

SLUŽBENI GLASNIK OPĆINE ŽUPA DUBROVAČKA

Broj 29	Godina XXVI.	Srebreno, 28. kolovoza 2026.	Uprava i uredništvo: Vukovarska 48, Srebreno, 20207 Mlini, tel. 487 - 476 List izlazi po potrebi.
---------	--------------	------------------------------	---

SADRŽAJ

OPĆINSKI NAČELNIK

01. POLITIKA I PROCEDURA korištenja sustava videonadzora Općine Župa dubrovačka.....	1
02. ODLUKA o imenovanju osoba ovlaštenih za pristup sustavu videonadzora i snimkama Općine Župa dubrovačka.....	19
03. ODLUKA o imenovanju službenika za zaštitu osobnih podataka u Općini Župa dubrovačka.....	23
04. ODLUKA o imenovanju povjerljive osobe i zamjenika povjerljive osobe u Općini Župa dubrovačka.....	24
05. ODLUKA o imenovanju povjerenika za etiku u Općini Župa dubrovačka.....	26

01.

Na temelju članka 24. i članka 32. Uredbe (EU) 2016/679 Europskog parlamenta i Vijeća od 27. travnja 2016. godine o zaštiti pojedinaca u vezi s obradom osobnih podataka i o slobodnom kretanju takvih podataka – Opće uredbe o zaštiti podataka, Zakona o provedbi Opće uredbe o zaštiti podataka („Narodne novine“, broj 42/18), Odluke o korištenju sustava videonadzora javnih površina na području Općine Župa dubrovačka („Službeni glasnik Općine Župa dubrovačka“, broj 26/26), Pravilnika o zaštiti osobnih podataka u Općini Župa dubrovačka („Službeni glasnik Općine Župa dubrovačka“, broj 26/26) i članka 48. Statuta Općine Župa dubrovačka („Službeni glasnik Općine Župa dubrovačka“, broj 8/09, 6/13, 3/18, 4/20, 6/20 – pročišćeni tekst, 5/21 i 9/21 – pročišćeni tekst), Općinski načelnik donosi

POLITIKU I PROCEDURU

KORIŠTENJA SUSTAVA VIDEONADZORA OPĆINE ŽUPA DUBROVAČKA

I. OPĆE ODREDBE

Članak 1.

(1) Ovom Politikom i procedurom korištenja sustava videonadzora, dalje u tekstu: Politika, utvrđuju se operativna, organizacijska i sigurnosna pravila za upravljanje sustavom videonadzora Općine Župa dubrovačka.

(2) Ovom Politikom osobito se uređuju:

1. uloge i odgovornosti osoba uključenih u upravljanje sustavom;
2. dodjela, izmjena i ukidanje prava pristupa;
3. način prijave i korištenja korisničkih računa;
4. pregled slike u stvarnom vremenu i pohranjenih snimki;
5. pretraživanje, izdvajanje, izvoz i dostavljanje snimki;
6. vođenje evidencija o pristupu i korištenju sustava;
7. čuvanje i automatsko brisanje snimki;
8. postupanje po zahtjevima nadležnih tijela i ispitanika;
9. tehničko održavanje i servisiranje sustava;
10. postupanje u slučaju povrede osobnih podataka ili drugog sigurnosnog incidenta;
11. redovita kontrola zakonitosti i sigurnosti sustava.

(3) Svrha ove Politike jest osigurati da se sustav videonadzora koristi zakonito, sigurno, odgovorno i isključivo u unaprijed utvrđene službene svrhe.

(4) Ovom Politikom ne uvode se nove svrhe videonadzora niti nove lokacije kamera. Svrhe, lokacije i pravne osnove moraju prethodno biti utvrđene u skladu s Odlukom o korištenju sustava videonadzora.

(5) Svako korištenje sustava protivno ovoj Politici smatra se neovlaštenim postupanjem.

Članak 2.

(1) Ova Politika primjenjuje se na sve sustave videonadzora kojima upravlja Općina Župa dubrovačka ili se njima u ime Općine upravlja putem ugovorenog izvršitelja obrade.

(2) Ova Politika primjenjuje se na:

1. kamere i drugu opremu za snimanje;
2. uređaje i poslužitelje za prijenos i pohranu snimki;
3. programska rješenja za upravljanje sustavom;
4. korisničke račune i pristupna prava;
5. lokalni i udaljeni pristup sustavu;
6. slike u stvarnom vremenu;
7. pohranjene i izdvojene snimke;
8. medije i uređaje na kojima se snimke privremeno ili trajno nalaze;
9. evidencije pristupa, izvoza, dostavljanja, brisanja i održavanja sustava.

(3) Ovu Politiku dužni su primjenjivati:

1. općinski načelnik;
2. pročelnik Jedinственog upravnog odjela;
3. službenik za zaštitu podataka;
4. osobe odgovorne za upravljanje sustavom videonadzora;
5. osobe ovlaštene za pristup sustavu i snimkama;
6. informatički administratori;
7. službenici i namještenici koji sudjeluju u postupanju sa snimkama;
8. izvršitelji obrade, serviseri i drugi vanjski pružatelji usluga;
9. druge osobe kojima se iznimno odobri pristup sustavu ili pojedinoj snimci.

(4) Osobe iz stavka 3. ovoga članka dužne su postupati u skladu s dodijeljenim ovlastima, dokumentiranim uputama Općine i načelom najmanjeg potrebnog pristupa.

(5) Ova Politika primjenjuje se zajedno s:

1. Odlukom o korištenju sustava videonadzora;
2. Pravilnikom o zaštiti osobnih podataka;
3. odlukom o imenovanju osoba ovlaštenih za pristup sustavu i snimkama;

4. ugovorima s izvršiteljima obrade;
5. tehničkom dokumentacijom sustava;
6. evidencijom lokacija i kamera;
7. drugim odgovarajućim internim aktima i uputama Općine.

(6) U slučaju nesklada između ove Politike i obvezujućeg propisa primjenjuje se važeći propis, a Politika će se bez nepotrebnog odgađanja odgovarajuće izmijeniti.

II. ULOGE I ODGOVORNOSTI

Članak 3.

(1) Općinski načelnik osigurava organizacijske, tehničke i financijske uvjete za zakonito i sigurno korištenje sustava videonadzora.

(2) Općinski načelnik osobito:

1. donosi akte kojima se uređuje videonadzor;
2. odlučuje o uspostavi, izmjeni i prestanku videonadzora na pojedinoj lokaciji;
3. imenuje osobe ovlaštene za pristup sustavu i snimkama;
4. određuje osobu odgovornu za upravljanje sustavom;
5. osigurava potrebne resurse i sigurnosne mjere;
6. odlučuje o provedbi korektivnih mjera nakon nadzora ili incidenta.

(3) Pročelnik Jedinog upravnog odjela:

1. koordinira provedbu ove Politike u radu upravnog tijela;
2. predlaže dodjelu i ukidanje korisničkih prava;
3. osigurava suradnju službenika i odgovornih osoba;
4. prati izvršavanje utvrđenih mjera i rokova;
5. obavještava općinskog načelnika o značajnim nepravilnostima.

(4) Osoba odgovorna za upravljanje sustavom videonadzora:

1. vodi operativni nadzor nad radom sustava;
2. koordinira dodjelu i ukidanje korisničkih računa;
3. vodi ili nadzire vođenje propisanih evidencija;
4. provjerava funkcionalnost kamera i uređaja za pohranu;
5. osigurava provedbu rokova čuvanja i automatskog brisanja snimki;
6. koordinira pregled, izdvajanje i dostavljanje snimki;
7. surađuje sa službenikom za zaštitu podataka i izvršiteljima obrade;
8. odmah prijavljuje uočene nepravilnosti i sigurnosne incidente.

(5) Službenik za zaštitu podataka:

1. savjetuje Općinu o zakonitosti obrade putem videonadzora;
2. daje mišljenje o novim lokacijama i značajnim promjenama sustava;
3. prati usklađenost korištenja sustava s propisima i internim aktima;
4. sudjeluje u procjeni učinka na zaštitu osobnih podataka;
5. sudjeluje u procjeni povreda osobnih podataka;
6. savjetuje pri postupanju po zahtjevima ispitanika;
7. predlaže korektivne i preventivne mjere;
8. surađuje s Agencijom za zaštitu osobnih podataka.

(6) Informatički administrator ili vanjski tehnički održavatelj:

1. održava tehničku ispravnost i sigurnost sustava;
2. provodi odobrene promjene konfiguracije;
3. osigurava sigurnosna ažuriranja i zaštitu korisničkih računa;
4. vodi zapise o servisnim i administrativnim radnjama;
5. ne pregledava sadržaj snimki osim kada je to nužno i posebno odobreno;
6. odmah prijavljuje tehničke kvarove i sigurnosne incidente.

(7) Ovlaštene osobe odgovorne su za zakonitost svakog pojedinačnog pristupa i radnje koju provedu u sustavu.

(8) Imenovanje službenika za zaštitu podataka, odgovorne osobe ili vanjskog izvršitelja ne prenosi na njih odgovornost Općine kao voditelja obrade.

III. KORISNIČKI RAČUNI I PRAVA PRISTUPA

Članak 4.

- (1) Pristup sustavu videonadzora dopušten je samo osobama koje su ovlaštene posebnom pisanom odlukom općinskog načelnika.
- (2) Prije dodjele pristupa mora se utvrditi:
1. postoji li opravdana službena potreba;
 2. kojim lokacijama i kamerama osoba treba pristupati;
 3. treba li osobi pristup slici u stvarnom vremenu ili pohranjenim snimkama;
 4. koje radnje osoba smije provoditi;
 5. koliko dugo ovlaštenje treba trajati;
 6. je li osoba upoznata s pravilima povjerljivosti i sigurnosti.
- (3) Svakoj ovlaštenoj osobi dodjeljuje se zaseban korisnički račun, kada to tehničke mogućnosti sustava dopuštaju.
- (4) Korisnički račun mora biti povezan s konkretnom fizičkom osobom i ne smije se ustupati ili dijeliti s drugim osobama.
- (5) Prava pristupa dodjeljuju se prema načelu najmanjeg potrebnog opsega i mogu obuhvaćati:
1. pregled slike u stvarnom vremenu;
 2. pregled pohranjenih snimki;
 3. pretraživanje snimki;
 4. izdvajanje i izvoz snimki;
 5. upravljanje korisničkim računima;
 6. tehničko održavanje sustava;
 7. druge posebno određene ovlasti.
- (6) Pravo pregleda slike u stvarnom vremenu ne daje automatski pravo pregleda pohranjenih snimki.
- (7) Pravo tehničkog administriranja sustava ne daje automatski pravo pregledavanja, izdvajanja ili dostavljanja sadržaja snimki.
- (8) Privremeni pristup može se dodijeliti za određenu službenu zadaću, događaj ili razdoblje, nakon čega se automatski ili ručno ukida.
- (9) Prava pristupa preispituju se:
1. najmanje jednom godišnje;
 2. nakon promjene radnog mjesta ili poslova;
 3. nakon dulje odsutnosti;
 4. nakon promjene organizacijskog ustroja;
 5. nakon sigurnosnog incidenta;
 6. nakon promjene tehničkog sustava;
 7. kada prestane opravdana službena potreba.
- (10) Korisnički račun mora se bez odgađanja onemogućiti kada:
1. osobi prestane služba, radni ili ugovorni odnos;
 2. osoba promijeni poslove zbog kojih više ne treba pristup;
 3. postoji sumnja na zlouporabu korisničkog računa;
 4. su pristupni podaci izgubljeni ili kompromitirani;
 5. osoba postupa protivno ovoj Politici;
 6. to zahtijevaju drugi opravdani sigurnosni razlozi.
- (11) Zahtjevi i odobrenja za dodjelu, izmjenu i ukidanje pristupa dokumentiraju se i čuvaju u skladu s utvrđenim rokovima.

Članak 5.

- (1) Ovlaštena osoba dužna je pri prijavi u sustav koristiti isključivo vlastito korisničko ime i pripadajuće sredstvo autentifikacije.
- (2) Lozinka za pristup sustavu mora:
 - 1. biti dovoljno složena;
 - 2. biti poznata samo korisniku;
 - 3. razlikovati se od lozinki koje korisnik koristi u privatne svrhe;
 - 4. biti promijenjena kada postoji sumnja da je kompromitirana;
 - 5. biti čuvana na način kojim se sprječava pristup drugih osoba.
- (3) Lozinke se ne smiju:
 - 1. zapisivati na vidljivim mjestima;
 - 2. slati nezaštićenom elektroničkom poštom;
 - 3. priopćavati telefonom ili usmeno neovlaštenim osobama;
 - 4. spremati u nezaštićene dokumente;
 - 5. dijeliti s kolegama, nadređenima, serviserima ili drugim osobama.
- (4) Kada sustav omogućuje višefaktorsku autentifikaciju, ona se primjenjuje najmanje za:
 - 1. administratorske korisničke račune;
 - 2. udaljeni pristup sustavu;
 - 3. korisnike s pravom izvoza ili brisanja snimki;
 - 4. druge račune s proširenim ovlastima.
- (5) Prije pristupa sustavu ovlaštena osoba mora provjeriti nalazi li se na mjestu na kojem neovlaštene osobe ne mogu vidjeti nadzorni zaslon.
- (6) Nadzorni zaslon ne smije ostati bez nadzora dok je korisnik prijavljen u sustav.
- (7) Korisnik se mora odjaviti iz sustava:
 - 1. nakon završetka rada;
 - 2. prije napuštanja radnog mjesta;
 - 3. prije nego što korištenje uređaja preuzme druga osoba;
 - 4. kada uoči neobično ili sumnjivo ponašanje sustava.
- (8) Radne stanice s pristupom videonadzoru moraju imati uključeno automatsko zaključavanje zaslona nakon primjerenog razdoblja neaktivnosti.
- (9) Udaljeni pristup sustavu dopušten je samo:
 - 1. s prethodno odobrenog uređaja;
 - 2. putem sigurnog komunikacijskog kanala;
 - 3. uz odgovarajuću autentifikaciju;
 - 4. kada postoji dokumentirana službena ili tehnička potreba;
 - 5. tijekom vremenski ograničenog razdoblja, kada je to moguće.
- (10) Pristup sustavu putem privatnog računala, mobilnog telefona ili drugog privatnog uređaja nije dopušten, osim kada je takav pristup posebno odobren, tehnički osiguran i evidentiran.
- (11) Zabranjeno je:
 - 1. omogućiti neovlaštenoj osobi uvid u sliku ili snimku;
 - 2. fotografirati ili snimati nadzorni zaslon;
 - 3. koristiti privatne uređaje za pohranu snimki;
 - 4. instalirati neodobrene programe na uređaje sustava;
 - 5. mijenjati položaj, postavke ili područje snimanja kamere bez odobrenja;
 - 6. isključivati sigurnosne zapise ili automatsko brisanje;
 - 7. pregledavati snimke iz znatiželje ili privatnih razloga;
 - 8. pretraživati sustav bez konkretne službene svrhe.
- (12) Svaka sumnja na neovlaštenu prijavu, kompromitiranu lozinku ili zlouporabu korisničkog računa mora se odmah prijaviti osobi odgovornoj za sustav i službeniku za zaštitu podataka.

IV. PREGLED I KORIŠTENJE SNIMKI

Članak 6.

- (1) Pregled slike u stvarnom vremenu dopušten je samo ovlaštenim osobama kojima je takva ovlast potrebna radi obavljanja službenih poslova i ostvarivanja svrhe videonadzora.
- (2) Slika u stvarnom vremenu može se pregledavati osobito radi:
1. zaštite života, zdravlja i sigurnosti osoba;
 2. zaštite imovine, objekata i javnih površina;
 3. uočavanja vandalizma, oštećenja imovine ili drugih protupravnih ponašanja;
 4. uočavanja nepropisnog odlaganja otpada, kada je to utvrđena svrha videonadzora;
 5. pravodobnog obavještanja policije, vatrogasaca, hitne medicinske službe, komunalnog redarstva ili drugog nadležnog tijela;
 6. provjere tehničke ispravnosti kamera i prijenosa slike.
- (3) Pregled slike u stvarnom vremenu ne smije se koristiti za:
1. kontinuirano praćenje određene osobe bez odgovarajuće pravne osnove;
 2. praćenje privatnih navika, kretanja ili ponašanja građana;
 3. nadzor zaposlenika i njihove radne učinkovitosti;
 4. osobne, privatne ili neslužbene svrhe;
 5. fotografiranje ili snimanje nadzornog zaslona privatnim uređajem;
 6. javno prikazivanje slike neovlaštenim osobama.
- (4) Ovlaštena osoba koja putem slike u stvarnom vremenu uoči događaj koji može ugroziti život, zdravlje, sigurnost ili imovinu dužna je, prema okolnostima, bez odgađanja obavijestiti nadležnu službu ili odgovornu osobu.
- (5) Kada je potrebno sačuvati snimku uočenog događaja, ovlaštena osoba mora što prije pokrenuti postupak njezina izdvajanja u skladu s ovom Politikom.
- (6) Nadzorni zasloni moraju biti postavljeni tako da njihov sadržaj nije vidljiv građanima, posjetiteljima i drugim neovlaštenim osobama.
- (7) Prostorija u kojoj se pregledava slika u stvarnom vremenu mora biti odgovarajuće zaštićena od neovlaštenog ulaska i pristupa sustavu.
- (8) Kada se pregled slike u stvarnom vremenu provodi samo povremeno, ovlaštena osoba pristupa sustavu isključivo tijekom vremena potrebnog za ostvarivanje konkretne službene svrhe.

Članak 7.

- (1) Pohranjene snimke smiju se pregledavati samo kada postoji konkretna, dokumentirana i zakonita službena potreba.
- (2) Pregled pohranjenih snimki može se provesti osobito radi:
1. utvrđivanja okolnosti sigurnosnog događaja;
 2. utvrđivanja štete, vandalizma, krađe ili drugog protupravnog ponašanja;
 3. postupanja po zahtjevu policije, suda, državnog odvjetništva, inspekcije ili drugog nadležnog tijela;
 4. postupanja po zahtjevu ispitanika;
 5. istraživanja povrede osobnih podataka ili drugog sigurnosnog incidenta;
 6. postavljanja, ostvarivanja ili obrane pravnih zahtjeva;
 7. provjere opravdane pritužbe na rad sustava videonadzora.
- (3) Prije pregleda pohranjene snimke ovlaštena osoba mora evidentirati ili na drugi način dokumentirati najmanje:
1. svrhu pregleda;
 2. datum i vrijeme pristupa;
 3. lokaciju i kameru;
 4. približno vremensko razdoblje koje će se pregledavati;
 5. predmet, događaj ili zahtjev na koji se pregled odnosi;
 6. pravnu osnovu ili službenu potrebu za pregledom.
- (4) Pregled se mora ograničiti na najmanje vremensko razdoblje i najmanji broj kamera potrebnih za ostvarivanje konkretne svrhe.
- (5) Nije dopušteno pretraživati pohranjene snimke bez unaprijed određene službene svrhe.

- (6) Kada se tijekom pregleda pronađe relevantna snimka, ovlaštena osoba može predložiti njezino izdvajanje iz redovnog ciklusa automatskog brisanja.
- (7) Ako se tijekom pregleda uoče podaci ili događaji koji nisu povezani sa svrhom pregleda, oni se ne smiju dalje koristiti, izdvajati ili dostavljati, osim ako ukazuju na neposrednu opasnost, teško protupravno ponašanje ili drugu okolnost zbog koje postoji zakonska obveza postupanja.
- (8) Pregled snimki u nazočnosti osobe koja nije ovlašten korisnik dopušten je samo kada:
1. za to postoji odgovarajuća pravna osnova;
 2. pregled odobri odgovorna osoba;
 3. identitet i svojstvo prisutne osobe budu prethodno provjereni;
 4. se pregled evidentira;
 5. se zaštite podaci drugih osoba zabilježenih na snimci.
- (9) Nakon završetka pregleda ovlaštena osoba mora se odjaviti iz sustava i, prema potrebi, evidentirati rezultat pregleda.

Članak 8.

- (1) Snimka se smije izdvojiti iz redovnog sustava pohrane samo kada je to nužno radi konkretne i zakonite svrhe.
- (2) O izdvajaju snimke odlučuje osoba odgovorna za upravljanje sustavom ili druga osoba kojoj je takva ovlast izričito dodijeljena.
- (3) Prije izdvajanja snimke mora se utvrditi:
1. svrha i pravna osnova izdvajanja;
 2. lokacija i kamera;
 3. datum i vremensko razdoblje snimke;
 4. razlog zbog kojeg snimku treba sačuvati izvan redovnog roka;
 5. predviđeni primatelj, ako se snimka izdvaja radi dostavljanja;
 6. rok do kojeg će se izdvojena snimka čuvati.
- (4) Izdvojena snimka mora biti ograničena na dio koji je nužan za ostvarivanje konkretne svrhe.
- (5) Kada je tehnički moguće, prije dostavljanja snimke potrebno je zaštititi osobne podatke osoba koje nisu povezane s događajem, osobito zamagljivanjem njihova lika, registarskih oznaka ili drugih identifikacijskih obilježja.
- (6) Izdvojena snimka označava se najmanje sljedećim podacima:
1. internom oznakom;
 2. lokacijom i oznakom kamere;
 3. datumom i vremenom snimanja;
 4. datumom izdvajanja;
 5. razlogom izdvajanja;
 6. imenom ovlaštene osobe koja je provela izdvajanje;
 7. rokom daljnjeg čuvanja.
- (7) Snimke se izvoze samo na:
1. službeni šifrirani prijenosni medij;
 2. zaštićeno službeno mrežno mjesto;
 3. zaštićeni elektronički sustav za razmjenu podataka;
 4. drugi prethodno odobreni i primjereno zaštićeni medij ili kanal.
- (8) Nije dopušten izvoz snimki na privatne USB uređaje, privatna računala, mobilne telefone, privatnu elektroničku poštu ili neodobrene servise za pohranu podataka.
- (9) Lozinka ili drugi podatak potreban za otvaranje zaštićene snimke dostavlja se drugim komunikacijskim kanalom od onoga kojim se dostavlja sama snimka.
- (10) Izdvojene snimke pohranjuju se odvojeno od redovnog sustava snimanja, uz ograničen pristup i odgovarajuću zaštitu od izmjene, kopiranja, gubitka i neovlaštenog otkrivanja.
- (11) Kada je potrebno dokazati vjerodostojnost snimke, čuva se izvorna datoteka, a za pregled ili dostavljanje izrađuje se radna preslika.
- (12) Izvorna izdvojena snimka ne smije se uređivati, skraćivati ili na drugi način mijenjati.

(13) Ako je radi zaštite prava drugih osoba potrebna obrada snimke, primjerice zamagljivanje, obrađena preslika mora se jasno razlikovati od izvorne snimke.

(14) Nakon prestanka svrhe zbog koje je snimka izdvojena, ona se briše ili sigurno uništava, a provedena radnja evidentira.

Članak 9.

(1) Svaki pristup sustavu videonadzora i svaka značajna radnja provedena nad snimkama moraju biti evidentirani na način koji omogućuje naknadnu provjeru zakonitosti i opravdanosti postupanja.

(2) Sustav videonadzora mora, kada je to tehnički moguće, automatski evidentirati:

1. korisnički račun osobe koja je pristupila sustavu;
2. datum i vrijeme prijave i odjave;
3. lokaciju ili uređaj s kojeg je pristup ostvaren;
4. kamere i snimke kojima je korisnik pristupio;
5. provedeno pretraživanje;
6. pregled, izdvajanje, izvoz, kopiranje i brisanje snimke;
7. promjene korisničkih prava;
8. promjene konfiguracije sustava;
9. neuspjele pokušaje prijave;
10. druge sigurnosno značajne radnje.

(3) Ako sustav ne omogućuje automatsko evidentiranje pojedine radnje, ovlaštena osoba dužna je radnju evidentirati u odgovarajućoj pisanoj ili elektroničkoj evidenciji.

(4) Evidencija pregleda i korištenja snimki sadržava najmanje:

1. datum i vrijeme pristupa;
2. ime i prezime ovlaštene osobe;
3. lokaciju i oznaku kamere;
4. vremensko razdoblje pregledane snimke;
5. svrhu i pravnu osnovu pristupa;
6. oznaku predmeta, zahtjeva ili događaja;
7. provedene radnje;
8. podatak je li snimka pronađena i izdvojena;
9. podatak kome je snimka dostavljena;
10. napomenu o završetku postupanja.

(5) Evidencija izdvojenih i dostavljenih snimki sadržava najmanje:

1. internu oznaku snimke;
2. datum izdvajanja;
3. razlog izdvajanja;
4. ime osobe koja je izdvojila snimku;
5. mjesto pohrane;
6. primatelja i pravnu osnovu dostavljanja;
7. datum i način dostave;
8. rok čuvanja;
9. datum i način brisanja ili uništenja.

(6) Evidencija servisnih i administratorskih pristupa vodi se odvojeno ili kao jasno prepoznatljiv dio jedinstvene evidencije.

(7) Zapisi o pristupu i korištenju sustava moraju biti zaštićeni od neovlaštene izmjene i brisanja.

(8) Pristup zapisima imaju samo osobe kojima su oni potrebni radi:

1. sigurnosnog nadzora;
2. unutarnje kontrole;
3. istraživanja sigurnosnog incidenta;
4. postupanja po zahtjevu nadležnog tijela;
5. praćenja usklađenosti sa zaštitom osobnih podataka.

- (9) Zapisi se ne smiju koristiti za kontinuirano praćenje rada zaposlenika, osim kada je provjera nužna radi istraživanja konkretnog incidenta, sumnje na zlouporabu ili druge zakonite svrhe.
- (10) Rok čuvanja zapisa o pristupu određuje se prema sigurnosnim potrebama i odgovarajućim propisima te mora biti dovoljno dug da omogući otkrivanje i istraživanje neovlaštenog postupanja.
- (11) Zapisi o pristupu i korištenju sustava pregledavaju se periodično te uvijek kada postoji sumnja na zlouporabu, sigurnosni incident ili neovlašten pristup.
- (12) O uočenim nepravilnostima odmah se obavještavaju osoba odgovorna za sustav, službenik za zaštitu podataka i, prema potrebi, općinski načelnik.

V. DOSTAVLJANJE SNIMKI I POSTUPANJE PO ZAHTJEVIMA

Članak 10.

- (1) Snimka videonadzora može se dostaviti policiji, sudu, državnom odvjetništvu, inspekcijskom tijelu i drugom nadležnom javnopravnom tijelu kada je dostavljanje propisano zakonom ili je potrebno radi obavljanja poslova iz njihove nadležnosti.
- (2) Zahtjev za dostavljanje snimke u pravilu se podnosi u pisanom ili drugom dokazivom obliku te treba sadržavati najmanje:
1. naziv i kontaktne podatke tijela koje podnosi zahtjev;
 2. ime, prezime i svojstvo službene osobe koja postupa u predmetu;
 3. pravnu osnovu i svrhu traženja snimke;
 4. oznaku službenog predmeta ili postupka;
 5. lokaciju na koju se zahtjev odnosi;
 6. datum i približno vremensko razdoblje tražene snimke;
 7. opis događaja ili drugih okolnosti potrebnih za pronalaženje snimke;
 8. način na koji se traži dostavljanje snimke.
- (3) Zahtjev se bez odgađanja dostavlja osobi odgovornoj za upravljanje sustavom videonadzora i, prema potrebi, službeniku za zaštitu podataka.
- (4) Prije postupanja po zahtjevu provjerava se:
1. identitet i ovlaštenje podnositelja;
 2. postoji li odgovarajuća pravna osnova za dostavljanje;
 3. je li tražena snimka još dostupna;
 4. jesu li lokacija i vremensko razdoblje dovoljno određeni;
 5. je li opseg tražene snimke nužan i razmjeran svrsi;
 6. je li potrebno zaštititi podatke drugih osoba zabilježenih na snimci.
- (5) Nadležnom tijelu dostavlja se samo dio snimke koji je potreban za postupanje u konkretnom predmetu.
- (6) Ako zahtjev obuhvaća šire vremensko razdoblje ili veći broj kamera nego što je potrebno, od podnositelja se može zatražiti dodatno pojašnjenje ili sužavanje zahtjeva.
- (7) U hitnim okolnostima, kada bi odgoda mogla ugroziti život, zdravlje, sigurnost osoba, očuvanje dokaza ili provedbu službenog postupka, po usmenom zahtjevu može se poduzeti privremeno izdvajanje snimke.
- (8) U slučaju iz stavka 7. ovoga članka identitet i svojstvo službene osobe moraju se pouzdano provjeriti, a zahtjev i poduzete radnje moraju se naknadno dokumentirati.
- (9) Snimka se dostavlja:
1. osobnom predajom ovlaštenoj službenoj osobi;
 2. putem službenog zaštićenog elektroničkog sustava;
 3. putem šifriranog medija;
 4. na drugi prethodno odobren i primjereno zaštićen način.
- (10) Prilikom osobne predaje snimke sastavlja se potvrda ili zapisnik o primopredaji koji sadržava najmanje:
1. internu oznaku snimke;
 2. naziv tijela kojem se snimka predaje;

3. oznaku predmeta i svrhu predaje;
 4. opis sadržaja i vremenskog razdoblja snimke;
 5. vrstu i oznaku medija;
 6. datum i vrijeme predaje;
 7. ime, prezime i potpis osobe koja snimku predaje;
 8. ime, prezime, svojstvo i potpis osobe koja snimku preuzima.
- (11) Kod elektroničkog dostavljanja evidentiraju se komunikacijski kanal, datum i vrijeme dostave, primatelj te potvrda primitka, kada je dostupna.
- (12) Snimka se drugim fizičkim i pravnim osobama može dostaviti samo kada za to postoji odgovarajuća pravna osnova, osobito radi postavljanja, ostvarivanja ili obrane pravnih zahtjeva.
- (13) Prije dostavljanja snimke osobi koja nije nadležno javnopravno tijelo mora se procijeniti:
1. opravdanost i nužnost dostavljanja;
 2. prava i interesi drugih osoba zabilježenih na snimci;
 3. mogućnost zamagljivanja ili uklanjanja njihovih identifikacijskih obilježja;
 4. mogućnost omogućavanja kontroliranog uvida umjesto predaje preslike;
 5. druge odgovarajuće mjere zaštite.
- (14) Snimke se ne dostavljaju medijima niti se javno objavljuju radi utvrđivanja ili prozivanja mogućeg počinitelja, osim kada je takvo postupanje izričito dopušteno zakonom ili ga provodi nadležno tijelo u okviru svojih ovlasti.
- (15) O svim zaprimljenim zahtjevima, odlukama i dostavljenim snimkama vodi se evidencija.

Članak 11.

- (1) Osoba koja smatra da je zabilježena sustavom videonadzora može Općini podnijeti zahtjev za ostvarivanje prava u vezi s obradom svojih osobnih podataka.
- (2) Zahtjev se može podnijeti:
1. osobno u pisarnici Općine;
 2. poštom;
 3. elektroničkom poštom;
 4. službeniku za zaštitu podataka;
 5. putem odgovarajućeg elektroničkog obrasca, ako je dostupan.
- (3) Zahtjev treba sadržavati dovoljno informacija za pronalaženje odgovarajuće snimke, a osobito:
1. ime i prezime podnositelja;
 2. kontaktne podatke;
 3. lokaciju na kojoj se osoba nalazila;
 4. datum i približno vrijeme snimanja;
 5. opis izgleda, odjeće, vozila ili drugih okolnosti potrebnih za pronalaženje snimke;
 6. opis prava koje osoba želi ostvariti.
- (4) Kada postoji opravdana sumnja u identitet podnositelja, Općina može zatražiti dodatne informacije potrebne za potvrdu identiteta.
- (5) Pri provjeri identiteta ne smije se tražiti više osobnih podataka nego što je potrebno za sigurno postupanje po zahtjevu.
- (6) Zahtjev se mora podnijeti što prije jer se redovne snimke automatski brišu nakon isteka utvrđenog roka čuvanja.
- (7) Ako je zahtjev dovoljno određen i snimka je još dostupna, osoba odgovorna za upravljanje sustavom procjenjuje treba li snimku privremeno izdvojiti iz redovnog ciklusa brisanja do dovršetka postupanja po zahtjevu.
- (8) Prije izdvajanja snimke potrebno je procijeniti:
1. je li podnositelj vjerojatno zabilježen na snimci;
 2. je li snimku moguće pronaći bez nerazmjernog pregleda velikog broja zapisa;
 3. sadrži li snimka podatke drugih osoba;
 4. postoji li druga svrha ili pravna obveza zbog koje se snimka mora čuvati;
 5. bi li izdvajanje nerazmjerno utjecalo na prava drugih osoba.

(9) Pravo na pristup može se ostvariti:

1. dostavljanjem preslike snimke;
2. omogućavanjem kontroliranog uvida u snimku;
3. dostavljanjem odgovarajuće fotografije ili isječka;
4. pružanjem pisanih informacija o obradi;
5. drugim prikladnim načinom kojim se ostvaruje svrha prava na pristup.

(10) Pri odabiru načina ostvarivanja prava prednost se daje rješenju kojim se istodobno štite prava podnositelja i prava drugih osoba zabilježenih na snimci.

(11) Kada snimka sadržava podatke drugih osoba, prije dostavljanja preslike primjenjuju se odgovarajuće zaštitne mjere, osobito:

1. zamagljivanje ili prekrivanje njihova lika;
2. zamagljivanje registarskih oznaka;
3. uklanjanje zvuka, ako bi sustav iznimno sadržavao zvučni zapis;
4. skraćivanje snimke na potrebno vremensko razdoblje;
5. ograničavanje na kameru ili kadar koji se odnosi na podnositelja.

(12) Ako tehnički nije moguće odgovarajuće zaštititi prava drugih osoba, podnositelju se može omogućiti kontrolirani uvid bez predaje preslike.

(13) Zahtjev za brisanje neće se prihvatiti ako je snimku potrebno čuvati radi:

1. izvršavanja zakonske obveze;
2. izvršavanja zadaće od javnog interesa ili službenih ovlasti Općine;
3. zaštite života, zdravlja ili imovine;
4. vođenja sudskog, upravnog, kaznenog, prekršajnog, inspekcijskog ili drugog postupka;
5. postavljanja, ostvarivanja ili obrane pravnih zahtjeva;
6. zaštite prava i sloboda drugih osoba.

(14) Zahtjev za ograničenje obrade može se prihvatiti tako da se snimka izdvoji, zaštititi od redovne uporabe i obrađuje samo u dopuštene svrhe dok ograničenje traje.

(15) Na zahtjev se odgovara bez nepotrebnog odgađanja, a najkasnije u roku od mjesec dana od njegova zaprimanja.

(16) Rok iz stavka 15. ovoga članka može se, prema potrebi, produljiti za dodatna dva mjeseca, uzimajući u obzir složenost i broj zahtjeva, o čemu se podnositelj obavještava unutar prvog mjeseca.

(17) Ako Općina ne postupi po zahtjevu, podnositelju se dostavljaju razlozi nepostupanja te informacije o mogućnosti podnošenja pritužbe Agenciji za zaštitu osobnih podataka i traženja sudske zaštite.

(18) O svim zahtjevima ispitanika, poduzetim radnjama, odlukama i odgovorima vodi se evidencija.

VI. ČUVANJE I BRISANJE SNIMKI

Članak 12.

(1) Snimke videonadzora čuvaju se samo onoliko dugo koliko je potrebno za ostvarivanje svrhe zbog koje su prikupljene.

(2) Redovni rok čuvanja utvrđuje se za svaku lokaciju pojedinačno i evidentira u:

1. evidenciji lokacija i kamera;
2. evidenciji aktivnosti obrade;
3. tehničkim postavkama sustava;
4. dokumentaciji procjene nužnosti i razmjernosti.

(3) Pri određivanju roka čuvanja uzimaju se u obzir:

1. konkretna svrha videonadzora;
2. vrsta i učestalost događaja zbog kojih je sustav uveden;
3. razdoblje u kojem se događaj uobičajeno može uočiti ili prijaviti;
4. osjetljivost lokacije;
5. broj osoba koje prolaze područjem snimanja;

6. rizici za privatnost i druga prava osoba;
 7. tehničke mogućnosti sustava;
 8. načelo ograničenja pohrane.
- (4) Redovni rok čuvanja snimki u pravilu iznosi najviše **30 dana**.
- (5) Za pojedinu lokaciju može se utvrditi kraći rok kada je on dovoljan za ostvarivanje svrhe videonadzora.
- (6) Rok dulji od 30 dana može se odrediti samo kada za to postoji dokumentirana i opravdana potreba, uz prethodno mišljenje službenika za zaštitu podataka.
- (7) Snimke se ne smiju čuvati dulje od šest mjeseci, osim ako:
1. je drugim zakonom propisan dulji rok;
 2. su izdvojene kao dokaz u sudskom, upravnom, kaznenom, prekršajnom, inspekcijskom ili drugom postupku;
 3. su potrebne radi postavljanja, ostvarivanja ili obrane pravnih zahtjeva;
 4. je njihovo privremeno čuvanje potrebno radi postupanja po pravodobno zaprimljenom zahtjevu ispitanika;
 5. postoji druga obvezujuća pravna osnova za daljnje čuvanje.
- (8) Sustav mora biti postavljen tako da nakon isteka redovnog roka automatski briše ili prepisuje snimke novim sadržajem.
- (9) Automatsko brisanje ne smije se ručno isključivati ili produljivati bez dokumentiranog odobrenja i opravdane službene potrebe.
- (10) Osoba odgovorna za sustav najmanje jednom godišnje provjerava:
1. odgovaraju li stvarne tehničke postavke utvrđenim rokovima;
 2. provodi li se automatsko brisanje pravilno;
 3. postoje li snimke koje se čuvaju dulje od dopuštenog roka;
 4. postoji li za svako produljeno čuvanje odgovarajuće obrazloženje.
- (11) O uočenim nepravilnostima odmah se obavještavaju osoba odgovorna za sustav, službenik za zaštitu podataka i tehnički održavatelj.

Članak 13.

- (1) Izdvojena snimka čuva se odvojeno od redovnog ciklusa pohrane samo dok postoji konkretna svrha zbog koje je izdvojena.
- (2) Za svaku izdvojenu snimku utvrđuje se:
1. razlog i pravna osnova izdvajanja;
 2. osoba ili tijelo koje je zatražilo izdvajanje;
 3. predmet ili događaj na koji se odnosi;
 4. mjesto i način pohrane;
 5. osobe koje imaju pravo pristupa;
 6. rok ponovnog pregleda potrebe čuvanja;
 7. datum ili kriterij brisanja.
- (3) Izdvojena snimka može se čuvati do:
1. njezine predaje nadležnom tijelu, kada Općina nema potrebu zadržati presliku;
 2. pravomoćnog ili konačnog završetka postupka;
 3. isteka rokova za pokretanje ili vođenje odgovarajućeg postupka;
 4. prestanka potrebe za postavljanjem, ostvarivanjem ili obranom pravnih zahtjeva;
 5. dovršetka postupanja po zahtjevu ispitanika;
 6. prestanka druge zakonite svrhe zbog koje je izdvojena.
- (4) Potreba daljnjeg čuvanja izdvojene snimke preispituje se najmanje jednom godišnje, a po potrebi i češće.
- (5) Nakon prestanka svrhe čuvanja snimka se briše bez nepotrebnog odgađanja.
- (6) Brisanje mora biti provedeno na način kojim se sprječava uobičajena obnova, ponovno korištenje ili neovlašten pristup sadržaju.
- (7) Ako se snimka nalazi na prijenosnom mediju koji se neće ponovno koristiti, medij se fizički uništava ili zbrinjava na siguran način.

(8) Ako se službeni medij ponovno koristi, prije ponovne uporabe mora se provesti sigurno brisanje njegova sadržaja.

(9) Brisanje izdvojene snimke evidentira se navođenjem najmanje:

1. interne oznake snimke;
2. razloga prestanka čuvanja;
3. datuma brisanja;
4. načina brisanja ili uništavanja;
5. imena osobe koja je provela ili potvrdila brisanje.

(10) Ako je snimka dostavljena drugom tijelu ili primatelju, Općina nije odgovorna za rokove njezina daljnjeg čuvanja kod toga primatelja, ali evidentira komu, kada i na kojoj pravnoj osnovi je snimka dostavljena.

(11) Radne i privremene preslike snimki moraju se obrisati odmah nakon završetka radnje zbog koje su izrađene.

(12) Snimke se ne smiju trajno čuvati radi moguće buduće uporabe ili stvaranja arhive događaja.

VII. ODRŽAVANJE SUSTAVA I SIGURNOSNI INCIDENTI

Članak 14.

(1) Sustav videonadzora mora se redovito održavati radi osiguravanja njegove tehničke ispravnosti, sigurnosti, dostupnosti i pravilne primjene utvrđenih rokova čuvanja snimki.

(2) Održavanje sustava može obavljati ovlaštena osoba Općine ili vanjski pružatelj usluge s kojim je Općina uredila međusobna prava i obveze.

(3) Kada vanjski pružatelj usluge tijekom održavanja može pristupiti osobnim podacima, smatra se izvršiteljem obrade te se odnos s njim uređuje pisanim ugovorom u skladu s člankom 28. Opće uredbe o zaštiti podataka.

(4) Redovito održavanje osobito obuhvaća:

1. provjeru rada kamera i kvalitete slike;
2. provjeru točnosti datuma i vremena sustava;
3. provjeru smjera, kuta i područja snimanja;
4. provjeru funkcionalnosti maskiranja i zatamnjenja prostora koji se ne smiju snimati;
5. provjeru uređaja i kapaciteta za pohranu;
6. provjeru pravilnog automatskog brisanja snimki;
7. provjeru korisničkih računa i prava pristupa;
8. provjeru zapisa o pristupu i sigurnosnih upozorenja;
9. sigurnosno ažuriranje programske i druge opreme;
10. provjeru zaštite udaljenog pristupa;
11. provjeru fizičke zaštite uređaja i prostorija;
12. druge radnje potrebne za siguran i pouzdan rad sustava.

(5) Servisiranje i održavanje planiraju se, kada je moguće, tako da se radnje provedu bez pristupa stvarnim snimkama.

(6) Kada je pristup stvarnim snimkama nužan radi utvrđivanja ili otklanjanja tehničkog problema, pristup mora biti:

1. prethodno odobren;
2. ograničen na najmanji potreban opseg;
3. vremenski ograničen;
4. proveden pod nadzorom ovlaštene osobe Općine, kada je to moguće;
5. evidentiran u zapisima sustava i servisnom zapisniku.

(7) Vanjski održavatelj ne smije samostalno pregledavati, kopirati, izdvajati, mijenjati ili dostavljati snimke.

(8) Za testiranje sustava u pravilu se koriste testni podaci ili slika koja ne sadržava osobne podatke. Stvarne snimke mogu se koristiti samo kada je to nužno i kada se primijene odgovarajuće mjere zaštite.

(9) Nakon završetka servisnog zahvata potrebno je provjeriti:

1. jesu li kamere pravilno usmjerene;
 2. jesu li rokovi čuvanja ostali pravilno postavljeni;
 3. jesu li aktivni sigurnosni zapisi;
 4. jesu li korisnička prava ostala nepromijenjena;
 5. je li uklonjen privremeni pristup serviseru;
 6. radi li sustav u skladu s utvrđenom svrhom.
- (10) O svakom servisnom zahvatu vodi se zapisnik koji sadržava najmanje:
1. datum i vrijeme zahvata;
 2. naziv lokacije i sustava;
 3. opis utvrđenog problema;
 4. opis provedenih radnji;
 5. ime osobe koja je provela zahvat;
 6. podatak je li ostvaren pristup stvarnim snimkama;
 7. podatak jesu li mijenjane postavke sustava;
 8. rezultat provjere nakon završetka zahvata;
 9. uočene rizike i preporučene dodatne mjere.
- (11) Ako se tijekom održavanja uoči sigurnosni nedostatak, neovlašten pristup, nepravilno snimanje ili druga moguća povreda osobnih podataka, održavatelj je dužan odmah obavijestiti osobu odgovornu za sustav i službenika za zaštitu podataka.
- (12) Udaljeni pristup vanjskog održavatelja mora se omogućiti samo kada je potreban za konkretan zahvat te se mora isključiti nakon njegova završetka.

Članak 15.

- (1) Kvarom sustava smatra se svaki tehnički događaj zbog kojeg kamera, uređaj za pohranu, programsko rješenje, komunikacijska veza ili druga sastavnica sustava ne radi pravilno ili nije dostupna.
- (2) Kvarom se osobito smatra:
1. prestanak snimanja pojedine kamere;
 2. gubitak ili značajno smanjenje kvalitete slike;
 3. prikaz netočnog datuma ili vremena;
 4. nepravilno usmjerenje kamere;
 5. prestanak automatskog brisanja snimki;
 6. nedostupnost pohranjenih snimki;
 7. popunjavanje raspoloživog prostora za pohranu;
 8. neuspjela prijava ovlaštenih korisnika;
 9. kvar sigurnosnih zapisa;
 10. neovlaštena ili neočekivana promjena konfiguracije;
 11. prekid električnog napajanja ili komunikacijske veze;
 12. druga nepravilnost koja utječe na zakonitost, sigurnost ili učinkovitost sustava.
- (3) Osoba koja uoči kvar dužna je bez odgađanja obavijestiti osobu odgovornu za upravljanje sustavom ili tehničkog održavatelja.
- (4) Prijava kvara treba sadržavati, ako su podaci poznati:
1. datum i vrijeme uočavanja;
 2. lokaciju i oznaku kamere ili uređaja;
 3. opis problema;
 4. podatak je li sustav potpuno ili djelomično nedostupan;
 5. moguće posljedice;
 6. radnje koje su već poduzete.
- (5) Osoba odgovorna za sustav procjenjuje:
1. utječe li kvar na ostvarivanje svrhe videonadzora;
 2. jesu li snimke izgubljene, oštećene ili nedostupne;
 3. postoji li mogućnost neovlaštenog pristupa;
 4. predstavlja li događaj moguću povredu osobnih podataka;

5. treba li pojedinu kameru ili dio sustava privremeno isključiti;
 6. treba li obavijestiti službenika za zaštitu podataka ili druge odgovorne osobe.
- (6) Otklanjanje kvara provodi se prema njegovoj hitnosti, mogućim posljedicama i važnosti lokacije.
- (7) Ako kvar uzrokuje snimanje prostora koji nije obuhvaćen utvrđenom svrhom, kamera se mora odmah preusmjeriti, maskirati ili privremeno isključiti.
- (8) Ako sustav ne provodi pravilno automatsko brisanje snimki, potrebno je bez odgađanja:
1. ograničiti pristup snimkama;
 2. utvrditi opseg prekomjerno sačuvanih podataka;
 3. provesti sigurno brisanje nakon otklanjanja kvara;
 4. dokumentirati uzrok i poduzete radnje;
 5. procijeniti predstavlja li događaj povredu osobnih podataka.
- (9) Ako su snimke koje su potrebne za službeni postupak izgubljene ili nedostupne, o tome se obavještava odgovorna osoba za predmet i, prema potrebi, nadležno tijelo.
- (10) Privremena nedostupnost sustava ne smije biti razlog za uvođenje neodobrenog zamjenskog snimanja privatnim uređajima ili drugim sustavima koji nisu obuhvaćeni aktima Općine.
- (11) O značajnim kvarovima vodi se evidencija koja sadržava opis događaja, trajanje nedostupnosti, posljedice, provedene radnje i datum ponovne uspostave sustava.
- (12) Nakon otklanjanja značajnog kvara provodi se provjera rada sustava i, prema potrebi, analiza uzroka radi sprječavanja ponavljanja istog događaja.

Članak 16.

- (1) Povredom osobnih podataka smatra se povreda sigurnosti koja dovodi ili može dovesti do slučajnog ili nezakonitog uništenja, gubitka, izmjene, neovlaštenog otkrivanja ili pristupa snimkama i drugim osobnim podacima iz sustava videonadzora.
- (2) Sigurnosnim incidentom osobito se smatra:
1. neovlašten pregled snimke;
 2. pregled snimke iz privatnih ili neslužbenih razloga;
 3. korištenje tuđeg korisničkog računa;
 4. otkrivanje ili gubitak pristupnih podataka;
 5. neovlašteno kopiranje, izvoz ili dostavljanje snimke;
 6. fotografiranje ili snimanje nadzornog zaslona privatnim uređajem;
 7. neovlaštena javna objava snimke;
 8. krađa ili gubitak uređaja ili medija sa snimkama;
 9. neovlaštena izmjena ili brisanje snimki;
 10. gubitak dostupnosti snimki potrebnih za službeni postupak;
 11. neovlašteni udaljeni pristup;
 12. zlonamjerni informatički napad;
 13. nepravilno postupanje izvršitelja obrade;
 14. svaki drugi događaj koji ugrožava povjerljivost, cjelovitost ili dostupnost podataka.
- (3) Svaka osoba koja sazna za mogući sigurnosni incident dužna ga je prijaviti odmah, neovisno o tome jesu li poznate sve okolnosti i posljedice.
- (4) Prijava se dostavlja:
1. osobi odgovornoj za upravljanje sustavom;
 2. službeniku za zaštitu podataka;
 3. neposredno nadređenoj osobi;
 4. tehničkom održavatelju, ako je potrebno radi zaustavljanja incidenta.
- (5) Nakon zaprimanja prijave bez odgađanja se poduzimaju mjere radi:
1. zaustavljanja i ograničavanja incidenta;
 2. sprječavanja daljnjeg neovlaštenog pristupa;
 3. zaštite snimki i drugih dokaza;
 4. onemogućavanja kompromitiranih korisničkih računa;
 5. promjene lozinki i drugih pristupnih podataka;

6. utvrđivanja uzroka, opsega i posljedica događaja;
 7. utvrđivanja osoba i snimki obuhvaćenih incidentom;
 8. sprječavanja ponavljanja događaja.
- (6) Službenik za zaštitu podataka koordinira procjenu povrede u suradnji s osobom odgovornom za sustav, tehničkim stručnjacima, izvršiteljem obrade i drugim osobama čije je sudjelovanje potrebno.
- (7) Pri procjeni povrede osobito se uzimaju u obzir:
1. vrsta i opseg incidenta;
 2. sadržaj snimki;
 3. broj pogođenih osoba;
 4. mogućnost identifikacije osoba;
 5. jesu li pogođene snimke djece ili drugih ranjivih osoba;
 6. mogućnost javne objave ili daljnje zlouporabe;
 7. moguće posljedice za privatnost, sigurnost i ugled osoba;
 8. mjere koje su poduzete radi ograničavanja posljedica.
- (8) Kada je vjerojatno da će povreda prouzročiti rizik za prava i slobode fizičkih osoba, Općina će o povredi izvijestiti Agenciju za zaštitu osobnih podataka bez nepotrebnog odgađanja i, ako je izvedivo, najkasnije u roku od 72 sata od saznanja za povredu.
- (9) Ako se prijava Agenciji ne podnese u roku od 72 sata, uz prijavu se navode razlozi zakašnjenja.
- (10) Kada je vjerojatno da će povreda prouzročiti visok rizik za prava i slobode fizičkih osoba, Općina će bez nepotrebnog odgađanja obavijestiti pogođene osobe, osim ako su ispunjeni uvjeti prema kojima takvo obavješćivanje nije potrebno.
- (11) Općina vodi evidenciju svih povreda osobnih podataka, uključujući povrede koje nisu prijavljene Agenciji ili pogođenim osobama.
- (12) Evidencija povrede sadržava najmanje:
1. datum i vrijeme nastanka i saznanja za povredu;
 2. opis povrede;
 3. kategorije i približan broj pogođenih osoba;
 4. kategorije i približan broj pogođenih snimki ili zapisa;
 5. moguće posljedice;
 6. procjenu rizika;
 7. poduzete korektivne i preventivne mjere;
 8. odluku o prijavi ili neprijavljivanju Agenciji;
 9. odluku o obavješćivanju pogođenih osoba;
 10. obrazloženje donesenih odluka;
 11. datum zatvaranja incidenta.
- (13) Vanjski izvršitelj obrade dužan je o svakom incidentu odmah obavijestiti Općinu, u roku koji omogućuje Općini pravodobno ispunjavanje njezinih zakonskih obveza.
- (14) Osoba koja incident prijavi u dobroj vjeri ne smije zbog same prijave biti stavljena u nepovoljniji položaj.

VIII. EDUKACIJA, NADZOR I ZAVRŠNE ODREDBE

Članak 17.

- (1) Prije dobivanja pristupa sustavu videonadzora ovlaštena osoba mora biti upoznata s ovom Politikom, dodijeljenim ovlastima, obvezom povjerljivosti i postupkom prijave sigurnosnog incidenta.
- (2) Edukacija ovlaštenih osoba provodi se:
1. prije prvog pristupa sustavu;
 2. najmanje jednom godišnje;
 3. nakon značajne izmjene sustava ili internih pravila;
 4. nakon povrede osobnih podataka ili utvrđene nepravilnosti;

5. kada se utvrdi potreba za dodatnim osposobljavanjem.
- (3) Edukacija osobito obuhvaća:
 1. svrhe i pravne osnove videonadzora;
 2. dopuštene i zabranjene načine korištenja sustava;
 3. sigurno korištenje korisničkih računa;
 4. pregled, izdvajanje i dostavljanje snimki;
 5. zaštitu prava osoba zabilježenih na snimkama;
 6. prepoznavanje i prijavu sigurnosnih incidenata;
 7. obvezu povjerljivosti;
 8. posljedice neovlaštenog postupanja.
- (4) O provedenim edukacijama vodi se evidencija koja sadržava datum, sadržaj edukacije, osobu koja ju je provela i popis sudionika.
- (5) Najmanje jednom godišnje provodi se pregled zakonitosti, opravdanosti, sigurnosti i učinkovitosti sustava videonadzora.
- (6) Godišnji pregled obuhvaća najmanje:
 1. opravdanost daljnjeg korištenja videonadzora na svakoj lokaciji;
 2. usklađenost stvarnog područja snimanja s utvrđenom svrhom;
 3. položaj i usmjerenje kamera;
 4. funkcionalnost maskiranja i zatamnjenja;
 5. rokove čuvanja i automatsko brisanje snimki;
 6. korisničke račune i prava pristupa;
 7. zapise o pristupima i korištenju snimki;
 8. evidenciju izdvojenih i dostavljenih snimki;
 9. ugovore i postupanje izvršitelja obrade;
 10. sigurnosne incidente i povrede osobnih podataka;
 11. zahtjeve ispitanika i nadležnih tijela;
 12. stanje obavijesti o videonadzoru;
 13. provedbu prethodno utvrđenih mjera.
- (7) Godišnji pregled koordinira osoba odgovorna za sustav u suradnji sa službenikom za zaštitu podataka, tehničkim održavateljem i drugim odgovornim osobama.
- (8) O provedenom pregledu sastavlja se izvješće koje sadržava:
 1. pregledano područje i dokumentaciju;
 2. utvrđeno stanje;
 3. utvrđene nedostatke i rizike;
 4. preporučene korektivne i preventivne mjere;
 5. odgovorne osobe;
 6. rokove za provedbu mjera;
 7. prijedlog nastavka, izmjene, ograničenja ili prestanka videonadzora na pojedinoj lokaciji.
- (9) Izvanredni pregled provodi se osobito nakon:
 1. značajne povrede osobnih podataka;
 2. pritužbe ispitanika;
 3. utvrđenog neovlaštenog pristupa;
 4. promjene područja ili svrhe snimanja;
 5. značajne tehničke promjene;
 6. naloga ili preporuke nadležnog tijela;
 7. saznanja o novom riziku.
- (10) Ako se utvrdi visok ili neposredan rizik za prava i slobode osoba, pristup sustavu ili rad pojedine kamere privremeno se obustavlja do otklanjanja nedostatka.
- (11) Utvrđeni nedostaci uklanjaju se u rokovima određenima u izvješću, ovisno o njihovoj ozbiljnosti i mogućim posljedicama.
- (12) Rezultati godišnjeg pregleda dostavljaju se općinskom načelniku koji odlučuje o potrebnim organizacijskim, tehničkim i financijskim mjerama.

Članak 18.

- (1) Ova Politika obvezna je za sve osobe koje upravljaju sustavom videonadzora, pristupaju slici u stvarnom vremenu ili pohranjenim snimkama te sudjeluju u održavanju sustava.
- (2) Ovlaštene osobe dužne su prije dodjele pristupa potpisati izjavu kojom potvrđuju da su upoznate s ovom Politikom i obvezom čuvanja povjerljivosti.
- (3) Postojeći korisnički računi i prava pristupa pregledat će se i uskladiti s ovom Politikom u roku od 30 dana od dana njezina stupanja na snagu.
- (4) Postojeće tehničke postavke sustava, uključujući rokove čuvanja, automatsko brisanje, sigurnosne zapise i udaljeni pristup, pregledat će se u roku od 60 dana.
- (5) Ugovori s vanjskim izvršiteljima obrade i tehničkim održavateljima pregledat će se i, prema potrebi, uskladiti u roku od tri mjeseca.
- (6) Za provedbu ove Politike uspostavljaju se i vode najmanje sljedeće evidencije i obrasci:
1. evidencija lokacija i kamera;
 2. evidencija ovlaštenih osoba i korisničkih prava;
 3. evidencija pristupa i pregleda snimki;
 4. obrazac zahtjeva za pregled ili izdvajanje snimke;
 5. evidencija izdvojenih snimki;
 6. evidencija zahtjeva nadležnih tijela i ispitanika;
 7. zapisnik o primopredaji snimke;
 8. evidencija servisnih zahvata;
 9. evidencija kvarova i nedostupnosti sustava;
 10. evidencija povreda osobnih podataka;
 11. obrazac godišnjeg pregleda sustava.
- (7) Obrasci i evidencije iz stavka 6. ovoga članka mogu se tehnički prilagođavati potrebama Općine, pod uvjetom da sadržavaju podatke potrebne za dokazivanje zakonitog i sigurnog postupanja.
- (8) Za pravilnu provedbu Politike odgovorne su sve osobe u okviru svojih dodijeljenih poslova i ovlasti.
- (9) Službenik za zaštitu podataka pruža savjete o primjeni ove Politike, ali odgovornost za zakonitost pojedinačnog pristupa i radnje ostaje na osobi koja je pristup ili radnju provela i odgovornim osobama Općine.
- (10) Neovlašteno korištenje sustava ili postupanje protivno ovoj Politici može predstavljati povredu službene ili radne dužnosti, povredu ugovorne obveze te osnovu za druge odgovarajuće postupke.
- (11) Na pitanja koja nisu uređena ovom Politikom primjenjuju se:
1. Opća uredba o zaštiti podataka;
 2. Zakon o provedbi Opće uredbе o zaštiti podataka;
 3. propisi kojima se uređuje privatna i tehnička zaštita;
 4. Odluka o korištenju sustava videonadzora;
 5. Pravilnik o zaštiti osobnih podataka Općine Župa dubrovačka;
 6. drugi odgovarajući propisi i akti Općine.
- (12) Ova Politika stupa na snagu danom donošenja.

KLASA: 650-05/26-01/9
URBROJ: 2117-8-01-26-2
Srebreno, 28. kolovoza 2026.

OPĆINSKI NAČELNIK

Marko Miloslavić, v.r.

Na temelju članka 29. Uredbe (EU) 2016/679 Europskog parlamenta i Vijeća od 27. travnja 2016. godine o zaštiti pojedinaca u vezi s obradom osobnih podataka i o slobodnom kretanju takvih podataka – Opće uredbe o zaštiti podataka, članka 28. Zakona o provedbi Opće uredbe o zaštiti podataka („Narodne novine“, broj 42/18), članka 9. i 19. Odluke o korištenju sustava videonadzora javnih površina na području Općine Župa dubrovačka („Službeni glasnik Općine Župa dubrovačka“, broj 26/26), Pravilnika o zaštiti osobnih podataka u Općini Župa dubrovačka („Službeni glasnik Općine Župa dubrovačka“, broj 26/26) i članka 48. Statuta Općine Župa dubrovačka („Službeni glasnik Općine Župa dubrovačka“, broj 8/09, 6/13, 3/18, 4/20, 6/20 – pročišćeni tekst, 5/21 i 9/21 – pročišćeni tekst), Općinski načelnik donosi

O D L U K U

O IMENOVANJU OSOBA OVLAŠTENIH ZA PRISTUP SUSTAVU VIDEONADZORA I SNIMKAMA OPĆINE ŽUPA DUBROVAČKA

Članak 1.

(1) Za pristup sustavu videonadzora i snimkama Općine Župa dubrovačka ovlašćuju se sljedeće osobe:

1. Ovlaštena osoba

Ime i prezime: FRANKO MEKIŠIĆ

Radno mjesto ili druga osnova ovlaštenja: Pročelnik Jedininstvenog Upravnog Odjela

Lokacije ili dijelovi sustava kojima osoba smije pristupati: Sve lokacije

2. Ovlaštena osoba

Ime i prezime: MARIO ZDRAULIĆ

Radno mjesto ili druga osnova ovlaštenja: Referent – Komunalno pomorski redar

Lokacije ili dijelovi sustava kojima osoba smije pristupati: Sve lokacije

3. Ovlaštena osoba

Ime i prezime: LUKA HERMAN

Radno mjesto ili druga osnova ovlaštenja: Referent - Komunalni redar

Lokacije ili dijelovi sustava kojima osoba smije pristupati: Sve lokacije

4. Ovlaštena osoba

Ime i prezime: BORIS POPOVIĆ

Radno mjesto ili druga osnova ovlaštenja: Referent – Prometni

redar

Lokacije ili dijelovi sustava kojima osoba smije pristupati: Sve lokacije

(2) Ako se za pristup sustavu ovlašćuje više osoba, njihova imena, radna mjesta, lokacije i opseg ovlasti mogu se utvrditi u Prilogu 1. ove Odluke.

(3) Prilog 1. iz stavka 2. ovoga članka sastavni je dio ove Odluke.

(4) Osobe iz stavka 1. ovoga članka smiju pristupati sustavu i snimkama samo u okviru ovlasti dodijeljenih ovom Odlukom.

Članak 2.

- (1) Svakoj imenovanoj osobi dodjeljuje se samo ona razina pristupa koja joj je nužna radi obavljanja službenih poslova.
- (2) Ovlaštenje može obuhvaćati jednu ili više sljedećih radnji:
 1. pregled slike u stvarnom vremenu;
 2. pregled pohranjenih snimki;
 3. pretraživanje snimki prema lokaciji, datumu i vremenu;
 4. izdvajanje snimki iz redovnog ciklusa brisanja;
 5. izvoz i izradu službene preslike snimke;
 6. dostavljanje snimke policiji, sudu, državnom odvjetništvu, inspekcijskom tijelu ili drugom ovlaštenom primatelju;
 7. omogućavanje kontroliranog uvida ispitaniku;
 8. upravljanje korisničkim računima i pravima pristupa;
 9. tehničko održavanje sustava;
 10. pregled zapisa o pristupu i drugim radnjama u sustavu.
- (3) Opseg ovlasti pojedine osobe određuje se u Prilogu 1. ove Odluke.
- (4) Pravo pregleda slike u stvarnom vremenu ne uključuje automatski pravo pregleda pohranjenih snimki.
- (5) Pravo pregleda pohranjenih snimki ne uključuje automatski pravo njihova izdvajanja, izvoza, kopiranja ili dostavljanja.
- (6) Administratorska ili tehnička prava ne daju automatski pravo pregledavanja sadržaja snimki.
- (7) Izdvajanje, izvoz i dostavljanje snimki može obavljati samo osoba kojoj je takva ovlast izričito dodijeljena.
- (8) Ovlaštena osoba smije pristupati samo lokacijama i kamerama koje su navedene u ovoj Odluci ili njezinu prilogu.

Članak 3.

- (1) Prije omogućavanja pristupa sustavu videonadzora ovlaštena osoba mora:
 1. biti upoznata s Odlukom o korištenju sustava videonadzora;
 2. biti upoznata s Politikom i procedurom korištenja sustava videonadzora;
 3. biti upoznata s pravilima zaštite osobnih podataka i informacijske sigurnosti;
 4. potpisati izjavu o povjerljivosti i odgovornom korištenju sustava;
 5. proći odgovarajuću edukaciju;
 6. biti upoznata s postupkom prijave sigurnosnog incidenta;
 7. preuzeti vlastite pristupne podatke na siguran način.
- (2) Svakoj ovlaštenoj osobi dodjeljuje se zaseban korisnički račun, kada to tehničke mogućnosti sustava dopuštaju.
- (3) Zajednički korisnički računi ne smiju se koristiti, osim kada zbog tehničkih obilježja sustava nije moguće osigurati pojedinačne račune i kada su uvedene druge mjere kojima se može utvrditi identitet osobe koja je pristupila sustavu.
- (4) Ovlaštena osoba ne smije ustupiti svoje korisničko ime, lozinku, pristupnu karticu ili drugo sredstvo autentifikacije drugoj osobi.
- (5) Udaljeni pristup sustavu može se omogućiti samo osobi kojoj je takva ovlast izričito dodijeljena, putem prethodno odobrenog uređaja i sigurnog komunikacijskog kanala.
- (6) Osoba odgovorna za tehničko upravljanje sustavom omogućit će pristup tek nakon što zaprimi ovu Odluku i potvrdi da su ispunjeni uvjeti iz stavka 1. ovoga članka.

Članak 4.

- (1) Ovlaštena osoba dužna je:
 1. pristupati sustavu samo kada postoji konkretna službena potreba;
 2. koristiti snimke isključivo u svrhe utvrđene odgovarajućim propisima i aktima Općine;
 3. ograničiti pregled na najmanji potreban broj kamera i najkraće potrebno vremensko razdoblje;

4. čuvati povjerljivost snimki i svih podataka do kojih dođe;
5. spriječiti pristup neovlaštenim osobama;
6. koristiti isključivo vlastiti korisnički račun;
7. odjaviti se iz sustava nakon završetka rada;
8. bez odgode prijaviti sumnju na neovlašten pristup, gubitak pristupnih podataka ili drugi sigurnosni incident;
9. postupati prema uputama Općine kao voditelja obrade;
10. sudjelovati u edukacijama i provjerama usklađenosti.

(2) Ovlaštenoj osobi zabranjeno je:

1. pregledavati snimke iz znatiželje, privatnih ili drugih neslužbenih razloga;
2. pratiti određenu osobu bez konkretne pravne osnove i službene potrebe;
3. fotografirati ili snimati nadzorni zaslon privatnim uređajem;
4. izrađivati neodobrene preslike snimki;
5. pohranjivati snimke na privatne uređaje ili korisničke račune;
6. slati snimke privatnom elektroničkom poštom ili putem neodobrenih komunikacijskih aplikacija;
7. dostavljati ili pokazivati snimke neovlaštenim osobama;
8. objavljivati snimke na mrežnim stranicama, društvenim mrežama ili u medijima;
9. mijenjati položaj kamera, rokove čuvanja, korisnička prava ili sigurnosne postavke bez odobrenja;
10. brisati ili mijenjati zapise o pristupu sustavu;
11. koristiti snimke protivno svrsi videonadzora.

(3) Obveza povjerljivosti traje i nakon prestanka ovlaštenja, službe, radnog odnosa ili drugog odnosa s Općinom.

(4) Neovlašteno korištenje sustava može predstavljati povredu službene ili radne dužnosti, povredu ugovorne obveze, povredu propisa o zaštiti osobnih podataka i osnovu za druge odgovarajuće postupke.

Članak 5.

(1) Svaki pristup sustavu videonadzora i značajna radnja provedena nad snimkama moraju biti evidentirani.

(2) Sustav mora, kada je to tehnički moguće, automatski evidentirati najmanje:

1. oznaku korisničkog računa;
2. datum i vrijeme pristupa;
3. mjesto ili uređaj s kojeg je pristup ostvaren;
4. snimke ili kamere kojima se pristupalo;
5. pregled, pretraživanje, izdvajanje, izvoz, kopiranje i brisanje snimki;
6. promjene korisničkih prava i tehničkih postavki;
7. neuspjele pokušaje prijave.

(3) Kada sustav ne omogućuje automatsko evidentiranje određene radnje, ovlaštena osoba dužna ju je upisati u odgovarajuću internu evidenciju.

(4) Ovlaštena osoba odgovorna je za svaki pristup i svaku radnju provedenu putem njezina korisničkog računa.

(5) Zapisi o pristupu mogu se pregledavati radi:

1. provjere zakonitosti i opravdanosti korištenja sustava;
2. istraživanja sigurnosnog incidenta;
3. utvrđivanja moguće zlouporabe;
4. postupanja po zahtjevu nadležnog tijela;
5. provođenja unutarnjeg nadzora i godišnjeg pregleda sustava.

(6) Nadzor nad korištenjem sustava provode osoba odgovorna za upravljanje sustavom i službenik za zaštitu podataka, svatko u okviru svojih ovlasti.

(7) Ovlaštena osoba dužna je na zahtjev dostaviti obrazloženje svrhe pojedinog pristupa ili radnje u sustavu.

Članak 6.

(1) Ovlaštenje se dodjeljuje: do opoziva.

(2) Ovlaštenje prestaje:

1. opozivom ove Odluke ili pojedinog ovlaštenja;
2. istekom razdoblja na koje je dodijeljeno;
3. prestankom službe, radnog, ugovornog ili drugog odnosa s Općinom;
4. promjenom radnog mjesta ili poslova zbog kojih pristup više nije potreban;
5. završetkom konkretne zadaće ili postupka;
6. utvrđenom zlouporabom ovlasti;
7. postojanjem sigurnosnog rizika;
8. na zahtjev ovlaštene osobe;
9. iz drugih opravdanih razloga.

(3) Ovlaštena osoba i njezin nadređeni dužni su bez odgode obavijestiti osobu odgovornu za sustav o svakoj okolnosti zbog koje je potrebno izmijeniti ili ukinuti prava pristupa.

(4) Nakon prestanka ovlaštenja potrebno je bez odgode:

1. onemogućiti korisnički račun;
2. ukinuti udaljeni pristup;
3. preuzeti pristupnu karticu, ključ, uređaj ili drugo sredstvo pristupa;
4. ukloniti osobu s popisa ovlaštenih korisnika;
5. evidentirati datum i razlog prestanka ovlaštenja.

(5) Privremeno onemogućavanje pristupa može se provesti odmah kada postoji sumnja na zlouporabu, gubitak pristupnih podataka ili drugi sigurnosni rizik.

(6) Opseg ovlasti preispituje se najmanje jednom godišnje i nakon svake kadrovske, organizacijske ili tehničke promjene.

Članak 7.

(1) Ova Odluka dostavlja se:

1. imenovanim ovlaštenim osobama;
2. osobi odgovornoj za upravljanje sustavom videonadzora;
3. osobi odgovornoj za tehničko upravljanje korisničkim računima;
4. službeniku za zaštitu podataka;
5. pročelniku Jedinostvenog upravnog odjela;
6. drugoj osobi kojoj je dostava potrebna radi provedbe Odluke.

(2) Imenovana osoba potpisom potvrđuje primitak ove Odluke, upoznatost s opsegom ovlasti i prihvaćanje obveze povjerljivosti.

(3) Ova Odluka i njezini prilozi interni su dokumenti s ograničenim pristupom i ne objavljuju se javno zbog zaštite osobnih podataka i sigurnosti sustava videonadzora.

(4) Na pitanja koja nisu uređena ovom Odlukom primjenjuju se Odluka o korištenju sustava videonadzora, Politika i procedura korištenja sustava videonadzora, Pravilnik o zaštiti osobnih podataka Općine Župa dubrovačka i drugi odgovarajući propisi.

(5) Ova Odluka stupa na snagu danom donošenja.

KLASA: 650-05/26-01/9

URBROJ: 2117-8-01-26-3

Srebreno, 28. kolovoza 2026.

OPĆINSKI NAČELNIK

Marko Miloslavić, v.r.

Na temelju članka 37. Uredbe (EU) 2016/679 Europskog parlamenta i Vijeća od 27. travnja 2016. o zaštiti pojedinaca u vezi s obradom osobnih podataka i o slobodnom kretanju takvih podataka te o stavljanju izvan snage Direktive 95/46/EZ (Opća uredba o zaštiti podataka), članka 1. Zakona o provedbi Opće uredbe o zaštiti podataka ("Narodne novine", broj 42/18) i članka 48. Statuta Općine Župa dubrovačka ("Službeni glasnik Općine Župa dubrovačka", broj 8/09, 6/13, 3/18, 4/20, 6/20 – pročišćeni tekst, 5/21 i 9/21 – pročišćeni tekst), Općinski načelnik Općine Župa dubrovačka donosi

O D L U K U

o imenovanju službenika za zaštitu osobnih podataka u Općini Župa dubrovačka

Članak 1.

Službenica **MARICA MISIR DRAGOJEVIĆ** imenuje se službenikom za zaštitu osobnih podataka Općine Župa dubrovačka.

Članak 2.

Imenovani službenik za zaštitu osobnih podataka iz članka 1. ove Odluke na primjeren se način i pravodobno uključuje u sva pitanja u pogledu zaštite osobnih podataka u Općini Župa dubrovačka.

Voditelj obrade, Općina Župa dubrovačka, podupire službenika za zaštitu osobnih podataka u izvršavanju zadaća i pruža mu potrebna sredstva za izvršavanje tih zadaća, ostvarivanje pristupa osobnim podacima i postupcima obrade te održavanje njegova stručnog znanja.

Službenik za zaštitu osobnih podataka izravno odgovara najvišoj rukovodećoj razini odnosno Općinskom načelniku Općine Župa dubrovačka.

Službenik za zaštitu osobnih podataka obvezan je čuvati tajnost ili povjerljivost u vezi s obavljanjem svojih zadaća, u skladu s pravom Europske unije i pravom Republike Hrvatske.

Službenik za zaštitu osobnih podataka može obavljati i druge zadaće i dužnosti. Općina Župa dubrovačka osigurava da te zadaće i dužnosti ne dovedu do sukoba interesa.

Službenik za zaštitu osobnih podataka obavlja najmanje sljedeće zadaće:

- informira i savjetuje voditelja obrade ili izvršitelja obrade te službenike i druge zaposlenike koji obavljaju obradu o njihovim obvezama iz Opće uredbe o zaštiti podataka te drugim odredbama prava Europske unije i Republike Hrvatske o zaštiti podataka;
- prati poštovanje Opće uredbe o zaštiti podataka te drugih odredaba prava Europske unije i Republike Hrvatske o zaštiti podataka i politika voditelja obrade ili izvršitelja obrade u odnosu na zaštitu osobnih podataka, uključujući raspodjelu odgovornosti, podizanje svijesti i osposobljavanje osoblja koje sudjeluje u postupcima obrade te povezane revizije;
- pruža savjete, kada je to zatraženo, u pogledu procjene učinka na zaštitu podataka i prati njezino izvršavanje u skladu s člankom 35. Opće uredbe o zaštiti podataka;
- surađuje s Agencijom za zaštitu osobnih podataka;
- djeluje kao kontaktna točka za Agenciju za zaštitu osobnih podataka o pitanjima u pogledu obrade, što uključuje i prethodno savjetovanje iz članka 36. Opće uredbe o zaštiti podataka, te savjetovanje, prema potrebi, o svim drugim pitanjima.

Pri obavljanju svojih zadaća službenik za zaštitu osobnih podataka vodi računa o riziku povezanom s postupcima obrade i uzima u obzir prirodu, opseg, kontekst i svrhe obrade.

Članak 3.

Službenik za zaštitu osobnih podataka dužan je čuvati povjerljivost svih informacija i podataka koje sazna u obavljanju svojih dužnosti, a ta obveza traje i nakon prestanka obavljanja dužnosti službenika za zaštitu osobnih podataka.

Članak 4.

Službeni kontakti podaci službenika za zaštitu osobnih podataka Općine Župa dubrovačka su:

- adresa i mjesto rada: Općina Župa dubrovačka, Vukovarska 48, 20207 Mlini
- e-mail: marica.misir@zupa-dubrovacka.hr
- broj telefona: +385 20 487 476

Kontakti podaci službenika za zaštitu osobnih podataka objavit će se i biti javno dostupni na službenoj mrežnoj stranici Općine Župa dubrovačka te će se priopćiti Agenciji za zaštitu osobnih podataka.

Članak 5.

Danom stupanja na snagu ove Odluke prestaje važiti ranija odluka kojom je imenovan službenik za zaštitu osobnih podataka Općine Župa dubrovačka.

Ova Odluka stupa na snagu danom donošenja, a objavit će se u "Službenom glasniku Općine Župa dubrovačka" i na službenoj mrežnoj stranici Općine Župa dubrovačka.

KLASA: 029-03/26-01/8

URBROJ: 2117-8-01-26-2

Srebreno, 28. kolovoza 2026.

OPĆINSKI NAČELNIK

Marko Miloslavić, v.r.

04.

Na temelju članka 20. Zakona o zaštiti prijavitelja nepravilnosti („Narodne novine“, broj 46/22 i 136/25), članka 2. Pravilnika o postupku imenovanja povjerljive osobe i njezina zamjenika te postupku unutarnjeg prijavljivanja nepravilnosti u Općini Župa dubrovačka („Službeni glasnik Općine Župa dubrovačka“, broj 26/26), i članka 48. Statuta Općine Župa dubrovačka („Službeni glasnik Općine Župa dubrovačka“, broj 8/09, 6/13, 3/18, 4/20, 6/20 – pročišćeni tekst, 5/21 i 9/21 – pročišćeni tekst), Općinski načelnik Općine Župa dubrovačka donosi

ODLUKU

**o imenovanju povjerljive osobe i zamjenika povjerljive osobe
u Općini Župa dubrovačka**

Članak 1.

Za povjerljivu osobu za unutarnje prijavljivanje nepravilnosti u Općini Župa dubrovačka imenuje se službenik MARIO ZVONO.

Za zamjenika povjerljive osobe imenuje se službenica SANJA VUKOVIĆ.

Imenovane osobe dale su pisanu suglasnost za imenovanje.

Članak 2.

Povjerljiva osoba obavlja poslove propisane Zakonom o zaštiti prijavitelja nepravilnosti i općim aktom Općine Župa dubrovačka kojim se uređuje postupak unutarnjeg prijavljivanja nepravilnosti, a osobito:

- zaprima prijave nepravilnosti i potvrđuje njihov primitak u zakonom propisanom roku,
- poduzima radnje iz svoje nadležnosti potrebne za zaštitu prijavitelja nepravilnosti,
- poduzima radnje radi ispitivanja nepravilnosti i prijavitelju daje povratnu informaciju,
- prema potrebi prosljeđuje prijavu tijelima ovlaštenim za postupanje prema sadržaju prijave,
- obavještava prijavitelja o ishodu ispitivanja prijave,
- vodi evidenciju zaprimljenih prijava,
- čuva identitet prijavitelja nepravilnosti i podatke zaprimljene u prijavi od neovlaštenog otkrivanja te
- obavlja druge poslove utvrđene Zakonom i općim aktom Općine.

Članak 3.

Zamjenik povjerljive osobe obavlja poslove povjerljive osobe u slučaju njezine odsutnosti, spriječenosti ili u drugim slučajevima propisanim Zakonom i općim aktom Općine.

Članak 4.

Povjerljiva osoba i njezin zamjenik dužni su svoje dužnosti obavljati zakonito, savjesno i nepristrano te su dužni štititi identitet prijavitelja nepravilnosti i povjerljivost svih podataka zaprimljenih u prijavi, u skladu sa Zakonom.

Općina Župa dubrovačka neće utjecati niti pokušati utjecati na postupanje povjerljive osobe i njezina zamjenika pri obavljanju poslova iz njihove nadležnosti.

Članak 5.

Kontaktne podaci povjerljive osobe i zamjenika povjerljive osobe:

- Povjerljiva osoba - Mario Zvono
- Telefon: +385 20 487 470
 - E-mail: mario.zvono@zupa-dubrovacka.hr
- Zamjenik povjerljive osobe - Sanja Vuković
- Telefon: +385 20 487 470
 - E-mail: sanja.vukovic@zupa-dubrovacka.hr

Kontaktne podaci i informacije potrebne za podnošenje prijave nepravilnosti objavit će se na mrežnoj stranici Općine Župa dubrovačka i učiniti dostupnima svim osobama u radnom okruženju.

Članak 6.

Ova Odluka stupa na snagu danom donošenja, a objavit će se u "Službenom glasniku Općine Župa dubrovačka" i na službenoj mrežnoj stranici Općine Župa dubrovačka.

KLASA: 029-03/26-01/9
URBROJ: 2117-8-01-26-3

Srebreno, 28. kolovoza 2026.

OPĆINSKI NAČELNIK

Marko Miloslavić, v.r.

05.

Na temelju članka 11. Zakona o sustavu unutarnjih kontrola u javnom sektoru (Narodne novine, br. 78/15, 102/19 i 105/25), članka 6. stavka 1. Pravilnika o sustavu unutarnjih kontrola u javnom sektoru (Narodne novine, br. 58/16) i članka 48. Statuta Općine Župa dubrovačka ("Službeni glasnik Općine Župa dubrovačka", broj 8/09, 6/13, 3/18, 4/20, 6/20 – pročišćeni tekst, 5/21 i 9/21 – pročišćeni tekst), Općinski načelnik Općine Župa dubrovačka donosi

O D L U K U

o imenovanju povjerenika za etiku u Općini Župa dubrovačka

Članak 1.

Službenica BARBARA BOGOJE imenuje se povjerenikom za etiku Općine Župa dubrovačka za primjenu načela, metoda i postupaka navedenih u Okviru u skladu sa zakonima i drugim propisima te internim aktima koji uređuju pojedina područja poslovanja Općine Župa dubrovačka.

Članak 2.

Imenovani službenik iz članka 1. ove Odluke na primjeren se način i pravodobno uključuje u sva pitanja u pogledu sustava unutarnjih kontrola u javnom sektoru u Općini Župa dubrovačka.

Članak 3.

Službeni kontaktni podaci povjerenika za etiku Općine Župa dubrovačka su:

- adresa i mjesto rada: Općina Župa dubrovačka, Vukovarska 48, 20207 Mlini
- e-mail: barbara.bogoje@zupa-dubrovacka.hr
- broj telefona: +385 20 487 485

Kontaktni podaci povjerenika za etiku objavit će se i biti javno dostupni na službenoj mrežnoj stranici Općine Župa dubrovačka.

Članak 4.

Ova Odluka stupa na snagu danom donošenja, a objavit će se u "Službenom glasniku Općine Župa dubrovačka".

KLASA: 004-01/26-01/2
URBROJ: 2117-8-01-26-2

Srebreno, 28. kolovoza 2026.

OPĆINSKI NAČELNIK

Marko Miloslavić, v.r.

