnega podjetja OKP ROGAŠKA SLATINA, d.o.o., mag. Bojan PIRŠ naslednji

P R A V I L N I K
O VAROVANJU OSEBNIH PODATKOV
V OKP ROGAŠKA SLATINA d.o.o.

Datum sprejema: 17.05.2018
Datum veljavnosti : od 25.05.2018 dalje

I .Splošne določbe

1.člen

S tem pravilnikom se določajo organizacijski in tehnični postopki in ukrepi za varovanje osebnih podatkov v OKP ROGAŠKA SLATINA, d.o.o.(v nadaljevanju: podjetje) z namenom, da se prepreči slučajno ali namerno nepooblaščeno uničevanje podatkov, njihova sprememba ali izguba kakor tudi nepooblaščen dostop, obdelavo, uporabo ali posredovanje osebnih podatkov.
Zaposleni in zunanji sodelavci podjetja, ki pri svojem delu obdelujejo in uporabljajo osebne podatke, morajo pri svojem delu spoštovati Zakon o varstvu osebnih podatkov, Uredbo EU 2016/679 (v nadaljevanju Uredba GDPR) in področno zakonodajo, ki ureja posamezno področje njihovega dela.

V prilogi 1 pravilnika so razlage nekaterih pojmov uporabljenih v tem pravilniku in v Uredbi GDPR ter temeljnih načel varstva osebnih podatkov, kot jih opredeljuje Uredba GDPR.

2. člen

Vsebine pravilnika:

- Odgovornost za varstvo osebnih podatkov ter izvajanje varnostnih ukrepov in postopkov
- Sprejem in posredovanje osebnih podatkov
- Vodenje evidence (kataloga) zbirk in obdelav osebnih podatkov
- Ocena učinka v zvezi z varstvom osebnih podatkov
- Beleženje obdelav in dostopov do osebnih podatkov ter brisanje podatkov
- Varovanje prostorov in računalniške opreme
- Varovanje sistemske in aplikativno programske računalniške opreme ter podatkov, ki se obdelujejo z računalniško opremo
- Obdelave, ki jih opravljajo zunanje pravne ali fizične osebe
- Ravnanje ob sumu ali ugotovitvah kršitev varstva osebnih podatkov
- Ravnanje v primeru posredovanih zahtev posameznikov glede na njihove pravice opredeljene v Uredbi GDPR

II. Odgovornost za varstvo osebnih podatkov

3.člen

Za izvajanje postopkov in ukrepov za zavarovanje osebnih podatkov so odgovorni vodje organizacijskih enot in imenovane pooblaščene osebe.

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

Pred nastopom dela na delovno mesto, kjer se obdelujejo osebni podatki, mora zaposleni podpisati posebno izjavo, ki ga zavezuje k varovanju osebnih podatkov **(priloga 2 k pravilniku).**

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

4. člen

Pooblaščena oseba za varstvo osebnih podatkov (DPO)

Direktor podjetja s sklepom imenuje pooblaščeno osebo za varstvo osebnih podatkov (v nadaljevanju : DPO). DPO ima dostop do osebnih podatkov in njihovih obdelav. Pri svojem delu vezanem na varstvo podatkov je pooblaščena oseba (DPO) neodvisna od napotkov vodilnih zaposlenih.

DPO ima naslednje naloge:

a) obveščanje upravljavca ali obdelovalca in zaposlenih, ki izvajajo obdelavo, ter svetovanje navedenim o njihovih obveznostih v skladu z uredbo GDPR;
b) spremljanje skladnosti z uredbo, drugimi določbami prava Unije ali prava države članice o varstvu podatkov in politikami upravljavca 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;
c) svetovanje, kadar je to zahtevano, glede ocene učinka v zvezi z varstvom podatkov in spremljanje njenega izvajanja;
d) sodelovanje z nadzornim organom;
e) delovanje kot kontaktna točka za nadzorni organ pri vprašanjih v zvezi z obdelavo, vključno s predhodnim posvetovanjem in, kjer je ustrezno, posvetovanje glede katere koli druge zadeve.

DPO mora imeti za svoje delo zagotovljene pogoje tako s strani podjetja kot obdelovalcev:

a) je **ustrezno in pravočasno vključen v vsa vprašanja in postopke**, povezane z varstvom osebnih podatkov, in ima možnost podati ustrezen nasvet, mnenje, predlog ali opozorilo,
b) ima **dostop do osebnih podatkov ter dejavnosti obdelave**,
c) ima na razpolago prostorska in tehnična sredstva, potrebna za izvajanje svojih nalog in za ohranjanje svojega strokovnega znanja,
d) **lahko posamezniki**, na katere se nanašajo osebni podatki, **z njim stopijo v stik** in se posvetujejo glede vseh vprašanj, povezanih z obdelavo njihovih osebnih podatkov in uresničevanjem njihovih pravic iz Splošne uredbe, ter
e) ima **neposreden dostop do vodstva upravljavca ali obdelovalca**, če oceni, da je to zaradi pomembnosti določene obdelave osebnih podatkov nujno.

III. Sprejem in posredovanje osebnih podatkov

5. člen

Sprejem osebnih podatkov

Sprejem osebnih podatkov je lahko osebno, po klasični pošti ali po elektronski pošti.
Pri osebnem prevzemu podatkov delavec istovetnost osebe preveri preko osebnega dokumenta (osebna izkaznica, potni list, vozniško dovoljenje).

Po klasični pošti: delavec, ki je zadolžen za sprejem in evidenco pošte, mora izročiti poštno pošiljko z osebnimi podatki direktno posamezniku, ali službi, na katero je ta pošiljka naslovljena.
Delavec, ki je zadolžen za sprejem in evidenco pošte, odpira in pregleduje vse poštne pošiljke in pošiljke, ki na drug način prispejo v podjetje - prinesejo jih stranke ali kurirji, razen v nadaljevanju opredeljenih izjem.
Delavec, ki je zadolžen za sprejem in evidenco pošte:

- ne odpira tistih pošiljk, ki so naslovljene na drugo organizacijo in so pomotoma dostavljena ter pošiljk, ki so označene kot osebni podatki ali za katere iz označb na ovojnici izhaja, da se nanašajo na natečaj ali razpis.
- ne sme odpirati pošiljk, naslovljenih 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 uradnega položaja in šele nato naslov podjetja.

Po elektronski pošti v skladu z **Navodili o uporabi službene elektronske pošte, ki je priloga štev. 3 k temu pravilniku.**

6. člen

Posredovanje osebnih podatkov

Osebne podatke je dovoljeno prenašati z informacijskimi, telekomunikacijskimi in drugimi sredstvi le ob izvajanju postopkov in ukrepov, ki nepooblaščenim osebam preprečujejo prilaščanje ali uničenje podatkov ter neupravičeno seznanjanje z njihovo vsebino.
Po klasični pošti:
POSEBNI (občutljivi) OSEBNI PODATKI se pošiljajo naslovnikom v zaprtih ovojnicah proti podpisu v dostavni knjigi ali z vročilnico. Osebni podatki se pošiljajo priporočeno.

Ovojnica, v kateri se posredujejo osebni podatki, mora biti izdelana na takšen način, da ovojnica ne omogoča, da bi bila ob normalni svetlobi ali pri osvetlitvi ovojnic z običajno lučjo vidna vsebina ovojnice. Prav tako mora ovojnica zagotoviti, da odprtja ovojnice in seznanitve z njeno vsebino ni mogoče opraviti brez vidne sledi odpiranja ovojnice.

Po elektronski pošti ali preko strežnika:
Osebni podatki se smejo posredovati preko telekomunikacijskih omrežij samo, če so posebej zavarovani s kriptografskimi metodami in elektronskim podpisom tako, da je zagotovljena nečitljivost podatkov med njihovim prenosom.

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

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

Vsako posredovanje osebnih podatkov se beleži v evidenco posredovanj, iz katere mora biti razvidno, kateri osebni podatki so bili posredovani, komu, kdaj in na kakšni podlagi.

Nikoli se ne posredujejo originali dokumentov, razen v primeru pisne odredbe sodišča. Originalni dokument se mora v času odsotnosti nadomestiti s kopijo.

IV. Vodenje evidence (kataloga) zbirk in obdelav osebnih podatkov

7. člen

Podjetje vodi osebne podatke v katalogih zbirk /evidencah osebnih podatkov, ki jih ustanovi na podlagi zakona in osebne podatke, ki jih vodi v okviru zakonsko določenih zbirk, na podlagi pogodbenega odnosa ali na podlagi soglasja osebe, na katero se podatki nanašajo.
Katalogi zbirk / evidenc in obdelav osebnih podatkov, ki jih vodi podjetje so priloga št. 4 k temu pravilniku.
Za vsako evidenco je določen skrbnik- pooblaščena oseba za obdelavo osebnih podatkov v zbirki.
Direktor določi pooblaščeno osebo iz predhodnega odstavka s pooblastilom.
Pooblastilo za obdelavo osebnih podatkov je priloga št. 5 k temu pravilniku.

V evidenci zbirk in obdelav so vodeni naslednji elementi (podčrtan element pomeni, da je element zahtevan z Uredbo GDPR):

- naziv zbirke;
- skrbnik zbirke/obdelave (oseba odgovorna za zbirko osebnih podatkov)
- upravljalec oziroma obdelovalec
- viri osebnih podatkov
- pravna podlaga in ali zahtevana pridobitev soglasja
- kategorije posameznikov na katere se osebni podatki nanašajo
- vrste osebnih podatkov (posebni osebni podatki so dodatno označeni)
- namen zbiranja (hrambe) in obdelave osebnih podatkov
- zunanji obdelovalci osebnih podatkov (če so)
- uporabniki osebnih podatkov in obdelav
- prenos v tretje države (če je)
- rok hrambe
- opisi varnostnih ukrepov (če je potrebno)
- povezane zbirke osebnih podatkov (povezave na ostale zbirke izven podjetja in med zbirkami v podjetju)
- potrebna ocena vpliva na varstvo osebnih podatkov (če, da tudi vrste tveganj in povezava na ocene tveganj)
- povezave (če so - na zakonodajo, soglasja, aplikacije, pogodbo z obdelovalcem in drugo).

Katalog zbirk osebnih podatkov se dopolnjuje ob vsaki spremembi vrste osebnih podatkov v posamezni zbirki.
Zaposleni, ki obdelujejo osebne podatke, morejo biti seznanjeni s katalogom zbirk osebnih podatkov, vpogled v katalog zbirk osebnih podatkov pa je potrebno omogočiti vsakomur, ki to potrebuje za izpolnjevanje njegovih delovnih obveznosti.

V. Ocena učinka v zvezi z varstvom osebnih podatkov

8. 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 ali tveganje za ugled podjetja, je potrebno izdelati oceno Učinka na varstvo osebnih podatkov. To pomeni najmanj za:

- obsežne obdelave posebnih vrst podatkov,
- sistematično in obsežno vrednotenje osebnih vidikov posameznikov (vključno z oblikovanjem profilov in je osnova za odločitve npr. ocenjevanje uspešnosti zaposlenih),
- obsežno sistematično spremljanje javno dostopnega območja.

V posamezni zbirki/obdelavi osebnih podatkov je označena potreba po oceni učinka na varstvo osebnih podatkov.

9. člen

Ocena učinka pomeni: opis okoliščin tveganja, ocena tveganja (verjetnost in vpliv in s tem dobimo stopnjo tveganja) in potrebne ukrepe za ublažitev tveganja. (Oceno učinka je potrebno izvesti najmanj na vsake tri leta ali ob spremembah tehnologij, okoliščin, ...).
Postopek za izvedbo ocene učinka :

- opis tveganja (opis okoliščin tveganja in v povezavi s katerimi zbirkami/obdelavami osebnih podatkov se pojavlja),
- izdelava ocene resnosti tveganja (oceniti verjetnost tveganja in vpliv tveganja na varstvo osebnih podatkov – oboje skupaj da oceno resnosti tveganja)
- v primeru pomembnega in visokega tveganja je nujno izvajati (in razvijati) ukrepe za zmanjševanje oziroma obvladovanje tveganj.

Za oceno verjetnosti je uporabljena pet stopenjska lestvica (1-skoraj nemogoče, 2-malo verjetno, 3-možno, 4-zelo verjetno,5 skoraj zagotovo) in za oceno vpliva na varstvo osebnih podatkov prav tako pet stopenjska lestvica (1-neznaten, 1-majhen, 2-zmeren, 4-velik, 5-kritičen vpliv). Zmnožek obeh ocen poda resnost tveganja, kjer so uporabljene 4 stopnje: nizko, srednje, pomembno in visoko tveganje.

Prepoznana tveganja so vodena v katalogu tveganj. Za vsako tveganje je določen skrbnik tveganj, ki mora najmanj enkrat na tri leta izvesti oceno vpliva na varstvo osebnih podatkov.

10. člen

Kadar ukrepi za zmanjšanje oziroma obvladovanje tveganja ne omogočajo, da obdelava ne bi povzročila veliko tveganje, se mora podjetje kot upravljalec pred obdelavo posvetovati z nadzornim organom (36. člen Uredbe GDPR) in od njega pridobiti mnenje ali lahko izvaja obdelavo osebnih podatkov.

VI. Beleženje obdelav in dostopov do osebnih podatkov (sledljivost oziroma revizijska sled)

11. člen

Upravljavci zbirk osebnih podatkov so dolžni osebne podatke, ki jih obdelujejo, ustrezno zavarovati.

Sledljivost obdelave osebnih podatkov pomeni kakršnokoli delovanje ali niz delovanj, ki se izvaja v zvezi z osebnimi podatki, ki so avtomatizirano obdelani ali ki so pri ročni obdelavi del zbirke osebnih podatkov ali so namenjeni vključitvi v zbirko osebnih podatkov, zlasti zbiranje, pridobivanje, vpis,

urejanje, shranjevanje, prilagajanje ali spreminjanje, priklicanje, vpogled, uporaba, razkritje s prenosom, sporočanje, širjenje ali drugo dajanje na razpolago, razvrstitev ali povezovanje, blokiranje, anonimiziranje, izbris ali uničenje; obdelava je lahko ročna ali avtomatizirana (sredstva obdelave). Glede na tveganje in naravo podatkov, ki se bodo obdelovali, je potrebno zagotoviti popolno revizijsko sled, torej tudi beleženje vsakega dostopa do podatkov.

Takšno raven sledljivosti je potrebno zagotoviti v primeru:

a) obdelave večjega števila osebnih podatkov (npr. mesečni obračun, obdelave dolžnikov, ipd.),
b) obdelave oziroma dostopa do občutljivih osebnih podatkov (kot so npr. zdravstveni podatki),
c) obdelave osebnih podatkov, katerih zloraba bi lahko imela hujše posledice za posameznika.

Sledljivost v elektronski obliki je potrebno zagotavljati s samodejnim beleženjem v aplikacijah (logi ozadju aplikacije), kjer je potrebno s dobaviteljem aplikacije dogovoriti način in obseg (za katere podatke in koliko časa) sledljivosti.
Za evidence, ki so v papirni obliki je potrebno voditi evidence dostopov npr. vpogledi v osebne mape zaposlenih in podobno.
Za videonadzor je to opredeljeno v Pravilniku za izvajanje videonadzora.

VII. Uničenje in brisanje osebnih podatkov

12. člen

Osebne podatke lahko vodimo v zbirkah osebnih podatkov le toliko časa, da je dosežen namen zaradi katerega zbiramo in vodimo ter obdelujemo osebne podatke. Po prenehanju potrebe po vodenju osebnih podatkov, le te ustrezno uničimo ali naredimo neberljive.

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

Podatki na klasičnih medijih (listine, kartoteke, register, seznam, ...) se uničijo na način, ki onemogoča čitanje vseh ali dela uničenih podatkov.

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

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

Pri prenosu nosilcev osebnih podatkov na mesto uničenja je potrebno zagotoviti ustrezno zavarovanje tudi v času prenosa.

VIII. Varovanje prostorov in računalniške opreme

13. člen

Prostori, v katerih se nahajajo nosilci osebnih podatkov, strojna in programska oprema (varovani prostori), morajo biti varovani z organizacijskimi ter fizičnimi in/ali tehničnimi ukrepi, ki onemogočajo nepooblaščenim osebam dostop do podatkov.

Dostop je mogoč le v rednem delovnem času, izven tega časa pa samo na podlagi dovoljenja vodje organizacijske enote. Ključi se ne puščajo v ključavnici v vratih od zunanje strani. Varovani prostori ne smejo ostajati nenadzorovani, oziroma se morajo zaklepati ob odsotnosti delavcev, ki jih nadzorujejo.

Izven delovnega časa morajo biti omare in pisalne mize z nosilci osebnih podatkov zaklenjene, računalniki in druga strojna oprema izklopljeni in fizično ali programsko zaklenjeni. Zaposleni ne smejo puščati nosilcev osebnih podatkov na mizah v prisotnosti oseb, ki nimajo pravice vpogleda vanje.

Nosilci osebnih podatkov, ki se nahajajo izven zavarovanih prostorov (hodniki, skupni prostori) morajo biti stalno zaklenjeni. Občutljivi osebni podatki se ne smejo hraniti izven varovanih prostorov.

14. člen

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

Vzdrževanje in popravila strojne računalniške in druge opreme je dovoljeno samo z vednostjo pooblaščene osebe, izvajajo pa ga lahko samo pooblaščeni servisi in vzdrževalci, s katerimi imamo sklenjeno ustrezno pogodbo.

Vzdrževalci prostorov, strojne in programske opreme, obiskovalci in poslovni partnerji se smejo gibati v zavarovanih prostorih samo z vednostjo pooblaščene osebe. 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).

Varovanje prostorov v času, ko v podjetju ni zaposlenih je urejeno z alarmnim sistemom.

IX. Varovanje sistemske in aplikativno programske računalniške opreme ter podatkov, ki se obdelujejo z računalniško opremo

15. člen

Dostop do programske opreme mora biti varovan tako, da dovoljuje dostop samo za to v naprej določenim zaposlenim 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 pooblaščene osebe, izvajajo pa ga lahko samo pooblaščeni servisi in organizacije in posamezniki, s katerimi imamo 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.

16. člen

Vsebina diskov mrežnega strežnika in lokalnih delovnih postaj, kjer se nahajajo osebni podatki, se sprotno preverja glede na prisotnost računalniških virusov. Ob pojavu računalniškega virusa se tega čimprej odpravi s pomočjo zunanje IT službe, obenem pa se ugotovi vzrok pojava virusa v računalniškem informacijskem sistemu.

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

Zaposleni ne smejo inštalirati programske opreme brez vednosti osebe, zadolžene za delovanje računalniškega informacijskega sistema. Prav tako ne smejo odnašati programske opreme iz delovnih prostorov brez odobritve vodje organizacijske enote in vednosti osebe, zadolžene za delovanje računalniškega informacijskega sistema(osebni računalniki, tablice, če jih zaposleni potrebujejo na terenu ali za delo na domu).

17. člen

Dostop do podatkov preko aplikativne programske opreme se varuje s sistemom gesel za avtorizacijo in identifikacijo uporabnikov programov in podatkov, sistem gesel pa mora omogočati tudi možnost naknadnega ugotavljanja, kdaj so bili posamezni osebni podatki vnešeni v zbirko podatkov, uporabljeni ali drugače obdelovani ter kdo je to storil.
Pooblaščena oseba določi režim dodeljevanja hranjenja in spreminjanja gesel.

Vsa gesla in postopki, ki se uporabljajo za vstop in administriranje mreže osebnih računalnikov (supervisorska oz. nadzorna 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 tam nahajajo.
Te kopije se hranijo v zato določenih mestih, ki morajo biti ognjevarna, zavarovana proti poplavam in elektromagnetnim motnjam, v okviru predpisanih klimatskih pogojev ter zaklenjena.

X. Obdelave osebnih podatkov , ki jih opravljajo zunanje pravne ali fizične osebe

18. člen

Z vsako zunanjo pravno ali fizično osebo, ki opravlja posamezna opravila v zvezi z zbiranjem, obdelovanjem, shranjevanjem ali posredovanjem osebnih podatkov in je registrirana za opravljanje takšne dejavnosti (pogodbeni obdelovalec), se sklene pisna pogodba. V takšni pogodbi morajo biti obvezno predpisani tudi pogoji in ukrepi za zagotovitev varstva osebnih podatkov in njihovega zavarovanja. Omenjeno velja tudi za zunanje osebe, ki vzdržujejo strojno in programsko opremo ter izdelujejo in instalirajo novo strojno ali programsko opremo.

Zunanje pravne ali fizične osebe smejo opravljati storitve obdelave osebnih podatkov samo v okviru naročnikovih pooblastil in podatkov ne smejo obdelovati ali drugače uporabljati za noben drug namen.
Kot vodilo za vsebino pogodb z zunanjimi obdelovalci je **Vzorec pogodbe z obdelovalcem , ki je priloga št. 6. k temu pravilniku.**

Zbirke in obdelave osebnih podatkov, ki jih vodijo oziroma izvajajo obdelovalci, so navedene tudi v evidenci zbirk in obdelav, ki je vodena v podjetju.

XI. Ravnanje ob sumu ali ugotovitvah kršitev varstva osebnih podatkov

19. člen

Zaposleni so dolžni o aktivnostih, ki so povezane z odkrivanjem ali nepooblaščenim uničenjem zaupnih podatkov, zlonamerni ali nepooblaščeni uporabi, prilaščanju, spreminjanju ali poškodovanju takoj obvestiti pooblaščeno osebo ali nadrejenega, sami pa poskušajo takšno aktivnost preprečiti.

Brez nepotrebnega odlašanja, najpozneje pa v roku 72 ur po seznanitvi s sumom ali kršitvijo je potrebno obvestiti Informacijskega pooblaščenca o vsaki kršitvi varstva osebnih podatkov, ki jo zaznamo, če je verjetno, da bo povzročila tveganje za posege v človekove pravice in temeljne svoboščine ter interese posameznikov, na katere se nanašajo osebni podatki.

Vodja IT in ostali zaposleni morajo takoj po zaznavi kršitve zavarovati dnevniške zapise in druge podatke, na podlagi katerih bi se dalo ugotoviti dejstva v zvezi s kršitvijo, ter jih na poziv predložiti Informacijskemu pooblaščencu.

Ko bi posamično obveščanje posameznikov, na katere se nanašajo osebni podatki, vključevalo nesorazmeren napor podjetja, kar vključuje tudi neučinkovitost obveščanja in vpliv na spoštovanja pravne varnosti ali bistvenih človekovih pravic ali temeljnih svoboščin, je možno opraviti tudi obveščanje preko medijev.

Obrazec za javljanje kršitev varstva osebnih podatkov je podan v prilogi štev. 7 tega pravilnika.

XII. Ravnanje v primeru posredovanih zahtev posameznikov glede na njihove pravice opredeljene v Uredbi GDPR

20. člen

Posameznik na katerega se podatki nanašajo ima naslednje pravice:

- od podjetja dobiti potrditev, ali se v zvezi z njim obdelujejo osebni podatki;
- zahtevati popravek in/ali izbris osebnih podatkov;
- zahtevati omejitev obdelave (nezakonita obdelava, obdelava netočnih podatkov, podatkov upravljalec ne potrebuje več);
- zahtevati prenosljivost podatkov (v berljivi obliki dobiti poročilo o namenih obdelave, vrstah osebnih podatkov, kdo so uporabniki, obdobje hrambe podatkov, če se - komu se podatki posredujejo).

Na podlagi tega lahko posameznih poda pisno zahtevo in če je ta upravičena mora vodja zbirke osebnih podatkov posamezniku:

- omogočiti vpogled in prepis podatkov iz zbirke podatkov, ki se nanašajo nanj,
- posredovati izpis podatkov iz zbirke podatkov, ki se nanašajo nanj,
- posredovati seznam subjektov, katerim so bili v določenem obdobju posredovani podatki iz zbirke podatkov, ki se nanašajo nanj.
- dopolniti ali popraviti podatke, za katere posameznik, na katerega se podatki nanašajo, dokaže, da so nepopolni, netočni ali neažurni ter

- izbrisati podatke (ali omejiti uporabo), za katere posameznik, na katerega se podatki nanašajo, upravičeno meni da so bili zbrani v nasprotju z določbami tega pravilnika ali Zakona o varstvu osebnih podatkov.

Posredovanje izpisa, dopolnitev ali izbris v zbirki mora vodja zbirke izvesti najkasneje v roku enega meseca po prejemu upravičene pisne zahteve posameznika.

XIII. Končne določbe

21.člen

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

22.člen

Ta pravilnik prejmejo službe oziroma delavci v čigar delovne obveznosti sodi zbiranje, urejanje, obdelava, spreminjanje, shranjevanje, posredovanje ali uporaba osebnih podatkov ali nosilcev osebnih podatkov.

23.člen

Delavci, ki delajo na delovnih mestih, kjer se zbirajo, urejajo, obdelujejo, spreminjajo, shranjujejo, posredujejo ali uporabljajo osebni podatki ali nosilci osebnih podatkov, morajo podpisati izjavo iz 3. člena tega pravilnika v roku 30 dni od dneva sprejema tega pravilnika.

24.člen

Z uveljavitvijo tega pravilnika preneha veljati Pravilnik o zavarovanju osebnih podatkov , sprejeti dne 08.09.2015.

Direktor:
mag. Bojan PIRŠ

OKP
JAVNO PODJETJE ZA
KOMUNALNE STORITVE
Rogaška Slatina, d.o.o.

Datum sprejema: 17.05.2018
Datum veljavnosti : od 25.05.2018 dalje

PRILOGE K PRAVILNIKU :

Priloga štev. 1: Obrazložitev pojmov uporabljenih v pravilniku

Priloga štev.2 : Izjava o varovanju osebnih podatkov

Priloga štev. 3 : Navodila o uporabi službene elektronske pošte, intraneta in interneta zaposlenih v OKP ROGAŠKA SLATINA, d.o.o.

Priloga štev. 4 : KATALOGOV ZBIRK (EVIDENC) OBDELAV OSEBNIH PODATKOV V OKP ROGAŠKA SLATINA d.o.o.,

Priloga štev.5 : Pooblastilo za obdelavo osebnih podatkov

Priloga štev. 6: Vzorec pogodbe o obdelavi osebnih podatkov

Priloga štev.7 : Prijava kršitve varstva osebnih podatkov Informacijskemu pooblaščencu

JAVNO PODJETJE ZA KOMUNALNE STORITVE ROGAŠKA SLATINA d.o.o.
3250 Rogaška Slatina, Celjska cesta 12, Tel.: (03) 81-21-400, ID za DDV: SI43438806, Matična št.: 5111501000
TRR: Delavska hranilnica d.d., SI56 6100 0002 0825 374, BIC: HDELSI22, e-mail: tajnistvo@okp.si, www.okp.si

Priloga št.1

Razlage nekaterih pojmov in temeljnih načel varstva osebnih podatkov uporabljenih v Pravilniku o varovanju osebnih podatkov v OKP ROGAŠKA SLATINA, d.o.o.

Izrazi, uporabljeni v tem pravilniku pomenijo:

- *Osebni podatki* pomenijo katerokoli informacijo v zvezi z določenim ali določljivim posameznikom (v nadaljnjem besedilu: posameznik, 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;
- *Zbirka* pomeni vsak strukturiran niz osebnih podatkov, ki vsebuje vsaj en osebni podatek, ki je dostopen na podlagi meril, ki omogočajo uporabo ali združevanje podatkov, ne glede na to, ali je niz centraliziran, decentraliziran ali razpršen na funkcionalni ali geografski podlagi. Strukturiran niz podatkov je niz podatkov, ki je organiziran na takšen način, da določi ali omogoči določljivost posameznika;
- *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;
- *Upravljavec* pomeni fizično ali pravno osebo, javni organ, agencijo ali drugo telo, ki samo ali skupaj z drugimi določa namene in sredstva obdelave; kadar namene in sredstva obdelave določa pravo Evropske unije ali pravo države članice, se lahko upravljavec ali posebna merila za njegovo imenovanje določijo s pravom Evropske unije ali pravom države članice;
- *Obdelovalec* pomeni fizično ali pravno osebo, javni organ, agencijo ali drugo telo, ki obdeluje osebne podatke v imenu upravljavca;
- *Uporabnik* pomeni fizično ali pravno osebo, javni organ, agencijo ali drugo telo, ki so mu bili osebni podatki razkriti, ne glede na to, ali je tretja oseba ali ne. Vendar pa se javni organi, ki lahko prejmejo osebne podatke v okviru posamezne poizvedbe v skladu s pravom Evropske unije ali pravom države članice, ne štejejo za uporabnike; obdelava teh podatkov s strani teh javnih organov poteka v skladu z veljavnimi pravili o varstvu podatkov glede na namene obdelave;
- *Privolitev posameznika*, na katerega se nanašajo osebni podatki 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;

- *Kršitev varnosti 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;
- *Posebni osebni podatki* so podatki o rasnem ali narodnostnem poreklu, političnem, verskem, filozofskem prepričanju, članstvu v sindikati, zdravstvenem stanju, spolnem življenju, vpisu alči izbrisu v ali iz kazenske evidence ali prekrškovne evidence ter biometrične značilnos;
- *Nosilec podatkov* so vse vrste sredstev, na katerih so zapisani ali posneti podatki (listine, akti, gradiva, spisi, računalniška oprema vključno z magneti, optični ali drugi računalniški mediji, fotokopije, zvočno in slikovno gradivo, mikrofilmi, naprave za prenos podatkov ipd.).

Temeljna načela varstva osebnih podatkov

Osebni podatki:

a) se obdelujejo zakonito, če so določene pravne podlage za njihovo konkretno obdelavo, ter da se obdelujejo pošteno in na pregleden način za posameznika, tako da se ne obdelujejo za prikrite ali drugače nepoštene namene, zato da se posamezniki lahko svobodno odločijo, ali bodo sodelovali pri obdelavi njihovih osebnih podatkov oziroma da lahko temu zakonito in učinkovito ugovarjajo (zakonitost, poštenost in preglednost);
b) se zbirajo za določene, izrecne in zakonite namene ter se ne smejo nadalje obdelovati na način, ki ni združljiv s temi nameni (omejitev namena);
c) so ustrezni, relevantni in omejeni na to, kar je potrebno za namene, za katere se obdelujejo (najmanjši obseg podatkov);
d) so 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 in posodobljenost);
e) se hranijo v obliki, ki dopušča identifikacijo posameznikov, na katere se nanašajo osebni podatki, le toliko časa, kolikor je potrebno za namene, za katere se osebni podatki obdelujejo, razen če je z zakonom določen drug rok hrambe (omejitev roka hrambe);
f) se obdelujejo na način, ki zagotavlja ustrezno varnost osebnih podatkov, vključno z zaščito pred nedovoljeno ali nezakonito obdelavo, pred nenamerno izgubo, uničenjem, poškodbo ali izgubo razpoložljivosti, z ustreznimi tehničnimi ali organizacijskimi ukrepi (celovitost, zaupnost in razpoložljivost).

JAVNO PODJETJE ZA KOMUNALNE STORITVE ROGAŠKA SLATINA d.o.o.
3250 Rogaška Slatina, Celjska cesta 12, Tel.: (03) 81-21-400, ID za DDV: SI43438806, Matična št.: 5111501000
TRR: Delavska hranilnica d.d., SI56 6100 0002 0825 374, BIC: HDELSI22, e-mail: tajnistvo@okp.si, www.okp.si

Priloga št.2

I Z J A V A
o varovanju osebnih podatkov

Spodaj podpisani : .....

zaposleni v OKP Rogaška Slatina d.o.o., na delovnem mestu:

.....

ki pri svojem delu obdelujem in uporabljam osebne podatke fizičnih oseb, sem seznanjen z naravo osebnih podatkov, ki jih ali jih bom kot delavec OKP ROGAŠKA SLATINA, d.o.o. zbiral, urejal, obdeloval, spreminjal, shranjeval, posredoval oziroma uporabljal pri svojem delu

i z j a v l j a m,

da bom kot poklicno in poslovno skrivnost varoval vse osebne podatke, s katerim se bom pri svojem delu seznanil.
Seznanjen sem s tem, da sem dolžan izvajati predpisane postopke in ukrepe za zavarovanje osebnih podatkov in varovati osebne podatke, za katere bom izvedel oziroma bom z njimi seznanjena pri opravljanju svojega dela v skladu z določbami Pravilnika o varovanju osebnih podatkov v OKP ROGAŠKA SLATINA, d.o.o. Obveza varovanja podatkov mi ne preneha s prenehanjem delovnega razmerja v podjetju.

Podpisani sem poučen, da je razkrivanje osebnih podatkov, s katerimi se bom pri svojem delu seznanil, nepooblaščenim osebam ali zloraba teh podatkov sankcionirana kot hujša kršitev delovnih obveznosti in kot kaznivo dejanje ter hkrati razlog za prenehanje pogodbe o zaposlitvi iz krivdnih razlogov.

Rogaška Slatina, ... Podpis.....

Priloga :
1x Pravilnik o varovanju osebnih
podatkov v OKP ROGAŠKA SLATINA, d.o.o.

JAVNO PODJETJE ZA KOMUNALNE STORITVE ROGAŠKA SLATINA d.o.o.
3250 Rogaška Slatina, Celjska cesta 12, Tel.: (03) 81-21-400, ID za DDV: SI43438806, Matična št.: 5111501000
TRR: Delavska hranilnica d.d., SI56 6100 0002 0825 374, BIC: HDELSI22, e-mail: tajnistvo@okp.si, www.okp.si

Priloga št.3

NAVODILA O UPORABI SLUŽBENE ELEKTRONSKE POŠTE, INTRANETA IN INTERNETA ZAPOSLENIH V OKP ROPGAŠKA SLATINA, d.o.o.

Uporaba službene elektronske pošte

Elektronska pošta se praviloma uporablja samo v službene namene. Uporaba v druge namene je dopustna le izjemoma, in sicer pod pogojem, da zaradi tega ni potrebno dodeljevati dodatnih diskovnih kapacitet, da se ne zmanjšuje prepustnost sistema elektronske pošte ali kakorkoli vpliva na zmanjševanje produktivnosti drugih uporabnikov. Uporaba sistema elektronske pošte na način, ki je v nasprotju z veljavnimi predpisi, je neetična (neprimerna, žaljiva...) ali škoduje ugledu podjetja, ni dovoljena.

Uporabnik ne sme odpirati elektronske pošte neznanega pošiljatelja in take, ki vsebuje izvršno kodo (npr. datoteka s končnico exe). Tako sporočilo mora uporabnik takoj izbrisati in o tem obvestiti zaposlenega za IT v podjetju.

Uporabnik mora poskrbeti za pravilno hranjenje poštnih sporočil, ki se nanašajo na poslovanje in dejavnost podjetja ter evidentiranje le-teh v dokumentnem sistemu podjetja. Ravno tako je dolžan poskrbeti za pravilno in redno arhiviranje svojega elektronskega predala, če ta preseže dovoljeno velikost.

IT skrbi za delovanje elektronske pošte. Zunanji e-poštni naslovi (Gmail, Hotmail, Siol, T-2, Arnes, ...) niso v pristojnosti organizacije in jih zaposleni ne smejo uporabljati za službeno korespondenco.

Če uporabnik preko e-pošte pošilja občutljive podatke (osebni podatki, poslovne skrivnosti, ..) mora e-pošto obvezno kriptirati .

V primeru, da uporabnik IKT krši ta navodila, ima vodja službe za plan, analizo in informatiko (na podlagi navodila vodja FRS pravico do ustreznih ukrepov, s katerimi zagotovi stabilnost in varnost delovanja informacijskega sistema.

V nujnih primerih lahko vodja IT ukrepa brez soglasja pooblaščene osebe, ki jo o tem naknadno pisno obvesti.

Uporaba intraneta in interneta

Pri uporabi intraneta in interneta mora uporabnik upoštevati splošna pravila in načela, ki veljajo za uporabo internet/intraneta v omrežju podjetja:

- uporabniku je dostop do interneta omogočen zaradi dostopa do baz podatkov oziroma storitev, ki jih potrebuje pri svojem delu. Zato se mora obnašali racionalno in internet uporabljati kot delovni pripomoček.
- omrežje sme uporabnik uporabljati le na službeni delovni postaji;
- pri vključitvi v omrežje in storitve ne sme uporabljati lažnih ali zavajajočih osebnih podatkov;
- nedopustno je pošiljati prispevke za nestrokovne ali osebne polemike, oglase, verižna sporočila ali početi karkoli, kar moti delo drugih uporabnikov;
- ni dovoljeno objavljati ali pošiljati podatkov z žaljivo ali pornografsko vsebino, tajnih podatkov ali podatkov, ki so zaščiteni z avtorskimi pravicami ali so v lasti drugih uporabnikov;
- uporabnik ne sme uporabljati interneta za prenos gradiva in podatkov, ki so neprimerni, žaljivi, nezakoniti ali nevarni.

JAVNO PODJETJE ZA KOMUNALNE STORITVE ROGAŠKA SLATINA d.o.o.
3250 Rogaška Slatina, Celjska cesta 12, Tel.: (03) 81-21-400, ID za DDV: SI43438806, Matična št.: 5111501000
TRR: Delavska hranilnica d.d., SI56 6100 0002 0825 374, BIC: HDELSI22, e-mail: tajnistvo@okp.si, www.okp.si

Priloga št. 4

KATALOGA ZBIRK / EVIDENC OBDELAV OSEBNIH PODATKOV V OKP ROGAŠKA SLATINA, d.o.o.

1. **Evidenca o zaposlenih delavcih**
2. **Evidenca o stroških dela**
3. **Evidenca o izrabi delovnega časa**
4. **Evidenca preventivnih zdravstvenih pregledov**
5. **Evidenca o usposabljanju za varno delo in preizkusih praktičnega znanja in za varstvo pred požarom**
6. **Evidenca uporabnikov komunalnih storitev**
7. **Evidenca izvajalcev del po delovršnih pogodbah**
8. **Evidenca o investitorjih, ki zaprosijo za izdajo projektnih pogojev in za izdajo soglasij**
9. **Evidenca o potnih nalogih z obračunom**
10. **Evidenca o vzdrževanih družinskih članih**
11. **Evidenca o študentih in dijakih na delovni praksi ali počitniškem delu in najetih delavcih**
12. **Evidenca uporabnikov službenih mobilnih telefonov, službenih vozil, drugih delovnih sredstev in zaščitnih sredstvih**
13. **Evidenca o poškodbah pri delu, kolektivnih nezgodah, nevarnih pojavih, ugotovljenih poklicnih boleznih v zvezi z delom ter o njihovih vzrokih**
14. **Evidenca o izobraževanjih, izpopolnjevanjih in usposabljanjih**
15. **Evidenca podatkov o iskalcih zaposlitve**
16. **Evidenca podatkov o članih nadzornega sveta**

JAVNO PODJETJE ZA KOMUNALNE STORITVE ROGAŠKA SLATINA d.o.o.
3250 Rogaška Slatina, Celjska cesta 12, Tel.: (03) 81-21-400, ID za DDV: SI43438806, Matična št.: 5111501000
TRR: Delavska hranilnica d.d., SI56 6100 0002 0825 374, BIC: HDELSI22, e-mail: tajnistvo@okp.si, www.okp.si

Priloga št. 5

POOBLASTILO
za vodenje zbirk osebnih podatkov

Na podlagi 2. odstavka 7.člena Pravilnika o varovanju osebnih podatkov v OKP ROGAŠKA SLATINA, d.o.o.

p o o b l a š č a m

delavca/delavko: .....

zaposlenega/zaposleno na delovnem mestu: .....

da obdeluje osebne podatke (zaposlenih delavcev v podjetju, uporabnike komunalnih storitev ...) OKP ROGAŠKA SLATIAN, d.o.o., vodene v naslednjih zbirkah osebnih podatkov:

To pooblastilo velja do preklica.

Direktor:
mag. Bojan PIRŠ

Priloga št. 6

OKP ROGAŠKA ŠKA SLATINA, d.o.o. , Celjska cesta 12, 3250 Rogaška Slatina, davčna številka : 43438806, ki ga zastopa direktor mag. Bojan PIRŠ, (v nadaljevanju upravljalec)

in

Naziv podjetja obdelovalca, naslov, poštna številka in pošta, DŠ SI XXXXXXXX, ki jo zastopa delovno mesto, priimek in ime (v nadaljevanju obdelovalec)

POGODBA O OBDELAVI OSEBNIH PODATKOV

1.člen
(namen pogodbe)

Predmet te pogodbe je ureditev pogodbene obdelave osebnih podatkov in določitev pravic in obveznosti, kot jih določa 28. člen Uredbe EU 2016/679 Evropskega parlamenta in sveta (v nadaljevanju Uredba GDPR).

Pogodbeni stranki se zavezujeta, da bosta pri izvajanju določil te pogodbe v celoti spoštovali določila Uredbe EU 2016/679 (v nadaljevanju Uredba GDPR), ne glede na to ali se bosta z osebnimi podatki seznanili pri neposrednem opravljanju storitev na lokaciji upravljalca ali pogodbenega obdelovalca, pri nadzoru izvajanja določil te pogodbe, preko pisne dokumentacije ali na kakršenkoli drug način.

2.člen
(predmet pogodbe)

S to pogodbo se pogodbeni obdelovalec zbirk osebnih podatkov upravljavcu osebnih podatkov zaveže, da bo zanj obdeloval osebne podatke v obsegu in na način, določen v tej pogodbi.

Upravljalec pogodbenemu obdelovalcu z namenom izvajanja pogodbene obdelave po določbi 28.člena GDPR , izroča vse osebne podatke, ki so potrebni za izvajanje stortiev po osnovni pogodbi o poslovnem sodelovanju.
Pogodbeni obdelovalec osebnih podatkov lahko omenjena dejanja izvaja za izpolnjevanje predmeta osnovne pogodbe o poslovnem sodelovnaju in jih ne sme izvajati za noben drug namen. Pogodbeni obdelovalec zlasti ne sme uporabljati osebnih podatkov za potrebe marketinga oz. izvajati kakršnokoli drugo obdelavo osebnih podatkov (npr. razkritje, širjenje podatkov, itd.), ki je sestavni del te pogodbe. Pogodbeni obdelovalec osebnih podatkov obdeluje osebne podatke v imenu in za račun upravljavca osebnih podatkov.

3.člen
(obveznosti pogodbenega obdelovalca v zvezi s postopki in ukrepi za varstvo osebnih podatkov)

Pogodbeni obdelovalec mora pri izvrševanju določil te pogodbe v zvezi z osebnimi podatki z organizacijskimi, tehničnimi in logično-tehničnimi postopki in ukrepi zagotoviti tako varovanje osebnih

podatkov, da se preprečuje slučajno ali namerno nepooblaščeno uničevanje podatkov, njihova sprememba ali izguba ter nepooblaščena obdelava tako, da se:

- varujejo prostori, oprema in sistemska programska oprema, vključno z vhodno-izhodnimi enotami,
- varuje aplikativna programska oprema, s katero se obdelujejo osebni podatki,
- preprečuje nepooblaščen dostop do osebnih podatkov pri njihovem prenosu, vključno s prenosom po telekomunikacijskih sredstvih in omrežjih,
- zagotavlja učinkovit način blokiranja, uničenja, izbrisa ali anonimiziranja osebnih podatkov,
- omogoča poznejše ugotavljanje, kdaj so bili posamezni podatki vneseni v zbirko osebnih podatkov, uporabljeni ali drugače obdelani in kdo je to storil,
- pri načrtovanju in vpeljevanju novih IT sistemov, se mora pogodbeni obdelovalec predhodno posvetovati z upravljavcem, da se pri vpeljavi novih IT sistemov zagotovi obdelava osebnih podatkov v skladu z veljavno zakonodajo ter spoštovanjem zasebnosti posameznikov.

Pogodbeni obdelovalec osebnih podatkov mora zagotoviti integriteto (nespremenljivost), zaupnost, dostopnost in sledljivost osebnih podatkov (5 let) ter mora kadar to izhaja iz narave obdelave pomagati upravljavcu osebnih podatkov pri izpolnjevanju njegovih obveznosti, da odgovori na zahteve za uresničevanje pravic posameznika na katerega se nanašajo osebni podatki kot je na primer posredovanje informacij, ki jih je potrebno zagotoviti posamezniku, pravica do izbrisa, pravica do popravka, pravica do omejitve obdelave, obveznost obveščanja v zvezi s popravkom ali izbrisom osebnih podatkov ali omejitvijo obdelave ter pravica do prenosljivosti obdelave.

Pogodbeni obdelovalec mora dati upravljavcu na voljo vse informacije, ki dokazujejo izpolnjevanje obveznosti iz pogodbe ter mora upravljavcu ali drugemu revizorju, ki ga pooblasti upravljavec omogočiti izvajanje revizij, tudi pregledov ter pri njih sodelovati.

4.člen
(varovanje prostorov in strojne opreme)

Prostori, v katerih se nahajajo zbirke osebnih podatkov in strojna ter programska oprema, ki omogoča dostop do teh podatkov, morajo biti varovani z organizacijskimi ter fizičnimi in tehničnimi ukrepi, ki onemogočajo nepooblaščenim osebam dostop do podatkov.
Prostori pogodbenega obdelovalca, v katerih se obdelujejo osebni podatki upravljavca morajo biti fizično varovani, npr. s kontrolo vstopa z vstopno kartico, videonadzorom vstopa, alarmom gibanja po prostorih, fizičnim varovanjem varnostnika itd.
Dostop v varovane prostore je dovoljen le tistim zaposlenim, katerih pravica do vstopa v posamezni prostor izhaja iz sistemizacije delovnih mest oz. drugega notranjega akta pogodbenega obdelovalca.

5.člen
(varovanje sistemske in aplikativne programske opreme)

Dostop do sistemske in aplikativne programske opreme mora biti varovan s sistemom gesel za avtorizacijo in identifikacijo uporabnikov (posebej na ravni sistemske programske opreme in aplikativne programske opreme), ki omogoča dostop samo določenim pooblaščenim delavcem in delavcem, ki za pogodbenega obdelovalca po pogodbi opravljajo ..... (opredeliti npr servisiranje računalniške in programske opreme.
Program oziroma aplikacija mora biti sestavljen 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 vzorcu. Razvojni programi in testne podatkovne zbirke morajo biti ločene od produkcijskega okolja.
Pri načrtovanju in vpeljevanju novih IT sistemov, se mora pogodbeni obdelovalec predhodno posvetovati z upravljavcem, da se pri vpeljavi novih IT sistemov zagotovi obdelava osebnih podatkov v skladu z veljavno zakonodajo ter spoštovanjem zasebnosti posameznikov.

6.člen
(varovanje podatkovnih nosilcev)

Nosilci osebnih podatkov morajo biti hranjeni v varovanih prostorih, izven varovanih prostorov (hodniki, skupni prostori ipd.) pa morajo biti vedno zaklenjeni v ognjevarni in protivlomno zaščiteni omari.

7.člen
(varovanje pri prenosu po telekomunikacijskih sredstvih)

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

8.člen
(organizacija delovnih procesov)

Pogodbeni obdelovalec osebnih podatkov v aktu o sistemizaciji delovnih mest oz. drugem notranjem aktu določi:

- vsebinske sklope pravic oz. dolžnosti v zvezi z obdelavo podatkov iz posameznih evidenc ter delovna mesta oz. osebe, ki so nosilci teh pravic oz. dolžnosti v zvezi z obdelavo podatkov iz posameznih evidenc (pooblaščene osebe za obdelavo osebnih podatkov).

Pri pogodbenem obdelovalcu lahko osebne podatke obdelujejo le osebe, določene v aktu iz prejšnjega odstavka. Vsi ostali delavci morajo za obdelavo osebnih podatkov pridobiti pisno pooblastilo vodstva pogodbenega obdelovalca.

9.člen
(ukrepi za zagotavljanje sledljivosti operacij do njih)

Pogodbeni obdelovalec osebnih podatkov zagotovi sledljivost vseh operacij, izvedenih na osebnih podatkih, tako da je omogočeno poznejše ugotavljanje, kdaj so bili posamezni osebni podatki uporabljeni ali vnešeni v zbirko osebnih podatkov in kdo je to storil, in sicer za obdobje, ko je mogoče zakonsko varstvo pravice posameznika zaradi nedopustnega posredovanja osebnih podatkov.
Upravljavec osebnih podatkov mora za vsako posredovanje osebnih podatkov zagotoviti, 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.
Pogodbeni obdelovalec je dolžan voditi evidenco vseh vrst dejavnosti obdelave, ki jih izvaja v imenu upravljavca, in vsebuje: naziv in kontaktne podatke morebitnega podobdelovalca in pooblaščene osebe za varstvo podatkov, vrste obdelave, ki se izvajajo v imenu upravljavca, prenose osebnih podatkov v tretjo državo ali mednarodno organizacijo, vključno z identifikacijo te tretje države ali mednarodne organizacije in dokumentacijo o ustreznih zaščitnih ukrepih ter splošni opis tehničnih in organizacijskih varnostnih ukrepov pri podobdelovalcu.

10.člen
(pogodbeni obdelovalci osebnih podatkov)

Pogodbeni obdelovalec osebnih podatkov lahko samo po predhodnem pisnem soglasju upravljavca poveri posamezna opravila v zvezi z obdelavo osebnih podatkov pogodbenemu podobdelovalcu, ki je registriran za opravljanje takšne dejavnosti in zagotavlja ustrezne postopke in ukrepe za varovanje osebnih podatkov. Ob sklenitvi pogodbe je/so to naslednji podobdelovalec/-ci, za katerega/-e upravljalec osebnih podatkov podaja soglasje: navesti npr.Pošta Slovenije, ZZI d.o.o.
Če je pogodbeni obdelovalec opravljanje teh dejanj upravičeno poveril tretji osebi (pogodbenemu podobdelovalcu) mora zagotoviti, da tretja oseba v celoti spoštuje določila te pogodbe. Za izvršitev obveznosti iz te pogodbe odgovarja pogodbeni obdelovalec tako, kot da bi jih opravil sam ter v celoti odgovarja upravljavcu osebnih podatkov za izpolnjevanje obveznosti pogodbenega podobdelovalca na področju varstva osebnih podatkov ter izpolnjevanje drugih obveznosti pogodbenega podobdelovalca.
Za vsakega pogodbenega podobdelovalca osebnih podatkov določi pogodbeni obdelovalec osebnih podatkov v pisni pogodbi o procesiranju do katerih zbirk oz. do katerih vrst osebnih podatkov v posamezni zbirki osebnih podatkov ima pogodbeni podobdelovalec dostop, kategorije posameznikov, na katere se nanašajo osebni podatki, predvideni roki za izbris osebnih podatkov s strani pogodbenega podobdelovalca, kakšna pooblastila ima pogodbeni podobdelovalec na teh zbirkah oz. vrstah podatkov (dostop, pregledovanje, spreminjanje, brisanje, posredovanje) ter kakšne ukrepe in postopke mora pogodbeni podobdelovalec sprejeti oz. izvajati za varstvo teh podatkov. Pogodbeni podobdelovalec mora za vsako obdelavo osebnih podatkov zagotoviti postopke in ukrepa za varstvo osebnih podatkov, ki so enako strogi ali strožji kot tisti, ki jih v skladu s to pogodbo izvaja pogodbeni obdelovalec osebnih podatkov.

Pogodbeni obdelovalec sme opravljati posamezna opravila v zvezi z obdelavo osebnih podatkov v okviru pooblastil pogodbenega obdelovalca in osebnih podatkov ne sme obdelovati za drug namen. Pogodbeni obdelovalec osebnih podatkov nadzoruje izvajanje teh postopkov in ukrepov pri pogodbenem podobdelovalcu.
V primeru spora med pogodbenim obdelovalcem osebnih podatkov in pogodbenim podobdelovalcem je dolžan pogodbeni podobdelovalec na podlagi zahteve pogodbenega obdelovalca osebne podatke, ki jih je pogodbeno obdeloval, nemudoma vrniti pogodbenemu obdelovalcu oz. upravljavcu. 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. V primeru prenehanja pogodbenega podobdelovalca se osebni podatki brez nepotrebnega odlašanja vrnejo pogodbenemu obdelovalcu osebnih podatkov.

Za skrbnika pogodbe in pooblaščeno osebo za varstvo podatkov s strani pogodbenega obdelovalca se imenuje:

- skrbnik pogodbe pri obdelovalcu
- pooblaščena oseba za varstvo podatkov: ime in priimek osebe (ali zunanjega DPO) v podjetju obdelovalca.....,

Kontaktni podatki pooblaščene osebe za varstvo podatkov se v skladu z zakonodajo na področju varstva osebnih podatkov objavijo in posredujejo nadzornemu organu.

11.člen
(obveznosti in pooblastila upravljalca)

Upravljavec zbirk osebnih podatkov oz. oseba, ki jo ta pooblasti, je dolžan nadzorovati izvajanje določil te pogodbe, pogodbeni obdelovalec pa mu mora to omogočiti. Nadzor se izvaja v delovnem času

pogodbenega obdelovalca, pri čemer upravljavec ni dolžan predhodno obvestiti pogodbenega obdelovalca o nameravanem prihodu. Oseba, ki vrši nadzor, mora pogodbenemu obdelovalcu izkazati upravljavčevo pooblastilo za izvajanje nadzora.
Za skrbnika pogodbe s strani upravljavca se imenuje g./ga _____.

ODŠKODNINSKA ODGOVORNOST
Pogodbeni obdelovalec je dolžan pri izpolnjevanju predmeta te pogodbe ravnati s skrbnostjo dobrega strokovnjaka.
Pogodbeni obdelovalec ne odgovarja za škodo, ki je pri izpolnjevanju te pogodbe povzročena s strani upravljavca. Če je za nastalo škodo ali otežitev položaja pogodbenega obdelovalca kriv tudi upravljavec oziroma kdo drug, za katerega je upravljavec odgovoren, se odškodninska odgovornost pogodbenega obdelovalca temu sorazmerno zmanjša. Pogodbeni obdelovalec ne odgovarja za izgubo, poškodbo, ali drugo obliko spremembe osebnih podatkov, do katere je prišlo zaradi višje sile. Za višjo silo se štejejo nepredvideni in nepričakovani dogodki, ki nastopijo neodvisno od volje pogodbenih strank in ki jih pogodbeni stranki nista mogli predvideti ob sklepanju pogodbe ter kakorkoli vplivajo na izvedbo pogodbenih obveznosti. Pogodbeni obdelovalec je dolžan pisno obvestiti upravljavca o nastanku višje sile v dveh dneh po nastanku le-te.

12.člen
(varovanje zaupnosti podatkov)

Pogodbeni obdelovalec je dolžan skrbeti, da bodo zaposleni in drugi posamezniki, ki opravljajo dela ali naloge obdelave osebnih podatkov, varovali tajnost vseh podatkov, s katerimi se seznanijo pri opravljanju njihovih del in nalog. Dolžnost varovanja tajnosti osebnih podatkov te osebe obvezuje tudi po prenehanju zaposlitve oz. opravljanja del ali nalog pogodbene obdelave.

Za zaupne se štejejo tudi podatki o poslovanju upravljavca, ki niso javno dostopni in za katere pogodbeni stranki izvesta pri izpolnjevanju določil te pogodbe, npr. finančni podatki, uporabljena delovna metodologija in orodja, itd.

Pogodbeni stranki lahko razkrijeta zaupne podatke samo tistim osebam, ki neposredno sodelujejo pri izvrševanju te pogodbe. Pri tem je potrebno s primernimi navodili in ukrepi, še zagotoviti, da prejemniki zaupnih podatkov le-teh ne uporabijo v nasprotju z določili pogodbe.
Kot neupravičeno razkritje zaupnih podatkov tretji osebi se šteje vsaka reprodukcija podatkov v ustni ali pisni obliki, v celoti ali deloma, ali njihova distribucija nepooblaščeni osebi, ter vsaka druga oblika razkritja zaupnih podatkov.
Pogodbeni obdelovalec je dolžan v primeru seznanitve s kršitvijo varstva osebnih podatkov, brez nepotrebnega odlašanja, pisno obvestiti upravljavca osebnih podatkov. Pisno obvestilo mora vsebovati opis kršitve varstva osebnih podatkov skupaj z vrstami in številom zadevnih evidenc osebnih podatkov ter kategorijami in številom zadevnih oseb. V pisnem obvestilu mora pogodbeni obdelovalec navesti tudi opis verjetnih posledic kršitve varstva osebnih podatkov.

Pogodbeni stranki sta dolžni varovati poslovno skrivnost tako v času izvrševanja te pogodbe kakor tudi po njeni izvršitvi ali morebitni razvezi.

13.člen
(trajanje pogodbe)

Ta pogodba je sklenjena za čas trajanja krovne pogodbe o poslovnem sodelovanju.

V primeru prenehanja oz. odpovedi pogodbe mora pogodbeni obdelovalec nemudoma prenehati obdelovati osebne podatke upravljavca. Izjemoma jih lahko obdeluje le še zaradi dokončanja začetih poslov po pogodbi, ki jih je dolžan zagotoviti. V primeru prenehanja oz. odpovedi pogodbe mora pogodbeni obdelovalec vse osebne podatke upravljavcu takoj vrniti, morebitne kopije teh podatkov pa mora takoj uničiti.

Če pogodbeni obdelovalec ne ravna v skladu s predmetom pogodbe in zato obstaja nevarnost uničenja, spremembe, izgube ali nepooblaščene obdelave osebnih podatkov, ga mora upravljavec na to opozoriti in mu določiti primeren rok za odpravo nepravilnosti. Če pogodbeni obdelovalec ne ravna v skladu z upravljavčevo zahtevo, lahko upravljavec odstopi od te pogodbe brez odpovednega roka in zahteva povrnitev nastale škode.

V primeru prenehanja pogodbenega obdelovalca mora le-ta zagotoviti, da se osebni podatki iz predmeta pogodbe oziroma njihove kopije brez nepotrebnega odlašanja vrnejo upravljavcu.

14.člen
(končne določbe)

V primeru sprememb vsebine tabele 1, ki je priloga k tej pogodbi, skleneta upravljavec in pogodbeni obdelovalec v roku 1 meseca po sprejetju teh sprememb aneks k tej pogodbi.
V primeru spora med upravljavcem in pogodbenim obdelovalcem je le-ta dolžan osebne podatke na podlagi upravljavčeve zahteve temu takoj vrniti. Morebitne kopije teh podatkov mora pogodbeni obdelovalec 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.
Pogodbeni stranki se sporazumeta, da bosta morebitne spore iz te pogodbe reševali sporazumno. Če sporazuma ne bo mogoče doseči, je za reševanje spora pristojno sodišče v .....

15.člen

Pogodba je sklenjena v dveh enakih izvodih, od katerih prejme vsaka stranka po en izvod.
Pogodba začne veljati z dnem, ko jo podpišeta obe pogodbeni stranki.

Upravljalec osebnih podatkov:	Pogodbeni obdelovalec osebnih podatkov:
Ime in priimek, funkcija zastopnika (podpis)	Ime in priimek, funkcija zastopnika (podpis)
_____	_____
Kraj in datum: _____	Kraj in datum: _____

JAVNO PODJETJE ZA KOMUNALNE STORITVE ROGAŠKA SLATINA d.o.o.
3250 Rogaška Slatina, Celjska cesta 12, Tel.: (03) 81-21-400, ID za DDV: SI43438806, Matična št.: 5111501000
TRR: Delavska hranilnica d.d., SI56 6100 0002 0825 374, BIC: HDELSI22, e-mail: tajnistvo@okp.si, www.okp.si

Priloga št. 7

PRIJAVA KRŠITVE VARSTVA OSEBNIH PODATKOV

Obvezno preberite!

- *Prijava kršitve varstva osebnih podatkov ima naravo pobude za uvedbo inšpekcijskega postopka po Zakonu o inšpekcijskem nadzoru (ZIN). Prijavitelj ni stranka morebitnega inšpekcijskega postopka.*
- *To vlogo se naslovi na Informacijskega pooblaščenca, Zaloška 59, 1000 Ljubljana ali na: gp.ip@ip-rs.si. Obrazec inšpekcijske prijave ni predpisan.*
- *Informacijski pooblaščenec vaših podatkov v skladu z določbami ZIN ne bo posredoval kršitelju ali drugim osebam (varovanje tajnosti prijave). Prijavo lahko vložite tudi anonimno, vendar vas v tem primeru, po zaključku postopka ne bomo mogli obvestiti o naših dejanjih in ugotovitvah.*

1. Podatki o prijavitelju

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

2. Osnovni podatki o kršitvi

Kdo oziroma kateri upravljavec naj bi po vašem mnenju kršil pravila varstva osebnih podatkov? *(osebno ime ali naziv pravne osebe, naslov in drugi kontaktni podatki)*	
Datum ali trajanje kršitve?	
Ali ste upravljavca opozorili na kršitev in od njega prejeli odgovor? *(če s temi dokumenti razpolagate, jih priložite)*	

3. Podrobnejši podatki o kršitvi (razlogi za prijavo)

Čim bolj podrobno opišite okoliščine dogodka oziroma ravnanja, pri katerem naj bi prišlo do kršitve oziroma zlorabe osebnih podatkov. Zlasti je pomembno, da navedete, zakaj menite, da je prišlo do kršitve, način storitve, katera oseba je to storila, kateri osebni podatki so bili nezakonito obdelovani, posledice kršitve, ali obstajajo kakšni dokazi o kršitvi in podobno: