

Na podlagi Zakona o varstvu osebnih podatkov (Uradni list RS, št. 163/22; v nadaljevanju: ZVOP-2) in 32. člena Splošne uredbe (EU) 2016/679 Evropskega parlamenta in Sveta z dne 27. aprila 2016 o varstvu posameznikov pri obdelavi osebnih podatkov in o prostem pretoku takih podatkov ter o razveljavitvi Direktive 95/46/ESM v nadaljevanju: Splošna uredba) je župan Občine Ormož, sprejel naslednji

PRAVILNIK

o postopkih in ukrepih za varnost osebnih podatkov

I. SPLOŠNE DOLOČBE

Vsebina in namen pravilnika

1. člen

S Pravilnikom o postopkih in ukrepih za varnost osebnih podatkov (v nadaljevanju: pravilnik) se določajo organizacijski in tehnični ukrepi za varnost osebnih podatkov pri upravljavcu. Ukrepi se uvajajo z namenom zagotavljanja skladnosti delovanja upravljavca s predpisi s področja varstva osebnih podatkov v vseh fazah obdelave osebnih podatkov, s ciljem da se prepreči slučajno ali namerno nepooblaščen uničevanje podatkov, njihova sprememba, izguba ali nepooblaščen obdelava osebnih podatkov.

Poleg tega pravilnika se pri obdelavi osebnih podatkov uporabljajo določbe Zakona o varstvu osebnih podatkov in Splošne uredbe (v nadaljevanju: predpisi s področja varstva osebnih podatkov), in sicer v vseh primerih, ki niso neposredno urejeni v tem pravilniku.

V tem pravilniku uporabljeni izrazi, ki se nanašajo na osebe in so zapisani v moški slovnični obliki, so uporabljeni kot nevtralni za moški in ženski spol.

Definicija pojmov

2. člen

V tem pravilniku uporabljeni pojmi so povzeti po 4. členu Splošne uredbe in 5. členu ZVOP-2, z namenom, da so vse, za upravljavca pomembne definicije pojmov, zbrane na enem mestu.

Definicije pojmov so mestoma poenostavljene in z namenom lažjega razumevanja podkrepljene s praktičnimi primeri, vendar pojmi v dvomu ohranjajo enak pomen kot ga določajo predpisi s področja varstva osebnih podatkov.

Ta pravilnik opredeljuje tudi nekaj pojmov, ki niso vključeni v predpise s področja varstva osebnih podatkov. V tem pravilniku so opredeljeni zaradi preglednosti in lažjega razumevanja vsebine npr. javni uslužbenec, javna oseba, skrbnik informacijskega sistema.

Splošni pojmi:

1. Osebni podatek – vsak podatek o posamezniku ne glede na obliko v kateri je izražen ter pomeni informacijo na podlagi katere je lahko posameznik določen ali določljiv. Določljiv posameznik je tisti, ki ga je mogoče neposredno ali posredno določiti, z navedbo identifikatorja, kot je ime, identifikacijska številka, podatek o lokaciji, spletni identifikator, ali z navedbo enega ali več dejavnikov, ki so značilni za fizično, fiziološko, genetsko, duševno, gospodarsko, kulturno ali družbeno identiteto tega posameznika;
2. Obdelava osebnih podatkov – pomeni vsako dejanje, ki se izvaja v zvezi z osebnimi podatki z avtomatiziranimi sredstvi (npr. obdelavo izvaja algoritem na podlagi vnesenih podatkov s strani posameznika) ali brez njih (npr. ročna obdelava). Kot obdelava se šteje 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 osebnih podatkov;
3. Zbirka osebnih podatkov – pomeni vsak strukturiran niz osebnih podatkov, ki je lahko centraliziran (npr. osebni podatki so hranjeni na enem mestu), decentraliziran (npr. osebni podatki so hranjeni na več mestih v enaki obliki) ali razpršen (npr. osebni podatki so hranjeni na različnih mestih delno v e-obliki in delno fizično v fasciklu ali celo pri različnih upravljavcih);
4. Povezovanje zbirk - je avtomatsko in elektronsko povezovanje zbirk, ki jih upravljajo upravljavci za različne namene ali po različnih pravnih podlagah, in sicer tako, da se določeni osebni podatki samodejno prenesejo ali vključijo v drugo povezano zbirko ali več povezanih zbirk, tudi če se izvaja le enosmeren pretok osebnih podatkov; zbirke so povezane, če se določeni osebni podatki iz ene zbirke neposredno vključijo v drugo zbirko in se tako druga zbirka poveča ali posodobi ali pa se osebni podatki v njej zaradi točnosti spremenijo;
5. Evidenca dejavnosti obdelave – je popis zbirk osebnih podatkov.

Fizične ali pravne osebe, ki obdelujejo osebne podatke oziroma so drugače povezane z obdelavo:

1. Posameznik – v smislu tega pravilnika je to oseba na katero se nanašajo osebni podatki;
2. Upravljavec osebnih podatkov – je fizična ali pravna oseba javnega ali zasebnega sektorja, ki sama ali skupaj z drugimi (npr. skupnimi upravljavci – npr. skupna občinska uprava in občina) določa namene in sredstva obdelave. V smislu tega pravilnika je upravljavec občina, ki na podlagi zakona, pisne privolitve posameznika, pogodbene obveznosti ali zaradi izvajanja javnih nalog oz. javnega interesa obdeluje osebne podatke;
3. Uporabnik osebnih podatkov – je fizična ali pravna oseba javnega ali zasebnega sektorja, ki se ji posredujejo ali razkrijejo osebni podatki.

Uporabniki je širok pojem, ki vključuje:

- tiste, ki delujejo pod neposrednim vodstvom upravljavca,
 - obdelovalce, ki osebne podatke obdelujejo v imenu upravljavca in po njegovih navodilih, kot npr. računovodski servis, ponudnik storitev informacijske podpore,
 - skupne upravljavce, ki skupaj določijo sredstva in namene obdelave osebnih podatkov npr. razmerje skupna občinska uprava in občina.
 - tretje osebe, ki nastopajo kot samostojni upravljavci osebnih podatkov, kot na primer ZZS, FURS, banke itd.;
4. Obdelovalec – pomeni fizično ali pravno osebo javnega ali zasebnega sektorja, ki obdeluje osebne podatke v imenu in navodilih upravljavca osebnih podatkov npr. zunanji vzdrževalec informacijskega sistema, zunanji računovodski servis;

5. Tretja oseba – je fizična ali pravna oseba javnega ali zasebnega sektorja, ki sme dostopati do osebnih podatkov zaradi zakonske ali pogodbene obveznosti. O tretji osebi običajno govorimo, ko gre za dejavnosti, ki jih upravljavec sam niti ne bi mogel izvesti in mora to storitev prepustiti drugemu izvajalcu. Tipični primeri tretjih oseb: medicina dela, ki prejme podatke o napotnem delavcu na zdravstveni pregled; banka ponudnika, ki obdela podatke o transakciji in se seznani tudi s podatki posameznika, ki je kupil blago ali storitev, kljub temu da ni njen komitent; odvetniška družba, ki v imenu stranke vodi pravni postopek;
6. Pooblaščen oseba za varstvo osebnih podatkov (DPO) – je oseba, ki je pooblaščen za opravljane nalog skladno z 39. členom Splošne uredbe in 48. členom ZVOP-2;
7. Skrbnik zbirke - je javni uslužbenec, ki je odgovoren za vzpostavitev, vodenje, vzdrževanje in hranjenje zbirke ter za zakonito in varno obdelavo osebnih podatkov v zbirki;
8. Javni uslužbenec – je oseba, ki ima z delodajalcem (upravljavcem) sklenjeno pogodbo o zaposlitvi in v okviru svojega dela obdeluje osebne podatke. Naloge obdelave osebnih podatkov lahko izhajajo že iz opisa delovnega mesta v sistemizaciji delovnih mest ali pa so javnem uslužbencu dodeljene s posebnim pooblastilom;
9. Druga oseba – je oseba, ki opravlja naloge obdelave osebnih podatkov na podlagi drugega pravnega razmerja npr. na podlagi pogodbe civilnega prava ali štipendiranja, opravljanja obvezne prakse;
10. Skrbnik informacijskega sistema – je oseba, ki je zadolžena za zagotavljanje nemotenega dela strojne in programske opreme in pomoč javnim uslužbencem in drugim osebam. Skrbnik informacijskih sistemov opravlja naslednja ključna dela: pripravlja ustrezna strojna in programska orodja, zagotavlja delovanje strojne in programske informacijske opreme, izvaja varnostne ukrepe na področju informacijskih sistemov, izvaja politiko gesel, zagotavlja nemoteno delovanje in vzdržuje informacijsko opremo ipd.
11. Upravičenec – je oseba, ki se lahko seznani z osebnimi podatki. Upravičenec je lahko posameznik na katerega se nanašajo osebni podatki ali pa stranka v postopku, ki lahko dokaže, da ima pravni interes, za seznanitev z osebnimi podatki.

Drugi pojmi:

12. Varovani prostori – so prostori v katerih se nahajajo nosilci podatkov (fizični in elektronski) ter sredstva računalniškega informacijskega sistema;
13. Računalniški informacijski sistem – vse elektronske naprave, ki so namenjene obdelavi, prenosu in hrambi podatkov;
14. Nosilci podatkov – so vse vrste sredstev, na katerih so zapisani ali posneti podatki (listine, akti, gradiva, spisi, računalniška oprema vključno z magnetnimi, optičnimi ali drugimi računalniškimi mediji, fotokopije, zvočno in slikovno gradivo, mikrofili, naprave za prenos podatkov, ipd.);

II. TEMELJI OBDELAVE OSEBNIH PODATKOV

Pred obdelavo osebnih podatkov

3. člen

Javni uslužbenci in druge osebe morajo biti preden nastopijo na delo v okviru katerega obdelujejo osebne podatke in začnejo obdelovati osebne podatke seznanjene z vsebino tega pravilnika. Poleg tega morajo podpisati tudi izjavo o varovanju osebnih podatkov skladno s 36. členom tega pravilnika.

Načela obdelave osebnih podatkov

4. člen

Upravljavec osebnih podatkov je skladno s predpisi s področja varstva osebnih podatkov dolžan zagotoviti, da so podatki skladno s predpisi s področja varstva osebnih podatkov:

- obdelani zakonito, pošteno in na pregleden način (načelo zakonitosti, pravičnosti in preglednosti),
- zbrani za določene, izrecne in zakonite namene ter se ne obdelujejo na načine, ki niso združljivi s temi nameni (načelo omejitve namena),
- ki se obdelujejo ustrezni, relevantni in omejeni na to, kar je potrebno za namene, za katere se obdelujejo (načelo najmanjšega obsega podatkov),
- točni in, kadar je potrebno, posodobljeni (načelo točnosti),
- hranjeni v obliki, ki dopušča identifikacijo posameznikov le toliko časa, kolikor je potrebno za namene, za katere se osebni podatki obdelujejo (načelo omejitve shranjevanja),
- obdelujejo na način, ki zagotavlja ustrezno varnost osebnih podatkov (načelo celovitosti in zaupnosti).

Javni uslužbenci so dolžni v vseh fazah obdelave osebnih podatkov spoštovati navodila upravljavca in pooblaščen osebe za varstvo osebnih potekov ter skrbeti, da obdelava osebnih podatkov poteka skladno s tem pravilnikom in zakonodajo s področja varstva osebnih podatkov. V kolikor tekom procesa obdelave osebnih podatkov ugotovijo, da bi lahko bilo kršeno katero izmed temeljnih načel, morajo o tem nemudoma obvestiti pooblaščen osebo za varstvo osebnih podatkov.

Pravna podlaga za obdelavo osebnih podatkov

5. člen

Temelj načela zakonitosti je ustrezna izbira pravne podlage za obdelavo osebnih podatkov. Upravljavec mora že pred začetkom obdelave osebnih podatkov skrbno izbrati in določiti pravno podlago za obdelavo podatkov. Predvsem v primeru dvoma o izbiri pravilne pravne podlage, je priporočljivo, da se izbira pravne podlage dokumentira.

Upravljavec obdeluje osebne podatke samo v primeru, če lahko obdelavo utemelji in izpolni pogoje ene od pravnih podlag, ki jih določa 6. člen Splošne uredbe in 6. člen ZVOP-2. Upravljavec lahko utemelji obdelavo osebnih podatkov na podlagi:

- a) Privolitve posameznika: posameznik je podal nedvoumno privolitev za obdelavo osebnih podatkov za določen namen (npr. posameznik se je prijavil na prejemanje novic občine);

- b) Pogodbe: obdelava je potrebna za izvajanje pogodbe, katere pogodbeni stranka je posameznik, na katerega se nanašajo osebni podatki ali pa je obdelava potrebna za izvedbo pripravljanih ukrepov, da se lahko pogodba sklene (npr. pogodba o najemu občinskega stanovanja);
- c) Zakonske obveznosti: obdelava je potrebna za izpolnjevanje upravljavčeve obveznosti, ki jo določa zakon (npr. delodajalec mora za namen izpolnjevanja obveznosti iz delovnega razmerja obdelovati osebne podatke javnega uslužbenca);
- d) Zaščite življenjskih interesov: obdelava je zakonita, če je potrebna za zaščito interesa, ki je bistven za življenje posameznika, na katerega se nanašajo osebni podatki, ali druge fizične osebe (npr. nujna civilna zaščita);
- e) Javnega interesa ali izvajanja javne oblasti: obdelava je potrebna za opravljanje naloge v javnem interesu ali pri izvajanju javne oblasti, dodeljene upravljavcu (npr. izvajanje nalog lokalne samouprave, odločanje o vlogah posameznikov, priprava razpisov ipd.);

Če obdelave osebnih podatkov ni možno umestiti pod nobeno od določenih pravnih podlag, je potrebno o tem obvestiti pooblaščen osebo za varstvo osebnih podatkov, ki upravljavcu oz. javnemu uslužbencu pomaga pri presoji in iskanju rešitev pri izbiri pravne podlage. Pooblaščen osebo za varstvo osebnih podatkov je potrebno obvestiti tudi v primeru, če obdelava osebnih podatkov že poteka in javni uslužbenec ali druga oseba ugotovi, da izbira pravne podlage ni bila pravilna ali ne obstaja. V tem primeru je potrebno prenehati z aktivno obdelavo ter počakati na navodila pooblaščen osebe.

III. OBDELAVA IN ZBIRKE OSEBNIH PODATKOV

Namen obdelave osebnih podatkov

6. člen

Namen obdelave osebnih podatkov se mora določiti že pred začetkom obdelave osebnih podatkov.

Obdelava osebnih podatkov za druge namene, kot tiste, za katere so bili osebni podatki prvotno zbrani, je dovoljena le, kadar je združljiva s prvotnimi nameni.

Združljivost namenov mora javni uslužbenec, ki je skrbnik zbirke osebnih podatkov, oceniti pred obdelavo podatkov, in sicer za vsak nov namen posebej. Pri tem mu lahko pomaga pooblaščen oseba za varstvo osebnih podatkov. Pri ocenjevanju mora upoštevati:

- ali obstaja kakšna povezava med prvotnim in novim namenom obdelave;
- okoliščine, v katerih so bili osebni podatki zbrani (razumna pričakovanja posameznika glede na razmerje med posameznikom in upravljavcem);
- naravo osebnih podatkov (ali gre za obdelavo posebne vrste osebnih podatkov);
- morebitne posledice, ki ga bo imela nadaljnja obdelava za posameznike, katerih osebni podatki se obdelujejo;
- ali obstajajo ustrezni zaščitni ukrepi - npr. šifriranje ali psevdonimizacija ter
- druge okoliščine, ki so odvisne od vsakega posameznega primera obdelave osebnih podatkov.

Če skrbnik zbirke ugotovi, da je nov namen združljiv s prvotnim namenom, se lahko zanj uporabi enaka pravna podlaga, kot tista, na podlagi katere so bili osebni podatki zbrani. Če pa skrbnik zbirke po preučitvi zgoraj zapisanih okoliščin ugotovi, da se nov namen razlikuje od prvotnega namena ter se s tem ne šteje za združljivega s prvotnim namenom, se mora o tem posvetovati s pooblaščen osebo za varstvo osebnih podatkov.

Posredovanje osebnih podatkov

7. člen

Za posredovanje osebnih podatkov se uporabljajo določila tega pravilnika in predpisi s področja varstva osebnih podatkov.

Javni uslužbenec lahko posreduje osebne podatke drugim osebam javnega sektorja ali drugim fizičnim ali pravnim osebam, če je za posredovanje dana pravna podlaga iz 5. člena tega pravilnika ter na podlagi zahteve iz prvega odstavka 41. člena ZVOP-2, razen če drug zakon določa drugače. Prejemnik podatkov sme osebne podatke obdelovati samo za namen, za uresničevanje katerega se mu posredujejo.

Javni uslužbenec sme z dovoljenjem direktorja občinske uprave posredovati osebne podatke na podlagi pisne vloge vlagatelja, v kateri mora biti jasno navedena določba zakona, ki predstavlja pravno podlago za pridobitev osebnih podatkov in izkazani drugi pogoji, skladno s katerimi je dopustno posredovanje na podlagi predpisov s področja varstva osebnih podatkov.

Pred posredovanjem osebnih podatkov je potrebno preveriti identiteto prejemnika osebnih podatkov, z vpogledom v njegov osebni dokument, ki nedvoumno izkazuje njegovo istovetnost, ga opozoriti na dolžnost varovanja osebnih podatkov in obveznost, da lahko pridobljene osebne podatke obdeluje izključno za namen, za uresničevanje katerega so se mu posredovali.

Osebni podatki, ki se posredujejo v fizični obliki, morajo biti posredovani v skladu z določbami predpisov, ki urejajo upravno poslovanje z dokumentarnim gradivom, oziroma 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.

Osebne podatke je dovoljeno posredovati z informacijskimi, komunikacijskimi in drugimi sredstvi le ob izvajanju postopkov in ukrepov, ki nepooblaščenim osebam preprečujejo prilaščanje ali uničenje podatkov ter neupravičeno seznanjanje z njihovo vsebino (npr. prenos osebnih podatkov po elektronski pošti mora biti varovan z geslom za identifikacijo, priporočena pošiljka naslovniku).

Dokument, ki vsebuje osebne podatke se posreduje v obliki fotokopije originala. V originalu se dokument, ki vsebuje osebne podatke posreduje le izjemoma, če tako določa zakon ali drug predpis (npr. v primeru pisne odredbe sodišča). Posredovani originalni dokument mora biti v času odsotnosti nadomeščen s fizično (fotokopijo) ali elektronsko (skenirano) kopijo. Kopija se ob vrnitvi izvirnika dokumenta uniči oziroma izbriše skladno s 39. členom tega pravilnika.

Postopek posredovanja osebnih podatkov

8. člen

Upravljavec vlagatelju zahteve osebne podatke posreduje najpozneje v 15 dneh od prejema popolne zahteve, če zakon ne določa drugače ali pa ga v tem roku pisno obvesti o razlogih, zaradi katerih mu zahtevanih osebnih podatkov ne bo posredoval. Upravljavec in vlagatelj zahteve se v roku iz prejšnjega stavka lahko dogovorita za njegovo podaljšanje.

Če upravljavec ne ravna v skladu s prejšnjim odstavkom, se šteje, da je zahteva zavrnjena. Če je zahteva za posredovanje osebnih podatkov delno ali v celoti zavrnjena, lahko vlagatelj zahteve v primeru, ko se zahteva nanaša na posredovanje osebnih podatkov iz uradnih evidenc ali javnih knjig, zahteva, da o njegovi vlogi najprej odloči nadzorni organ (v nadaljevanju: Informacijski pooblaščenec). Kadar ta zavrne zahtevo ali kadar na prvi stopnji odloča Informacijski pooblaščenec sam, lahko vlagatelj zahteva sodno varstvo, o katerem odloča pristojno sodišče v skladu z zakonom, ki ureja upravni spor. V primeru zavrnitve zahteve za posredovanje osebnih podatkov iz zbirk, ki niso uradne evidence ali javne knjige, lahko vlagatelj zahteva sodno varstvo, o katerem odloča sodišče s splošno pristojnostjo v skladu z zakonom, ki ureja nepravdni postopek.

Ta člen se ne uporablja, če fizična ali pravna oseba ali oseba javnega sektorja uveljavlja pravico do pregleda in prepisa spisa iz sodnih, upravnih ali drugih spisov v skladu z drugim zakonom.

Sledljivost posredovanj

9. člen

Upravljavec osebnih podatkov za vsako posredovanje osebnih podatkov zagotovi, da je mogoče pozneje ugotoviti sledljivost opravljenih posredovanj.

Za vsako posredovanje osebnih podatkov mora upravljavec voditi evidenco ali narediti uradni zaznamek, v katerem je opredeljeno:

- kateri osebni podatki so bili posredovani,
- osebno ime/firmo in naslov oz. sedež osebe, ki so ji bili posredovani osebni podatki, z dodano opombo ali je bilo posredovanje opravljeno po uradni dolžnosti,
- datum in ura posredovanja osebnih podatkov ter
- pravna podlaga, na kateri so bili posredovani osebni podatki
- namen oziroma iz katerih razlogov oziroma za potrebe katerega postopka so bili osebni podatki posredovani,

razen če drug zakon za posredovanje posameznih vrst podatkov določa drugače oziroma je to razvidno iz dnevnika obdelave po 22. členu ZVOP-2.

Evidentirani podatki iz prejšnjega odstavka se v pisni ali elektronski obliki vodijo kot del podatkov zadeve o kateri se vodi postopek. Oblika uradnega zaznamka je odvisna od nosilca podatkov, ki vsebuje posredovani osebni podatek (spis, informacijski sistem za podporo pisarniškemu poslovanju).

Če osebni podatek, ki se posreduje, ni del podatkov zadeve o kateri se vodi postopek, se evidentiranje opravi neposredno v zbirko osebnih podatkov, katere del so posredovani osebni podatki.

Evidentiranje na podlagi tega člena naredi skrbnik zbirke osebnih podatkov ali javni uslužbenec, ki je osebne podatke posredoval. Podatke iz evidence mora upravljavec hraniti dve leti, razen če zakon za posredovanje posameznih vrst podatkov določa drugačen rok.

Pregledovanje, prepisovanje in kopiranje osebnih podatkov s strani strank oziroma upravičencev

10. člen

Za pregledovanje, prepisovanje in kopiranje dokumentov, ki vsebujejo osebne podatke, se uporabljajo določbe predpisov, ki urejajo splošni upravni postopek in upravno poslovanje z dokumentarnim gradivom.

Če želi stranka pregledati, prepisati ali kopirati dokument, ki vsebuje osebne podatke, je potrebno preveriti njeno identiteto z vpogledom v njegov osebni dokument, ki nedvoumno izkazuje njegovo istovetnost. Oseba mora biti zmožna kot verjetno izkazati, da ima od pregledovanja, prepisovanja in preslikovanja pravni interes (v nadaljevanju: upravičenec).

Pri vsakem posameznem pregledovanju, prepisovanju in kopiranju dokumentov po tem členu, ki vsebujejo osebne podatke, se naredi uradni zaznamek, ki se vloži v spis. Iz uradnega zaznamka, ki ga mora podpisati tudi stranka oziroma upravičenec, mora biti razvidna številka spisa, datum in ura pregleda, vrsta dokumenta, katerega kopija se je posredovala upravičencu, osebno ime stranke oziroma upravičenca, njegov naslov, številka in vrsta dokumenta, iz katerega je ugotovljena identiteta ter namen, zaradi katerega je bil opravljen pregled, prepis oziroma kopiranje dokumenta.

Stranko oziroma upravičenca je pred pregledom, prepisovanjem in kopiranjem dokumentov, ki vsebujejo osebne podatke, potrebno opozoriti na dolžnost varovanja takšnih podatkov. Opozorilo mora biti sestavni del uradnega zaznamka iz prejšnjega odstavka.

IV. ZBIRKE OSEBNIH PODATKOV IN EVIDENCA DEJAVNOSTI OBDELAVE

Vzpostavitev zbirke

11. člen

Skrbnik zbirke ob vzpostavitvi zbirke izpolni evidenco dejavnosti obdelave v skladu s 14. členom tega pravilnika, ki jo predloži v pregled direktorju občinske uprave in pooblaščenim osebam za varstvo podatkov.

Skrbnik zbirke je odgovoren zlasti za:

- opredelitev namena obdelave osebnih podatkov in določitev vrst osebnih podatkov, ki se bodo zbirali in drugače obdelovali;
- spoštovanje načel varstva osebnih podatkov, vključno z določitvijo pravne podlage za obdelavo osebnih podatkov in določitvijo roka obdelave osebnih podatkov;
- pridobitev predhodnega mnenja pooblaščenih oseb za varstvo osebnih podatkov v primeru nadaljnje obdelave osebnih podatkov, zagotovitev informacije posamezniku o tem drugem namenu in po potrebi za pridobitev privolitve posameznika za nadaljnjo obdelavo;

- zbiranje najmanjšega možnega obsega osebnih podatkov, ki jih upravljavec potrebuje za uresničitev namena obdelave;
- obdelavo zahtevkov in uveljavljanja pravic posameznika v povezavi z zbirko, za katero skrbi;
- ustrezen izbris osebnih podatkov v zbirki po poteku roka hrambe;
- učinkovito in skladno obravnavo kršitev varnosti osebnih podatkov);
- letni pregled in posodabljanje opisov zbirke v evidenci dejavnosti obdelave;
- obveščanje pooblaščenih oseb za varstvo osebnih podatkov o kršitvah varnosti osebnih podatkov, morebitnih težavah pri obdelavi osebnih podatkov in drugih pomembnih vprašanjih v zvezi z osebnimi podatki.

Zbirke osebnih podatkov

12. člen

V zbirki se lahko obdelujejo le tisti osebni podatki, ki imajo ustrezno pravno podlago v skladu s 5. členom tega pravilnika, po določbah Splošne uredbe, ZVOP-2 ali drugega predpisa.

Zbirke, ki nastanejo na podlagi privolitve posameznikov se morajo voditi v ločeni zbirki.

Povezovanje zbirk

13. člen

Zbirke iz uradnih evidenc in javnih knjig je dovoljeno povezovati le pod pogoji iz 87. člena ZVOP-2.

Evidenca dejavnosti obdelave

14. člen

Evidenca dejavnosti obdelave, ki je v elektronski in pisni obliki, vsebuje informacije iz 30. člena Splošne uredbe.

Evidenco dejavnosti obdelave vzpostavi, ureja in posodablja skrbnik zbirke, ki mora o vsaki novi evidenci ali spremembi obstoječe evidence, slednjo predložiti v pregled pooblaščenim osebam za varstvo podatkov.

Vsak javni uslužbenec, ki obdeluje osebne podatke iz določene zbirke osebnih podatkov, mora biti seznanjen z evidenco dejavnosti obdelave.

Upravljavec lahko z namenom zagotavljanja transparentnosti obdelave osebnih podatkov vodi seznam, iz katerega je za vsako zbirko jasno razvidno, katera oseba je odgovorna za posamezno zbirko (skrbnik zbirke) ter katere osebe lahko zaradi narave svojega dela obdelujejo osebne podatke, ki se nanašajo na posamezno zbirko.

Ocena učinkov na varstvo osebnih podatkov

15. člen

Upravljavec je dolžan skladno s 35. členom Splošne uredbe pred obdelavo osebnih podatkov opraviti pisno oceno učinka predvidenih dejanj obdelave, v primeru ko obstaja verjetnost, 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. V eni oceni je lahko obravnavan niz podobnih dejanj obdelave, ki predstavljajo podobno stopnjo tveganja.

Pri izvedbi ocene učinka se mora zaprositi za mnenje pooblaščen osebo za varstvo osebnih podatkov in sicer zlasti glede vprašanja ali je ocena učinkov v zvezi z varstvom podatkov potrebna, katero metodologija naj se uporabi pri izvajanju ocene učinka v zvezi z varstvom podatkov, ali naj oceno učinka v zvezi z varstvom podatkov izvede interno ali naj jo odda v zunanje izvajanje, katere zaščitne ukrepe naj se uporabi za zmanjševanje morebitnih tveganj za pravice in interese posameznikov, na katere se nanašajo osebni podatki, in ali je bila ocena učinka v zvezi z varstvom podatkov pravilno izvedena in ali so njene ugotovitve (ali naj se obdelava nadaljuje ali ne in kateri zaščitni ukrepi naj se uporabijo) v skladu s Splošno uredbo. Če se upravljavec s pridobljenim mnenjem pooblaščen osebe za varstvo podatkov ne strinja, je dolžan v dokumentaciji ocene učinka posebej pisno utemeljiti, zakaj mnenja ni upošteval.

Informacijskega pooblaščenca se mora zaprositi za mnenje v skladu z 36. členom Splošne uredbe o varstvu podatkov, kadar iz ocene učinka izhaja, da bi obdelava povzročila veliko tveganje, če upravljavec ne bi sprejel ukrepov za ublažitev tveganja.

Če je obdelava potrebna za izpolnitev zakonske obveznosti ali za opravljanje nalog v javnem interesu ali pri izvajanju javne oblasti upravljavca in je bila ocena učinka že izvedena v okviru splošne ocene učinkov med sprejemanjem te pravne podlage, se ocene učinka ne opravi, razen če zakon določa drugače.

V. VAROVANJE OSEBNIH PODATKOV

Varovanje osebnih podatkov

16. člen

Naloga upravljavca osebnih podatkov je varovanje osebnih podatkov, ki jih obdeluje. V ta namen mora sprejeti določene tehnične oz. organizacijske ukrepe za zavarovanje teh podatkov skladno s 24., 25. in 32. členom Splošne uredbe, s katerimi se preprečuje slučajno ali namerno nepooblaščen uničevanje podatkov, njihova sprememba, izguba ali kakršnakoli nepooblaščen obdelava.

Z obdelavo se mora zagotavljati celovitost, zaupnost in dostopnost osebnih podatkov.

Celovitost osebnih podatkov

17. člen

Celovitost osebnih podatkov pomeni zagotavljanje nesprejemljivosti in točnosti podatkov. To pomeni, da mora upravljavec zagotoviti, da osebnih podatkov ni mogoče nepooblaščen spreminjati.

Celovitost se zagotavlja z uporabo sistemov in aplikativne programske opreme, ki onemogoča spreminjanje zajetih podatkov ter z različnimi ukrepi kot so uporaba uporabniških imen in gesel, elektronskega podpisa itd.

Celovitost podatkov se zagotavlja tudi s fizičnim varovanjem prostorov, nosilcev osebnih podatkov, sistemske in aplikativne programske opreme.

Organizacijsko se celovitost podatkov zagotavlja s tem, da imajo dostop do posameznega podatka, v obsegu dodeljenih uporabniških pravic, le javni uslužbenci in druge osebe, ki jih veže dolžnost varovanja osebnih podatkov skladno s 36. členom tega pravilnika.

Zaupnost osebnih podatkov

18. člen

Zaupnost osebnih podatkov pomeni njihovo nerazkrivanje nepooblaščenim fizičnim in pravnim osebam javnega in zasebnega sektorja.

Zaupnost podatkov se zagotavlja s fizičnim varovanjem prostorov, sistemske in aplikativne programske opreme ter podatkovnih nosilcev. Podobno kot pri integriteti, se tudi zaupnost podatkov zagotavlja z uporabo uporabniških imen in gesel na ravni sistemske in aplikativne programske opreme, s katero se obdelujejo podatki. Podatki so lahko kodirani ali šifrirani ali pa mora sistem za upravljanje s podatki na drug način zagotavljati, da do njih ne morejo dostopati nepooblaščene osebe.

Organizacijsko se zaupnost podatkov zagotavlja tudi z aktom o sistemizaciji delovnih mest, kjer se za vsako delovno mesto opredelijo pravice in pooblastila za obdelavo osebnih podatkov. V kolikor akt o sistemizaciji delovnih mest tega ne ureja ali če oseba, ki obdeluje osebne podatke ni v delovnem razmerju pri upravljavcu, se lahko posamezniku podeli pooblastilo za obdelavo osebnih podatkov. Javni uslužbenci in druge osebe, pred začetkom obdelave osebnih podatkov podpišejo posebno izjavo, kot to določa 36. člen tega pravilnika.

Dostopnost osebnih podatkov

19. člen

Dostopnost osebnih podatkov pomeni, da so podatki na voljo vedno, ko jih potrebuje upravljavec oziroma oseba, ki obdeluje osebne podatke.

Dostopnost podatkov se zagotavlja z ukrepi, ki omogočajo neprekinjen in trajen dostop do podatkov, vse do njihovega izbrisa kot je določeno v nadaljevanju tega pravilnika. Za zagotovitev neprekinjenega in trajnega dostopa do podatkov se izvajajo naslednji ukrepi: izdelava varnostnih kopij podatkov (back-up), arhiviranje podatkov, vzporedne evidence, izdelava izvedenih evidenc itd.

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

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

a) VAROVANI PROSTORI

Varovani prostori

20. člen

Prostori, v katerih se nahajajo nosilci osebnih podatkov in strojna ter programska oprema, ki omogoča dostop do teh podatkov, morajo biti varovani z organizacijskimi in tehničnimi ukrepi, ki onemogočajo nepooblaščenim osebam dostop do podatkov.

Dostop do varovanih prostorov

21. člen

Dostop v varovane prostore je dovoljen le tistim javnim uslužbencem ali drugim osebam, ki pri upravljavcu obdelujejo osebne podatke, katerih pravica do vstopa v posamezni prostor izhaja opisa delovnih nalog, pogodbe ali pooblastila direktorja občinske uprave.

Dostop do varovanih prostorov je mogoč le v rednem delovnem času, izven delovnega časa pa samo na podlagi dovoljenja direktorja občinske uprave.

Dostop nepooblaščenih oseb do varovanih prostorov

22. člen

Vstop v varovane prostore upravljavca je pod pogoji, določenimi v tem členu, dovoljen tudi osebam, ki niso javni uslužbenci in druge osebe, ki pri upravljavcu obdelujejo osebne podatke.

Nepooblaščene osebe v varovane prostore upravljavca osebnih podatkov ne smejo vstopati ali se zadrževati brez prisotnosti javnega uslužbenca ali druge osebe, ki v prostoru opravlja delo.

Vstop v varovane prostore upravljavca osebnih podatkov je izjemoma poleg javnih uslužbencev in drugih oseb, ki pri upravljavcu obdelujejo osebne podatke, dovoljen tistim pogodbenim obdelovalcem (npr. vzdrževalcem prostorov, strojne in programske opreme), ki imajo z upravljavcem sklenjene pogodbe o obdelavi osebnih podatkov, skladno s 40. členom tega pravilnika.

Varovanje varovanih prostorov

23. člen

Prostori, ki so namenjeni poslovanju s strankami, morajo biti urejeni tako, da nepooblaščenim osebam ni omogočen vpogled v osebne podatke v času obdelave ali dela na njih. Vpogled v podatke, se lahko omogoči le posamezniku na katerega se nanašajo osebni podatki, ki se obdelujejo in ima le-ta pravico do vpogleda v svoje lastne osebne podatke.

Javni uslužbenec ali druga oseba mora vestno in skrbno nadzorovati varovani prostor in ob koncu delovnega časa zakleniti pisarno v kateri opravlja delo.

Javni uslužbenec ali druga oseba, ki zadnja zapusti prostore upravljavca, mora preveriti ali so vsi varovani prostori zaklenjeni in če so zaprta okna v prostorih. V kolikor je pri upravljavcu nameščen alarmni sistem, se mora ob koncu delovnega časa, vklopiti.

Varovani prostori ne smejo ostajati nenadzorovani, oziroma se morajo redno zaklepati v času odsotnosti javnih uslužbencev ali drugih oseb, ki jih nadzorujejo (npr. če med delovnim časom zapusti prostor npr. za čas malice, sestanka). Ključi se ne smejo nikoli puščati v ključavnici vrat pisarne.

b) NOSILCI OSEBNIH PODATKOV

Varovanje nosilcev osebnih podatkov

24. člen

Javni uslužbenci ali druge osebe, ki pri upravljavcu obdelujejo osebne podatke, ne smejo puščati nosilcev osebnih podatkov na vidnem mestu (npr. na mizah, omarah) v prisotnosti oseb, ki nimajo pravice do vpogleda vanje.

Nosilce osebnih podatkov morajo javni uslužbenci ali druge osebe, ki pri upravljavcu obdeluje osebne podatke, varno shraniti ob koncu delovnega časa oziroma v vseh primerih, ko so dlje časa odsotni s prostora ter poskrbeti, da osebni podatki niso izpostavljeni nevarnosti vpogleda s strani nepooblaščenih oseb.

V kolikor javni uslužbenec ali druga oseba, ki pri upravljavcu obdeluje osebne podatke, ne more zakleniti pisarne (npr. vrata ne omogočajo zaklepanja ali si pisarno deli z drugim javnim uslužbencem ali drugo osebo), mora ob odsotnosti pospraviti nosilce osebnih podatkov v omaro, predalnik pisalne mize ali drugo pisarniško pohištvo ter pohištvo zakleniti. Računalniki in druga uporabniška programska oprema mora biti ugasnjena ali v mirovanju, na način da je ob njeni aktivaciji potrebno vnesti geslo.

Pisarniška oprema, ki se nahaja na hodnikih in drugih skupnih prostorih mora biti vedno zaklenjena, razen kadar je neposredno v uporabi. Ključe te opreme hrani javni uslužbenec ali druga oseba, ki pri upravljavcu obdeluje osebne podatke, ki se hranijo na hodnikih in drugih skupnih prostorih.

Nosilce podatkov, ki vsebujejo osebne podatke, lahko javni uslužbenec ali druga oseba, ki pri upravljavcu obdeluje osebne podatke, odnaša izven prostorov upravljavca le na podlagi predhodne poučitve glede varovanja nosilcev podatkov in dovoljenjem direktorja občinske uprave.

c) STROJNA IN PROGRAMSKA RAČUNALNIŠKA OPREMA

Varovanje strojne opreme

25. člen

Strojno opremo za obdelavo podatkov se uporablja v skladu s tehničnimi navodili izdelovalca opreme, določili tega pravilnika ter predpisi s področja varstva osebnih podatkov.

Strojna oprema se lahko nahaja in uporablja samo v prostorih in na način, ki ustreza predpisanim pogojem za uporabo te opreme.

S strojno opremo lahko upravljajo samo pooblaščen javni uslužbenci in druge osebe, ki pri upravljavcu obdelujejo osebne podatke.

Strežniki, na katerih se nahajajo podatki, morajo biti ustrezno organizacijsko in tehnično varovani.

Varovanje računalniške programske opreme - dostop

26. člen

Dostop do računalniške programske opreme, s katero se hranijo ali obdelujejo osebni podatki, mora biti varovan na način (npr. s sistemom gesel), ki omogoča dostop le pooblaščenim javnim uslužbencem in drugim osebam, ki pri upravljavcu obdelujejo osebne podatke, in samo v obsegu, ki je potreben za njihovo nemoteno opravljanje dela.

Za namen popravila računalniške programske opreme lahko imajo dostop tudi obdelovalci, pod pogoji določenimi v 40. členu tega pravilnika.

Delo na računalniški programski opremi

27. člen

Popravljanje, spreminjanje in dopolnjevanje sistemske in aplikativne programske opreme je dovoljeno samo na podlagi odobritve direktorja občinske uprave, izvajajo pa jo lahko samo pooblaščen javni uslužbenci ali obdelovalci, pod pogoji določenimi v 22. členu tega pravilnika.

Varovanje računalniške programske opreme – poseg

28. člen

Javni uslužbenec in druga oseba, ki pri upravljavcu obdeluje osebne podatke, pooblaščen za shranjevanje in obdelavo osebnih podatkov na računalniku, mora skrbeti, da v primeru servisiranja, popravila, spreminjanja ali dopolnjevanja sistemske ali aplikativne programske opreme ob morebitnem kopiranju osebnih podatkov, po prenehanju potrebe po kopiji, kopijo uničiti.

Javni uslužbenec in druga oseba, ki pri upravljavcu obdeluje osebne podatke in je pooblaščen za obdelavo in ravnanje z osebnimi podatki na računalniku, mora biti v času servisiranja računalnika in programske opreme ves čas prisotna in nadzirati, da ne pride do nedopustnega ravnanja z osebnimi podatki.

Za namen servisnega posega na daljavo se lahko skrbnik informacijskega sistema, le na zahtevo in potrditev javnega uslužbenca ali druge osebe, priklopi na njen računalnik (t.i. remote desktop).

V primeru izkazane potrebe po popravilu računalnika, na čigar disku se nahajajo osebni podatki, izven prostorov upravljavca in brez kontrole pooblaščenega javnega uslužbenca, se morajo podatki z diska računalnika izbrisati na način, ki onemogoča dostop do podatkov. Če tak izbris ni mogoč, se mora popravilo opraviti v prostorih upravljavca v prisotnosti pooblaščenega javnega uslužbenca. Popravilo računalnika lahko izvajajo samo obdelovalci, ki imajo z upravljavcem sklenjeno ustrezno pogodbo o obdelavi osebnih podatkov.

Ob predaji opreme v servis obdelovalcu, mora skrbnik informacijskega sistema in obdelovalec, ki sprejema opremo v popravilo, izpolniti predajni zapisnik. Izvajalci posega morajo spremembe in dopolnitve sistemske in aplikativne programske opreme ustrezno dokumentirati.

Varovanje računalniške programske opreme - gesla

29. člen

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

Vsakemu javnemu uslužbencu in drugi osebi, se s sistemom gesel priredi skupina pravic in pooblastil na računalniški programski opremi.

Dostop do računalniške programske opreme javnemu uslužbencu in drugim osebam, ki pri upravljavcu obdelujejo osebne podatke, omogoči oseba, ki je pri upravljavcu skrbnik informacijskega sistema. Oseba, ki ji je omogočen dostop mora ob prvi prijavi v sistem zamenjati v naprej generirano dostopno geslo ter ga periodično menjati skladno z navodili.

Javni uslužbenec in druga oseba, ki pri upravljavcu obdeluje osebne podatke je sama odgovorna za varnost svojega gesla in za vsak izveden postopek obdelave. Uporabljenega gesla se morajo generirati skladno z navodili upravljavca, ki določi tudi režim dodeljevanja in spreminjanja gesel.

Varovanje računalniške programske opreme – administrativna gesla

30. člen

Vsa gesla, ki se uporabljajo za vstop in za administriranje v mreži osebnih računalnikov, administriranje z elektronsko pošto in administriranje prek aplikativnih programov, se hranijo v zaprtih ovojnicah in jih varuje pred dostopom nepooblaščenih oseb (npr. v ognjevarni omari).

Administrativna gesla se smejo uporabiti samo v izjemnih in nujnih primerih. Vsaka uporaba takšnega gesla se dokumentira.

Po uporabi gesel iz zaprtih ovojnic skrbnik informacijskega sistema, določi nova gesla ter zagotovi, da se ta hranijo na zgoraj opisan način.

Varovanje računalniške programske opreme - varnost

31. člen

Vsebine diskov mrežnega strežnika in lokalnih delovnih postaj, na katerih so shranjeni osebni podatki, je treba zaščititi z ustreznimi protivirusnimi programi in jih redno preverjati.

Pred priključitvijo prenosnega računalnika oziroma drugih medijev, ki niso last upravljavca in so namenjeni uporabi v računalniškem informacijskem sistemu upravljavca, je treba preveriti glede prisotnosti računalniških virusov.

Ob pojavu računalniškega virusa se tega v čim krajšem možnem času odpravi s pomočjo skrbnika informacijskega sistema ali obdelovalca, obenem pa se ugotovi vzrok pojava virusa v računalniškem informacijskem sistemu.

Javni uslužbenci in druge osebe, ki pri upravljavcu obdelujejo osebne podatke, ne smejo inštalirati programske opreme brez vednosti skrbnika informacijskega sistema.

Javni uslužbenci in druge osebe, ki pri upravljavcu obdelujejo osebne podatke, ne smejo odnašati računalniške programske opreme iz prostorov upravljavca brez izrecne odobritve direktorja občinske uprave.

Tiskalniki in druge naprave za razmnoževanje dokumentov

32. člen

Javni uslužbenci in druge osebe, ki pri svojem delu obdelujejo osebne podatke, ki v okviru izvajanja svojih nalog, na napravah, ki jih uporablja večje število javnih uslužbencev ali drugih oseb, kopirajo ali drug tehnični način razmnožujejo ali tiskajo dokumente, ki vsebujejo osebne podatke, po končanem kopiranju ali tiskanju ne smejo puščati dokumentov v, na ali ob napravah.

d) UPORABA INFORMACIJSKIH TEHNOLOGIJ

Elektronska pošta in uporaba druge programske opreme na računalniku

33. člen

Elektronska pošta in računalnik se uporabljata v službene namene.

Ne glede na prejšnji odstavek se elektronska pošta in ostala programska oprema na računalniku lahko uporabljata v omejenem obsegu in razumnih mejah tudi v zasebne namene. V kolikor se pojavi sum, da elektronsko pošto in računalnik prekomerno uporablja v zasebne namene, lahko skrbnik informacijskega sistema, na utemeljeno pisno zahtevo župana ali direktorja občinske uprave opravi nadzor količine uporabe elektronske pošte, a zgolj z vidika obsega priponk, ki obremenjujejo strežnik. Pri čemer se ne sme pregledovati vsebine elektronske pošte.

Za zagotovitev varnosti in nemotenega delovanja lahko upravljavec omeji:

- največjo velikost elektronskih sporočil pri pošiljanju ali sprejemanju elektronskih sporočil skupaj s priponko,
- pošiljanje nekaterih vrst priponk, med katerimi so vse izvršljive datoteke in datoteke, ki jih ni mogoče preveriti s sistemi za odkrivanje računalniških virusov in
- spreminjanje nastavitev predala elektronske pošte.

V primeru prenehanja delovnega razmerja je dolžan javni uslužbenec v času odpovednega roka svojo zasebno pošto izbrisati in direktorju občinske uprave ali javnemu uslužbencu, ki bo prevzel njegovo

delo, predati vso pomembno elektronsko pošto, povezano z njegovim delom in obveznostmi, ki jih je še potrebno opraviti. Če javni uslužbenec tega ne stori in upravljavcu zaradi tega nastane škoda, se vzpostavi podlaga za odškodninsko odgovornost. Po 90 dneh od prenehanja delovnega razmerja se elektronski naslov ukine, e-sporočila in kopije le-teh pa se izbrišejo.

Elektronske pošte ni dovoljeno samodejno preusmerjati na druge naslove. Javni uslužbenec ali druga oseba, ki pri upravljavcu obdeluje osebne podatke, je dolžna pred napovedano odsotnostjo urediti samodejni odzivnik z obvestilom o odsotnosti, ki lahko vključuje tudi kontaktne podatke osebe, ki jo bo v času odsotnosti nadomeščala.

Vpogled v vsebino oz. nadzor elektronske pošte in ostale programske opreme javnega uslužbenca ali druge osebe je dovoljen na podlagi odredbe sodišča ali pisne privolitve javnega uslužbenca ali druge osebe. Poleg v kateri sta poleg sestavin iz 13. člena Splošne uredbe, opredeljena tudi upravičenec do vpogleda in časovno obdobje dovoljenega vpogleda.

Vpogled v vsebino oz. nadzor elektronske pošte in ostale programske opreme javnega uslužbenca ali druge osebe, brez pisne privolitve ali odredbe sodišča se lahko opravi na podlagi pisnega sklepa župana ali direktorja občinske uprave le v izjemnih primerih (npr. nenadna odpoved delavca, smrt delavca, težja bolezen) in če namena ni mogoče doseči na milejši način (npr. nujno potrebno za pravočasno izvedbo nalog in do informacij ni bilo mogoče priti pravočasno na drug milejši način). Vpogled opravi tri-članska komisija, ki jo v pisnem sklepu imenuje župan ali direktor občinske uprave. V njej mora biti vsaj en predstavnik javnih uslužbencev, ki ni funkcionar. O vpogledu mora komisija napisati zapisnik in z njim nemudoma seznaniti javnega uslužbenca ali drugo osebo, v katere elektronsko pošto se je vpogledalo.

O namenih uporabe elektronske pošte in ostale programske opreme in možnosti nadzora morajo biti javni uslužbenci in druge osebe, ki pri upravljavcu obdelujejo osebne podatke pisno obveščeni. Kot zadostno obvestilo se šteje objava tega pravilnika na internem strežniku upravljavca ali obvestilo o njegovem sprejemu poslano vsem javnim uslužbencem in drugim osebam po elektronski pošti, skupaj z informacijo o tem na kakšen način se lahko z vsebino pravilnika seznanijo.

Vsa elektronska sporočila, ki se ne potrebujejo več za službene namene, je treba redno brisati iz poštne predala.

Internet

34. člen

Internet se uporablja v službene namene.

Ne glede na prejšnji odstavek se internet lahko uporablja v omejenem obsegu in razumnih mejah tudi v zasebne namene.

Uporaba interneta vsebinsko ni omejena. Župan ali direktor občinske uprave lahko s posebnim sklepom odredi blokado določenih spletnih strani in storitev:

- ki lahko vsebujejo škodljivo programsko kodo ali kako drugače ogrožajo informacijska premoženja in sisteme občinske uprave,

- ki lahko negativno vplivajo na razpoložljivost in odzivnost informacijskih in komunikacijskih sistemov,
- ki kršijo avtorske pravice,
- katerih vsebina lahko neposredno ali posredno ogrozi informacijsko ali drugo varnost občine,
- katerih vsebina bi bila lahko žaljiva za posamezne osebe ali skupine oseb,
- če bi tak dostop lahko škodil ugledu občine ali
- če bi tak dostop lahko povzročil odškodninsko odgovornost občine.

Blokado dostopa do določenih spletnih strani izvede skrbnik informacijskega sistema, na podlagi pisnega sklepa župana ali direktorja občinske uprave. O blokadi se po elektronski pošti obvesti vse javne uslužbenke in druge osebe.

Če se pojavi utemeljen sum, da javni uslužbenec ali druga oseba ne spoštuje omejitev iz drugega in tretjega odstavka tega člena se lahko na podlagi pisnega sklepa župana ali direktorja občinske uprave opravi vpogled v podatke o obiskih spletnih strani javnega uslužbenca ali druge osebe brez njenega pisnega soglasja le v izjemnih primerih (kot npr. reševanje uporabniških težav, reševanje varnostnih incidentov) in če namena ni mogoče doseči na milejši način. Vpogled se opravi na enak način kot vpogled v elektronsko pošto skladno s prejšnjim členom tega pravilnika.

O namenih uporabe interneta, blokade določenih spletnih strani in storitev ter možnosti nadzora iz tega člena morajo biti javni uslužbenci in druge osebe pisno obveščeni. Kot zadostno obvestilo se šteje objava tega pravilnika na internem strežniku upravljavca ali obvestilo o njegovem sprejemu poslano vsem javnim uslužbencem in drugim osebam po elektronski pošti, skupaj z informacijo o tem na kakšen način se lahko z vsebino pravilnika seznanijo.

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

Odgovornost in nadzor

35. člen

Za izvajanje postopkov in ukrepov za zagotavljanje varnosti osebnih podatkov so odgovorni vsi javni uslužbenci in druge osebe, ki pri upravljavcu obdelujejo osebne podatke.

Nadzor nad izvajanjem postopkov in ukrepov, določenih s tem pravilnikom opravlja direktor občinske uprave, pooblaščen oseba za varstvo osebnih podatkov in skrbnik informacijskega sistema.

Izjava o varovanju osebnih podatkov

36. člen

Pred sklenitvijo delovnega razmerja ali drugega pravnega razmerja z upravljavcem, na podlagi katerega se obdelujejo osebni podatki, mora oseba podpisati posebno izjavo, ki jo zavezuje k varovanju osebnih podatkov.

Iz podpisane izjave mora biti razvidno, da se je oseba še pred obdelavo osebnih podatkov seznaniła z določbami tega pravilnika ter določbami predpisov s področja varstva osebnih podatkov, izjava pa

mora vsebovati tudi pouk o posledicah kršitve pravilnika in drugih predpisov s področja varstva osebnih podatkov.

Vsak, ki obdeluje osebne podatke, je dolžan izvajati s tem pravilnikom predpisane postopke in ukrepe za varnost osebnih podatkov in varovati osebne podatke, za katere je izvedel oziroma bil z njimi seznanjen pri opravljanju svojega dela. Obveza varovanja podatkov je trajna in ne preneha s prenehanjem delovnega ali drugega pravnega razmerja.

Kršitev določil pravilnika

37. člen

Kršitev določil tega pravilnika predstavlja kršitev obveznosti iz delovnega razmerja.

Odgovornost iz prejšnjega odstavka ne izključuje kazenske, odškodninske ali druge odgovornosti.

Če je kršitev storila oseba, ki je pri upravljavcu v delovnem razmerju, se uvede tudi disciplinski postopek zoper storilca ali prične s postopkom redne ali izredne odpovedi pogodbe o zaposlitvi, odvisno od teže in posledic kršitev.

VII. HRAMBA IN BRISANJE OSEBNIH PODATKOV

Hramba osebnih podatkov

38. člen

Osebni podatki se lahko skladno s točko (e) prvega odstavka 5. člena Splošne uredbe shranjujejo le toliko časa, kolikor je potrebno za doseg namena, za katerega se zbirajo in nadaljnje obdelujejo.

Po preteku določenega roka se osebni podatki zbršejo, uničijo, blokirajo ali anonimizirajo, razen če so na podlagi zakona, ki ureja arhivsko gradivo in arhive, opredeljeni kot arhivsko gradivo, oziroma če zakon za posamezne vrste osebnih podatkov ne določa drugače.

Brisanje

39. člen

Brisanje osebnih podatkov na računalniških medijih se opravi na način, po postopku in metodi, ki onemogoča restavriranje izbrisanih podatkov.

Osebni podatki, vsebovani na fizičnih (papirnih) nosilcih (listine, kartoteke, register, seznam ipd.), se brišejo z uničenjem nosilcev, ki onemogoča branje uničenih podatkov. Nosilci se fizično uničijo (npr. razrežejo v rezalniku papirja) v prostorih upravljavca.

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

Nosilci osebnih podatkov se po potrebi komisijsko uničijo v prostorih upravljavca ali pod nadzorom pooblaščenega delavca družbe pri organizaciji, ki se ukvarja z uničevanjem dokumentacije. Pri prenosu

nosilcev osebnih podatkov na mesto uničenja je potrebno zagotoviti ustrezno zavarovanje tudi v času prenosa, na način da je onemogočena razpoznavnost ali obnovitev osebnih podatkov, kar je posebej urejeno v pogodbi, ki jo skleneta upravljavec in organizacija, ki se ukvarja z uničevanjem dokumentacije.

Na enak način kot izvirniki in končne verzije dokumentov, se uniči tudi pomožna dokumentacija oziroma predloge dokumentov.

VIII. STORITVE, KI JIH ZA UPRAVLJAVCA OPRAVLJAJO ZUNANJE PRAVNE ALI FIZIČNE OSEBE (OBDELOVALCI)

Pogodbena obdelava

40. člen

Z vsako zunanjo pravno ali fizično osebo, ki opravlja posamezne naloge v zvezi z obdelavo osebnih podatkov v imenu in za račun upravljavca (v nadaljevanju: obdelovalec), upravljavec sklene pisno pogodbo v skladu z 28. členom Splošne uredbe.

Pogodba iz prejšnjega odstavka mora obvezno vsebovati postopke in ukrepe za zagotovitev varnosti osebnih podatkov. Iz pogodbe mora biti razviden domet pravic in obveznosti upravljavca v zvezi z osebnimi podatki, saj upravljavec na obdelovalca ne more prenesti več pravic, kot jih ima sam, s čimer omejitve, ki veljajo za upravljavca, predstavljajo tudi omejitve za obdelovalca.

Obdelovalci, ki za upravljavca opravljajo pogodbeno dogovorjene storitve izven prostorov upravljavca, morajo imeti vsaj enako strog način varovanja osebnih podatkov, kakor ga predvideva ta pravilnik, kar se posebej določi v pogodbi o obdelavi osebnih podatkov.

Obdelovalci lahko opravljajo storitve obdelave osebnih podatkov samo v okviru pooblastil iz pogodbe iz prvega odstavka tega člena in podatkov ne smejo obdelovati ali drugače uporabljati za noben drug namen, kot tisti, ki ga je določil upravljavec. Če obdelovalec osebne podatke obdeluje tudi za druge namene ali na kakšen drug način preseže upravljavčeva navodila glede obdelave, se šteje, da obdelovalec v tem delu podatke obdeluje kot upravljavec ter je s tem zavezan k enakim obveznostim kot upravljavec (obstoj in izkazovanje pravne podlage, primeren obseg obdelovanih podatkov, itd.).

Če obdelovalec ne izpolnjuje svojih obveznosti ali deluje v neskladju s pogodbo o obdelavi osebnih podatkov, lahko v razmerju do upravljavca in posameznikov odškodninsko odgovarja. Poleg tega pa mu lahko Informacijski pooblaščenec izreče tudi ukrepe zaradi nespoštovanja določil Splošne uredbe, ZVOP-2 in drugih predpisov s področja varstva osebnih podatkov.

Upravljavec je s pomočjo pooblaščenih oseb za varstvo osebnih podatkov dolžan vzpostaviti seznam pogodbenih obdelovalcev, ki vsebuje: naziv in sedež pravne osebe ali ime in priimek fizične osebe, ime in priimek oseb, ki izvajajo zunanje storitve ter kontaktne podatke teh oseb (naslov e-pošte in telefonska številka).

IX. POOBLAŠČENA OSEBA ZA VARSTVO OSEBNIH PODATKOV (DPO)

Dolžnost imenovanja pooblaščenice osebe

41. člen

Upravljavec je zavezan imenovati pooblaščenico osebo za varstvo osebnih podatkov, saj izpolnjuje pogoje iz točke (a) prvega odstavka 37. člena Splošne uredbe.

Upravljavec imenuje pooblaščenico osebo s sklepom.

Naloge pooblaščenice osebe za varstvo osebnih podatkov

42. člen

Pooblaščenica oseba za varstvo osebnih podatkov upravljavcu s strokovnim in neodvisnim izvajanjem nalog pomaga pri zagotavljanju skladnosti obdelave osebnih podatkov s predpisi s področja varstva osebnih podatkov.

Pooblaščenica oseba za varstvo osebnih podatkov izvaja naslednje naloge:

- obvešča upravljavca ali obdelovalca in javne uslužbence ter druge osebe o pravicah in dolžnostih na področju varstva osebnih podatkov;
- spremlja skladnost poslovanja oz. obdelav podatkov s predpisi s področja varstva osebnih podatkov in internimi politikami o varnosti,
- pripravlja predloge za izvedbo ukrepov,
- pripravlja naloge za izvedbo ukrepov,
- organizira in/ali izvaja notranja usposabljanja,
- po potrebi opravlja revizije obdelav osebnih podatkov,
- po potrebi spremlja ali pomaga pri pripravi ocen učinka,
- sodeluje z Informacijskim pooblaščencom pri nadzorih in pri posvetovanjih,
- Informacijskemu pooblaščenцу poroča o kršitvah varstva osebnih podatkov,
- sodeluje s posamezniki, na katere se nanašajo osebni podatki, ki se na upravljavca obračajo glede vprašanj, povezanih z obdelavo osebnih podatkov in/ali uveljavljanjem pravic,
- dokumentira zaznane in sporočene kršitve,
- pripravlja interna navodila in o njihovi vsebini obvešča javne uslužbence in druge osebe,
- daje pobude za odpravo pomanjkljivosti ali zmanjšanje tveganj na področju varstva osebnih podatkov,
- pripravlja zaprosila za podajo mnenj Informacijskemu pooblaščenцу v primeru zahtevnejših vprašanj glede varstva osebnih podatkov.

Pristojnosti pooblaščenice osebe za varstvo osebnih podatkov

43. člen

Upravljavec je dolžan pooblaščenici osebi za varstvo osebnih podatkov predati vse potrebne informacije v zvezi z varstvom osebnih podatkov, zagotoviti, da je ustrezno in pravočasno vključena v vse zadeve v zvezi z varstvom osebnih podatkov ter zagotoviti sredstva potrebna za opravljanje nalog za varstvo osebnih podatkov in ohranjanje njenega strokovnega znanja.

Pooblaščen osebni podatki za varstvo osebnih podatkov je neodvisna in svobodna pri izvajanju svojih nalog. Enak položaj ima do pogodbenih obdelovalcev osebnih podatkov. O svojem delu poroča direktorju občinske uprave.

Pooblaščen osebni podatki za varstvo osebnih podatkov je zagotovljena ustrezna in pravočasna obveščenost o vseh zadevah v zvezi z varstvom osebnih podatkov, ki so del izvajanja nalog in pristojnosti upravljalca. Obveščanje pooblaščen osebe za varstvo osebnih podatkov se izvaja:

- z njegovim udeleževanjem na sestankih kolegijev, oddelkov, enot ali projektnih oz. delovnih skupin, ki in ko obravnavajo področja, ki posegajo tudi na področje varstva in obdelave osebnih podatkov,
- z neposrednim dostopom do javnih uslužbencev in drugih oseb, ki obdelujejo osebne podatke,
- z dostopom do dokumentarnega gradiva, ki obravnava zadeve varstva osebnih podatkov,
- z neposrednim dostopom do zbirk osebnih podatkov, evidenc dejavnosti obdelave, zapisov revizijskih sledi in drugih podatkov, ki jih potrebuje za izvajanje svojih nalog.

X. PRAVICE POSAMEZNIKA

Pravice posameznikov

44. člen

Upravljaec zagotavlja posamezniku, na katerega se nanašajo osebni podatki, v zvezi z osebnimi podatki, izpolnjevanje naslednjih pravic:

- Prejem informacij o obdelavi osebnih podatkov in informacij za zagotovitev poštene in pregledne obdelave v skladu s 13. členom Splošne uredbe.
- Dostop do osebnih podatkov in informacij v zvezi z obdelavo osebnih podatkov v skladu s 15. členom Splošne uredbe.
- Pravico do popravka netočnih podatkov v skladu s 16. členom Splošne uredbe.
- Pravico do izbrisa oz. pozabe osebnih podatkov, katerih obdelava ni potrebna za izpolnjevanje pravne obveznosti države članice v skladu s 17. členom Splošne uredbe.
- Pravico do omejitve obdelave v skladu s 18. členom Splošne uredbe.
- Druge pravice posameznika v zvezi z obdelavo v skladu s Splošno uredbo, kadar je to predvideno.

Postopkovne določbe

45. člen

Upravljaec o zahtevah posameznikov v zvezi z uveljavljanjem pravic, ki so urejene od 15. do 22. člena Splošne uredbe in drugih zahtevkih posameznika s področja varstva osebnih podatkov odločajo na podlagi zakona, ki ureja splošni upravni postopek, če drug zakon ne določa drugače. Kadar upravljaec ugotovi zahtevo posameznika, ne izda posebne odločbe, temveč o tem napravi uradni zaznamek in posameznika seznani z odločitvijo.

Kadar upravljaec zahtevi posameznika ne ugotovi, izda odločbo, ki poleg sestavin, določenih z zakonom, ki ureja splošni upravni postopek, v pouku o pravnem sredstvu vsebuje tudi navedbo pravice do

pritožbe pri Informacijskem pooblaščenču v roku 15 dni od vročitve odločbe v zadevi, po določbah točke (f) prvega odstavka 15. člena Splošne uredbe. Upravljavec z zaznamkom navede tudi razloge neugoditve zahtevku, v primeru očitne neutemeljenosti ali pretiranosti zahteve iz 17. člena ZVOP-2.

Upravljavec na vsako zahtevo posameznika, na katerega se nanašajo osebni podatki, odgovori brez nepotrebnega odlašanja in najpozneje v enem mesecu.

Uresničevanje pravic posameznikov

46. člen

Postopek uveljavljanja pravic pred upravljavcem in obdelovalcem je urejen od 12. do 21. člena ZVOP-2.

Poleg informacij, sporočil, odgovorov in ukrepanj upravljavca od 15. do 22. člena Splošne uredbe, ki se zagotavljajo brezplačno, se brezplačno zagotavljajo tudi informacije, sporočila, odgovori in ukrepanja upravljavca glede uveljavljanja pravic in zahtevkov s področja varstva osebnih podatkov, dostopa do osebnih podatkov, njihovega pridobivanja in obdelave.

Upravljavec zagotavlja čim lažje uresničevanje pravic posameznikov. Upravljavec v primeru obdelave osebnih podatkov z elektronskimi sredstvi teži k omogočanju elektronskega vlaganja zahtev.

Kadar so zahtevki posameznika očitno neutemeljeni ali pretirani, zlasti ker se ponavljajo, lahko upravljavec kljub temu zahtevi ugotovi, če je po vsebini utemeljena, in posamezniku zaračuna razumne stroške. Razumni stroški vključujejo samo materialne stroške posredovanja informacij, sporočil, odgovorov oziroma izvajanja zahtevanega ukrepanja. Če upravljavec ugotovi, da bodo posamezniku v zvezi z njegovim zahtevkom nastali stroški, posameznika o tem vnaprej obvesti. Višina stroškov je določena s podzakonskim predpisom.

Zavarovanje osebnih podatkov, ki so predmet postopka

47. člen

Upravljavec od prejema zahteve iz 15. do 22. člena Splošne uredbe, ne sme izbrisati, odsvojiti ali spremeniti zahtevanih osebnih podatkov, ki so predmet postopka, dnevnikov obdelav in drugih povezanih informacij, ne glede na potek predpisanih ali interno določenih rokov hrambe, dokler o zadevi ni pravnomočno odločeno, po pravnomočnosti pa skladno s pravnomočno odločitvijo v zadevi.

XI. UKREPANJE V PRIMERU VARNOSTNIH INCIDENTOV

Opredelitev varnostnih incidentov

48. člen

Incident predstavlja enega ali več nezaželenih ali nepričakovanih dogodkov, za katere je zelo verjetno, da bi lahko ogrozili normalno delovanje izvajanja upravljavčevih nalog in dolžnosti oziroma zaupnost, celovitost ali razpoložljivost podatkov, ki jih obdeluje upravljavec.

Incidenti so:

- izguba, uničenje ali zloraba osebnih podatkov in posebnih vrst osebnih podatkov, ki vpliva na zaupnost, celovitost ali razpoložljivost podatkov,
- namerno ali nenamerno poškodovanje ali zloraba računalniškega informacijskega sistema (uničenje ali poškodbe strojne opreme, okužbe z zlonamerno programsko opremo, vdori v računalniški informacijski sistem), ki vpliva na razpoložljivost podatkov,
- kraja opreme (strojne ali programske),
- izpad delovanja računalniškega informacijskega sistema (strojna oprema, programska oprema, komunikacije), ki vpliva na razpoložljivost podatkov in storitev,
- kršenje zakonodaje,
- neupoštevanje določil varnostnih pravil s strani javnih uslužbencev ali drugih oseb.

Ukrepi v primeru varnostnih incidentov

49. člen

Javni uslužbenci in druge osebe so dolžne preprečevati zlorabe osebnih podatkov in morajo z osebnimi podatki, s katerimi se seznanijo pri svojem delu, ravnati vestno in skrbno ter na način in po postopkih, ki jih določa ta pravilnik.

Javni uslužbenci in druge osebe so dolžne o aktivnostih, ki so povezane z odkrivanjem ali nepooblaščenim uničenjem zaupnih podatkov, zlonamerni ali nepooblaščen uporabi, prilaščanju ali spreminjanju osebnih podatkov takoj obvestiti neposredno nadrejenega, same pa morajo z zakonitimi ukrepi, v obsegu svojega znanja in sposobnosti, takšno aktivnost preprečiti in omejiti.

Direktor občinske uprave o varnostnem incidentu nemudoma obvesti pooblaščen osebno za varstvo osebnih podatkov ter ob pomoči za to usposobljenih javnih uslužbencev ali drugih oseb v roku 48 ur od seznaitve s kršitvijo varnosti osebnih podatkov preveri ali je do kršitve dejansko prišlo (npr. tako, da opravi razgovore), ali so bili izvedeni vsi potrebni ukrepi (npr. zavarovanje sledi, sprejem tehničnih in organizacijskih zaščitnih ukrepov, sprejem naknadnih ukrepov za zagotovitev, da se tveganje za pravice in svoboščine posameznikov verjetno ne bo več udejanjilo) in če ugotovi, da niso bili poskrbi, da se kršitev odpravi. S pomočjo pooblaščen osebno za varstvo osebnih podatkov naredi oceno ali so bile s kršitvijo varnosti osebnih podatkov ogrožene pravice in svoboščine posameznika oziroma ali bo kršitev povzročila (veliko) tveganje za pravice in svoboščine posameznikov ter pripravi pisno poročilo o kršitvi varstva osebnih podatkov.

V primeru, da je prišlo do kršitve varstva osebnih podatkov zaradi težav na računalniškem omrežju, izvede ukrepe in opravi druge obveznosti iz prejšnjega odstavka skrbnik informacijskega sistema.

Pooblaščen osebno za varstvo osebnih podatkov je dolžna v primeru kadar je verjetno, da bi bile s kršitvijo varnosti osebnih podatkov ogrožene pravice in svoboščine posameznika brez nepotrebnega odlašanja, najpozneje v 72 urah po seznaitvi s kršitvijo varnosti osebnih podatkov, poslati obvestilo Informacijskemu pooblaščenču z opisom vrste kršitve, sporočilom o kontaktnih podatkih pooblaščen osebno za varstvo podatkov, opisom verjetnih posledic, opisom sprejetih oziroma nameranih ukrepov za obravnavanje in ublažitev škodljivih učinkov kršitev in opisom razlogov, če obvestilo Informacijskemu pooblaščenču ni bilo podano v 72 urah.

Pooblaščenca oseba za varstvo osebnih podatkov je dolžna brez nepotrebnega odlašanja posamezniku, na katerega se osebni podatki nanašajo, pri ugotovitvi kršitve varnosti osebnih podatkov poslati obvestilo le, kadar obstaja veliko tveganje za njegove pravice in svoboščine posameznikov in če upravljavec ni izvedel ustreznih tehničnih in organizacijskih zaščitnih ukrepov ali ni sprejel naknadnih ukrepov za zagotovitev, da se veliko tveganje za pravice in svoboščine posameznikov verjetno ne bo več udejanjilo ali če bi to zahtevalo nesorazmeren napor. Obvestilo mora vsebovati sporočilo o vrsti kršitve, kontaktne podatke pooblaščenca osebe za varstvo podatkov, opis verjetnih posledic in opis sprejetih oziroma nameranih ukrepov za obravnavanje in ublažitev škodljivih učinkov kršitev.

Ukrepi zoper osebo odgovorno za varnostni incident

50. člen

V primeru zlorabe osebnih podatkov s strani javnega uslužbenca ali druge osebe, mora župan zoper tistega, ki je zlorabil osebne podatke ali je nepooblaščen vdril v zbirko, ustrezno ukrepati.

Za zlorabo osebnih podatkov šteje vsaka uporaba osebnih podatkov v namene, ki niso v skladu z zakonsko določenimi nameni zbiranja ali nameni, določenimi v evidenci dejavnosti obdelave. Za poskus zlorabe šteje poskus uporabe osebnih podatkov v nedovoljene namene.

Če obstaja pri vdoru v zbirko sum, da je ta storjen z namenom zlorabiti osebne podatke ali jih uporabiti v nasprotju z nameni za katere so zbrani ali če je do zlorabe osebnih podatkov že prišlo, mora župan poleg uvedbe disciplinskega postopka zoper storilca ali izreka opomina pred redno odpovedjo pogodbe o zaposlitvi ali poleg redne odpovedi pogodbe o zaposlitvi iz krivdnih razlogov ali poleg izredne odpovedi pogodbe o zaposlitvi, ali odpovedi drugega pravnega razmerja, vdor ali zlorabo oziroma poskus zlorabe prijaviti organom pregona.

XII. KONČNE DOLOČBE

Veljavnost pravilnika

51. člen

Ta pravilnik prične veljati naslednji dan po njegovem sprejemu.

Pravilnik se objavi na običajen način pri upravljavcu, tako da se z njim seznaniijo vsi javni uslužbenci in druge osebe, ki pri upravljavcu obdelujejo osebne podatke.

Spremembe in dopolnitve tega pravilnika se sprejmejo po postopku in na enak način kot ta pravilnik.

Številka: 071-0001/2025
Ormož, dne 31. 1. 2025



Občina Ormož
Župan Danijel Vrbnjak

