Občina Laško
Mestna ulica 2, 3270 Laško
ŽUPAN

Na podlagi določb Uredbe (EU) 2016/679 Evropskega Parlamenta in Sveta z dne 27. 04. 2016 o varstvu posameznikov pri obdelavi osebnih podatkov in o prostem pretoku takih podatkov ter o razveljavitvi Direktive 95/46/ES (v nadaljevanju: GDPR), določil Zakona o varstvu osebnih podatkov (Ur. l. RS, št. 163/22, v nadaljevanju: ZVOP-2), ter 37. člena Statuta Občine Laško (Uradni list RS, št. 79/2015-UPB1, 68/18, 61/19, 157/20), sprejme župan Občine Laško naslednji

PRAVILNIK O ZAVAROVANJU OSEBNIH PODATKOV

I. SPLOŠNE DOLOČBE

Vsebina in namen pravilnika
1. člen

(1) S tem pravilnikom se določajo organizacijski in tehnični postopki ter ukrepi za zavarovanje osebnih podatkov v Občini Laško (v nadaljevanju: upravljavec) z namenom, da se prepreči naključno ali namerno nepooblaščeno uničevanje podatkov, njihova sprememba ali izguba, kakor tudi nepooblaščen dostop, obdelava, uporaba ali posredovanje osebnih podatkov.
(2) Zaposleni pri upravljavcu in zunanji sodelavci, ki pri svojem delu obdelujejo in uporabljajo osebne podatke, morajo biti seznanjeni z GDPR, ZVOP-2 in drugo področno zakonodajo, ki ureja posamezno področje njihovega dela, ter z vsebino tega pravilnika.

Osebni podatki
2. člen

Osebni podatek pomeni katero koli informacijo v zvezi z določenim ali določljivim posameznikom. Določljiv posameznik je tisti, ki ga je mogoče neposredno ali posredno določiti, zlasti z navedbo identifikatorja, kot je ime, identifikacijska številka, podatki o lokaciji, spletni identifikator, ali z navedbo enega ali več dejavnikov, ki so značilni za fizično, fiziološko, genetsko, duševno, gospodarsko, kulturno ali družbeno identiteto tega posameznika.

Obdelava osebnih podatkov pomeni vsako dejanje ali niz dejanj, ki se izvaja v zvezi z osebnimi podatki ali nizi osebnih podatkov z avtomatiziranimi sredstvi ali brez njih.

Zbirka osebnih podatkov pomeni vsak strukturiran niz osebnih podatkov, ki so dostopni v skladu s posebnimi merili, niz pa je lahko centraliziran, decentraliziran ali razpršen na funkcionalni ali geografski podlagi.

Upravljalec osebnih podatkov pomeni fizično ali pravno osebo, javni organ, agencijo ali drugo telo, ki samo ali skupaj z drugimi določa namene in sredstva obdelave.

Obdelovalec osebnih podatkov pomeni fizično ali pravno osebo, javni organ, agencijo ali drugo telo, ki obdeluje osebne podatke v imenu upravljalca.

Prepoved diskriminacije glede obdelave osebnih podatkov
3. člen

(1) Obdelava osebnih podatkov je prepovedana, če se izvaja na način ali ima za posledico nedopustno diskriminacijo glede na narodnost, raso, barvo kože, veroizpoved, etnično pripadnost, spol, jezik, politično ali drugo prepričanje, spolno usmerjenost, spolno identiteto, premoženjsko stanje, kraj rojstva, izobrazbo, družbeni položaj, invalidnost, državljanstvo, kraj oziroma vrsto

prebivališča, zdravstveno stanje, genske predispozicije ali katero koli drugo osebno okoliščino posameznice in posameznika.

(2) Kadar se nenamerno zberejo osebni podatki, za katere je očitno, da niso potrebni za konkretno obdelavo, se izbrišejo brez nepotrebnega odlašanja, drugače nepovratno uničijo ali vrnejo posamezniku, na katerega se nanašajo, ali upravljavcu ali obdelovalcu, ki jih je poslal.

II. OBDELAVA OSEBNIH PODATKOV

Splošno
4. člen

(1) Obdelava je zakonita le takrat in v obsegu, kadar je izpolnjen vsaj eden od pogojev, določenih v 6. členu GDPR.
(2) Posameznik, o katerem se vodijo osebni podatki, oz. pooblaščenec posameznika ali zakoniti zastopnik posameznika, o katerem se pri upravljavcu vodijo njegovi osebni podatki, lahko vpogleda v osebne podatke, vodene o njem in jih ima pravico popraviti in dopolniti, izbrisati, omejiti obdelavo ali jih prenesti k drugemu upravljavcu.

Evidentiranje dokumentov
5. člen

Za evidentiranje dokumentov in zadev, ki vsebujejo osebne podatke, se uporabljajo določbe predpisov, ki urejajo upravno poslovanje z dokumentarnim gradivom.

Posredovanje osebnih podatkov
6. člen

(1) Osebni podatki, ki jih ima upravljavec, se na zahtevo uporabnika lahko posredujejo samo tistim uporabnikom, ki se izkažejo z ustrezno zakonsko podlago, ali na podlagi pisne zahteve ali privolitve posameznika, na katerega se podatki nanašajo.
(2) Osebni podatki se po uradni dolžnosti posredujejo samo tistim uporabnikom, ki imajo ustrezno zakonsko podlago.
(3) Posredovanje osebnih podatkov iz prvega odstavka tega člena lahko uporabnik zahteva pisno ali ustno. Ob vložitvi pisne vloge mora uporabnik jasno navesti določbo zakona, ki ga pooblašča za pridobitev osebnih podatkov, ali pa mora k vlogi priložiti pisno zahtevo oziroma privolitev posameznika, na katerega se podatki nanašajo. Če uporabnik zahteva posredovanje osebnih podatkov ustno, sme odgovorna oseba ali pooblaščeni obdelovalec v primeru dvoma o obstoju pisne zahteve oziroma privolitve posameznika, na katerega se podatki nanašajo, od uporabnika zahtevati, naj jih predloži.
(4) Posredovanje posebnih vrst osebnih podatkov iz prvega odstavka tega člena lahko uporabnik zahteva le pisno. Pisna vloga mora biti po vsebini enaka pisni vlogi iz prejšnjega odstavka.
(5) 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.
(6) Osebni podatki, ki se posredujejo uporabniku 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.
(7) Posebne vrste osebnih podatkov je dovoljeno posredovati preko komunikacijskih omrežij samo, če so posebej zavarovani s kriptografskimi metodami tako, da je zagotovljena nečitljivost podatkov med njihovim prenosom.
(8) Originalni dokument, ki vsebuje osebne podatke, se lahko posreduje uporabniku samo na podlagi pisne odredbe sodišča. Posredovani originalni dokument mora biti v času odsotnosti nadomeščen s fizično (fotokopijo) ali elektronsko (skenirano) kopijo.

Evidenca posredovanj
7. člen

(1) Vsako posredovanje osebnih podatkov iz prejšnjega člena se zaznamuje z navedbo naslednjih podatkov:
- kateri osebni podatki so bili posredovani,
- osebno ime/firmo in naslov/sedež osebe, ki so ji bili posredovani osebni podatki, oziroma navedba, da je bilo posredovanje opravljeno po uradni dolžnosti,
- datum in ura posredovanja osebnih podatkov,
- pravna podlaga, na kateri so bili posredovani osebni podatki.

(2) Uradni zaznamek iz prejšnjega odstavka je v pisni ali elektronski obliki 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).
(3) Če osebni podatek, ki se posreduje, ni del podatkov zadeve, o kateri se vodi postopek, se uradni zaznamek iz prvega odstavka tega člena v obliki iz prejšnjega odstavka, evidentira neposredno v zbirko osebnih podatkov, ki ji pripada posredovani osebni podatek.
(4) Uradni zaznamek iz prvega odstavka tega člena naredi odgovorna oseba ali pooblaščeni obdelovalec, ki je osebne podatke posredoval uporabniku.

Stroški zagotavljanja informacij
8. člen

(1) Poleg informacij, sporočil, odgovorov in ukrepanj upravljavca iz 15. do 22. člena GDPR, 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 po tem ali drugem zakonu.

(2) Kadar so zahtevki posameznika, na katerega se nanašajo osebni podatki, očitno neutemeljeni ali pretirani, zlasti ker se ponavljajo, lahko upravljavec kljub temu zahtevi ugodi, če je po vsebini utemeljena, in posamezniku zaračuna razumne stroške. Razumni stroški vključujejo samo materialne stroške posredovanja informacij, sporočil, odgovorov oziroma izvajanja zahtevanega ukrepanja.

(3) V primerih neugoditve zahtevkom ali drugim upravičenjem upravljavec z zaznamkom navede tudi razloge glede očitne neutemeljenosti ali pretiranosti zahteve. Če upravljavec ugotovi, da bodo nastali stroški v skladu z določbami tega člena, posameznika o tem vnaprej obvesti.

(4) Višino stroškov posredovanja osebnih podatkov, pravila o zaračunavanju, načinu vnaprejšnjega obveščanja posameznika o nastalih stroških predpiše minister, pristojen za pravosodje, v soglasju z ministrom, pristojnim za zdravje, po predhodnem mnenju nadzornega organa.

Posredovanje osebnih podatkov znotraj upravljavca
9. člen

(1) Dokumenti, ki vsebujejo osebne podatke zaposlenega pri upravljavcu, se zaposlenemu, na katerega se osebni podatki nanašajo, posredujejo v skladu s tretjim odstavkom 6. člena tega pravilnika.
(2) Osebni podatki zaposlenih pri upravljavcu in ostalih oseb se lahko posredujejo znotraj upravljavca tudi tistim osebam, ki jih potrebujejo v okviru opravljanja svojih del in nalog.
(3) Oseba iz četrtega odstavka 7. člena mora zaznamovati vsako posredovanje posebnih vrst osebnih podatkov znotraj upravljavca v skladu s prejšnjim členom.
(4) Personalne mape zaposlenih pri upravljavcu se skrbno hranijo v ognjevarni in vodotesni omari in imajo dostop do njih le tiste osebe, ki jih za to pooblasti odgovorna oseba upravljavca.

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

(1) 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.
(2) Pred pregledom, prepisovanjem in kopiranjem dokumentov, ki vsebujejo osebne podatke, je potrebno preveriti identiteto stranke oziroma vsakega drugega, ki verjetno izkaže, da ima od pregledovanja, prepisovanja in preslikovanja pravno korist (v nadaljevanju: upravičenec) z vpogledom v njegovo osebno izkaznico, potni list, vozniško dovoljenje ali drug dokument, ki nedvoumno izkazuje njegovo istovetnost.
(3) 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.
(4) 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.

Kopiranje in tiskanje osebnih podatkov s strani zaposlenih
11. člen

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

Hramba, rok hrambe in brisanje osebnih podatkov
12. člen

(1) Osebni podatki se lahko shranjujejo le toliko časa, kolikor je rok hrambe določen za posamezno zbirko osebnih podatkov v evidenci dejavnosti obdelav osebnih podatkov. Rok hrambe osebnih podatkov je omejen na najkrajše možno obdobje in le, dokler je hramba potrebna za dosego namena obdelave, zaradi katerega so se osebni podatki zbirali in nadalje obdelovali, razen če drug zakon za posamezne obdelave določa rok hrambe.
(2) Po preteku roka hranjenja se osebni podatki zbrišejo, uničijo, blokirajo ali anonimizirajo, razen če niso na podlagi zakona, ki ureja arhivsko gradivo in arhive, opredeljeni kot arhivsko gradivo, oziroma če zakon za posamezne vrste osebnih podatkov ne določa drugače.
(3) Za brisanje osebnih podatkov v elektronski obliki se uporabi takšna metoda brisanja, da je nemogoča ponovna obnovitev vseh ali dela brisanih podatkov.
(4) Osebni podatki v fizični obliki se uničijo na način, s katerim se zagotovi, da postane osebni podatek nerazpoznaven in neobnovljiv (npr. rezalnik papirja).
(5) Uničenje nosilcev podatkov in pomožnega gradiva se zagotovi v skladu z določbami predpisov, ki urejajo upravno poslovanje z dokumentarnim gradivom.
(6) Prepovedano je odmetavati odpadne nosilce podatkov, ki vsebujejo osebne podatke, na način, ki omogoča obnovitev ali razpoznavnost osebnih podatkov (npr. v koš za smeti).
(7) Pri prenosu nosilcev podatkov, ki vsebujejo posebne vrste osebnih podatkov, na mesto uničenja, je potrebno zagotoviti ustrezno zavarovanje tudi v času prenosa, zlasti tako, da je onemogočena razpoznavnost ali obnovitev osebnih podatkov.
(8) Mesto, kjer se nahaja dokumentacija z osebnimi podatki, mora biti vedno zaklenjeno. Ključ od zavarovanih omar imajo samo pooblaščeni delavci, ki jih določi predstojnik upravljavca. Dokumentacija se hrani v zaklenjenih omarah tako, da so dokumenti zavarovani pred zunanjim uničenjem.

