



REPUBLIKA HRVATSKA
DUBROVAČKO-NERETVANSKA ŽUPANIJA
OPĆINA ŽUPA DUBROVAČKA
Općinski načelnik

Na temelju članka 6. stavka 1. točke (e), članka 24., 25. i 35. 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 te o stavljanju izvan snage Direktive 95/46/EZ – Opće uredbe o zaštiti podataka, članka 25., 26., 27., 28., 29. i 32. Zakona o provedbi Opće uredbe o zaštiti podataka („Narodne novine“, broj 42/18), Zakona o privatnoj zaštiti („Narodne novine“, broj 16/20 i 114/22), članka 11. i 12. Pravilnika o načinu i uvjetima obavljanja poslova privatne zaštite na javnim površinama („Narodne novine“, broj 36/12) 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 korištenju sustava videonadzora javnih površina na području Općine Župa dubrovačka

I. OPĆE ODREDBE

Članak 1.

(1) Ovom Odlukom uređuju se uvjeti uspostave, korištenja i održavanja sustava videonadzora javnih površina na području Općine Župa dubrovačka.

(2) Ovom Odlukom osobito se uređuju:

1. svrha i pravna osnova korištenja sustava videonadzora;
2. uvjeti za određivanje lokacija i područja snimanja;
3. načela nužnosti i razmjernosti obrade osobnih podataka;
4. tehničke i organizacijske mjere zaštite osobnih podataka;
5. način upravljanja sustavom i pristupa snimkama;
6. osobe ovlaštene za pristup sustavu i snimkama;
7. rokovi čuvanja i način brisanja snimki;
8. izdvajanje i dostavljanje snimki nadležnim tijelima;
9. obveze označavanja područja pod videonadzorom i informiranja javnosti;
10. prava ispitanika;
11. nadzor nad zakonitošću i sigurnošću korištenja sustava.

(3) Sustav videonadzora koristi se i održava u skladu s propisima kojima se uređuju zaštita osobnih podataka, privatna zaštita, tehnička zaštita i informacijska sigurnost.

(4) Detaljna pravila upravljanja sustavom, korisničkih ovlasti, pristupa snimkama, postupanja sa snimkama i postupanja u slučaju sigurnosnog incidenta uređuju se Politikom odnosno Procedurom korištenja sustava videonadzora Općine Župa dubrovačka.

Članak 2.

(1) Pojmovi koji se koriste u ovoj Odluci imaju značenje utvrđeno Općom uredbom o zaštiti podataka, Zakonom o provedbi Opće uredbe o zaštiti podataka, Zakonom o privatnoj zaštiti i drugim odgovarajućim propisima.

(2) Pojedini pojmovi u smislu ove Odluke imaju sljedeće značenje:

1. **sustav videonadzora** jest tehnički sustav kojim se pomoću kamera prikupljaju, prenose, pregledavaju i pohranjuju videosnimke;
2. **snimka videonadzora** jest zapis slike fizičke osobe, vozila, događaja ili prostora koji je nastao korištenjem sustava videonadzora;
3. **javna površina** jest površina namijenjena općoj uporabi ili površina kojom Općina upravlja u okviru svojih zakonskih ovlasti;
4. **područje snimanja** jest prostor obuhvaćen vidnim poljem pojedine kamere;
5. **ovlaštena osoba** jest osoba koju Općinski načelnik posebnom pisanom odlukom ovlasti za pristup sustavu videonadzora i snimkama;
6. **ispitanik** jest fizička osoba čiji je lik, kretanje, vozilo ili drugo obilježje koje omogućuje njezinu identifikaciju zabilježeno sustavom videonadzora;
7. **izvršitelj obrade** jest vanjski pružatelj usluge koji u ime Općine održava sustav, pohranjuje snimke ili na drugi način obrađuje osobne podatke.

(3) Voditelj obrade osobnih podataka prikupljenih putem sustava videonadzora jest **Općina Župa dubrovačka**.

(4) Općinu Župa dubrovačka kao voditelja obrade zastupa Općinski načelnik.

(5) Kontaktni podaci Općine, službenika za zaštitu podataka i druge informacije o obradi osobnih podataka putem videonadzora objavljuju se na mrežnoj stranici Općine i navode na odgovarajućim obavijestima o videonadzoru.

II. SVRHA I PRAVNA OSNOVA VIDEONADZORA

Članak 3.

(1) Videonadzor javnih površina može se uspostaviti i koristiti isključivo kada je to nužno i opravdano radi:

1. zaštite života, zdravlja i sigurnosti osoba;
2. zaštite imovine Općine Župa dubrovačka;
3. zaštite objekata i prostora kojima Općina upravlja ili koje koristi;

4. zaštite komunalne, prometne i druge javne infrastrukture;
5. zaštite dječjih igrališta, sportskih, rekreacijskih i drugih javnih površina;
6. prevencije i utvrđivanja vandalizma, oštećenja imovine i drugih protupravnih ponašanja;
7. prevencije i utvrđivanja nepropisnog odlaganja otpada, kada je videonadzor nužan za izvršavanje poslova Općine;
8. utvrđivanja okolnosti sigurnosnih događaja i incidenata;
9. izdvajanja dokaza za potrebe sudskih, upravnih, prekršajnih, kaznenih i drugih postupaka pred nadležnim tijelima;
10. izvršavanja drugih zakonom propisanih poslova i zadaća Općine za koje je videonadzor nužan i razmjern.

(2) Za svaku lokaciju videonadzora mora se utvrditi konkretna svrha snimanja.

(3) Snimke se ne smiju koristiti za svrhe koje nisu u skladu sa svrhama utvrđenima ovom Odlukom, dokumentacijom pojedine lokacije i važećim propisima.

(4) Sustav videonadzora ne smije se koristiti za proizvoljno praćenje pojedinaca, njihovih navika, kretanja ili ponašanja.

(5) Snimke se ne smiju koristiti u promotivne, komercijalne, privatne ili druge neslužbene svrhe.

Članak 4.

(1) Pravna osnova za obradu osobnih podataka putem sustava videonadzora jest izvršavanje zadaća od javnog interesa i izvršavanje službenih ovlasti Općine Župa dubrovačka, u skladu s člankom 6. stavkom 1. točkom (e) Opće uredbe o zaštiti podataka i člankom 32. Zakona o provedbi Opće uredbe o zaštiti podataka.

(2) Videonadzor se može uspostaviti samo kada je ispunjen najmanje jedan od sljedećih uvjeta:

1. videonadzor je nužan za izvršavanje zakonom propisanih poslova i zadaća Općine;
2. videonadzor je nužan radi zaštite života i zdravlja ljudi;
3. videonadzor je nužan radi zaštite imovine, objekata, infrastrukture ili javnih površina.

(3) Prije uspostave sustava videonadzora ili uvođenja nove lokacije mora se utvrditi:

1. konkretan sigurnosni ili drugi opravdani problem;
2. svrha koja se namjerava postići;
3. može li se ista svrha učinkovito ostvariti drugim, manje invazivnim mjerama;
4. područje koje je nužno obuhvatiti snimanjem;
5. razdoblje i način rada sustava;
6. rizici za privatnost i druga prava osoba;
7. potrebne tehničke i organizacijske mjere zaštite.

(4) Videonadzor se neće uspostaviti ako interesi, temeljna prava i slobode ispitanika pretežu nad interesom Općine za provođenje videonadzora.

(5) Opseg, intenzitet i trajanje snimanja moraju biti razmjerni svrsi koja se želi postići i ograničeni na najmanju moguću mjeru.

(6) Videonadzor se ne smije koristiti kao zamjena za organizacijske, fizičke, komunalne ili druge mjere koje mogu učinkovito ostvariti istu svrhu uz manje zadiranje u privatnost.

(7) Kada planirana obrada uključuje sustavno praćenje javno dostupnog područja u velikoj mjeri ili može prouzročiti visok rizik za prava i slobode fizičkih osoba, prije početka obrade provodi se procjena učinka na zaštitu osobnih podataka.

Članak 5.

(1) Područje snimanja pojedine kamere mora biti ograničeno na prostor koji je nužno obuhvatiti radi ostvarivanja utvrđene svrhe videonadzora.

(2) Sustav videonadzora može obuhvatiti:

1. javne površine;
2. objekte i zemljišta u vlasništvu Općine;
3. objekte, prostore i površine kojima Općina upravlja ili koje koristi na temelju odgovarajuće pravne osnove;
4. neposredne pristupe takvim objektima i prostorima, kada je to nužno radi njihove zaštite.

(3) Sustav videonadzora mora se postaviti i konfigurirati tako da se izbjegava snimanje:

1. privatnih nekretnina i dvorišta;
2. prozora i unutrašnjosti stambenih ili poslovnih prostora;
3. prostora koji nisu povezani sa svrhom videonadzora;
4. površina kojima Općina ne upravlja, osim u tehnički neizbježnom i najmanjem mogućem opsegu.

(4) Kada se snimanje prostora iz stavka 3. ovoga članka ne može u potpunosti izbjeći, moraju se primijeniti tehničke mjere ograničenja vidnog polja, maskiranja, zatamnjenja ili drugog odgovarajućeg načina zaštite privatnosti.

(5) Kamere se moraju usmjeriti tako da snimaju najmanju površinu potrebnu za ostvarivanje utvrđene svrhe.

(6) Sustavom videonadzora nije dopušteno tonsko snimanje, osim ako je ono izričito dopušteno posebnim zakonom.

(7) Sustav videonadzora ne smije se koristiti za:

1. automatsko prepoznavanje lica;
2. biometrijsku identifikaciju osoba;
3. profiliranje osoba;
4. automatizirano donošenje odluka;

5. analizu ponašanja, emocija ili drugih osobnih obilježja;
6. praćenje radne učinkovitosti zaposlenika;

osim ako je takva obrada izričito dopuštena zakonom i prethodno su ispunjene sve propisane pretpostavke.

(8) Točne lokacije kamera, područje njihova snimanja, tehničke karakteristike i svrha svake lokacije vode se u posebnoj službenoj evidenciji i tehničkoj dokumentaciji sustava videonadzora.

Članak 6.

(1) Odluku o uspostavi videonadzora na pojedinoj lokaciji donosi Općinski načelnik na temelju obrazloženog prijedloga nadležne ustrojstvene jedinice, stručne službe ili druge odgovorne osobe.

(2) Obrazloženi prijedlog iz stavka 1. ovoga članka mora sadržavati najmanje:

1. naziv i opis lokacije;
2. vlasnički ili drugi pravni status prostora;
3. opis sigurnosnog, komunalnog ili drugog problema;
4. svrhu uspostave videonadzora;
5. podatke o ranijim incidentima, oštećenjima ili drugim okolnostima koje opravdavaju snimanje, kada su dostupni;
6. obrazloženje zbog čega se svrha ne može učinkovito ostvariti drugim, manje invazivnim mjerama;
7. prijedlog broja i položaja kamera;
8. predloženo područje i vrijeme snimanja;
9. procjenu mogućeg utjecaja na privatnost i prava ispitanika;
10. prijedlog roka čuvanja snimki;
11. opis predloženih tehničkih i organizacijskih mjera zaštite;
12. procjenu potrebnih financijskih i tehničkih sredstava.

(3) Prije donošenja odluke o novoj lokaciji pribavlja se mišljenje službenika za zaštitu podataka.

(4) Kada je to potrebno zbog prirode, opsega, okolnosti ili svrhe snimanja, prije uvođenja videonadzora provodi se procjena učinka na zaštitu osobnih podataka.

(5) Ako se poslovi privatne zaštite na javnim površinama obavljaju putem ovlaštenog pružatelja usluga, prije uspostave sustava moraju se ispuniti i uvjeti propisani propisima o privatnoj zaštiti.

(6) Videonadzor na novoj lokaciji ne smije se pustiti u uporabu prije nego što su:

1. utvrđeni svrha i pravna osnova;
2. postavljene propisane obavijesti o videonadzoru;
3. utvrđene ovlaštene osobe;
4. uspostavljene tehničke i organizacijske mjere zaštite;

5. uređeni odnosi s izvršiteljima obrade;
6. lokacija evidentirana u službenoj evidenciji sustava videonadzora.

(7) Privremeno korištenje videonadzora dopušteno je samo kada za to postoji konkretna, dokumentirana i vremenski ograničena potreba te uz primjenu svih pravila iz ove Odluke.

Članak 7.

(1) Općina vodi ažurnu evidenciju svih lokacija na kojima se koristi sustav videonadzora.

(2) Evidencija iz stavka 1. ovoga članka za svaku lokaciju sadržava najmanje:

1. redni broj i naziv lokacije;
2. adresu ili drugi precizan opis položaja;
3. pravni status prostora;
4. svrhu videonadzora;
5. pravnu osnovu obrade;
6. broj i vrstu kamera;
7. opis područja koje pojedina kamera snima;
8. podatak snima li sustav neprekidno ili u određenom vremenu;
9. mjesto pohrane snimki;
10. rok čuvanja snimki;
11. podatke o ovlaštenim osobama;
12. podatke o izvršitelju obrade ili održavatelju sustava;
13. datum početka korištenja;
14. datum posljednjeg pregleda opravdanosti;
15. podatak o provedenoj procjeni učinka, kada je primjenjivo.

(3) Uz evidenciju lokacija čuva se odgovarajuća tehnička dokumentacija koja može sadržavati:

1. položaj i smjer kamera;
2. prikaz vidnog polja;
3. podatke o maskiranim ili zatamnjenim područjima;
4. tehničke specifikacije uređaja;
5. način pohrane i zaštite snimki;
6. mrežnu i korisničku konfiguraciju;
7. evidenciju održavanja i servisnih zahvata;
8. zapisnike o pregledima i testiranjima sustava.

(4) Tehnička dokumentacija i detaljan prikaz položaja kamera nisu javno dostupni ako bi njihova objava mogla ugroziti sigurnost sustava, osoba, imovine ili provedbu svrhe videonadzora.

(5) Evidencija lokacija i tehnička dokumentacija ažuriraju se bez odgađanja nakon:

1. postavljanja ili uklanjanja kamere;
2. promjene položaja ili vidnog polja kamere;
3. promjene svrhe ili pravne osnove;
4. promjene roka čuvanja;
5. promjene mjesta pohrane;
6. promjene izvršitelja obrade;
7. značajne promjene tehničkog sustava.

(6) Za ažurnost evidencije odgovorna je osoba koju odredi Općinski načelnik, u suradnji sa službenikom za zaštitu podataka i osobom odgovornom za tehničko održavanje sustava.

Članak 8.

(1) Sustavom videonadzora upravlja Općina Župa dubrovačka putem ovlaštenih osoba i, prema potrebi, ugovorenih izvršitelja obrade.

(2) Upravljanje sustavom obuhvaća:

1. nadzor rada kamera i uređaja za pohranu;
2. upravljanje korisničkim računima i pravima pristupa;
3. pregled, izdvajanje i izvoz snimki;
4. zaštitu snimki od neovlaštenog pristupa, izmjene, kopiranja i brisanja;
5. redovito održavanje i sigurnosno ažuriranje sustava;
6. vođenje zapisa o pristupima i radnjama korisnika;
7. pravodobno brisanje snimki nakon isteka roka čuvanja;
8. postupanje u slučaju sigurnosnog incidenta;
9. periodično ispitivanje funkcionalnosti i sigurnosti sustava.

(3) Sustav mora biti tehnički postavljen tako da omogućuje:

1. pristup samo ovlaštenim osobama;
2. korištenje pojedinačnih korisničkih računa;
3. odgovarajuću autentifikaciju korisnika;
4. automatsko evidentiranje pristupa snimkama;
5. evidentiranje pregleda, izvoza, kopiranja i brisanja snimki, kada je to tehnički moguće;
6. automatsko brisanje snimki nakon isteka utvrđenog roka;

7. zaštitu snimki tijekom prijenosa i pohrane;
 8. ograničavanje i maskiranje nepotrebnog područja snimanja.
- (4) Zabranjena je uporaba zajedničkih korisničkih računa, osim kada zbog tehničkih obilježja sustava nije moguće osigurati pojedinačne račune i kada su uvedene druge mjere kojima se može utvrditi koja je osoba pristupila sustavu.
- (5) Administratorska prava dodjeljuju se samo osobama kojima su nužna za tehničko održavanje sustava i ne daju automatski pravo pregleda sadržaja snimki.
- (6) Pristup sustavu putem udaljene veze dopušten je samo kada je nužan, primjereno zaštićen i odobren od strane odgovorne osobe.
- (7) Sustav videonadzora mora biti fizički i tehnički zaštićen od neovlaštenog pristupa, krađe, oštećenja, neovlaštene izmjene i gubitka podataka.
- (8) Poslužitelji, uređaji za pohranu i druga oprema na kojoj se čuvaju snimke moraju se nalaziti u zaključanom ili na drugi način kontroliranom prostoru.
- (9) Redovito održavanje sustava provodi se na način kojim se u najmanjoj mogućoj mjeri omogućuje pristup stvarnim snimkama.

Članak 9.

- (1) Pristup sustavu videonadzora i snimkama dopušten je samo osobama koje Općinski načelnik ovlasti posebnom pisanom odlukom.
- (2) Odlukom iz stavka 1. ovoga članka za svaku ovlaštenu osobu utvrđuje se najmanje:
1. ime i prezime;
 2. radno mjesto ili druga osnova ovlaštenja;
 3. lokacija ili dio sustava kojem može pristupiti;
 4. opseg ovlasti;
 5. svrha pristupa;
 6. vrijeme trajanja ovlaštenja.
- (3) Ovlaštenje može obuhvaćati jednu ili više sljedećih radnji:
1. pregled slike u stvarnom vremenu;
 2. pregled pohranjenih snimki;
 3. pretraživanje snimki prema vremenu i lokaciji;
 4. izdvajanje i izvoz snimke;
 5. dostavljanje snimke ovlaštenom primatelju;
 6. tehničko održavanje sustava bez uvida u sadržaj, kada je to moguće;
 7. upravljanje korisničkim računima i sigurnosnim postavkama.

(4) Pravo pregleda snimki dodjeljuje se u najmanjem potrebnom opsegu i samo osobama kojima je takav pristup nužan radi obavljanja službenih poslova.

(5) Ovlaštene osobe dužne su:

1. koristiti sustav samo u službene i unaprijed utvrđene svrhe;
2. čuvati povjerljivost snimki i drugih podataka;
3. spriječiti pristup neovlaštenim osobama;
4. ne izrađivati preslike ili snimke zaslona bez odobrenja;
5. odmah prijaviti sumnju na neovlašten pristup ili drugu povredu;
6. postupati prema ovoj Odluci, Politici korištenja sustava i drugim internim uputama;
7. sudjelovati u odgovarajućoj edukaciji.

(6) Ovlaštena osoba ne smije pregledavati snimke iz osobne znatiželje, privatnih razloga ili u svrhe koje nisu povezane s njezinim službenim ovlastima.

(7) Ovlaštenje se ukida bez odgađanja kada:

1. prestane potreba za pristupom;
2. osoba promijeni radno mjesto ili poslove;
3. prestane službeni, radni ili ugovorni odnos;
4. dođe do zlouporabe ovlasti;
5. to zahtijevaju sigurnosni ili drugi opravdani razlozi.

(8) Prava pristupa preispituju se najmanje jednom godišnje te nakon svake organizacijske, kadrovske ili tehničke promjene.

(9) Popis ovlaštenih osoba vodi se kao interni dokument s ograničenim pristupom.

(10) Osobe koje povremeno trebaju pristup snimkama mogu dobiti vremenski ograničeno pisano ovlaštenje za konkretan događaj, postupak ili snimku.

Članak 10.

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

(2) Redovni rok čuvanja snimki utvrđuje se za svaku lokaciju posebno, uzimajući u obzir:

1. svrhu videonadzora;
2. vrstu i učestalost sigurnosnih događaja;
3. razdoblje u kojem se događaj uobičajeno može otkriti;
4. rizik za prava i slobode ispitanika;
5. tehničke značajke sustava;
6. načelo smanjenja količine podataka i ograničenja pohrane.

(3) Snimke se u pravilu čuvaju najduže **30 dana**, osim ako je za pojedinu lokaciju obrazloženo utvrđen kraći ili dulji rok.

(4) Snimke se ne smiju čuvati dulje od šest mjeseci, osim ako je drugim zakonom propisan dulji rok ili su snimke izdvojene kao dokaz u sudskom, upravnom, prekršajnom, kaznenom, inspekcijskom ili drugom službenom postupku.

(5) Po isteku utvrđenog roka snimke se automatski i nepovratno brišu prepisivanjem novim sadržajem ili drugim odgovarajućim tehničkim postupkom.

(6) Snimka se može izdvojiti iz redovnog ciklusa brisanja samo kada:

1. prikazuje sigurnosni incident, štetu, kazneno djelo, prekršaj ili drugi događaj važan za službeni postupak;
2. je zaprimljen zahtjev policije, suda, državnog odvjetništva, inspekcije ili drugog ovlaštenog tijela;
3. je potrebna radi postavljanja, ostvarivanja ili obrane pravnih zahtjeva;
4. je zaprimljen pravodoban zahtjev ispitanika koji se odnosi na konkretnu snimku;
5. je potrebno istražiti povredu osobnih podataka ili drugi sigurnosni incident.

(7) Za svaku izdvojenu snimku evidentiraju se:

1. datum i vrijeme izdvajanja;
2. lokacija i vremensko razdoblje snimke;
3. razlog izdvajanja;
4. pravna osnova;
5. osoba koja je snimku izdvojila;
6. mjesto i način pohrane;
7. osobe ili tijela kojima je dostavljena;
8. novi rok čuvanja;
9. datum i način brisanja.

(8) Izdvojene snimke čuvaju se odvojeno od redovnih snimki, uz ograničen pristup i odgovarajuće sigurnosne mjere.

(9) Nakon pravomoćnog ili konačnog završetka postupka odnosno prestanka druge svrhe zbog koje je snimka izdvojena, snimka se briše bez nepotrebnog odgađanja, osim ako postoji druga zakonska osnova za njezino čuvanje.

(10) Trajno čuvanje snimki videonadzora nije dopušteno.

Članak 11.

(1) Pohranjene snimke smiju se pregledavati samo kada postoji konkretna službena potreba povezana sa svrhom videonadzora.

(2) Pregled snimki može se provesti osobito radi:

1. utvrđivanja okolnosti sigurnosnog događaja ili incidenta;
2. utvrđivanja oštećenja ili otuđenja imovine;
3. utvrđivanja vandalizma ili drugog protupravnog ponašanja;
4. postupanja po zakonitom zahtjevu policije, suda, državnog odvjetništva, inspekcije ili drugog nadležnog tijela;
5. postupanja po zahtjevu ispitanika;
6. utvrđivanja povrede osobnih podataka ili drugog sigurnosnog incidenta;
7. postavljanja, ostvarivanja ili obrane pravnih zahtjeva Općine.

(3) Prije pregleda snimke ovlaštena osoba dužna je, kada je to moguće, utvrditi:

1. svrhu pregleda;
2. lokaciju kamere;
3. datum i približno vrijeme događaja;
4. osobu ili događaj na koji se pregled odnosi;
5. pravnu osnovu za pregled.

(4) Pregled snimki mora se ograničiti na vremensko razdoblje, lokaciju i sadržaj koji su potrebni za ostvarivanje konkretne svrhe.

(5) Snimka se smije izdvojiti ili izvesti iz sustava samo kada je to potrebno radi:

1. dostavljanja ovlaštenom tijelu ili drugom zakonitom primatelju;
2. čuvanja dokaza za potrebe službenog postupka;
3. postupanja po zahtjevu ispitanika;
4. provođenja unutarnje istrage sigurnosnog incidenta;
5. zaštite pravnih interesa Općine ili treće osobe.

(6) Izdvojena snimka mora se označiti na način koji omogućuje utvrđivanje:

1. lokacije i oznake kamere;
2. datuma i vremena nastanka snimke;
3. vremenskog razdoblja koje snimka obuhvaća;
4. datuma izdvajanja;
5. razloga i pravne osnove izdvajanja;
6. osobe koja je provela izdvajanje;
7. primatelja kojem je snimka namijenjena;

8. roka njezina daljnjeg čuvanja.

(7) Izvoz snimke provodi se na službeni i primjereno zaštićen medij ili putem zaštićenog elektroničkog kanala.

(8) Izdvojena snimka, kada je to tehnički moguće i potrebno radi provjere njezine vjerodostojnosti, mora sadržavati oznaku datuma, vremena i lokacije snimanja.

(9) Zabranjeno je:

1. snimanje sadržaja zaslona privatnim uređajem;
2. fotografiranje snimke mobilnim telefonom;
3. izrada neodobrenih preslika;
4. slanje snimke privatnom elektroničkom poštom ili putem neodobrenih komunikacijskih aplikacija;
5. objavljivanje snimke na društvenim mrežama, mrežnim stranicama ili u medijima bez odgovarajuće pravne osnove.

(10) Svaki pregled, izdvajanje, izvoz, kopiranje, dostavljanje i brisanje izdvojene snimke evidentira se automatskim zapisom sustava ili posebnom pisanom evidencijom.

(11) Kada izdvojena snimka više nije potrebna za svrhu zbog koje je izdvojena, briše se ili sigurno uništava bez nepotrebnog odgađanja.

Članak 12.

(1) Snimke videonadzora mogu 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 mora biti podnesen u pisanom ili drugom dokazivom obliku i sadržavati najmanje:

1. naziv tijela koje zahtjev podnosi;
2. pravnu osnovu zahtjeva;
3. svrhu za koju se snimka traži;
4. lokaciju na koju se zahtjev odnosi;
5. datum i približno vremensko razdoblje tražene snimke;
6. podatke o službenoj osobi kojoj se snimka dostavlja;
7. oznaku predmeta ili postupka, ako postoji.

(3) U hitnim okolnostima zahtjev se može zaprimiti usmeno, pod uvjetom da se identitet i ovlaštenje službene osobe mogu pouzdano utvrditi te da se zahtjev i izvršena dostava naknadno dokumentiraju.

(4) Prije dostavljanja snimke provjerava se:

1. je li zahtjev podnijelo ovlašteno tijelo ili osoba;

2. postoji li odgovarajuća pravna osnova;
3. je li traženi sadržaj nužan i razmjeran svrsi;
4. sadrži li snimka podatke drugih osoba čija prava treba zaštititi;
5. postoji li tehnička mogućnost izdvajanja samo potrebnog dijela snimke.

(5) Nadležnom tijelu dostavlja se samo dio snimke koji je potreban za postupanje po konkretnom zahtjevu.

(6) Snimka se dostavlja na način koji štiti njezinu povjerljivost, cjelovitost i vjerodostojnost.

(7) Prilikom osobne predaje sastavlja se zapisnik ili potvrda o primopredaji koja sadržava najmanje:

1. naziv i oznaku snimke;
2. datum i vrijeme predaje;
3. svrhu dostavljanja;
4. pravnu osnovu;
5. način i medij predaje;
6. ime, prezime i potpis osobe koja snimku predaje;
7. ime, prezime, svojstvo i potpis osobe koja snimku preuzima.

(8) Kod elektroničke dostave mora se koristiti službeni i primjereno zaštićen komunikacijski kanal, uz odgovarajuću potvrdu primitka kada je to moguće.

(9) Snimke se drugim fizičkim ili pravnim osobama mogu dostaviti samo kada za to postoji izričita pravna osnova ili kada je dostavljanje nužno radi postavljanja, ostvarivanja ili obrane pravnih zahtjeva, uz prethodnu procjenu prava i interesa svih pogođenih osoba.

(10) Snimke se ne dostavljaju medijima, ne objavljuju se radi pronalaženja počinitelja niti se koriste za javno prozivanje osoba, osim kada je takvo postupanje izričito dopušteno zakonom ili ga provodi nadležno tijelo u okviru svojih ovlasti.

(11) O svim zaprimljenim zahtjevima, donesenim odlukama i dostavljenim snimkama vodi se posebna evidencija.

Članak 13.

(1) Osoba čiji su osobni podaci zabilježeni sustavom videonadzora može, pod uvjetima utvrđenima Općom uredbom o zaštiti podataka, ostvarivati osobito:

1. pravo na informacije o obradi;
2. pravo na pristup osobnim podacima;
3. pravo na brisanje osobnih podataka;
4. pravo na ograničenje obrade;
5. pravo na prigovor na obradu;

6. pravo na podnošenje pritužbe Agenciji za zaštitu osobnih podataka.

(2) Zahtjev se podnosi Općini Župa dubrovačka ili službeniku za zaštitu podataka, u pisanom ili drugom dokazivom obliku.

(3) Zahtjev koji se odnosi na određenu snimku treba sadržavati dovoljno informacija za pronalaženje snimke, a osobito:

1. datum i približno vrijeme snimanja;
2. lokaciju na kojoj se osoba nalazila;
3. opis izgleda, odjeće, vozila ili drugih okolnosti potrebnih za identifikaciju;
4. opis prava koje osoba želi ostvariti;
5. kontaktne podatke za dostavu odgovora.

(4) Ako postoji opravdana sumnja u identitet podnositelja, Općina može zatražiti dodatne podatke potrebne za potvrdu identiteta.

(5) Zahtjev za pristup ili čuvanje snimke treba podnijeti što prije jer se snimke automatski brišu nakon isteka utvrđenog roka čuvanja.

(6) Zaprimanje zahtjeva ne znači da se snimka automatski mora trajno sačuvati, nego se potreba njezina izdvajanja procjenjuje prema okolnostima zahtjeva, svrsi obrade i pravima drugih osoba.

(7) Kada snimka sadržava osobne podatke drugih osoba, Općina će prije omogućavanja pristupa poduzeti odgovarajuće mjere njihove zaštite, koje mogu uključivati:

1. zamagljivanje ili prekrivanje likova i drugih identifikacijskih obilježja;
2. izdvajanje samo odgovarajućeg dijela snimke;
3. omogućavanje kontroliranog uvida bez predaje preslike;
4. dostavu fotografije ili drugog prikladnog prikaza umjesto cijele snimke;
5. odbijanje ili ograničavanje pristupa u dijelu u kojem bi se povrijedila prava drugih osoba.

(8) Pravo na brisanje nije primjenjivo kada je snimku potrebno čuvati radi:

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

(9) Općina će na zahtjev odgovoriti bez nepotrebnog odgađanja, a najkasnije u roku od mjesec dana od njegova zaprimanja, uz mogućnost produljenja roka pod uvjetima utvrđenima Općom uredbom o zaštiti podataka.

(10) Ako Općina ne postupi po zahtjevu, ispitaniku će dostaviti obrazloženje i informacije o mogućnosti podnošenja pritužbe Agenciji za zaštitu osobnih podataka i traženja sudske zaštite.

(11) O zahtjevima ispitanika i poduzetim radnjama vodi se evidencija u skladu s Pravilnikom o zaštiti osobnih podataka Općine Župa dubrovačka.

Članak 14.

(1) Svaka javna površina ili drugi prostor obuhvaćen sustavom videonadzora mora biti jasno i vidljivo označen najkasnije prilikom ulaska u područje snimanja.

(2) Obavijest o videonadzoru mora biti postavljena na mjestu i visini koji omogućuju osobi da je uoči prije ulaska u područje snimanja.

(3) Obavijest mora sadržavati najmanje:

1. jasnu i razumljivu oznaku da je prostor pod videonadzorom;
2. odgovarajući grafički simbol kamere;
3. naziv voditelja obrade – Općina Župa dubrovačka;
4. svrhu videonadzora ili sažetu informaciju o svrsi;
5. kontakt putem kojeg ispitanik može dobiti dodatne informacije i ostvariti svoja prava;
6. upućivanje na mjesto na kojem je dostupna potpuna obavijest o obradi osobnih podataka.

(4) Potpuna obavijest o obradi osobnih podataka putem videonadzora objavljuje se na mrežnoj stranici Općine i sadržava osobito:

1. identitet i kontaktne podatke Općine;
2. kontaktne podatke službenika za zaštitu podataka;
3. svrhe i pravnu osnovu obrade;
4. opis kategorija prostora koji se snimaju;
5. kategorije primatelja snimki;
6. rokove čuvanja;
7. informacije o izvršiteljima obrade, kada je primjenjivo;
8. prava ispitanika i način njihova ostvarivanja;
9. pravo podnošenja pritužbe Agenciji za zaštitu osobnih podataka;
10. druge informacije propisane Općom uredbom o zaštiti podataka.

(5) Obavijest ne smije biti zaklonjena, nečitljiva, oštećena ili postavljena na mjestu na kojem ju nije moguće pravodobno uočiti.

(6) Stanje obavijesti o videonadzoru redovito se provjerava, a oštećene, uklonjene ili nečitljive oznake zamjenjuju se bez nepotrebnog odgađanja.

(7) Ako područje snimanja ima više uobičajenih ulaza ili pristupnih pravaca, obavijest se postavlja na svakom takvom mjestu.

(8) U slučaju privremenog videonadzora područje se mora označiti tijekom cijelog vremena provođenja snimanja.

(9) Postavljanje same oznake ne može nadomjestiti obvezu postojanja zakonite, nužne i razmjerne svrhe videonadzora.

Članak 15.

(1) Općina može poslove tehničkog održavanja, servisiranja, pohrane snimki ili druge poslove povezane sa sustavom videonadzora povjeriti vanjskom pružatelju usluge koji pruža dovoljna jamstva za primjenu odgovarajućih tehničkih i organizacijskih mjera zaštite.

(2) Odnos Općine i izvršitelja obrade uređuje se pisanim ugovorom ili drugim obvezujućim pravnim aktom u skladu s člankom 28. Opće uredbe o zaštiti podataka.

(3) Ugovorom se osobito uređuju:

1. predmet, svrha, priroda i trajanje obrade;
2. vrste osobnih podataka i kategorije ispitanika;
3. obrada isključivo prema dokumentiranim uputama Općine;
4. obveza povjerljivosti svih osoba koje imaju pristup sustavu;
5. tehničke i organizacijske mjere zaštite;
6. uvjeti pristupa stvarnim snimkama;
7. vođenje zapisa o pristupu i servisnim radnjama;
8. angažiranje podizvršitelja;
9. postupanje u slučaju povrede osobnih podataka;
10. pomoć Općini pri postupanju po zahtjevima ispitanika;
11. povrat ili brisanje podataka nakon prestanka ugovora;
12. pravo Općine na provjeru i nadzor izvršitelja.

(4) Izvršitelj obrade ne smije pregledavati, kopirati, izdvajati, koristiti ili dostavljati snimke, osim kada je to nužno za izvršavanje dokumentiranih uputa Općine.

(5) Pristup serviseru stvarnim snimkama mora se izbjegavati kada se tehnički problem može otkloniti bez takvog pristupa.

(6) Kada je pristup stvarnim snimkama nužan, mora biti:

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

(7) Za testiranje, razvoj i edukaciju u pravilu se ne koriste stvarne snimke. Kada je njihova uporaba iznimno nužna, moraju se primijeniti odgovarajuće mjere anonimizacije, ograničenja pristupa ili druge zaštitne mjere.

(8) Izvršitelj obrade dužan je Općinu obavijestiti o svakoj sumnji na povredu osobnih podataka ili sigurnosni incident odmah nakon saznanja, a najkasnije u roku utvrđenom ugovorom.

(9) Ugovoreni rok za obavješćivanje mora Općini omogućiti pravodobnu procjenu incidenta i, ako je potrebno, prijavu Agenciji za zaštitu osobnih podataka u zakonskom roku.

(10) Izvršitelj ne smije angažirati podizvršitelja bez prethodnog pisanog odobrenja Općine.

(11) Nakon prestanka ugovornog odnosa moraju se bez odgađanja ukinuti svi udaljeni pristupi, korisnički računi i druga ovlaštenja izvršitelja.

(12) O svakom servisnom zahvatu vodi se zapisnik koji sadržava najmanje datum, vrijeme, opis radova, ime osobe koja je radove provela, podatak o pristupu snimkama i opis eventualnih promjena konfiguracije sustava.

VII. SIGURNOSNI INCIDENTI, NADZOR I PRESTANAK KORIŠTENJA SUSTAVA

Članak 16.

(1) Povredom osobnih podataka u sustavu videonadzora smatra se sigurnosni incident koji dovede ili može dovesti do slučajnog ili nezakonitog uništenja, gubitka, izmjene, neovlaštenog otkrivanja ili neovlaštenog pristupa snimkama i drugim podacima iz sustava videonadzora.

(2) Povredom osobnih podataka osobito se smatra:

1. neovlašten pregled snimki;
2. pregled snimki u privatne ili druge neslužbene svrhe;
3. neovlašteno izdvajanje, kopiranje ili izvoz snimki;
4. fotografiranje ili snimanje sadržaja nadzornog zaslona privatnim uređajem;
5. neovlašteno dostavljanje ili objavljivanje snimki;
6. gubitak ili krađa uređaja, medija ili opreme na kojoj se nalaze snimke;
7. neovlašten pristup sustavu putem korisničkog računa;
8. brisanje, izmjena ili uništenje snimki protivno utvrđenim pravilima;
9. gubitak dostupnosti snimki potrebnih za službeni postupak;
10. neovlaštena promjena položaja, postavki ili područja snimanja kamere;
11. neovlašten pristup vanjskog održavatelja ili druge treće osobe;
12. svaki drugi događaj koji ugrožava povjerljivost, cjelovitost ili dostupnost snimki.

(3) Ovlaštena osoba, službenik, namještenik, izvršitelj obrade ili druga osoba koja sazna za moguću povredu osobnih podataka dužna je o tome odmah obavijestiti:

1. službenika za zaštitu podataka;
2. osobu odgovornu za upravljanje sustavom videonadzora;
3. svojeg neposredno nadređenog;

4. osobu odgovornu za informacijsku sigurnost ili tehničko održavanje sustava, kada je potrebno.

(4) Prijava sigurnosnog incidenta podnosi se odmah, neovisno o tome jesu li u trenutku prijave poznate sve okolnosti i posljedice događaja.

(5) Nakon saznanja za moguću povredu bez odgađanja se poduzimaju mjere radi:

1. zaustavljanja ili ograničavanja povrede;
2. sprječavanja daljnjeg neovlaštenog pristupa;
3. zaštite i očuvanja snimki i drugih dokaza;
4. promjene ili ukidanja kompromitiranih korisničkih prava;
5. utvrđivanja uzroka, opsega i posljedica povrede;
6. utvrđivanja osoba i snimki obuhvaćenih povredom;
7. sprječavanja ponavljanja istog ili sličnog događaja.

(6) Procjenu povrede koordinira službenik za zaštitu podataka u suradnji s osobom odgovornom za sustav videonadzora, informatičkim stručnjakom, izvršiteljem obrade i drugim osobama čije je sudjelovanje potrebno.

(7) Pri procjeni povrede osobito se uzimaju u obzir:

1. vrsta i opseg povrede;
2. sadržaj i osjetljivost snimki;
3. broj pogođenih osoba;
4. mogućnost identifikacije osoba;
5. mogućnost daljnjeg širenja ili javne objave snimki;
6. moguće posljedice za privatnost, sigurnost i ugled osoba;
7. jesu li pogođena djeca ili druge ranjive osobe;
8. jesu li snimke zaštićene enkripcijom ili drugim sigurnosnim mjerama;
9. mjere koje su odmah poduzete radi ograničavanja posljedica.

(8) Kada je vjerojatno da će povreda osobnih podataka 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 ispitanike, osim kada su ispunjeni uvjeti prema kojima obavješćivanje nije potrebno.

(11) Općina vodi evidenciju svih povreda osobnih podataka povezanih sa sustavom videonadzora, neovisno o tome jesu li prijavljene Agenciji ili ispitanicima.

(12) Evidencija povreda sadržava najmanje:

1. opis događaja;
2. datum i vrijeme nastanka i saznanja za povredu;
3. kategorije pogođenih osoba i snimki;
4. procjenu mogućih posljedica;
5. procjenu razine rizika;
6. poduzete korektivne i preventivne mjere;
7. odluku o prijavljivanju ili neprijavljivanju Agenciji;
8. odluku o obavješćivanju ili neobavješćivanju ispitanika;
9. obrazloženje donesenih odluka;
10. datum zatvaranja incidenta.

(13) Detaljan način prijave, procjene, dokumentiranja i rješavanja povrede uređuje se Politikom odnosno Procedurom korištenja sustava videonadzora.

Članak 17.

(1) Općina redovito prati zakonitost, opravdanost, sigurnost i učinkovitost korištenja sustava videonadzora.

(2) Najmanje jednom godišnje provodi se pregled sustava koji obuhvaća:

1. opravdanost daljnjeg korištenja videonadzora na svakoj lokaciji;
2. usklađenost stvarnog područja snimanja s utvrđenom svrhom;
3. mogućnost ostvarivanja svrhe drugim, manje invazivnim mjerama;
4. položaj, usmjerenje i vidno polje kamera;
5. funkcionalnost maskiranja i drugih ograničenja područja snimanja;
6. rokove čuvanja i pravilnost automatskog brisanja snimki;
7. popis ovlaštenih osoba i opseg njihovih prava;
8. zapise o pristupu, pregledavanju, izdvajanju i dostavljanju snimki;
9. stanje tehničkih i organizacijskih mjera zaštite;
10. ugovore i postupanje izvršitelja obrade;
11. stanje i vidljivost obavijesti o videonadzoru;
12. zaprimljene zahtjeve ispitanika;
13. sigurnosne incidente i povrede osobnih podataka;
14. provedbu preporučenih korektivnih mjera.

(3) Godišnji pregled provodi osoba odgovorna za sustav videonadzora u suradnji sa službenikom za zaštitu podataka i osobom odgovornom za tehničko održavanje sustava.

(4) O provedenom pregledu sastavlja se zapisnik ili izvješće koje sadržava:

1. popis pregledanih lokacija i sustava;
2. utvrđeno stanje;
3. uočene nepravilnosti 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.

(5) Službenik za zaštitu podataka može u svako doba predložiti izvanredni pregled sustava, osobito nakon:

1. povrede osobnih podataka;
2. pritužbe ispitanika;
3. utvrđenog neovlaštenog pristupa;
4. značajne tehničke ili organizacijske promjene;
5. promjene svrhe ili područja snimanja;
6. naloga ili preporuke nadležnog tijela;
7. saznanja o novom riziku za prava i slobode ispitanika.

(6) Ovlaštene osobe, izvršitelji obrade i osobe odgovorne za pojedine lokacije dužne su službeniku za zaštitu podataka omogućiti pristup informacijama, evidencijama i dokumentaciji potrebnoj za provedbu nadzora.

(7) Utvrđeni nedostaci otklanjaju se u roku određenom u izvješću, ovisno o njihovoj ozbiljnosti i riziku.

(8) Kada se utvrdi neposredan ili visok rizik za prava i slobode ispitanika, pristup sustavu, pojedina kamera ili cijela lokacija mogu se privremeno isključiti do otklanjanja nedostatka.

(9) Procjena učinka na zaštitu osobnih podataka preispituje se kada dođe do promjene rizika, tehnologije, područja snimanja, svrhe obrade ili drugih značajnih okolnosti.

(10) Općinski načelnik razmatra godišnje izvješće i odlučuje o mjerama potrebnima za unaprjeđenje zakonitosti, sigurnosti i učinkovitosti sustava.

Članak 18.

(1) Korištenje videonadzora na pojedinoj lokaciji mora se ograničiti, izmijeniti, privremeno obustaviti ili trajno ukinuti kada:

1. prestane svrha zbog koje je videonadzor uveden;

2. više nije moguće dokazati njegovu nužnost i razmjernost;
3. ista svrha može biti ostvarena drugim, manje invazivnim mjerama;
4. videonadzor ne daje očekivane rezultate;
5. rizici za prava i slobode ispitanika postanu nerazmjerni koristi sustava;
6. nisu osigurane odgovarajuće tehničke i organizacijske mjere zaštite;
7. sustav ili pojedina kamera snimaju prostor koji nije potreban za utvrđenu svrhu;
8. to naloži Agencija za zaštitu osobnih podataka ili drugo nadležno tijelo;
9. prestane pravna osnova za korištenje prostora ili provođenje videonadzora;
10. nastupe druge okolnosti zbog kojih daljnje snimanje nije zakonito ili opravdano.

(2) O izmjeni, privremenoj obustavi ili prestanku korištenja videonadzora odlučuje Općinski načelnik na temelju obrazloženog prijedloga odgovorne osobe, službenika za zaštitu podataka ili druge nadležne osobe.

(3) U hitnim slučajevima u kojima postoji neposredna opasnost od nezakonite obrade ili povrede prava ispitanika odgovorna osoba može privremeno isključiti pojedinu kameru ili ograničiti pristup sustavu, uz obvezu da o tome odmah obavijesti Općinskog načelnika i službenika za zaštitu podataka.

(4) Prije značajne promjene položaja, vidnog polja, načina rada ili svrhe pojedine kamere provodi se ponovna procjena nužnosti, razmjernosti i rizika.

(5) Promjena tehničke konfiguracije kojom se značajno proširuje područje snimanja smatra se uvođenjem nove ili značajno izmijenjene obrade te se na nju primjenjuju odredbe ove Odluke o uspostavi nove lokacije.

(6) Nakon prestanka korištenja videonadzora na pojedinoj lokaciji potrebno je:

1. isključiti i, prema potrebi, ukloniti kamere i drugu opremu;
2. ukinuti korisničke račune i pristupna prava povezana s lokacijom;
3. ukloniti obavijesti o videonadzoru;
4. izbrisati snimke nakon isteka primjenjivih rokova čuvanja;
5. sačuvati izdvojene snimke koje su potrebne za službene postupke;
6. ažurirati evidenciju lokacija i evidenciju aktivnosti obrade;
7. dokumentirati datum, razlog i način prestanka korištenja.

(7) Oprema koja se prenosi na drugu lokaciju ili ponovno koristi mora se prethodno provjeriti i, kada je potrebno, sigurno izbrisati ili vratiti na početne postavke.

(8) Zapisnici, evidencije pristupa, evidencije dostavljanja snimki, ugovorna dokumentacija i druga dokumentacija o radu sustava čuvaju se prema rokovima utvrđenima propisima i aktima Općine.

VIII. PRIJELAZNE I ZAVRŠNE ODREDBE

Članak 19.

(1) Općinski načelnik donijet će Politiku odnosno Proceduru korištenja sustava videonadzora u roku od 60 dana od dana stupanja na snagu ove Odluke.

(2) Općinski načelnik donijet će posebnu odluku o imenovanju osoba ovlaštenih za pristup sustavu videonadzora i snimkama prije omogućavanja pristupa tim osobama, a najkasnije u roku od 30 dana od dana stupanja na snagu ove Odluke.

(3) Postojeće lokacije i sustavi videonadzora uskladit će se s ovom Odlukom u roku od šest mjeseci od dana njezina stupanja na snagu.

(4) U roku iz stavka 3. ovoga članka potrebno je najmanje:

1. popisati sve kamere i lokacije;
2. utvrditi svrhu i pravnu osnovu svake lokacije;
3. pregledati područja i kutove snimanja;
4. provjeriti snimaju li se nepotrebno privatni ili drugi prostori;
5. utvrditi i tehnički primijeniti rokove čuvanja;
6. uspostaviti automatsko evidentiranje pristupa snimkama;
7. pregledati i ažurirati korisnička prava;
8. postaviti ili zamijeniti propisane obavijesti;
9. urediti ugovorne odnose s izvršiteljima obrade;
10. ažurirati evidenciju aktivnosti obrade;
11. provesti procjenu učinka kada je potrebna;
12. provesti početnu edukaciju ovlaštenih osoba.

(5) Za svaku postojeću lokaciju sastavit će se obrazac ili zapisnik o procjeni nužnosti i razmjernosti daljnjeg korištenja videonadzora.

(6) Ako se za pojedinu postojeću lokaciju ne može dokazati zakonitost, nužnost i razmjernost videonadzora, snimanje će se obustaviti do ispunjenja potrebnih uvjeta ili će se sustav trajno ukloniti.

(7) Sastavni dio provedbene dokumentacije ove Odluke čine:

1. evidencija lokacija i kamera;
2. tehnička dokumentacija sustava;
3. evidencija ovlaštenih osoba;
4. evidencija pristupa i uporabe snimki;
5. evidencija zahtjeva za dostavljanje snimki;
6. evidencija izdvojenih snimki;
7. evidencija servisnih zahvata;

8. evidencija povreda osobnih podataka;
9. obavijest o obradi osobnih podataka putem videonadzora;
10. zapisnici o godišnjim i izvanrednim pregledima sustava.

(8) Na pitanja koja nisu uređena ovom Odlukom primjenjuju se Opća uredba o zaštiti podataka, Zakon o provedbi Opće uredbe o zaštiti podataka, propisi o privatnoj zaštiti, Pravilnik o zaštiti osobnih podataka Općine Župa dubrovačka i drugi odgovarajući propisi i akti.

(9) Ova Odluka objavit će se u „Službenom glasniku Općine Župa dubrovačka“, a stupa na snagu osmoga dana od dana objave.

KLASA: 650-05/26-01/9

URBROJ: 2117-8-01-26-1

Srebreno, 18. kolovoza 2026.



PRILOG 1.
POPIS OVLAŠTENIH OSOBA I OPSEG DODIJELJENIH OVLASTI

Ovlaštena osoba broj 1.

Ime i prezime:

Radno mjesto ili osnova ovlaštenja:

Razdoblje ovlaštenja:

Lokacije i kamere kojima osoba smije pristupati:

Dodijeljene ovlasti:

- ☐ pregled slike u stvarnom vremenu
- ☐ pregled pohranjenih snimki
- ☐ pretraživanje snimki
- ☐ izdvajanje snimki
- ☐ izvoz i izrada službene preslike
- ☐ dostavljanje snimki nadležnim tijelima
- ☐ omogućavanje kontroliranog uvida ispitaniku
- ☐ pregled zapisa o pristupu
- ☐ upravljanje korisničkim računima
- ☐ tehničko održavanje bez prava pregleda snimki
- ☐ udaljeni pristup sustavu
- ☐ drugo: _____

Posebna ograničenja ili uvjeti:

Datum omogućavanja pristupa:

Korisnički račun:

Datum prestanka pristupa:

Razlog prestanka:

Potpis ovlaštene osobe:

Potpis osobe koja je omogućila pristup:

Ovlaštena osoba broj 2.

Ime i prezime:

Radno mjesto ili osnova ovlaštenja:

Razdoblje ovlaštenja:

Lokacije i kamere kojima osoba smije pristupati:

Dodijeljene ovlasti:

- ☐ pregled slike u stvarnom vremenu
- ☐ pregled pohranjenih snimki
- ☐ pretraživanje snimki
- ☐ izdvajanje snimki
- ☐ izvoz i izrada službene preslike
- ☐ dostavljanje snimki nadležnim tijelima
- ☐ omogućavanje kontroliranog uvida ispitaniku
- ☐ pregled zapisa o pristupu
- ☐ upravljanje korisničkim računima
- ☐ tehničko održavanje bez prava pregleda snimki
- ☐ udaljeni pristup sustavu
- ☐ drugo: _____

Posebna ograničenja ili uvjeti:

Datum omogućavanja pristupa:

Korisnički račun:

Datum prestanka pristupa:

Razlog prestanka:

Potpis ovlaštene osobe:

Potpis osobe koja je omogućila pristup:

PRILOG 1.
POPIS OVLAŠTENIH OSOBA I OPSEG DODIJELJENIH OVLASTI

Ovlaštena osoba broj 1.

Ime i prezime:

Radno mjesto ili osnova ovlaštenja:

Razdoblje ovlaštenja:

Lokacije i kamere kojima osoba smije pristupati:

Dodijeljene ovlasti:

- ☐ pregled slike u stvarnom vremenu
- ☐ pregled pohranjenih snimki
- ☐ pretraživanje snimki
- ☐ izdvajanje snimki
- ☐ izvoz i izrada službene preslike
- ☐ dostavljanje snimki nadležnim tijelima
- ☐ omogućavanje kontroliranog uvida ispitaniku
- ☐ pregled zapisa o pristupu
- ☐ upravljanje korisničkim računima
- ☐ tehničko održavanje bez prava pregleda snimki
- ☐ udaljeni pristup sustavu
- ☐ drugo: _____

Posebna ograničenja ili uvjeti:

Datum omogućavanja pristupa:

Korisnički račun:

Datum prestanka pristupa:

Razlog prestanka:

Potpis ovlaštene osobe:

Potpis osobe koja je omogućila pristup:

Ovlaštena osoba broj 2.

Ime i prezime:

Radno mjesto ili osnova ovlaštenja:

Razdoblje ovlaštenja:

Lokacije i kamere kojima osoba smije pristupati:

Dodijeljene ovlasti:

- ☐ pregled slike u stvarnom vremenu
- ☐ pregled pohranjenih snimki
- ☐ pretraživanje snimki
- ☐ izdvajanje snimki
- ☐ izvoz i izrada službene preslike
- ☐ dostavljanje snimki nadležnim tijelima
- ☐ omogućavanje kontroliranog uvida ispitaniku
- ☐ pregled zapisa o pristupu
- ☐ upravljanje korisničkim računima
- ☐ tehničko održavanje bez prava pregleda snimki
- ☐ udaljeni pristup sustavu
- ☐ drugo: _____

Posebna ograničenja ili uvjeti:

Datum omogućavanja pristupa:

Korisnički račun:

Datum prestanka pristupa:

Razlog prestanka:

Potpis ovlaštene osobe:

Potpis osobe koja je omogućila pristup: