Na podlagi 25. člena Zakona o varstvu osebnih podatkov - ZVOP-1 (Uradni list RS, 86/04, 113/05 in 67/07) in 40. člena Statuta (Ur. l. RS, št. 34/99, 63/00, 93/00 in 115/2007) Občine Žužemberk izdaja župan Občine Žužemberk naslednji

PRAVILNIK

o zavarovanju osebnih podatkov

I. SPLOŠNE DOLOČBE

1. člen
Vsebina pravilnika

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

2. člen
Namen pravilnika

S postopki in ukrepi, določenimi v tem pravilniku, se v občini kot upravljavcu osebnih podatkov preprečuje slučajno ali namerno nepooblaščeno spreminjanje, izguba ali uničenje osebnih podatkov ter njihova nepooblaščena uporaba, obdelava, hramba, posredovanje in prenos, in sicer tako, da se:

- varujejo prostori, v katerih se obdelujejo osebni podatki;
- varuje oprema, ki se uporablja za obdelavo osebnih podatkov;
- zagotavlja, da imajo dostop do osebnih podatkov samo osebe, ki so podpisale izjavo o varovanju teh podatkov in se morajo z njimi seznaniti zaradi opravljanja delovnih nalog;
- nepoklicanim preprečuje dostop do osebnih podatkov med njihovo obdelavo in med fizičnim prenašanjem ali prenosom s pomočjo informacijskih in telekomunikacijskih sredstev;
- zagotavlja učinkovit način blokiranja, uničenja, izbrisa ali anonimiziranja osebnih podatkov in
- omogoča poznejše ugotavljanje, kdaj so bili posamezni osebni podatki vneseni v zbirko osebnih podatkov, uporabljeni ali drugače obdelani in kdo je to storil, in sicer za obdobje, ko je mogoče zakonsko varstvo pravice posameznika zaradi nedopustnega posredovanja ali obdelave osebnih podatkov.

3. člen
Pomen izrazov

V tem pravilniku uporabljeni izrazi imajo naslednji pomen:

1. ZVOP-1 - Zakon o varstvu osebnih podatkov (Uradni list RS, št. 86/04,113/05 in 67/07);
2. Posameznik - je določena ali določljiva fizična oseba, na katero se nanaša osebni podatek; fizična oseba je določljiva, če se lahko neposredno ali posredno identificira, predvsem s sklicevanjem na identifikacijsko številko ali na enega ali več dejavnikov, ki so značilni za njegovo fizično, fiziološko, duševno, ekonomsko, kulturno ali družbeno identiteto, pri čemer način identifikacije ne povzroča velikih stroškov ali ne zahteva veliko časa;
3. Osebni podatek - je katerikoli podatek, ki se nanaša na posameznika, ne glede na obliko, v kateri je izražen;
4. Občutljivi osebni podatek - je podatek 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, če je z njihovo uporabo mogoče določiti posameznika v zvezi s kakšno od prej navedenih okoliščin;

5. Zbirka osebnih podatkov - je vsak strukturiran niz 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;
6. Obdelava 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);
7. Upravljavec osebnih podatkov - je fizična ali pravna oseba ali druga oseba javnega ali zasebnega sektorja, ki sama ali skupaj z drugimi določa namene in sredstva obdelave osebnih podatkov oziroma oseba, določena z zakonom, ki določa tudi namene in sredstva obdelave;
8. Uporabnik osebnih podatkov - je fizična ali pravna oseba ali druga oseba javnega ali zasebnega sektorja, ki se ji posredujejo ali razkrijejo osebni podatki;
9. Pogodbeni obdelovalec – je fizična ali pravna oseba, ki obdeluje osebne podatke v imenu in na račun upravljavca osebnih podatkov.
10. Pogodbeni vzdrževalec – je fizična ali pravna oseba, ki vzdržuje ali popravlja strojno oziroma programsko računalniško opremo ter izdeluje in namešča novo strojno ali programsko računalniško opremo za obdelavo osebnih podatkov.
11. Nosilec podatkov - so vse vrste sredstev, na katerih so zapisani ali posneti podatki (listine, akti, gradiva, spisi, računalniška oprema vključno s magnetni, optični ali drugi računalniški mediji, fotokopije, zvočno in slikovno gradivo, mikrofilmi, naprave za prenos podatkov, ipd.);

4. člen
Uporaba pravilnika

1) Zaposleni in drugi sodelavci, ki pri svojem delu obdelujejo in uporabljajo osebne podatke, morajo biti seznanjeni z Zakonom o varovanju osebnih podatkov, z zakoni in drugimi predpisi, ki urejajo posamezna področja njihovega dela ter vsebino tega pravilnika.
2) Po tem pravilniku morajo ravnati zaposleni in druge osebe, ki v občini obdelujejo osebne podatke.
3) Pred nastopom dela na delovnem mestu, na katerem se obdelujejo osebni podatki, mora oseba iz prejšnjega odstavka podpisati izjavo, ki jo zavezuje k varovanju osebnih podatkov.
4) Iz podpisane izjave mora biti razvidno, da je podpisnik seznanjen z določbami tega pravilnika ter določbami ZVOP-1, izjava pa mora vsebovati tudi pouk o posledicah kršitve tega pravilnika in zakona.
5) Po tem pravilniku morata ravnati tudi pogodbeni obdelovalec oziroma pogodbeni vzdrževalec občine.

5. člen

Vsi dokumenti , ki vsebujejo zbirko osebnih podatkov morajo biti obravnavani tudi v skladu z Uredbo o upravnem postopku (Ur. l. RS, št. 20/05), Pravilnikom o izvrševanju Uredbe o upravnem postopku (Ur. l. RS, št. 75/05) in Navodilom za določanje rokov hranjenja dokumentarnega gradiva organov javne uprave (Ur. L. RS, št. 81/05).

II. OBDELAVA OSEBNIH PODATKOV

6. člen
Vzpostavitev zbirke osebnih podatkov

1) Posamezno zbirko osebnih podatkov pri upravljavcu vzpostavi direktor občinske uprave (v nadaljevanju: direktor).
2) Direktor je odgovorna oseba, oziroma določi osebo, ki je odgovorna za obdelavo podatkov posamezne zbirke osebnih podatkov (v nadaljevanju: odgovorna oseba).

7. člen
Opis zbirk osebnih podatkov

Opis zbirk osebnih podatkov, katerih upravljavec je občina, se vodi v katalogu zbirk osebnih podatkov (opisu zbirk osebnih podatkov), ki se vodi v skladu z 26. členom ZVOP-1.

8. člen
Obdelava osebnih podatkov

1) Občina, kot upravljavec osebnih podatkov, obdelujejo le tiste osebne podatke, katerih obdelavo in vrsto podatkov, ki se obdelujejo, določa zakon, ali če je za obdelavo določenih osebnih podatkov podana osebna privolitev posameznika.
2) Ne glede na prejšnji odstavek lahko občina obdeluje osebne podatke posameznikov, ki so z njo sklenili pogodbo, ali pa so na podlagi pobude posameznika z njo v fazi pogajanj za sklenitev pogodbe, če je obdelava osebnih podatkov potrebna in primerna za izvedbo pogajanj za sklenitev pogodbe ali za izpolnjevanje pogodbe.
3) Ne glede na prvi odstavek tega člena lahko občina obdeluje osebne podatke, če je to nujno zaradi uresničevanja zakonitih interesov in ti interesi očitno prevladujejo nad interesi posameznika, na katerega se osebni podatki nanašajo.
4) Občina lahko občutljive osebne podatke obdeluje le v primerih, določenih v 13. členu ZVOP-1. Ti podatki morajo biti pri obdelavi posebej označeni in zavarovani.

9. člen
Katalog zbirke osebnih podatkov

1) Odgovorna oseba je dolžna za vsako zbirko osebnih podatkov 15 dni pred vzpostavitvijo zbirke osebnih podatkov vzpostaviti katalog zbirke osebnih podatkov z vsebino, določeno v 26. členu ZVOP-1.
2) Odgovorna oseba je dolžna skrbeti za točnost in ažurnost kataloga. V ta namen mora katalog zbirk osebnih podatkov osvežiti oziroma dopolniti ob vsaki spremembi vrste osebnih podatkov v zbirki osebnih podatkov.
3) Direktor državnemu nadzornemu organu za varstvo osebnih podatkov najmanj 15 dni pred vzpostavitvijo zbirke osebnih podatkov ali pred vnosom nove vrste osebnih podatkov posreduje podatke iz 1., 2., 4., 5., 6., 9., 10., 11., 12. in 13. točke 26. člena ZVOP-1 katalogov zbirk osebnih podatkov.
4) Spremembo vrste osebnih podatkov (5. točka kataloga), ki se obdelujejo v zbirki iz prejšnjega odstavka, direktor državnemu nadzornemu organu za varstvo osebnih podatkov posreduje najkasneje v 8 dneh od dneva spremembe.
5) Pooblaščeni obdelovalec se s katalogom zbirke osebnih podatkov, ki je predmet pogodbene obdelave, seznani tako, da postane katalog zbirke osebnih podatkov priloga in sestavni del pogodbe o ureditvi medsebojnih razmerij v zvezi s pogodbeno obdelavo.
6) Vpogled v katalog zbirke osebnih podatkov se omogoči vsakomur, ki to zahteva. Zahtevek reši odgovorna oseba.

10. člen
Seznam odgovornih oseb in pooblaščenih obdelovalcev

1) Direktor oziroma oseba, ki jo pisno pooblasti, je dolžan skrbeti za ažurnost seznama, iz katerega je za vsako zbirko osebnih podatkov razvidno, kdo je odgovorna oseba za posamezno zbirko osebnih podatkov ter kdo so pooblaščeni obdelovalci teh osebnih podatkov.
2) V seznam iz prejšnjega odstavka se vpisujejo naslednji podatki:
   - naziv zbirke osebnih podatkov,
   - osebno ime in delovno mesto odgovorne osebe,
   - osebno ime in delovno mesto oseb, ki zaradi narave njihovega dela pri upravljavcu podatkov obdelujejo osebne podatke ter
   - identifikacijski podatki (ime oz. naziv ter naslov oz. sedež) pooblaščenega obdelovalca.

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

11. člen
Pogodbena obdelava

1) Občina, ki posamezna opravila v zvezi z obdelavo osebnih podatkov zaupa pogodbenemu obdelovalcu, medsebojna razmerja s pogodbenim obdelovalcem uredi s pisno pogodbo, določeno v drugem odstavku 11. člena ZVOP-1.
2) Pogodbeni obdelovalec lahko opravlja storitve obdelave osebnih podatkov samo v okviru pooblastil iz pogodbe iz prvega odstavka tega člena in podatkov ne sme obdelovati za noben drug namen.
3) Pogodbeni obdelovalec, ki za upravljavca osebnih podatkov pogodbeno dogovorjene storitve opravlja izven upravljavčevih službenih prostorov, mora imeti vsaj tako stopnjo varovanja obdelave osebnih podatkov, kakor ga predvideva ta pravilnik. Če pogodbeni obdelovalec nima akta o postopkih in ukrepih za zavarovanje podatkov, izdanega na podlagi 25. člena ZVOP-1, se ga v pogodbi iz prvega odstavka tega člena zaveže, da bo pri obdelavi osebnih podatkov, s katerimi upravlja družba, ravnal po določbah tega pravilnika.
4) Direktor lahko določi osebo, ki pri pogodbenem obdelovalcu nadzoruje izvajanje postopkov in ukrepov zavarovanja osebnih podatkov, ki so predmet pogodbene obdelave.
5) V primeru spora lahko direktor od pogodbenega obdelovalca zahteva, da mu nemudoma vrne osebne podatke, ki so predmet izvajanja pogodbeno dogovorjene obdelave podatkov, morebitne kopije teh podatkov pa uniči, ali, če tako določa zakon, izroči pristojnemu državnemu organu.

12. člen
Pogodbeno vzdrževanje

1) Določbe drugega odstavka 11. člena ZVOP-1 in prejšnjega člena tega pravilnika se smiselno uporabljajo tudi za ureditev razmerij upravljavca osebnih podatkov s pogodbenim vzdrževalcem.

2) Strojna in programska računalniška oprema se praviloma vzdržuje v prostorih občine, če pa se naprave, v katerih so shranjeni osebni podatki, odnesejo k pogodbenemu vzdrževalcu, je potrebno izvesti ukrepe, ki preprečujejo, da bi med vzdrževalnimi deli do osebnih podatkov dostopale nepooblaščene osebe.

IV. VAROVANJE PROSTOROV IN NOSILCEV PODATKOV

13. člen
Varovanje vstopa v prostore

1) Prostori občine, v katerih se nahajajo nosilci podatkov, ki vsebujejo osebne podatke, ter strojna in programska oprema, s katero se obdelujejo osebni podatki (v nadaljevanju:

varovani prostori), so varovani z organizacijskimi ter fizičnimi oziroma tehničnimi ukrepi, ki nepooblaščenim osebam onemogočajo dostop do osebnih podatkov.

2) Zaposleni lahko v varovane prostore vstopijo le v rednem delovnem času, zunaj rednega delovnega časa pa le z dovoljenjem direktorja ali osebe, ki jo je pooblastil. Druge osebe lahko v varovane prostore vstopijo le v spremstvu ali ob navzočnosti zaposlenega delavca.
3) Varovani prostori morajo biti pod stalnim nadzorom zaposlenih, ki v njih delajo. Ob odsotnosti mora zaposleni pisarno zakleniti. Mehanski ključi se ne smejo puščati v ključavnici v vratih. Način hrambe teh ključev in osebe, pooblaščene za dostop do ključev, določi direktor. Če se za zaklepanje pisarn in drugih prostorov uporabljajo elektronske ključavnice, način uporabe teh ključavnic določi direktor.
4) Osebe, ki niso zaposlene v občini (npr. vzdrževalci prostorov, strojne in programske opreme, obiskovalci, poslovni partnerji), se smejo v varovanih prostorih gibati samo pod nadzorom zaposlenega, ki skrbi za varovani prostor, v katerem se oseba giba.
5) Zaposleni, ki nimajo dostopa do osebnih podatkov (čistilke, varnostniki idr.), se lahko izven delovnega časa gibljejo samo v tistih varovanih prostorih, kjer je vpogled v osebne podatke onemogočen tako, da so nosilci podatkov shranjeni v zaklenjenih omarah in pisalnih mizah, računalniki in druga strojna oprema pa izklopljeni ali kako drugače fizično ali programsko zaklenjeni.
6) V prostorih, ki so namenjeni poslovanju s strankami, morajo biti nosilci podatkov in računalniški prikazovalniki nameščeni tako, da stranke nimajo vpogleda vanje.
7) Varovani prostori, v katerih se nahajajo nosilci podatkov, ki vsebujejo občutljive osebne podatke, morajo biti varovani tako, da je zagotovljen popoln nadzor nad delom in gibanjem v teh prostorih.
8) V primeru videonadzora območja objekta in vstopnih točk v objekt ureja poseben akt, ki ga izda direktor.

14. člen
Varovanje nosilcev podatkov, ki vsebujejo osebne podatke

1) Zaposleni ne smejo puščati nosilcev osebnih podatkov na mizah ali drugih vidnih površinah v prisotnosti oseb, ki nimajo pravice vpogleda vanje.
2) Nosilci podatkov, ki vsebujejo občutljive osebne podatke, in drugi nosilci podatkov, za katere direktor tako določi, se morajo hraniti v zaklenjeni varnostni omari ali blagajni, nameščeni v varovanem prostoru.
3) Nosilce podatkov, ki vsebujejo osebne podatke, lahko izven prostorov upravljavca osebnih podatkov odnašata direktor in odgovorna oseba, ostali zaposleni pa samo z dovoljenjem direktorja ali osebe, ki jo pooblasti.
4) Nosilcev podatkov, ki vsebujejo občutljive osebne podatke, se ne sme odnašati izven prostorov družbe, razen izjemoma, z dovoljenjem direktorja, če je to nujno potrebno za reševanje zadeve, ki vsebuje te občutljive osebne podatke.
5) V prostorih, ki so namenjeni poslovanju s strankami, morajo biti nosilci podatkov, ki vsebujejo osebne podatke, in računalniški zasloni nameščeni tako, da stranke nimajo vpogleda vanje.

15. člen
Varovanje enot za shranjevanje osebnih podatkov

1) V varovanih prostorih morajo biti po zaključku delovnega časa oziroma po končanem delu izven delovnega časa omare, pisalne mize, blagajne in drugo pisarniško pohištvo z nosilci podatkov, ki vsebujejo osebne podatke (v nadaljnjem besedilu: shranjevalne enote), zaklenjene, računalniki in druga strojna oprema pa izklopljeni in fizično ali programsko zaklenjeni.
2) Shranjevalne enote, ki se nahajajo izven varovanih prostorov (hodniki, skupni prostori), morajo biti vedno, kadar niso v uporabi, zaklenjene.

V. SPREJEM, POŠILJANJE IN POSREDOVANJE OSEBNIH PODATKOV

16. člen
Sprejem osebnih podatkov

1) Delavec, ki je zadolžen za sprejem in evidenco pošte, ravna s pošto kot določajo določila pisarniškega poslovanja.
2) Delavec, ki je zadolžen za sprejem in evidenco pošte, ne odpira tistih pošiljk, ki so označeni kot osebni podatek ali občutljiv osebni podatek.

17. člen
Pošiljanje osebnih podatkov

1) Osebne podatke je dovoljeno pošiljati po pošti ter prenašati z informacijskimi, telekomunikacijskimi in drugimi sredstvi le ob izvajanju postopkov in ukrepov, ki nepooblaščenim preprečujejo prilaščanje ali uničenje osebnih podatkov.
2) Osebni podatki, ki se uporabniku osebnih podatkov posredujejo v fizični obliki, morajo biti posredovani priporočeno in 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.
3) Osebne podatke je z informacijskimi in komunikacijskimi sredstvi dovoljeno posredovati le ob izvajanju varnostnih postopkov in ukrepov, ki nepooblaščenim osebam preprečujejo prilaščanje ali uničenje podatkov ter neupravičeno seznanjanje z njihovo vsebino. Taki varnostni postopki in ukrepi obsegajo uporabo kriptozaščite ali drugih ukrepov varnega elektronskega poslovanja.
4) Če se posreduje originalni dokument, ki vsebuje osebne podatke, mora biti v času odsotnosti nadomeščen s fizično oziroma elektronsko kopijo.
5) Občutljivi osebni podatki pa se pošiljajo v zaprtih ovojnicah proti podpisu v dostavni knjigi ali z vročilnico. Občutljivi osebni podatki, ki se posredujejo z informacijskimi in komunikacijskimi sredstvi, morajo biti posebej dodatno zavarovani z kriptografskimi metodami in elektronskim podpisom.

18. člen
Posredovanje osebnih podatkov

1) Osebni podatek, s katerim upravlja občina, se na zahtevo posreduje ali razkrije samo tistim uporabnikom osebnih podatkov, ki se izkažejo z ustrezno zakonsko podlago ali s pisno zahtevo oziroma privolitvijo posameznika, na katerega se podatki nanašajo. Zahtevo za posredovanje obravnava direktor, odgovorna oseba ali druga oseba, ki jo pooblasti direktor.
2) Zahteva za posredovanje osebnih podatkov je lahko pisna ali ustna. Ob vložitvi pisne zahteve mora uporabnik osebnih podatkov jasno navesti določbo zakona, ki ga pooblašča za pridobitev osebnih podatkov, ali pa mora k zahtevi priložiti pisno zahtevo oziroma privolitev posameznika, na katerega se podatki nanašajo. Če uporabnik zahteva posredovanje osebnih podatkov ustno, lahko direktor, odgovorna oseba ali druga oseba, ki jo pooblasti direktor, v primeru dvoma o obstoju pisne zahteve oziroma privolitve posameznika, na katerega se podatki nanašajo, od uporabnika osebnih podatkov zahteva, naj jih predloži.
3) Posredovanje občutljivih osebnih podatkov mora biti posebej označeno in zavarovano.
4) *Pri posredovanje osebnih podatkov med organi javne uprave je potrebno upoštevati tudi določbe Uredbe o pridobivanju in posredovanju podatkov med organi javne uprave za potrebe upravnih postopkov (Ur. l. RS, št. 38/02 in 129/03).*

19. člen
Evidenca posredovanj

1) Vsako posredovanje osebnih podatkov iz prejšnjega člena se zabeleži z navedbo naslednjih podatkov:
   - kateri osebni podatki so bili posredovani,
   - komu (ime oz. firma in naslov oz. sedež osebe) so bili posredovani osebni podatki,
   - datum in ura posredovanja osebnih podatkov ter
   - podlaga (zakon ali osebna privolitev prizadetega posameznika), na kateri so bili posredovani osebni podatki.
2) Zapis iz prejšnjega odstavka se v pisni ali elektronski obliki, odvisno od nosilca podatkov, s katerim se posreduje osebni podatek, zabeleži v zbirko osebnih podatkov, ki ji pripada posredovani osebni podatek, in sicer v posebno rubriko "Evidenca posredovanj osebnih podatkov".
3) Zabeležbo iz prvega odstavka tega člena naredi odgovorna oseba ali pooblaščeni obdelovalec, ki je osebne podatke posredoval uporabniku.

20. člen
Pregledovanje in prepisovanje (kopiranje) upravnih spisov

1) Pregledovanje in prepisovanje (kopiranje) upravnih spisov in dajanje obvestil o poteku postopka se opravlja v skladu z določbami 82. člena Zakona o splošnem upravnem postopku ter Uredbo o upravnem postopku,

2) Pregledovanje in prepisovanje upravnih spisov je ob prisotnosti uradne osebe dovoljena le strankam v postopku in osebam, ki v svoji pisni vlogi verjetno izkažejo, da imajo od tega pravno korist. Pred pregledom, oziroma, prepisovanjem upravnega spisa je potrebno preveriti identiteto stranke, oziroma, opravičenca.

3) Pri vsakem pregledovanju, oziroma prepisovanju podatkov iz upravnega spisa se naredi uradni zaznamek, ki se vloži v spis. Iz uradnega zaznamka, ki ga mora podpisati tudi upravičenec, mora biti razvidna številka spisa, datum in ura pregleda, osebno ime upravičenca, njegov naslov, številka in vrsta dokumenta iz katerega je ugotovljena identiteta ter namen, zaradi katerega je bil opravljen pregled, oziroma prepis. Upravičenca je potrebno opozoriti na dolžnost varovanja osebnih podatkov, kar mora biti razvidno tudi iz uradnega zaznamka.

21. člen
Dostop do osebnih podatkov v okviru poslovanja občine

1) Osebni podatki iz zbirk osebnih podatkov občine so v okviru poslovanja dostopni tistim zaposlenim, ki jih potrebujejo za izvajanje svojih delovnih nalog in ki so podpisali izjavo iz 4. člena tega pravilnika.
2) Dokumenti, ki vsebujejo osebne podatke zaposlenih, se zaposlenemu, na katerega se osebni podatki nanašajo, posredujejo na način, določen v tretjem in četrtem odstavku 14. člena tega pravilnika.
3) Vsak dostop zaposlenih do občutljivih osebnih podatkov mora odgovorna oseba ali pooblaščeni obdelovalec zabeležiti v "Evidenco posredovanj osebnih podatkov".

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

22. člen
Varovanje računalniške opreme

1) Vklop oziroma zagon računalnikov mora biti zaščiten z geslom ali z drugim sistemom avtentikacije uporabnika. Računalniki in druga strojna oprema morajo biti izven delovnega časa

izklopljeni ali programsko zaklenjeni, kar velja tudi v primeru daljše zapustitve pisarne oziroma delovnega prostora (npr. zaradi odmora med delom, sestanka, opravka zunaj podjetja ipd.).

2) Vzdrževanje in popravilo strojne in programske računalniške opreme, s katero se obdelujejo osebni podatki, je dovoljeno samo z odobritvijo osebe, ki jo direktor zadolži za skrb za delovanje računalniškega informacijskega sistema družbe (v nadaljnjem besedilu: skrbnik sistema).
3) Računalniško opremo vzdržuje in popravlja pogodbeni vzdrževalec, če pa ta dela izvede izvajalec, ki ni pogodbeni vzdrževalec, jih mora posebej odobriti direktor ali oseba, ki jo pooblasti. Spremembe in dopolnitve sistemske in aplikativne programske opreme morajo biti ustrezno dokumentirane.
4) Zaposleni ne smejo nameščati programske opreme in odnašati programske opreme iz prostorov družbe brez vednosti skrbnika sistema.
5) Za vse podatke, ki se obdelujejo in hranijo na strežniku informacijskega sistema, in za vso programsko opremo strežnika, se vodi kopija in dvojnik kopije. Dvojnik kopije mora biti varno shranjen na lokaciji izven objekta, v katerem je nameščen strežnik. Za ažurnost kopij skrbi skrbnik sistema oziroma pogodbeni obdelovalec ali pogodbeni vzdrževalec, kadar tako določa pogodba o obdelavi osebnih podatkov ali vzdrževanju informacijskega sistema.
6) Postopki in ukrepi, ki jih ta pravilnik določa za shranjevanje in varovanje osebnih podatkov, veljajo tudi za uporabniško programsko opremo, namenjeno obdelavi osebnih podatkov.

23. člen
Protivirusno varovanje

1) Diski omrežnega strežnika in osebnih računalnikov, na katerih se nahajajo osebni podatki, se varujejo s protivirusno programsko opremo. O vsakem pojavu računalniškega virusa mora biti obveščen skrbnik sistema, ki poskrbi, da se virus odpravi in ugotovi vzrok pojava virusa v informacijskem sistemu družbe.
2) Vsi podatki in programska oprema, ki so namenjeni uporabi v informacijskemu sistemu, in prispejo k upravljavcu osebnih podatkov na medijih za prenos računalniških podatkov ali preko komunikacijskih kanalov, morajo biti pred uporabo protivirusno pregledani.

24. člen
Varovanje dostopa do interneta

1) Priključna točka informacijskega sistema na internet mora biti opremljena z varnostno pregrado (*firewall*) in drugo varnostno opremo za spremljanje in evidentiranje aktivnosti uporabnikov ter preprečevanje vdorov in vnosa škodljivih vsebin v informacijski sistem.
2) Varnostna pregrada iz prejšnjega odstavka mora zagotavljati:
   - upravljanje dostopov zaposlenih do interneta;
   - omejitev dostopa zaposlenih do določenih vsebin na svetovnem spletu ali uporabe določenih drugih storitev interneta;
   - zaznavanje in preprečevanje poskusov vdorov v informacijski sistem;
   - preprečevanje in odkrivanje poskusov vnosov računalniških virusov.

VI. KONTROLA IDENTITETE IN POOBLASTIL UPORABNIKA UPRAVLJAVČEVEGA INFORMACIJSKEGA SISTEMA ALI UPRAVLJAVČEVEGA OSEBNEGA RAČUNALNIKA

25. člen
Identificiranje in avtoriziranje dostopa do informacijskega sistema ali osebnega računalnika

1) Dostop do podatkov in uporaba drugih virov informacijskega sistema ali osebnega računalnika (v nadaljevanju: informacijski sistem) je varovan s sistemom, ki preveri identiteto uporabnika in njegova pooblastila za dostop do podatkov in drugih virov informacijskega sistema.

2) Sistem ugotavljanja identitete in preverjanja pooblastil uporabnika informacijskega sistema mora biti zgrajen tako, da onemogoča lažno predstavitev identitete ali zlorabo identitete drugega uporabnika.
3) Kadar kontrola in evidentiranje dostopa do podatkov in drugih virov informacijskega sistema temelji na osebnem geslu, si mora geslo določiti uporabnik sam, geslo sme veljati največ tri mesece uporabe, pri zamenjavi gesla pa uporabnik ne sme uporabiti iste kombinacije znakov.
4) Dostop uporabnika do informacijskega sistema mora biti po zaporednem vnosu treh nepravilnih gesel blokiran. Za deblokado uporabnika je pooblaščen skrbnik sistema.
5) Izjemoma sme na opremi, ki jo pisno določi direktor, geslo veljati daljše časovno obdobje.
6) Če se za preverjanje identitete in pooblastil uporabnika informacijskega sistema uporabljajo digitalna potrdila, generatorji dostopnih kod in podobno, način uporabe teh pripomočkov oziroma naprav z navodilom določi direktor.
7) S sistemom kontrole in evidentiranja dostopa do podatkov in drugih virov informacijskega sistema upravlja skrbnik sistema ali druga oseba, ki jo določi direktor.

26. člen
Varnostna shema

1) Vsakemu uporabniku informacijskega sistema se dostop omeji le na tiste osebne podatke in informacijske servise, ki jih potrebuje za izvajanje svojih delovnih nalog.
2) Na podlagi tako določenih pravic skrbnik sistema vzpostavi in vzdržuje seznam uporabnikov sistema, iz katerega so za vsakega uporabnika sistema razvidni njegovi identifikacijski podatki in njegove pravice dostopa do posameznih osebnih podatkov (v nadaljevanju: varnostna shema).
3) Ob spremembi pravic posameznega uporabnika (na primer: prekinitev delovnega razmerja, premestitev in podobno) skrbnik sistema varnostno shemo ustrezno popravi.

VI. BRISANJE, UNIČENJE, BLOKIRANJE ALI ANONIMIZIRANJE OSEBNIH PODATKOV

27. člen
Hramba osebnih podatkov

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.

28. člen
Brisanje ali uničenje osebnih podatkov

1) Osebni podatki v fizični obliki se uničijo na način, s katerim se zagotovi, da postane osebni podatek nerazpoznaven in neobnovljiv.
2) Za brisanje osebnih podatkov v elektronski obliki se uporabi takšna metoda brisanja, ki onemogoča rekonstrukcijo brisanih podatkov.
3) Uničenje nosilcev podatkov in pomožnega gradiva se zagotovi v skladu s prvim in drugim odstavkom tega člena.
4) Izrabljeni, neuporabni in okvarjeni nosilci podatkov, ki vsebujejo osebne podatke, se do uničenja zbirajo na varnem mestu, ki ga določi direktor.
5) Prenos nosilcev osebnih podatkov na mesto uničenja in uničenje na način, ki onemogoča razpoznavnost ali obnovitev osebnih podatkov, izvede odgovorna oseba. Pri prenosu je potrebno zagotoviti ustrezno zavarovanje.
6) Uničenje nosilcev podatkov in pomožnega gradiva, ki vsebujejo občutljive osebne podatke, nadzoruje posebna tričlanska komisija, ki jo imenuje direktor. Komisijo sestavljajo zaposleni občine, en član komisije pa je odgovorna oseba.
7) O uničenju nosilcev podatkov in pomožnega gradiva odgovorna oseba oziroma komisija sestavi zapisnik.

V. UKREPANJE OB SUMU VARNOSTNEGA DOGODKA

29. člen
Obveščanje

1) Zaposleni pri upravljavcu osebnih podatkov so dolžni o aktivnostih, ki so povezane z odkrivanjem ali nepooblaščenim uničenjem osebnih podatkov, z zlonamerno ali nepooblaščeno uporabo, prilaščanjem, spreminjanjem ali poškodovanjem osebnih podatkov takoj obvestiti direktorja ali odgovorno osebo, sami pa morajo poskusiti takšno aktivnost z zakonitimi ukrepi preprečiti.
2) O morebitnem suma storitve kaznivega dejanja, vezanega na varnost obdelave osebnih podatkov pri upravljavcu, policijo ali tožilstvo obvešča direktor ali oseba, ki jo pooblasti.

VI. ODGOVORNOST ZA IZVAJANJE POSTOPKOV IN UKREPOV ZA ZAVAROVANJE OSEBNIH PODATKOV

30. člen
Izvajanje postopkov in ukrepov zavarovanja

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

31. člen
Nadzor nad izvajanjem zavarovanja

Nadzor nad izvajanjem postopkov in ukrepov za zavarovanje osebnih podatkov, določenih s tem pravilnikom, izvaja direktor ali oseba, ki jo je pooblastil.

32. člen
Odgovornost za kršitev

1) Zaposleni v občini so za kršitev določil tega pravilnika odgovorni disciplinsko, druge osebe, ki sodelujejo pri obdelavi osebnih podatkov, pa na temelju pogodbenih obveznosti.
2) Odgovornost iz prejšnjega odstavka ne izključuje prekrškovne, kazenske ali odškodninske odgovornosti.

VIII. KONČNA DOLOČBA

33. člen
Začetek veljavnosti

Ta pravilnik začne veljati 15. dan po objavi na oglasni deski in spletni strani občine.

Številka: 071-2/2009-1
V Žužemberku, dne 06.04.2009

ŽUPAN
Franc ŠKUFCA l.r.