III. EVIDENCE DEJAVNOSTI OBDELAVE OSEBNIH PODATKOV

13. člen

Opis zbirk osebnih podatkov, katerih upravljavec je občina, se vodi v evidenci dejavnosti obdelave osebnih podatkov kot to določa 30. člen GDPR. Evidence dejavnosti se vodijo v pisni in elektronski obliki tako, da jih je mogoče na zahtevo Informacijskega pooblaščenca predložiti v pregled.

14. člen

(1) Evidenca dejavnosti obdelave vsebuje vsaj naslednje informacije:
- naziv
- kontaktne podatke upravljavca
- podatke o pooblaščeni osebi za varstvo osebnih podatkov
- namen obdelave osebnih podatkov
- kategorije posameznikov, na katere se nanašajo osebni podatki v zbirki
- vrste osebnih podatkov
- kategorije uporabnikov, ki so jim bili ali jim bodo razkriti osebni podatki
- informacije o prenosih osebnih podatkov v tretjo državo ali mednarodno organizacijo
- rok hrambe
- tehnične in organizacijske varnostne ukrepe.

(2) Evidence obdelave se dopolnjujejo ob vsaki spremembi vrste osebnih podatkov v posamezni zbirki. Zaposleni, ki obdelujejo osebne podatke, morejo biti seznanjeni z evidencami obdelave osebnih podatkov.
(3) Upravljavec je dolžan voditi ažuren seznam, iz katerega je za vsako evidenco dejavnosti obdelave jasno razvidno, katera oseba je odgovorna za posamezno zbirko osebnih podatkov ter katere osebe lahko zaradi narave svojega dela obdelujejo osebne podatke, ki se nanašajo na posamezno zbirko osebnih podatkov.

IV. PODROČNE UREDITVE VARSTVA OSEBNIH PODATKOV

Elektronska pošta in uporaba druge programske opreme na računalniku
15. člen

(1) Elektronska pošta in računalnik se uporabljata v službene namene.
(2) 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. Vsebina elektronske pošte v zasebne namene ne sme biti neprimerna ali žaljiva.
(3) Oseba, zadolžena za delovanje računalniškega informacijskega sistema pri upravljavcu, lahko na posebej utemeljeno pisno zahtevo vodstva upravljavca v prisotnosti komisije iz 4. odstavka tega člena, v izrednih primerih (nenadna odpoved delavca, smrt delavca, ali drug izreden dogodek) vpogleda v elektronsko pošto le, če je to nujno potrebno za vodenje delovnega procesa.
(4) Vpogled v vsebino e-pošte zaposlenega opravi 3 članska komisija, ki jo vsakokrat imenuje odgovorna oseba upravljavca. V njej mora biti vsaj en predstavnik zaposlenih, ki ni vodstveni delavec. O vpogledu mora komisija napisati zapisnik. Komisija ima tudi pravico na tej e-pošti urediti avtomatski odzivnik, da je zaposleni odsoten oz. nedosegljiv in da se je potrebno obrniti na centralo upravljavca.
(5) Če se pojavi utemeljen sum, da zaposleni ne spoštujejo omejitev iz drugega odstavka tega člena, lahko oseba, zadolžena za delovanje računalniškega informacijskega sistema, na posebej utemeljeno pisno zahtevo vodstva upravljavca opravi nadzor količine uporabe elektronske pošte, a zgolj z vidika obsega priponk, ki obremenjujejo strežnik. Pri tem se ne sme pregledovati vsebine elektronske pošte.

(6) O namenu uporabe elektronske pošte in ostale programske opreme iz prvega in drugega odstavka tega člena ter možnosti nadzora iz tretjega in četrtega odstavka tega člena mora biti zaposleni pisno obveščen.
(7) Vpogled v telefonske prometne podatke priključkov, katerih lastnik je upravljavec, lahko odgovorna oseba upravljavca zahteva od operaterjev telekomunikacijskih storitev ali vzdrževalca hišne centrale le takrat, kadar pride med upravljavcem in zaposlenim do kakršnegakoli spora glede višine stroškov porabe konkretnega službenega telefona.

Internet
16. člen

(1) Internet se uporablja v službene namene.
(2) Ne glede na prejšnji odstavek se internet lahko uporablja v omejenem obsegu in razumnih mejah tudi v zasebne namene. Internetne strani, ki se pregledujejo v zasebne namene, ne smejo vsebovati neprimerne ali žaljive vsebine.
(3) Odgovorna oseba upravljavca lahko s posebno odredbo odredi blokado določenih spletnih strani, ki jo izvede oseba, zadolžena za delovanje računalniškega informacijskega sistema, na podlagi pisne odredbe upravljavca.
(4) O blokadi se obvesti vse zaposlene po elektronski pošti in ali na drug primeren način.

V. VAROVANJE PROSTOROV IN RAČUNALNIŠKE OPREME (NOSILCEV PODATKOV, STROJNE IN PROGRAMSKE OPREME)

Varovanje prostorov
17. člen

(1) Prostori, v katerih se nahajajo nosilci podatkov, ki vsebujejo osebne podatke in morebitne druge varovane podatke, strojno in programsko opremo (v nadaljevanju: varovani prostori), morajo biti varovani z organizacijskimi in/ali tehničnimi ukrepi iz tega pravilnika, ki onemogočajo nepooblaščenim osebam dostop do podatkov.
(2) Dostop do varovanih prostorov je mogoč le v rednem delovnem času, izven njega pa samo na podlagi dovoljenja odgovorne osebe upravljavca.
(3) Varovani prostori ne smejo ostajati nenadzorovani, oziroma se morajo obvezno zaklepati ob odsotnosti delavcev, ki jih nadzorujejo. Ključi se ne smejo puščati v ključavnici v vratih.
(4) V varovanih prostorih morajo biti po zaključku delovnega časa oziroma po končanem delu izven delovnega časa omare in pisalne mize z nosilci podatkov, ki vsebujejo osebne podatke, zaklenjene, računalniki in druga strojna oprema pa izklopljeni in fizično ali programsko zaklenjeni. Ključe hrani zaposleni, ki nadzoruje posamezen varovani prostor, na zavarovanem mestu v varovanem prostoru.
(5) Omare, mize in drugo pohištvo z nosilci podatkov, ki vsebujejo osebne podatke, ki se nahajajo na hodnikih in v drugih skupnih prostorih mora biti stalno zaklenjeno. Ključe hrani zaposleni, ki nadzoruje posamezno omaro, mizo in drugo pohištvo, na zavarovanem mestu v varovanem prostoru, ki ga nadzoruje.
(6) Osebe, ki niso zaposlene pri delodajalcu (npr. obiskovalci, vzdrževalci prostorov, vzdrževalci strojne in programske opreme, poslovni partnerji) se smejo gibati v varovanih prostorih samo ob prisotnosti zaposlenega, ki takrat skrbi za varovani prostor, kjer se oseba giba. V primeru, da prisotnosti zaposlenega v tem času ni možno zagotoviti, je potrebno pred vstopom nezaposlenih oseb ustrezno zaščititi vso dokumentacijo v teh prostorih, ki vsebuje osebne podatke (zaklepanje omar in predalov, čista miza,...).
(7) Posebne vrste osebnih podatkov se ne smejo hraniti izven varovanih prostorov.

Varovanje nosilcev podatkov, ki vsebujejo osebne podatke
18. člen

(1) Zaposleni ne smejo puščati nosilcev podatkov, ki vsebujejo osebne podatke, na vidnem mestu (npr. na mizah) v prisotnosti oseb, ki nimajo pravice vpogleda vanje (politika čiste mize).
(2) Nosilce podatkov, ki vsebujejo osebne podatke, lahko zaposleni odnašajo izven prostorov delodajalca samo z dovoljenjem odgovorne osebe upravljavca.
(3) Nosilcev podatkov, ki vsebujejo posebne vrste osebnih podatkov, zaposleni ne smejo odnašati izven prostorov delodajalca, razen izjemoma z dovoljenjem odgovorne osebe upravljavca, če je to nujno potrebno za reševanje zadeve, ki vsebuje te posebne vrste osebnih podatkov.
(4) V prostorih, ki so namenjeni poslovanju s strankami, morajo biti nosilci podatkov, ki vsebujejo osebne podatke, nameščeni tako, da stranke nimajo dostopa niti vpogleda vanje.

Varovanje strojne in programske opreme
19. člen

(1) Vzdrževanje in popravila strojne računalniške in druge opreme je dovoljeno samo z vednostjo osebe, zadolžene za delovanje računalniškega informacijskega sistema, izvajajo pa ga lahko samo pooblaščeni servisi in vzdrževalci, ki imajo z upravljavcem sklenjeno ustrezno pogodbo.
(2) Dostop do programske opreme mora biti varovan tako, da dovoljuje dostop samo zaposlenim, ki jih določi oseba, zadolžena za delovanje računalniškega informacijskega sistema, v soglasju z odgovorno osebo upravljavca, ali pravnim ali fizičnim osebam, ki v skladu s pogodbo opravljajo dogovorjene storitve.
(3) Popravljanje, spreminjanje in dopolnjevanje sistemske in aplikativne programske opreme je dovoljeno samo na podlagi odobritve osebe, zadolžene za delovanje računalniškega informacijskega sistema, izvajajo pa ga lahko samo pooblaščeni servisi in organizacije ter posamezniki, ki imajo z upravljavcem sklenjeno ustrezno pogodbo. Izvajalci morajo spremembe in dopolnitve sistemske in aplikativne programske opreme ustrezno dokumentirati.
(4) Za shranjevanje in varovanje aplikativne programske opreme veljajo enaka določila, kot za ostale podatke iz tega pravilnika.
(5) Vsebina diskov mrežnega strežnika in lokalnih delovnih postaj, kjer se nahajajo osebni podatki, se vsakodnevno preveri z vidika prisotnosti računalniških virusov. Ob pojavu računalniškega virusa se tega čim prej odpravi, obenem pa se ugotovi vzrok pojava virusa v računalniškem informacijskem sistemu upravljavca.
(6) Vsi podatki in programska oprema, ki so namenjeni uporabi v računalniškem informacijskem sistemu, in prispejo k upravljavcu na medijih za prenos računalniških podatkov ali preko komunikacijskih kanalov, morajo biti pred uporabo preverjeni z vidika prisotnosti računalniških virusov.
(7) Zaposleni ne smejo inštalirati programske opreme brez vednosti osebe, zadolžene za delovanje računalniškega informacijskega sistema. Prav tako ne smejo odnašati programske opreme iz prostorov upravljavca brez odobritve odgovorne osebe upravljavca in vednosti osebe, zadolžene za delovanje računalniškega informacijskega sistema.
(8) Pristop do podatkov preko programske opreme se varuje s sistemom gesel za avtorizacijo in identifikacijo uporabnikov programov in podatkov. Sistem gesel mora omogočati tudi možnost naknadnega ugotavljanja, kdaj so bili posamezni osebni podatki vneseni v zbirko podatkov, uporabljeni ali drugače obdelani ter kdo je to storil.
(9) Oseba, zadolžena za delovanje računalniškega informacijskega sistema, določi režim dodeljevanja, hranjenja in spreminjanja gesel.

Politika upravljanja in varovanja gesel
20. člen

(1) Vsako dodeljeno geslo je strogo zaupna informacija in ga je potrebno ob prvi prijavi spremeniti.
(2) Gesla morajo biti sestavljena iz najmanj 6 različnih znakov, ki ne vsebujejo šumnikov.
(3) Gesla se menjavajo najmanj vsakih 6 mesecev.

VI. POGODBENA OBDELAVA OSEBNIH PODATKOV

Pogodbena obdelava
21. člen

(1) Kadar zbiranje, obdelovanje, shranjevanje ali posredovanje osebnih podatkov v imenu upravljavca izvaja obdelovalec kot zunanja pravna ali fizična oseba, ki je registrirana za opravljanje takšne dejavnosti, mora za to obstajati pisna pogodba ali drug ustrezen akt.
(2) Upravljavec mora izbrati ustreznega obdelovalca, ki osebne podatke obdeluje skladno z GDPR.
(3) Zunanje pravne ali fizične osebe smejo opravljati storitve obdelave osebnih podatkov samo v okviru naročnikovih pooblastil in podatkov ne smejo obdelovati ali drugače uporabljati za noben drug namen.
(4) Obdelovalec lahko najame pod-obdelovalca (podizvajalca posameznih obdelav) le s pisnim dovoljenjem upravljavca.
(5) GDPR predpisuje minimalni obseg sestavin pogodbe ali drugega pravnega akta, ki mora zlasti določati, da obdelovalec:

- lahko osebne podatke obdeluje samo po dokumentiranih navodilih upravljavca,
- zagotovi, da so osebe, ki so pooblaščene za obdelavo osebnih podatkov, zavezane k zaupnosti ali jih k zaupnosti zavezuje ustrezen zakon;
- sprejme vse ukrepe, potrebne za varnost osebnih podatkov;
- zaposli drugega obdelovalca le, če je prej pridobil posebno ali splošno pisno dovoljenje upravljavca in da zagotovi, da veljajo med obdelovalcem in pod-obdelovalcem enake obveznosti kot med upravljavcem in obdelovalcem in da je med njima sklenjena pisna pogodba;
- upravljavcu pomaga pri izpolnjevanju njegovih obveznosti, da odgovori na zahteve za uresničevanje pravic posameznika, na katerega se nanašajo osebni podatki;
- upravljavcu pomaga pri zagotavljanju varnosti obdelave osebnih podatkov, uradnem obveščanju o kršitvah in oceni učinkov na varstvo osebnih podatkov;
- po zaključku storitve obdelave izbriše ali vrne vse osebne podatke upravljavcu, razen kadar hrambo predpisuje zakon;
- da upravljavcu na voljo vse informacije, potrebne za dokazovanje izpolnjevanja obveznosti iz 28. člena GDPR, ter upravljavcu ali drugemu revizorju, ki ga pooblasti upravljavec, omogoči izvajanje revizij, tudi pregledov, in pri njih sodeluje.

(6) Poleg pogodbenih obveznosti do upravljavca je obdelovalec po GDPR neposredno odgovoren da:

- ne angažira pod-obdelovalcev brez predhodnega pisnega dovoljenja upravljavca;
- sodeluje z nadzornim organom;
- zagotavlja varnost obdelave osebnih podatkov;
- vodi evidence dejavnosti obdelav;
- upravljavca obvesti o kršitvi;
- po potrebi imenuje pooblaščeno osebo za varstvo osebnih podatkov;
- imenuje predstavnika znotraj EU, kadar je to potrebno.

(7) Če obdelovalec ne izpolni svojih obveznosti po GDPR ali pa deluje v neskladju s pogodbo z upravljavcem, lahko odgovarja odškodninsko v razmerju do upravljavca in posameznikov, lahko pa je podvržen tudi globam in popravljalnim ukrepom nadzornega organa.

VII. UKREPANJE OB SUMU ALI UGOTOVITVAH KRŠITEV VARSTVA OSEBNIH PODATKOV

Obveščanje
22. člen

(1) Zaposleni so dolžni o aktivnostih, ki so povezane z odkrivanjem ali nepooblaščenim uničenjem osebnih podatkov, zlonamerni ali nepooblaščeni uporabi, prilaščanju, spreminjanju ali poškodovanju

osebnih podatkov, takoj obvestiti pooblaščeno osebo ali odgovorno osebo upravljavca, sami pa morajo poskusiti z zakonitimi ukrepi takšno aktivnost preprečiti. Zaposleni, ki izve ali sumi, da je prišlo do zlorabe osebnih podatkov, mora v okviru prijave podati vse ugotovitve in lastna opažanja glede zlorabe osebnih podatkov.
(2) Upravljavec je dolžan brez nepotrebnega odlašanja, najpozneje pa v roku 72 ur po seznanitvi s sumom ali kršitvijo, obvestiti Informacijskega pooblaščenca o vsaki kršitvi varstva osebnih podatkov, ki jo zaznamo, če je verjetno, da bi bile s kršitvijo ogrožene pravice in svoboščine posameznikov.
(3) Kadar je verjetno, da kršitev varstva osebnih podatkov povzroči veliko tveganje za pravice in svoboščine posameznikov, mora upravljavec kršitev sporočiti tudi posamezniku, na katerega se nanašajo osebni podatki.
(4) Če bi posamično obveščanje posameznikov, na katere se nanašajo osebni podatki, vključevalo nesorazmeren napor delodajalca, kar vključuje tudi neučinkovitost obveščanja in vpliv na spoštovanje pravne varnosti ali bistvenih človekovih pravic ali temeljnih svoboščin, je možno opraviti tudi obveščanje preko medijev.

VIII. ODGOVORNOST ZA IZVAJANJE VARNOSTNIH UKREPOV IN POSTOPKOV

Izvajanje ukrepov in postopkov
23. člen

(1) Vsak, ki obdeluje osebne podatke, je dolžan izvajati vse s tem pravilnikom predpisane ukrepe in postopke za zavarovanje osebnih podatkov in varovati osebne podatke, za katere je izvedel oziroma bil z njimi seznanjen pri opravljanju svojega dela. Obveznost varovanja podatkov ne preneha s prenehanjem delovnega razmerja.
(2) Zaposlene je potrebno redno obveščati in ozaveščati o pomenu poznavanja področja osebnih podatkov ter skrbeti za njihovo stalno izobraževanje iz tega področja.

Odgovornost za izvajanje
24. člen

Za izvajanje postopkov in ukrepov za zavarovanje osebnih podatkov, določenih s tem pravilnikom, so odgovorne osebe, ki jih imenuje oziroma pooblasti upravljavec oz. osebe, ki zaradi narave svojega dela obdelujejo osebne podatke.

Izjava
25. člen

(1) Pred nastopom dela na delovno mesto, kjer se obdelujejo osebni podatki, mora zaposleni podpisati posebno izjavo, ki ga zavezuje k varovanju osebnih podatkov in drugih zaupnih podatkov. Izjavo morajo podpisati tudi obstoječi zaposleni ob sprejemu tega pravilnika.
(2) Iz podpisane izjave mora biti razvidno, da je podpisnik seznanjen z določbami tega pravilnika ter določbami veljavne zakonodaje, izjava pa mora vsebovati tudi pouk o posledicah kršitve tega pravilnika in zakona.

Odgovornost za kršitev
26. člen

(1) Kršitev določil tega pravilnika s strani zaposlenih pomeni kršenje obveznosti iz delovnega razmerja, ostali pa za kršitve odgovarjajo na temelju pogodbenih obveznosti.
(2) Odgovornost iz prejšnjega odstavka ne izključuje kazenske ali odškodninske odgovornosti.

IX. POOBLAŠČENA OSEBA

Pooblaščena oseba za varstvo osebnih podatkov
27. člen

(1) Upravljavec s sklepom imenuje pooblaščeno osebo za varstvo osebnih podatkov (v nadaljevanju: DPO), ki je pri svojem delu neodvisna od napotkov vodstva upravljavca. Kontaktni podatki o DPO so javno objavljeni na spletni strani upravljavca in je o njih seznanjen tudi Informacijski pooblaščenec kot nadzorni organ. Upravljavec lahko določi tudi namestnika pooblaščene osebe.
(2) Za pooblaščeno osebo za varstvo osebnih podatkov in njenega namestnika je lahko določen posameznik, ki izpolnjuje naslednje pogoje:
1. je poslovno sposoben,
2. ima znanja oziroma praktične izkušnje s področja varstva osebnih podatkov in
3. ni bil pravnomočno obsojen na kazen zapora najmanj šestih mesecev oziroma ni bil pravnomočno obsojen za kaznivo dejanje glede zlorabe osebnih podatkov.
(3) DPO izvaja nadzor nad izvajanjem postopkov in ukrepov, določenih s tem pravilnikom in pri opravljanju svojih nalog upošteva tveganje, povezano z dejanji obdelave, ter naravo, obseg, okoliščine in namene obdelave. Pooblaščena oseba na neodvisen način opravlja naloge iz 39. člena Splošne uredbe in zlasti svetuje pri ocenjevanju tveganj glede varnosti osebnih podatkov v zvezi z vsemi obdelavami osebnih podatkov v zbirkah, ki jih izvaja upravljavec oziroma obdelovalec, pri katerem je določena.
(4) Upravljavec zagotavlja vse potrebno, da je DPO ustrezno in pravočasno vključen v vse zadeve v zvezi z varstvom osebnih podatkov pri upravljavcu.

X. KONČNE DOLOČBE

Začetek veljavnosti
28. člen

(1) Z dnem začetka veljavnosti tega pravilnika preneha veljati Pravilnik o zavarovanju osebnih podatkov, št.: 007-04/2018, z dne 19. 7. 2018.
(2) Ta pravilnik se objavi na oglasni deski upravljavca in na intranet portalu občine in prične veljati naslednji dan po objavi.
(2) Z določbami tega pravilnika morajo biti seznanjeni vsi zaposleni pri upravljavcu, pogodbeni obdelovalci osebnih podatkov in drugi zunanji sodelavci.

V Laškem, dne 23. 11. 2023

Številka: 007-04/2018

OBČINA 1 LAŠKO

Občina Laško
župan
Marko Šantej

.....