Ocena učinka na varstvo osebnih podatkov (DPIA) za sistem videonadzora na javnih površinah v Občini Ankaran – verzija 2

Ocena učinka v zvezi z varstvom osebnih podatkov v skladu s 35. členom splošne uredbe o varstvu podatkov

Podrobnosti o upravljavcu

Upravljavec	Občina Ankaran
Zakoniti zastopnik:	Gregor Strmčnik
Pooblaščena oseba za varstvo podatkov	DATAINFO.SI, d.o.o. e-pošta: dpo@datainfo.si

Povzetek:

Opišite povzetek zakaj uvedba dodatnih kamer, argumenti.

Občina Ankaran se od ustanovitve dalje sooča s porastom vandalizma in kaznivih dejanj na različnih javnih površinah. Ne glede na prisotnost policije in redarjev se nekatera nezakonita dejanja ponavljajo. Slednje prinašajo vedno večje stroške, tako občini kot posameznikom, ki so pri tem oškodovani.

Videonadzor je uveden za zagotavljanje nadzora javne infrastrukture in premoženja, varnosti javnih površin, ljudi in okolja, učinkovitega preganjanja storilcev kaznivih dejanj ter predvsem za doseganje odvračalnega učinka oziroma preprečevanja neželenih dejanj.

V sklopu nadgradnje videonadzora, v verziji dva, se dodajajo nove lokacije javnih površin, kjer se je zaradi porasta kaznivih dejanj in vandalizma pojavila potreba po postavitvi nadzora. Zaradi prenosa lastništva parkirišča Debeli rtič kopališče na Ministrstvo za notranje zadeve se že vzpostavljen videonadzor na tem parkirišču ukinja. Nove lokacije so izbrane na podlagi analize območij, kjer so v preteklosti, kljub okrepljenemu nadzoru, zaznana najpogostejša kazniva dejanja in povzročena največja materialna škoda. Hkrati so nekatere predvidene lokacije namestitve videonadzora iz verzije 1 bile opuščene.

Ukrep v povezavi z vzpostavitvijo videonadzora je nujen, saj z drugimi, milejšimi ukrepi, niso bili doseženi želeni cilji. Pri obdelavi osebnih podatkov bo upravljavec zagotovil spoštovanje vseh zahtev evropske in nacionalne zakonodaje o varstvu osebnih podatkov, ki vključuje tudi spoštovanje načela sorazmernosti pri obdelavi osebnih podatkov in zagotavljanjem varnosti osebnih podatkov pred nepooblaščenim dostopom ter varnostnimi incidenti. Interesi ali temeljne pravice in svoboščine posameznikov, katerih osebni podatki se obdelujejo, ne prevladujejo nad interesi upravljavca

1. korak: Ugotovite potrebo po DPIA

Cilj uporabe video nadzornega sistema je doseči višjo stopnjo varnosti za premoženje in ljudi, ki je ni možno zagotoviti brez uporabe video nadzornega sistema.
Na podlagi dosedanjih izkušenj in ukrepov Občine Ankaran ter izkazanih tveganj in rizikov katerim so izpostavljene določene javne površine in javna infrastruktura, namen iz prejšnjega odstavka ni bil dosežen z milejšimi ukrepi.

Trenutne in predvidena nove lokacije namestitve kamer so:

1. parkirišče in občinska stavba na Lazaretu 4 - že postavljen videonadzor,
2. parkirišče Debeli rtič osrednje - že postavljen videonadzor ,
3. mandrač v Valdoltri – že postavljen videonadzor,
4. parkirišče Ankaran center,
5. mandrač, parkirišče na Sveti Katarini – že postavljen videonadzor,
6. parkirišče Bevkova ulica – nova lokacija,
7. parkirišče Vlahovičeva ulica 1 – nova lokacija,

8. parkirišče Vlahovičeva ulica 2 – nova lokacija,
9. parkirišče Kocjančičeva ulica – nova lokacija,
10. parkirišče Regentova ulica 6 do 10 – nova lokacija,
11. parkirišče Hrvatinova ulica – nova lokacija,
12. parkirišče OŠV Ankaran – nova lokacija,
13. Občinska stavba na Železniški cesti 1 – nova lokacija.

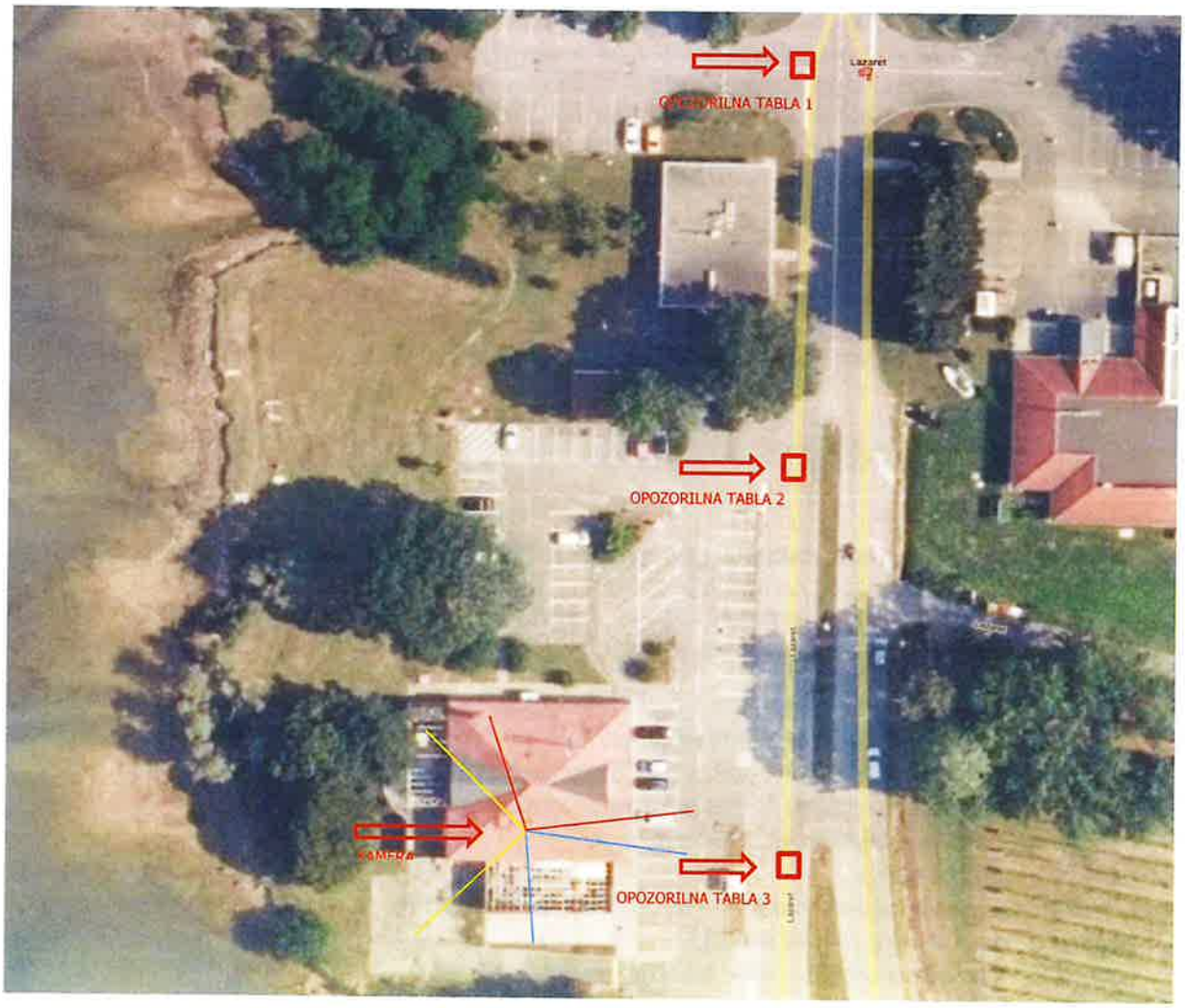
Podrobni podatki o posameznih lokacijah, razlogih in lokaciji posameznih kamer:

1. parkirišče in občinska stavba na Lazaretu 4

Razlogi:
- nedovoljeno kampiranje
- vlomi
- vandalizem
- varovanje servisnega vhoda v objekt
- varovanje parkomata

Lokacija in usmeritev videonadzora:
- kamera na strehi objekta Lazaret 4 v vse smeri

Snemanje:
- pasivno snemanje
- lokalni snemalnik v objektu
- objekt je že povezan v omrežje OA



2. Parkirišče Debeli rtič - osrednje

Razlogi:
- varovanje parkomata
- vandalizem na parkirišču - namerno poškodovanje vozil

Lokacija in usmeritev videonadzora:
Tri kamere iz droga javne razsvetljave usmerjene:
- na parkomat
- na vhod v parkirišče
- na izhod iz parkirišča
- na dostop iz vinograda (kraje, vandalizem)

Snemanje:
- pasivno snemanje
- snemalnik je postavljen v posebno zaklenjeno omarico ob drogu javne razsvetljave
- omrežni dostop do snemalnika iz omarice ob prehodu za pešce na Jadranski cesti (cca 150-200m)

3. Valdoltra – Mandrač

Razlog:
- Varovanje plovil v mandraču.
- Večkrat zaznane kraje na plovilih in vandalizem

Lokacija in usmeritev videonadzora:
- štiri kamere (ena panoramska), ki pokrivajo celoten mandrač ter dostop do le tega skladno s spodnjo shemo.

Snemanje:
- snemanje je pasivno;
- snemalnik je nameščen ob zapornici nasproti gostinskega lokala; nahaja se v posebni zaklenjeni električni omarici;
- dostop do snemalnika je možen fizično ali preko oddaljenega dostopa.

4. Ankaran center

Razlog:
- varovanje parkomata - večkrat poškodovan
- varovanje parkirišča – večkrat poškodovana vozila, kraja katalizatorjev
- varovanje parka – vandalizem, poškodovana urbana oprema

Lokacija in usmeritev videonadzora:
- tri kamere na drogu javne razsvetljave iz smeri pošte proti vhodu v center in na del parkirišča skladno s spodnjo shemo
- dve kameri na drogu javne razsvetljave nad parkomatom pred trgovino Mercator skladno s spodnjo shemo
- dve kameri na drogu javne razsvetljave za trgovino Mercator skladno s spodnjo shemo

Snemanje:
- pasivno snemanje
- snemanje na lokalno SD kartico, snemalnik v prostorih občine Ankaran
- možnost vzpostavitve WiFi linka do kamere iz prostorov občine Ankaran
- dostop do snemalnika je možen fizično ali preko oddaljenega dostopa

5. Mandrač Sv. Katarina

Razlog:

- varovanje plovil v mandraču in vozil na parkirišču,
- večkrat zaznane kraje in vandalizem na plovilih in vozilih, tako podnevi kot tudi ponoči.

Lokacija in usmeritev videonadzora:

- 11 (enajst) kamer, ki pokrivajo celoten mandrač in parkirišče, skladno s spodnjo shemo.

Snemanje:

- snemanje je pasivno;
- snemalnik je nameščen ob robu parkirišča in je dvojno varovan; nahaja se v posebni zaklenjeni omarici, opremljeni z alarmom, ki je nameščena v zaklenjeni električni omarici;
- dostop do snemalnika je možen fizično ali preko oddaljenega dostopa

6. Parkirišče Bevkova ulica,

Razlog:
- vandalizem in kaznivo dejanje poškodovanje tuje stvari
- vlomi v sosednje hiše

Lokacija in usmeritev videonadzora:
- dve kameri na dveh drogovih javne razsvetljave skladno s spodnjo shemo

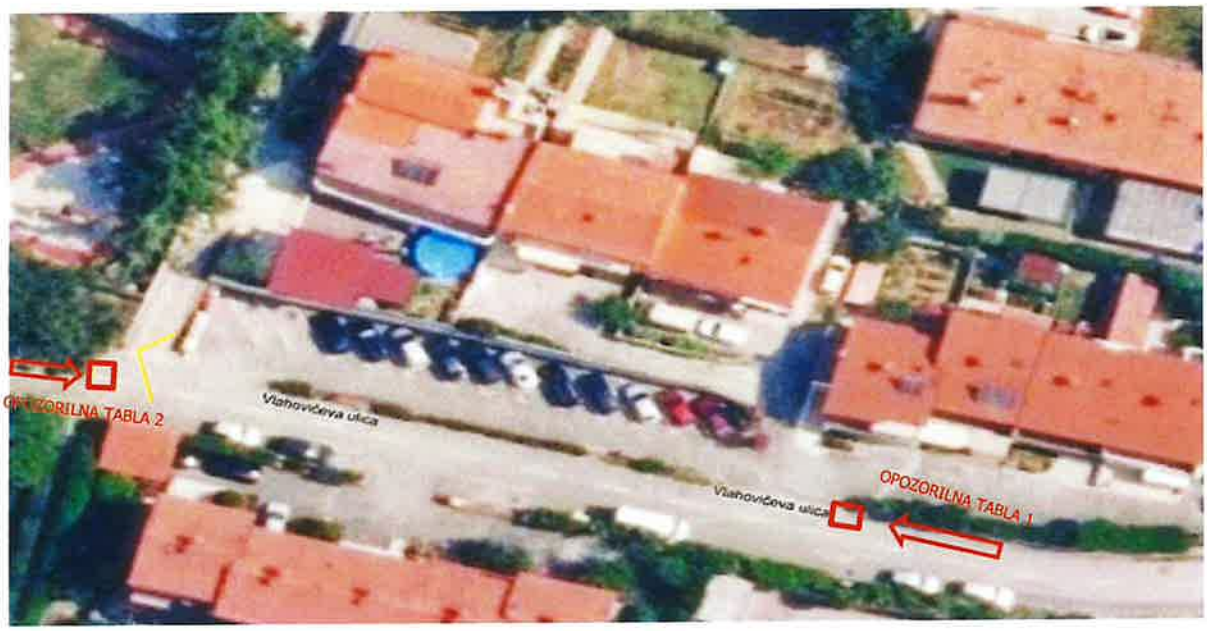
Snemanje:
- pasivno snemanje
- snemalnik bo postavljen v komunikacijski omarici ob drogu javne razsvetljave
- dostop do snemalnika je možen fizično ali preko oddaljenega dostopa

7. parkirišče Vlahovičeva ulica 1,

Razlog:
- vlomi v sosednje hiše
- vandalizem in kaznivo dejanje poškodovanje tuje stvari

Lokacija in usmeritev videonadzora:
- ena kamera na drogu javne razsvetljave skladno s spodnjo shemo

Snemanje:
- pasivno snemanje
- snemalnik bo postavljen v komunikacijski omarici ob drogu javne razsvetljave
- dostop do snemalnika je možen fizično ali preko oddaljenega dostopa



8. Parkirišče Vlahovičeva ulica 2,

Razlog:
- vlomi v sosednje hiše
- vandalizem in kaznivo dejanje poškodovanje tuje stvari

Lokacija in usmeritev videonadzora:
- ena kamera na drogu javne razsvetljave skladno s spodnjo shemo

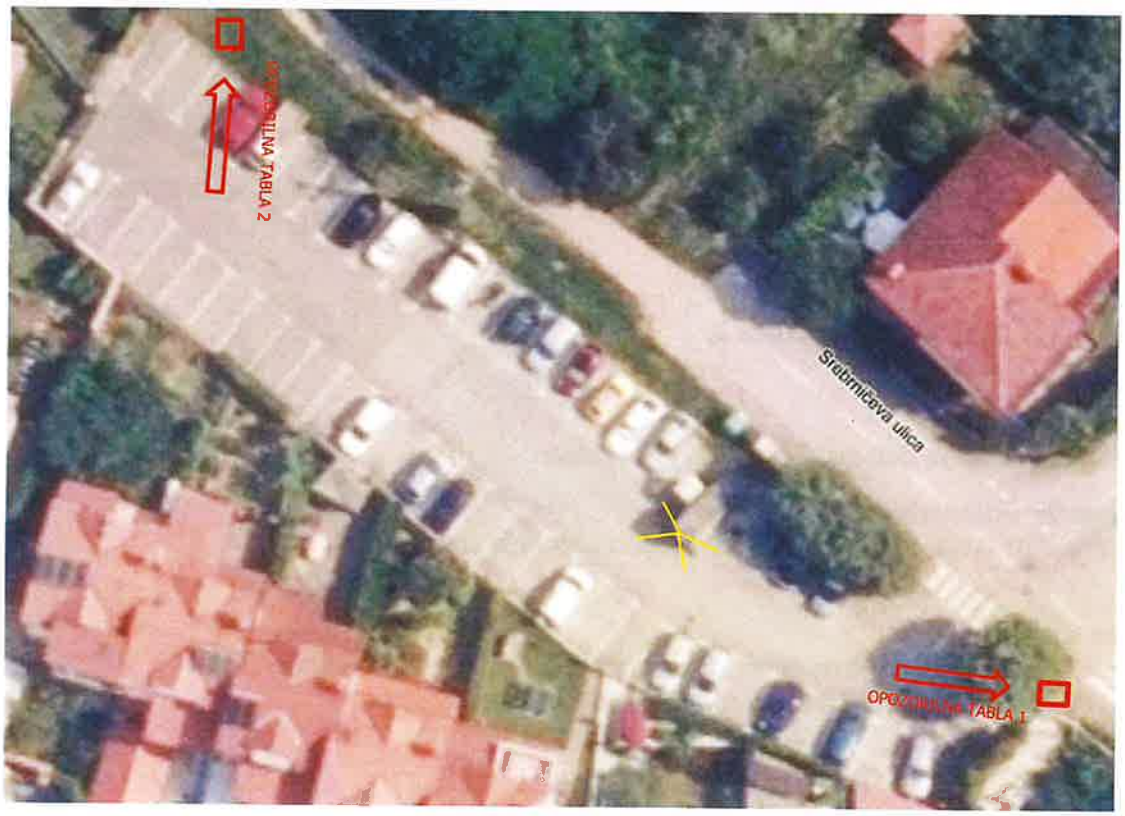
Snemanje:
- pasivno snemanje
- snemalnik bo postavljen v komunikacijski omarici ob drogu javne razsvetljave
- dostop do snemalnika je možen fizično ali preko oddaljenega dostopa

9. Parkirišče Kocjančičeva ulica,

Razlog:
- vlomi v sosednje hiše
- vandalizem in kaznivo dejanje poškodovanje tuje stvari

Lokacija in usmeritev videonadzora:
- dve kameri na drogu nad vhodom v zaklonišče skladno s spodnjo shemo

Snemanje:
- pasivno snemanje
- snemalnik bo postavljen v komunikacijski omarici ob drogu javne razsvetljave
- dostop do snemalnika je možen fizično ali preko oddaljenega dostopa



10. Parkirišče Regentova ulica 6-10,

Razlog:
- vandalizem
- kaznivo dejanje poškodovanje tuje stvari

Lokacija in usmeritev videonadzora:
- tri kamere na drogovih javne razsvetljave skladno s spodnjo shemo orientirana na nadzor vstopa in izstopa iz parkirišča

Snemanje:
- pasivno snemanje
- snemalnik bo postavljen v komunikacijski omarici ob drogu javne razsvetljave, dostop je možen fizično ali preko oddaljenega dostopa.

11. Hrvatinova ulica,

Razlog:
- vandalizem
- kaznivo dejanje poškodovanje tuje stvari

Lokacija in usmeritev videonadzora:
- dve kameri na drogu javne razsvetljave skladno s spodnjo shemo

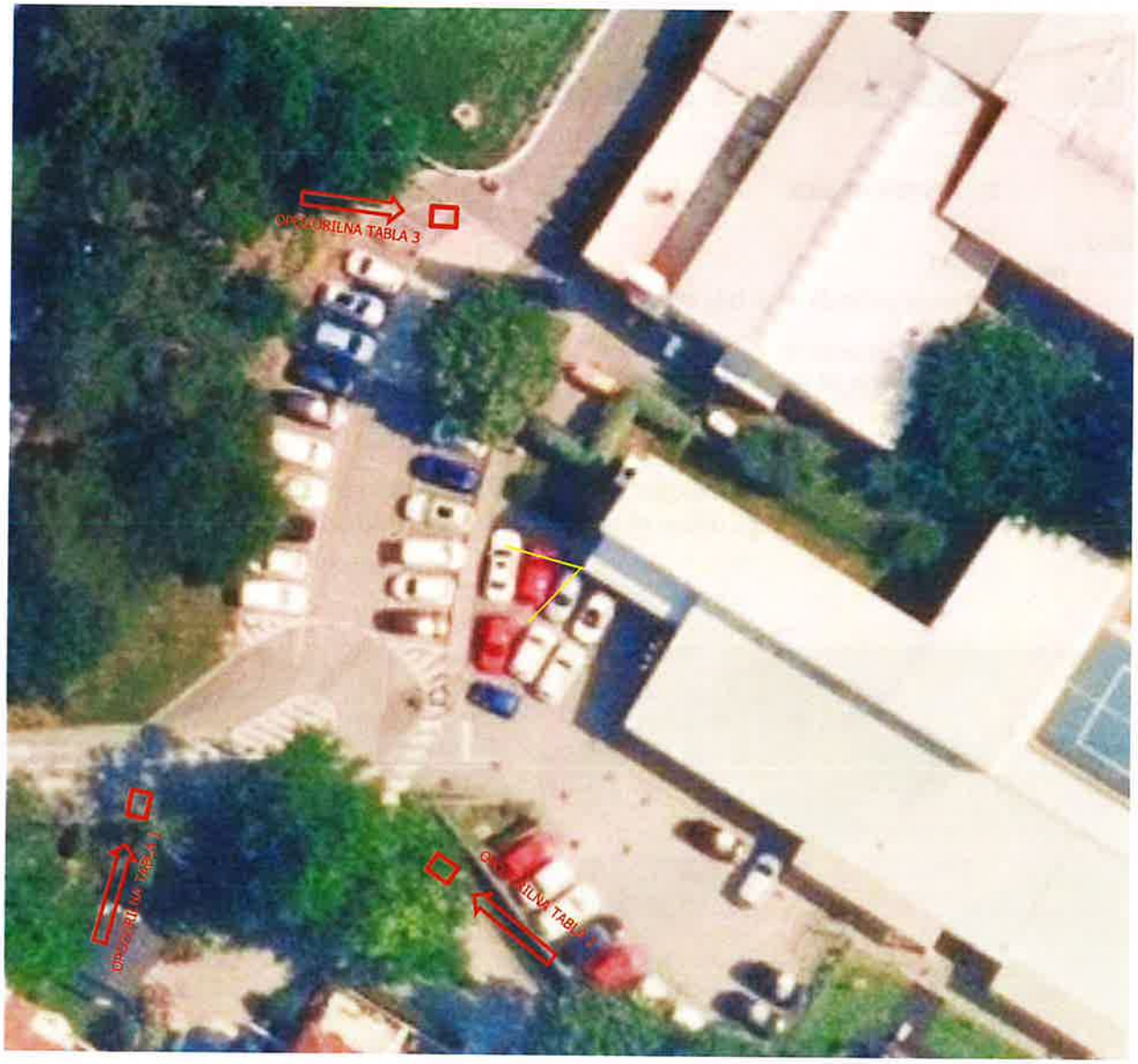
Snemanje:
- pasivno snemanje
- snemalnik bo postavljen v komunikacijski omarici ob drogu javne razsvetljave
- dostop do snemalnika je možen fizično ali preko oddaljenega dostopa

12. Parkirišče pred OŠV Ankaran

Razlog:
- vandalizem
- kaznivo dejanje poškodovanje tuje stvari

Lokacija in usmeritev videonadzora:
- kamera na stavbi vrtca skladno s spodnjo shemo.

Snemanje:
- pasivno snemanje v času delovanja javne razsvetljave
- snemalnik bo postavljen v komunikacijski omarici na stavbi vrtca ob kameri
- dostop do snemalnika je možen fizično ali preko oddaljenega dostopa



13. Občinska stavba na Železniški cesti 1

Razlog:
- Vlom in kraja

Lokacija in usmeritev videonadzora:
- 7 kamer kamere na občinski stavbi skladno s spodnjo shemo
- objekt je ograjen z ograjo.

Snemanje:
- pasivno snemanje
- lokalni snemalnik v objektu
- objekt je že povezan v omrežje OA

V členu št. 35 Splošne uredbe o varstvu podatkov (v nadaljevanju Splošna uredba)[1] je določeno, da kadar obstaja možnost, da bi lahko vrsta obdelave, ob upoštevanju narave, obsega, okoliščin in namenov obdelave povzročila veliko tveganje za pravice in svoboščine posameznikov, upravljavec pred obdelavo opravi oceno učinka predvidenih dejanj obdelave na varstvo osebnih podatkov. Ocena učinka v zvezi z varstvom podatkov iz odstavka 1 se zahteva zlasti v primeru obsežnega sistematičnega spremljanja javno dostopnega območja.

Prav tako Informacijski pooblaščenec Republike Slovenije v kriterijih glede Ocene učinka v zvezi z varstvom podatkov[2] predlaga, da je smiselna izvedba Ocene učinka v primeru sistematičnega nadzora, zlasti v primerih,

[1] Uredba (EU) 2016/679 Evropskega parlamenta in Sveta z dne 27. aprila 2016 o varstvu posameznikov pri obdelavi osebnih podatkov in o prostem pretoku takih podatkov ter o razveljavitvi Direktive 95/46/ES (Splošna uredba o varstvu podatkov).
[2] https://www.ip-rs.si/zakonodaja/reforma-evropskega-zakonodajnega-okvira-za-varstvo-osebnih-podatkov/klju%C4%8Dna-podro%C4%8Dja-uredbe/ocena-u%C4%8Dinka-v-zvezi-z-varstvom-podatkov/#kdajizvesti

kjer se posameznik ne more izogniti obdelavi njegovih osebnih podatkov. Kot primer tovrstnega sistematičnega nadzora, kjer je izvedba Ocene učinka obvezna, je naveden tudi videonadzorni sistem.

Zaradi prej navedenega smo skladno s členom št. 35 Splošne uredbe izvedli oceno učinkov v zvezi z varstvom podatkov (angl. Data Protection Impact Assessment ali DPIA).

Pri pripravi ocene učinkov smo za metodologijo izvedbe upoštevali naslednje smernice oziroma dokumentacijo:

- Smernice glede ocene učinka v zvezi z varstvom podatkov in opredelitve, ali je „verjetno, da bi [obdelava] povzročila veliko tveganje", za namene Uredbe (EU) 2016/679[3]
- Smernice 1/2020 o obdelavi osebnih podatkov v okviru povezanih vozil in aplikacij, povezanih z mobilnostjo (European Data protection Board),[4]
- Smernice Informacijskega pooblaščenca Republike Slovenije: Uporaba GPS sledilnih naprav in varstvo osebnih podatkov,[5]
- Smernice Informacijskega pooblaščenca Republike Slovenije: Ocene učinkov na varstvo podatkov,[6]
- Smernice Informacijskega pooblaščenca Republike Slovenije: Presoje vplivov na zasebnost pri projektih eUprave, [7]
- Standard ISO/IEC29134, [8]
- Smernice angleškega informacijskega pooblaščenca pri DPIA (Privacy impact assessment), [9]
- Metodologijo PECB: Data Protection Impact Assessment Process. [10]

2. korak: Opišite obdelavo

Opišite naravo obdelave

Opišite naravo obdelave: kako boste zbirali, uporabljali, shranjevali in brisali podatke? Kaj je vir podatkov? Ali boste podatke delili s kom? Morda se vam bo zdelo koristno, da se sklicujete na diagram poteka ali drug način opisovanja podatkovnih tokov. Katere vrste obdelave, ki so opredeljene kot verjetno visoko tvegane, so vključene?

Vsaka od zgoraj naštetih lokacij ima lokalno nameščen snemalnik, ki zbira posnetke videonadzornih kamer. Omogočen je oddaljen dostop do snemalnikov, vendar le iz internega računalniškega omrežja občine Ankaran oziroma v okviru pogodbeno dogovorjenih servisnih dostopov.

Dostop do sistema je zaščiten z individualnimi uporabniškimi računi in gesli. Do sistema dostopajo pooblaščene osebe upravljavca ter pogodbeni obdelovalci, in sicer izključno v okviru pogodbenih nalog.

Upravljavec zagotavlja redno tehnično preverjanje delovanja videonadzornega sistema z namenom zagotavljanja njegove zanesljivosti, razpoložljivosti in varnosti.

Tehnično preverjanje izvaja pooblaščena oseba, imenovana s sklepom župana. Pooblaščena oseba se v sistem prijavi izključno z namenom preverjanja tehničnega statusa sistema (npr. delovanje kamer, snemanja, povezljivosti in drugih sistemskih komponent), pri čemer je dostop omejen na najmanjši potreben obseg in čas.

---

[3] https://www.ip-rs.si/fileadmin/user_upload/Pdf/Mednarodno_delovanje/wp248_rev.01_sl.pdf
[4] https://edpb.europa.eu/sites/default/files/consultation/edpb_guidelines_202001_connectedvehicles.pdf
[5] https://www.ip-rs.si/publikacije/priro%C4%8Dniki-in-smernice/smernice-po-splo%C5%A1ni-uredbi-o-varstvu-podatkov-gdpr/uporaba-gps-sledilnih-naprav-in-varstvo-osebnih-podatkov
[6] https://www.ip-rs.si/?id=101
[7] https://www.ip-rs.si/fileadmin/user_upload/Pdf/smernice/Presoje_vplivov_na_zasebnost.pdf
[8] https://www.iso.org/obp/ui/#iso:std:iso-iec:29134:ed-1:v1:en
[9] https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-impact-assessments/
[10] www.pecb.com

V okviru teh aktivnosti pooblaščena oseba ne izvaja vpogleda v posnetke niti njihovega pregleda. Takšen dostop je omejen na tehnične podatke o delovanju sistema in ne vključuje obdelave osebnih podatkov v smislu pregleda videoposnetkov.

Vsi dostopi do sistema se beležijo v revizijskih sledovih, ki omogočajo naknadno preverjanje zakonitosti, namenskosti in obsega dostopov.

Tehnično preverjanje predstavlja organizacijski in tehnični ukrep za zagotavljanje pravilnega delovanja sistema.

Posnetki se samodejno brišejo, ko dosežejo starost treh mesecev. V primeru izrednega dogodka se lahko posamezni posnetki zavarujejo pred izbrisom in hranijo toliko časa, kolikor je potrebno za dosego namena njihove uporabe (npr. kazenski ali odškodninski postopek).

Posnetki se lahko posredujejo organom pregona, sodiščem ali drugim upravičenim subjektom na podlagi ustrezne pravne podlage ter posameznikom, na katere se nanašajo, ob izpolnjevanju pogojev za uveljavljanje pravic po predpisih o varstvu osebnih podatkov.

Opišite obseg obdelave

Opišite obseg obdelave: kakšna je narava podatkov in ali vključuje podatke posebne kategorije ali kaznivega dejanja? Koliko podatkov boste zbirali in uporabljali? Kako pogosto? Kako dolgo ga boste obdržali? Koliko posameznikov je prizadetih? Katero geografsko območje zajema?

Občina izvaja sistematično zbiranje slikovnih posnetkov javnih površin. Vpogled in nadaljnja obdelava posnetkov se izvajata izključno ob nastanku izrednih dogodkov ali na podlagi zakonitih zahtevkov.

Beležijo se naslednji podatki: slikovni posnetek osebe, registrska oznaka vozila, kraj, datum in čas posnetka.

Prizadeti so posamezniki, ki se nahajajo na območju izvajanja videonadzora. Snemanje se izvaja vse dni v letu 24 ur dnevno. Posnetki se hranijo tri mesece, razen v primerih, ko so zavarovani zaradi konkretnega postopka.

Opišite kontekst obdelave

Opišite kontekst obdelave: kakšna je narava vašega odnosa s posamezniki?

Videonadzor se izvaja na javno dostopnih površinah, zato občina s posamezniki nima neposrednega pogodbenega razmerja. Posamezniki so pred vstopom na območje snemanja ustrezno obveščeni o izvajanju videonadzora.

Koliko nadzora bodo imeli?

Posamezniki lahko uveljavljajo pravice v skladu s predpisi o varstvu osebnih podatkov. Občina izvaja obdelavo osebnih podatkov v obsegu, ki je nujen za dosego zakonitega namena.

Ali bi pričakovali, da boste njihove podatke uporabili na ta način?

Da.

Pred vstopom na področje izvajanja videonadzora bodo seznanjeni s pogoji. Ali vključujejo otroke ali druge ranljive skupine?

Videonadzoru bodo podvržene vse osebe, ki bodo zašle na območje snemanja.

Ali obstajajo predhodni pomisleki glede te vrste obdelave ali varnostnih napak?
Ne.

Ali obstajajo aktualna vprašanja javnega pomena, ki bi jih morali upoštevati?

Ne.

Ali ste podpisani v kateri koli odobreni kodeks ravnanja ali certifikacijsko shemo (ko je kateri koli odobren)?

Ne.

Opišite namene obdelave
Opišite namene obdelave: kaj želite doseči? Kakšen je predviden učinek na posameznike? Kakšne so prednosti obdelave – za vas in širše?

Namen uvedbe videonadzora je zmanjšanje tveganj za oškodovanje javnega in zasebnega premoženja ter povečanje varnosti ljudi.
Videonadzor omogoča učinkovitejše odkrivanje in preiskovanje kaznivih dejanj ter zagotavljanje dokaznega gradiva v kazenskih, odškodninskih ali drugih postopkih.
Učinek na posameznike predstavlja poseg v zasebnost v obsegu snemanja njihove prisotnosti na javnih površinah, vendar je ta poseg omejen na nujno potreben obseg ter zavarovan z ustreznimi tehničnimi in organizacijskimi ukrepi.
Občina zagotavlja transparentnost izvajanja videonadzora z obveščanjem preko spletne strani, družabnih omrežij in občinskega glasila Amfora.

3. korak: Postopek posvetovanja

Razmislite, kako se posvetovati z ustreznimi zainteresiranimi stranmi: opišite, kdaj in kako boste iskali mnenja posameznikov – ali utemeljite, zakaj to ni primerno. Koga še morate vključiti v svojo organizacijo? Ali morate za pomoč prositi svoje procesorje? Ali se nameravate posvetovati s strokovnjaki za informacijsko varnost ali s kakšnimi drugimi strokovnjaki?

Zainteresirana javnost je bila vključena v proces skozi objavo namere o uvedbi tehničnega varovanja v občinskem glasilu ter na spletni strani občine. Na enak način bo seznanjena ob nadgradnji sistema. Pri pripravi predloga je sodelovala Policija in Medobčinsko redarstvo. Z nadgradnjo tehničnega varovanja se je seznanil Občinski svet. Potrebno je vključiti vse akterje, ki so do sedaj sodelovali pri postavitvi obstoječih nadzornih sistemov.

4. korak: Ocenite nujnost in sorazmernost

Opišite ukrepe za skladnost in sorazmernost, zlasti:

Samo zbiranje podatkov ima določen vpliv na zasebnost posameznikov, saj zmanjšuje stopnjo anonimnosti na javnih površinah. Vendar bi bila brez uvedbe videonadzora lahko ogrožena varnost ljudi in premoženja, zlasti v nočnem času. Videonadzor je zato ocenjen kot nujen in sorazmeren ukrep za dosego zakonitega cilja. Tveganje se bo zmanjšalo s krajšanjem roka za shranjevanje posnetkov ter zagotovitvijo varnostnih mehanizmov, ki bodo preprečili zlorabe. Videonadzor je ocenjen kot nujen in sorazmeren ukrep za dosego zakonitega cilja.

Kakšna je vaša zakonita podlaga za obdelavo?

Pravna podlaga za izvajanje videonadzora je člen 6(1)(e) Splošne uredbe o varstvu podatkov (obdelava, potrebna za opravljanje naloge v javnem interesu) v povezavi z določbami ZVOP-2, ki urejajo izvajanje videonadzora na javno dostopnih površinah.
Obdelava se izvaja z namenom zagotavljanja varnosti ljudi ter varovanja javnega in zasebnega premoženja.

Ali obdelava dejansko doseže vaš namen?

Videonadzor omogoča preventivno delovanje ter učinkovitejše odkrivanje in preiskovanje kaznivih dejanj oziroma drugih škodnih dogodkov. Posnetki lahko služijo kot dokazno gradivo v kazenskih, odškodninskih ali drugih postopkih.
Sistem je usmerjen v pasivno zbiranje podatkov, vpogled in nadaljnja obdelava pa se izvajata le ob izrednih dogodkih ali zakonitih zahtevkih.

Ali obstaja drug način za dosego enakega rezultata?

Občina je preučila milejše ukrepe (npr. povečana prisotnost redarstva, policije, dodatna osvetlitev), vendar ti ne zagotavljajo enake ravni preventivnega učinka in možnosti naknadnega dokazovanja dogodkov.
Videonadzor je ocenjen kot primeren in sorazmeren ukrep za dosego zastavljenega namena.

Kako boste zagotovili kakovost podatkov in minimizacijo podatkov?

Sistem beleži izključno slikovne posnetke javnih površin ter pripadajoče podatke (datum, čas, kraj posnetka). Snemanje zvoka ni omogočeno.
Rok hrambe je omejen na tri mesece, razen v primeru zavarovanja posnetkov za potrebe konkretnega postopka.
Dostop do sistema je omejen na nujno potreben obseg, vpogled pa se izvaja le ob izrednih dogodkih.

Katere informacije boste dali posameznikom?

Območja izvajanja videonadzora so ustrezno označena z obvestili, ki vsebujejo informacije o upravljavcu, in namenu obdelave. Dodatne informacije so dostopne na spletni strani občine, do katere je mogoče dostopati preko QR kode, ki vodi na Politiko varstva podatkov.

Kako boste pomagali podpreti njihove pravice?

Posamezniki lahko uveljavljajo pravice do dostopa, izbrisa, omejitve obdelave in druge pravice v skladu s predpisi o varstvu osebnih podatkov.
Zahteve se obravnavajo skladno z internimi pravili o varstvu osebnih podatkov in v zakonsko določenih rokih.

Katere ukrepe izvajate, da zagotovite skladnost obdelovalcev?

Upravljavec sodeluje z dvema zunanjima izvajalcema, ki nastopata kot pogodbeni obdelovalci osebnih podatkov:
– izvajalec IT podpore (operater sistema),
– izvajalec montaže, vzdrževanja in servisa videonadzorne opreme.
Z obema obdelovalcema je sklenjena pogodba oziroma aneks o obdelavi osebnih podatkov skladno s 28. členom GDPR.
Dostop obdelovalcev do sistema je omejen na nujno potreben obseg, individualiziran z uporabniškimi računi ter predmet revizijske sledi. Upravljavec redno preverja ustreznost dodeljenih pooblastil.

Kako varujete morebitne mednarodne prenose?

Podatki se ne izvažajo v tretje države.

Zakonitost
Upravljavec ugotavlja, da uvaja projekt v skladu s trenutno veljavno zakonodajo na področju varstva osebnih podatkov. Pravna podlaga za zbiranje, hrambo ali druge vrste obdelav osebnih podatkov je utemeljena na naslednjih pravnih temeljih:

V konkretnem primeru je pravno podlago za obdelavo osebnih podatkov mogoče utemeljiti na podlagi določil Splošne uredbe o varstvu podatkov (Splošna uredba, ang. GDPR), Zakona o varstvu osebnih podatkov (ZVOP-2) in področne zakonodaje, kot je pojasnjeno v nadaljevanju.

Informacije za posameznike in njihove pravice
Upravljavec mora posameznikom v skladu s členom 13 oziroma 14 Splošne uredbe zagotoviti naslednje informacije:

- identiteto in kontaktne podatke upravljavca in njegovega predstavnika, kadar ta obstaja,
- kontaktne podatke pooblaščene osebe za varstvo podatkov, kadar ta obstaja,
- namene, za katere se osebni podatki obdelujejo, kakor tudi pravno podlago za njihovo obdelavo,
- zakonite interese, za uveljavljanje katerih si prizadeva upravljavec
- uporabnike ali kategorije uporabnikov osebnih podatkov, če obstajajo.

Upravljavec mora posamezniku zagotoviti tudi naslednje informacije, ki so potrebne za zagotavljanje poštene in pregledne obdelave v zvezi s posameznikom, na katerega se nanašajo osebni podatki:

- obdobje hrambe osebnih podatkov ali, kadar to ni mogoče, merila, ki se uporabijo za določitev tega obdobja;
- obstoj pravice, da se od upravljavca zahtevajo dostop do osebnih podatkov in popravek ali izbris osebnih podatkov ali omejitev obdelave v zvezi s posameznikom, na katerega se nanašajo osebni podatki, ali obstoj pravice do ugovora obdelavi in pravice do prenosljivosti podatkov,
- pravico do vložitve pritožbe pri nadzornem organu,
- obstoj avtomatiziranega sprejemanja odločitev, vključno z oblikovanjem profilov iz člena 22(1) in (4) Splošne uredbe, ter vsaj v takih primerih smiselne informacije o razlogih zanj, kot tudi pomen in predvidene posledice take obdelave za posameznika, na katerega se nanašajo osebni podatki.

Dopustno je, da upravljavec osnovne informacije navede na vidnem mestu pred vstopom v območje videonadzora. S pomočjo objave Politike varstva podatkov pa pripravi podrobne informacije na spletni strani.

Osnutek obvestila, ki se namesti:
OBMOČJE VIDEONADZORA
Namen: Varovanje ljudi in premoženja.
Upravljalec podatkov:
Občina Ankaran
E-pošta: info@obcina-ankaran.si
Telefon: +386 (0)5 66 53 000

Več informacij o obdelavi osebnih podatkov in uveljavljanju pravic posameznikov je dostopnih preko QR kode.

AREA VIDEOSORVAGLIATA
Finalita: Protezione delle persone e dei beni.
Titolare del trattamento:
Comune di Ancarano
E-mail: info@obcina-ankaran.si
Telefono: +386 (0)5 66 53 000

Ulteriori informazioni sul trattamento dei dati personali e sull'esercizio dei diritti sono disponibili tramite codice QR.

Zaposleni posamezniki bodo o sistemu, njegovi uporabi in mehanizmih varovanja ter pravicah, ki iz tega izhajajo obveščeni tudi preko sprejetega internega akta (pravilnika), s katerim se podrobneje ureja delovanja sistema.

Preverjanje obdelovalcev

Upravljavec za izvajanje videonadzornega sistema sodeluje z zunanjimi izvajalci, ki v okviru pogodbenih nalog lahko dostopajo do sistema videonadzora in s tem do osebnih podatkov (posnetkov).

Zunanji izvajalci nastopajo v vlogi pogodbenih obdelovalcev osebnih podatkov v smislu člena 28 Splošne uredbe o varstvu podatkov (GDPR). To vključuje:

– zunanjega izvajalca IT podpore, ki opravlja funkcijo operaterja sistema in upravlja ter administrira videonadzorni sistem,
– zunanjega izvajalca, ki izvaja montažo, vzdrževanje in servisiranje videonadzorne opreme ter ima v okviru teh nalog dostop do sistema ali posnetkov.

Z obema obdelovalcema ima upravljavec sklenjeno pogodbo oziroma aneks o obdelavi osebnih podatkov skladno s 28. členom GDPR. Pogodbe določajo predmet, trajanje, naravo in namen obdelave ter obveznosti in pravice upravljavca in obdelovalcev.

Obdelovalca osebne podatke obdelujeta izključno na podlagi dokumentiranih navodil upravljavca ter zagotavljata ustrezne tehnične in organizacijske ukrepe za varstvo osebnih podatkov. Dostop do sistema je omejen na nujno potreben obseg ter je časovno in funkcionalno omejen glede na vrsto storitve.

Upravljavec redno preverja izpolnjevanje pogodbenih obveznosti obdelovalcev.

Iznos podatkov v tretje države

Upravljavec mora izbrati takega ponudnika storitve (obdelovalca), ki v primeru programskih rešitev ali oblačnih storitev (podobdelovalci) uporablja take storitve, ki omogočajo omejitev iznosa podatkov izključno na države znotraj EU. V nasprotnem primeru mora v skladu s Splošno uredbo zagotoviti enak standard varovanja osebnih podatkov, kot velja po Splošni uredbi in posameznikom nuditi informacije o tem, da namerava upravljavec prenesti osebne podatke uporabniku v tretji državi ali mednarodni organizaciji, ter o obstoju ali neobstoju sklepa Komisije o ustreznosti ali v primeru prenosov iz člena 46 ali 47 ali drugega pododstavka člena 49(1) Splošne uredbe sklic na ustrezne ali primerne zaščitne ukrepe in sredstva za pridobitev njihove kopije ali kje so na voljo.

Korak 5: Prepoznava in ocena tveganj

Za oceno tveganj je uporabljena metodologija, pri kateri se za posamezna tveganja določi najprej verjetnost, da do realizacije tveganja oziroma grožnje pride, nato se določi kakšen vpliv ima realizacija tveganja na pravice in svoboščine posameznika, na katerega se nanašajo osebni podatki, ter se izračuna skupna ocena tveganja, ki predstavlja zmnožek verjetnosti in resnosti vpliva.

Verjetnost tveganja/grožnje ocenjujemo s stopnjami 1 (nizka), 2 (srednja), 3 (visoka) in 4 (zelo visoka). Pri tem se uporabljajo naslednje smernice in kazalci za oceno.

- 4 - pomeni verjetnost uresničitve oz. realizacije grožnje vsak mesec ali pogosteje.
- 3 - pomeni verjetnost uresničitve oz. realizacije grožnje vsako leto.
- 2 - pomeni verjetnost uresničitve oz. realizacije grožnje na nivoju med 5 in 10 let.
- 1 - pomeni verjetnost uresničitve oz. realizacije grožnje vsakih 10 let ali redkeje.

Škoda (učinek tveganja/grožnje) ocenjujemo s stopnjami 1 (nizka), 2 (srednja), 3 (visoka) in 4 (zelo visoka). Škoda se ocenjuje z vidika vpliva na pravice in svoboščine posameznika (poseg v zasebnost, izguba nadzora nad osebnimi podatki, možnost nepooblaščenega spremljanja ali razkritja podatkov), ne z vidika poslovne ali finančne škode upravljavca. Pri tem se uporabljajo naslednje smernice in kazalci za oceno.

- Za 4 (zelo visoka stopnja) predstavlja posebej hud poseg v zasebnost posameznika, sistematično in dolgotrajno spremljanje gibanja ali razkritje občutljivih okoliščin, ki lahko povzroči resne ali trajne negativne posledice za posameznika.
- Za stopnjo 3 (visoka stopnja) je značilen pomemben poseg v zasebnost posameznika ali nepooblaščen dostop oziroma razkritje posnetkov, ki lahko povzroči znatne, vendar ne trajne posledice za posameznika.
- Za stopnjo 2 (srednja stopnja) je značilen omejen poseg v zasebnost ali posamičen nepooblaščen vpogled brez hujših posledic za posameznika.
- Za stopnjo 1 (nizka stopnja) pomeni minimalen vpliv na zasebnost brez zaznavnih posledic.

Skupna ocena tveganja predstavlja zmnožek ocene verjetnosti in učinka. Pri tem se uporabljajo naslednje zaključki glede na pridobljeno oceno:

- Od 12 do 16 je zelo veliko tveganje in predstavlja nesprejemljivo tveganje,
- Od 8 do 11 je veliko tveganje in še vedno predstavlja nesprejemljivo tveganje.
- Od 4 do 7 predstavlja srednje in sprejemljivo tveganje
- Od 1 do 3 predstavlja nizko in sprejemljivo tveganje.

	Opišite vir tveganja in naravo možnega vpliva na posameznike. Po potrebi vključite povezana tveganja skladnosti in občine.	**Verjetnost tveganja/ grožnje**	**Škoda (učinek tveganja/grožnje)**	**Skupna ocena tveganja**
1	**Tveganje nedovoljenega dostopanja do osebnih podatkov s strani zaposlenih ali pogodbenih sodelavcev** Neupravičen ali prekoračen vpogled v posnetke s strani pooblaščenih oseb ali pogodbenih obdelovalcev (IT operater ter vzdrževalec sistema) lahko pomeni poseg v zasebnost posameznika ter razkritje informacij o njegovem gibanju in drugih osebnih podatkih. Tveganje	2	3	**6**

	zajema tudi možnost zlorabe s strani oseb, ki imajo dostop do sistema, pri čemer lahko pride do neupravičene seznanitve s podatki ali drugih škodljivih posledic, vključno z materialno škodo. Posebno pozornost zahteva tudi dostop do sistema, namenjen tehničnemu preverjanju delovanja, saj obstaja možnost njegove zlorabe za neupravičen vpogled v posnetke. Takšen scenarij lahko vodi do nedovoljene obdelave osebnih podatkov.			
2	**Tveganje izgube, kraje, nedovoljene odstranitve osebnih podatkov ter nepooblaščene ali nenamerne spremembe osebnih podatkov** Nezakonito razkritje posnetkov lahko povzroči poseg v zasebnost ter izgubo nadzora nad osebnimi podatki posameznika.	2	3	**6**
3	**Tveganje prekomernega zbiranja, združevanja in povezovanja osebnih podatkov** Neskladna postavitev kamer ali širše snemanje od potrebnega lahko pomeni nesorazmeren poseg v zasebnost.	2	2	**4**
4	**Tveganje neupoštevanja posameznikovih pravic pri obdelavi osebnih podatkov** Onemogočeno uveljavljanje pravice do dostopa, izbrisa ali omejitve obdelave pomeni poseg v pravice posameznika.	2	2	**4**
5	**Tveganje obdelave osebnih podatkov brez ustrezne pravne podlage ali vednosti posameznika o tem** Posameznik ni ustrezno seznanjen z obdelavo njegovih podatkov.	1	3	**3**
6	**Tveganje posredovanja osebnih podatkov tretjim osebam ali v tretje države brez ustrezne pravne podlage** Razkritje posnetkov brez pravne podlage pomeni resen poseg v zasebnost.	1	3	**3**
7	**Tveganje hrambe osebnih podatkov preko dovoljenih rokov** Dolgotrajno shranjevanje omogoča nepotrebno spremljanje gibanja posameznika.	2	3	**6**
8	**Tveganje uporabe osebnih podatkov v nasprotju z namenom** Uporaba posnetkov za druge namene pomeni nedopusten poseg v pravice posameznika.	2	3	**6**
9	**Tveganja povezana z avtomatiziranim odločanjem** Sistem ne vključuje avtomatiziranega odločanja, zato je tveganje minimalno.	1	1	**1**
10	**Tveganja povezana z nedelovanjem sistema** Nezmožnost zagotovitve dokaznega gradiva lahko vpliva na pravno varstvo posameznika.	2	2	**4**

Korak 6: Prepoznava ukrepov za zmanjšanje tveganj

	Tveganje	Ukrepi in možnosti za zmanjšanje ali odpravo tveganja	Tveganje pred ukrepi	Verjetnost tveganja/ grožnje po ukrepih	Škoda (učinek tveganja/ grožnje) po ukrepih	Končno tveganje ob upoštevanju ukrepov	Tveganje je
1	Tveganje nedovoljenega dostopanja do osebnih podatkov s strani zaposlenih	Omejena možnost dostopa do podatkov na pooblaščene zaposlene z dodeljenim uporabniškim imenom in geslom. Redno preverjanje ustreznosti dodeljenih pooblastil za dostop do podatkov v sistemih. Osebe, ki imajo možnost obdelave podatkov morajo biti pooblaščeni. Z zunanjimi izvajalci (pogodbenimi obdelovalci) je sklenjena pogodba o obdelavi osebnih podatkov skladno s 28. členom Splošne uredbe o varstvu podatkov (GDPR). Dostop obdelovalcev do sistema je omejen na nujno potreben obseg glede na vrsto storitve ter je časovno in funkcionalno omejen. Vključena je revizijska sled dostopov in vpogledov v sistem, zlasti v primerih obdelave osebnih podatkov. Redno izobraževanje zaposlenih o varstvu osebnih podatkov. Ustrezno varovanje mehanizmov za avtentikacijo – dostop je omogočen le z individualnim uporabniškim imenom in geslom, ki je dodeljeno izključno pooblaščenim osebam. Interna pravila določajo pravice IT skrbnika (administratorja) ter obseg in način izvajanja tehničnega vzdrževanja sistema.	6	1	3	**3**	Zmanjšano, sprejemljivo tveganje
2	Tveganje izgube, kraje, nedovoljene odstranitve osebnih podatkov ter nepooblaščene ali nenamerne spremembe osebnih podatkov	Interna pravila, v katerih so opredeljeni postopki varnostnega kopiranja in hranjenja podatkov (lokalno in na dislocirani lokaciji). Za ponudnika hrambe podatkov je izbran priznan in zanesljiv ponudnik, ki lahko izkaže visok nivo varnosti. Revizijska sled za dostope in spremembe. Ustrezno varovanje mehanizmov za avtentikacijo.	6	1	3	**3**	Zmanjšano, sprejemljivo tveganje

	Tveganje	Ukrepi in možnosti za zmanjšanje ali odpravo tveganja	Tveganje pred ukrepi	Verjetnost tveganja/ grožnje po ukrepih	Škoda (učinek tveganja/ grožnje) po ukrepih	Končno tveganje ob upoštevanju ukrepov	Tveganje je
3	Tveganje prekomernega zbiranja, združevanja in povezovanja osebnih podatkov	Redno preverjanje sklenjenih sporazumov z upravljavci. Redno preverjanje ali za izvajanje obstaja pravna podlaga. Omejena možnost dostopa do podatkov na pooblaščene zaposlene z dodeljenim uporabniškim imenom in geslom. Prilagoditi čas hrambe osebnih podatkov na najkrajši možni čas, da lahko dosežemo želen namen.	4	1	2	2	Zmanjšano, sprejemljivo tveganje
4	Tveganje neupoštevanja posameznikovih pravic pri obdelavi osebnih podatkov	Interni akti, predvsem pa politika zasebnosti, kjer je opredeljeno uveljavljanje pravic posameznika. Objava ustreznega dokumenta z opisom pravic in postopkom uveljavljanja pravic posameznikom, katerih podatki se obdelujejo. Aktivno vključevanje pooblaščene osebe za varstvo podatkov, ki skrbi za zaščito pravic posameznikov v primeru zahtev oziroma uveljavljanje pravic.	4	1	2	2	Zmanjšano, sprejemljivo tveganje
5	Tveganje obdelave osebnih podatkov brez ustrezne pravne podlage ali vednosti posameznika o tem	Obvezna namestitev obvestila namestitev na spletno stran, da se posameznik nedvoumno seznani z dejstvom o snemanju z možnostmi uveljavljanja pravic (npr. kratek opis in QR koda na obvestilu, v politiki zasebnosti). Testni izpis revizijske sledi vpogledov v videonadzorni sistem (kdo in kdaj je vpogledoval). Interna navodila za zaposlene, ki imajo pooblastilo upravljanja s sistemom sledenja. Sprejeti interni akt (pravilnik), s katerim se podrobneje ureja delovanja videonadzornega sistema.	3	1	2	2	Zmanjšano, sprejemljivo tveganje

	Tveganje	Ukrepi in možnosti za zmanjšanje ali odpravo tveganja	Tveganje pred ukrepi	Verjetnost tveganja/ grožnje po ukrepih	Škoda (učinek tveganja/ grožnje) po ukrepih	Končno tveganje ob upoštevanju ukrepov	Tveganje je
6	Tveganje posredovanja osebnih podatkov tretjim osebam ali v tretje države brez ustrezne pravne podlage	Pregled razmerij s pogodbeni obdelovalci in sklenitev ustreznih pogodb o obdelavi osebnih podatkov ter uvrstitev na seznam obdelovalcev. Redno preverjanje pogodbenih (pod) obdelovalcev, ki skrbijo za videonadzorni sistem najmanj enkrat letno.	3	1	2	2	Zmanjšano, sprejemljivo tveganje
7	Tveganje hrambe osebnih podatkov preko dovoljenih rokov	Interna pravila z opredelitvijo rokov hrambe podatkov v sistemu. Avtomatiziran postopek brisanja podatkov snemanja in drugih osebnih podatkov uporabnika v sistemu po preteku rokov hrambe. Vodenje in redno preverjanje Evidence dejavnosti obdelave z opredelitvijo rokov hrambe podatkov.	6	1	2	2	Zmanjšano, sprejemljivo tveganje
8	Tveganje uporabe osebnih podatkov v nasprotju z namenom	Omejena možnost dostopa do podatkov na pooblaščene zaposlene z dodeljenim uporabniškim imenom in geslom. Vključena je revizijska sledi v sistemu za primere, v katerih se obdeluje osebne podatke. Ustrezno varovanje mehanizmov za avtentikacijo – dostop je omogočen le z individualnim uporabniškim imenom in geslom, ki je dodeljeno izključno pooblaščenemu zaposlenemu. Pooblaščena oseba, ki ima dostop do sistema ima omejene dostopne pravice glede na delovne naloge, ki jih opravlja (nivojski dostopi). Redno izobraževanje zaposlenih s področja varstva podatkov.	6	1	2	2	Zmanjšano, sprejemljivo tveganje

	Tveganje	Ukrepi in možnosti za zmanjšanje ali odpravo tveganja	Tveganje pred ukrepi	Verjetnost tveganja/ grožnje po ukrepih	Škoda (učinek tveganja/ grožnje) po ukrepih	Končno tveganje ob upoštevanju ukrepov	Tveganje je
9	Tveganja povezana z avtomatiziranim odločanjem	Informiranje posameznikov o možnostih uveljavljanja pravic, glede avtomatizirane obdelave podatkov (Politika zasebnosti). Sprejeta interna pravila in postopki pri upravljavcu v primerih ko posameznik uveljavlja pravice glede avtomatizirane obdelave. Vključena je revizijska sled in nivojski dostopi predvsem za primere, v katerih se obdeluje osebne podatke. Redno preverjanje in nadzor nad vključenimi funkcionalnostmi in pravilnostjo delovanja sistema.	**1**	1	1	1	Sprejemljivo tveganje
10	Tveganja povezana z nedelovanjem sistema	Interna pravila glede vzdrževanja opreme. Sklenjena vzdrževalna pogodba za redno vzdrževanje sistema z zunanjim izvajalcem. Redno izdelovanje varnostnih kopij podatkov.	**4**	1	2	2	Zmanjšano, sprejemljivo tveganje

Nujni skupni ukrepi:

- Določitev internih pravil glede uporabe sistema (pooblastila, dopustnost vpogledov, revizijska sled, roki hrambe, anonimizacija ...);
- Redni letni pregled pooblaščene osebe za varstvo podatkov, preverjanje pogodbenega obdelovalca;
- Ponovno preverjanje Ocene učinka (DPIA) v roku 1 leta oz. ob spremembi zakonodaje in redno ponavljanje preverjanja;
- Preverjanje vpogledov v sistem in priprava poročila;
- Redno letno izobraževanje zaposlenih na področju varstva osebnih podatkov.

7. korak: Zaključek in povzetek rezultatov

Preverjanje elementov, ki jih mora vsebovati ocena učinkov, na osnovi Smernic EDPB:

	Podan je sistematičen opis obdelave (člen 35(7a)):
✓	• Upoštevani so narava, obseg, okoliščine in nameni obdelave (uvodna določba 90);
✓	• Opredeljen je nabor podatkov, upravljavci in uporabniki ter roki hrambe;
✓	• Podan je opis podatkovnih tokov in udeleženih subjektov;
✓	• Podan je opis sredstev obdelave (strojne in programske opreme, omrežij, človeških virov in uporabljenih komunikacijskih sredstev);
✓	• Upoštevana je skladnost z odobrenimi kodeksi ravnanja (člen 35(8)).
	Podana je ocena nujnosti in sorazmernosti (člen 35(7b)):
	Opredeljeni so ukrepi za zagotavljanje skladnosti, ki vključujejo:
	1.) ukrepe, ki prispevajo k upoštevanju nujnosti in sorazmernosti, in spoštovanju temeljnih načel:
✓	• določeni, izrecni in zakoniti namen(i) (člen 5(1b));
✓	• zakonitost obdelave (člen 6);
✓	• obdelava je ustrezna, relevantna in omejena na to, kar je potrebno za namene, za katere se obdelujejo podatki (člen 5(1c));
✓	• upoštevani je omejitev shranjevanja – roki hrambe (člen 5(1e))
	2.) ukrepe, ki prispevajo k varstvu pravic posameznika:
✓	• informiranje posameznika o obdelavi podatkov (členi 12, 13 in 14);
✓	• pravica do seznanitve in prenosljivosti podatkov (člena 15 in 20);
✓	• pravica do popravka in izbrisa podatkov (člena 16, 17 in 19);
✓	• pravica do ugovora in omejitve obdelave (členi 18, 19 in 21);
✓	• odnosi s (pogodbenimi) obdelovalci (člen 28);
✓	• varovalke glede prenosa podatkov v tretje države (Poglavje V.);
✓	• predhodno posvetovanje (člen 36).
	Obvladovana so tveganja za pravice in svoboščine posameznika:
	Podana je ocena izvora, narave, posebnosti in resnosti tveganj (uvodna določba 84), pri čemer so tveganja ocenjena z vidika posameznika, tako da:
✓	• so upoštevani viri tveganj (uvodna določba 90);
✓	• so upoštevani možni učinki na pravice posameznika v primeru nezakonitega dostopa, spremembe ali izgube podatkov;
✓	• sta ocenjeni verjetnost in resnost tveganj (uvodna določba 90).
	Opredeljeni so ukrepi za obvladovanje tveganj (člen35(7d) in uvodna določba 90).
	Vključene so zainteresirane strani:
✓	• Pridobljeno je mnenje pooblaščene osebe za varstvo podatkov (člen 35(2));
✓	• Pridobljena so mnenja posameznikov oziroma predstavnikov posameznikov, kjer je to primerno (člen 35(9)).

Zaključek in priporočila

Na podlagi izvedene ocene učinkov na varstvo osebnih podatkov se ugotavlja, da:

- so vsa prepoznana tveganja po izvedbi tehničnih in organizacijskih ukrepov sprejemljiva,
- ni zaznati preostalih tveganj, ki bi terjala predhodno posvetovanje z Informacijskim pooblaščencem (člen 36 GDPR),
- obdelava osebnih podatkov v okviru videonadzora javnih površin je nujna, sorazmerna in skladna z zakonitim namenom zagotavljanja varnosti ljudi in premoženja,
- ukrepi skladnosti so ustrezno določeni, vključno z rednim preverjanjem pooblaščene osebe za varstvo podatkov in periodičnim pregledom sistema.

Priporočila za nadaljnje ukrepanje:

1. Posodobitev DPIA ob vsaki večji spremembi sistema (npr. razširitev lokacij, sprememba tehnologije ali rokov hrambe).
2. Redno usposabljanje zaposlenih glede varstva osebnih podatkov in ravnanja s posnetki.
3. Letni notranji pregled dostopov do posnetkov in revizijskih sledi.
4. Redno preverjanje ustreznosti usmerjenosti kamer in sorazmernosti nadzora.
5. Spremljanje zakonodajnih sprememb (GDPR, ZVOP-2, smernice IP RS) in po potrebi prilagoditev ukrepov.

IZJAVA O PREVERITVI IN SPREJEMLJIVOSTI TVEGANJ

Ocena učinkov v zvezi z varstvom osebnih podatkov (DPIA) - Sistem videonadzora na javnih površinah v Občini Ankaran

Na podlagi izvedene ocene učinkov v zvezi z varstvom osebnih podatkov (v skladu s 35. členom Uredbe (EU) 2016/679 – GDPR) je bila za izvajanje videonadzora na javnih površinah izvedena celovita presoja tveganj ter določeni ustrezni tehnični in organizacijski ukrepi za njihovo obvladovanje.

Ugotovljeno je bilo naslednje:

1. Obdelava osebnih podatkov je nujna in sorazmerna glede na zakoniti namen – zagotavljanje varnosti ljudi, javnega reda ter zaščite premoženja.
2. Vsa prepoznana tveganja za pravice in svoboščine posameznikov so bila ocenjena in zmanjšana na sprejemljivo raven.
3. Po izvedbi predvidenih ukrepov ni zaznanih preostalih tveganj, ki bi bila opredeljena kot visoka, zato predhodno posvetovanje z Informacijskim pooblaščencem ni potrebno (člen 36 GDPR).
4. Upravljavec se zavezuje, da bo:
    - redno preverjal učinkovitost tehničnih in organizacijskih ukrepov,
    - izvajal letno preverjanje skladnosti s strani pooblaščene osebe za varstvo podatkov,
    - posodobil to oceno učinkov ob spremembah sistema ali zakonodaje.

Na podlagi izvedene presoje se ocenjuje, da je obdelava osebnih podatkov v okviru sistema videonadzora na javnih površinah skladna z zahtevami GDPR in nacionalne zakonodaje ter da so tveganja za posameznike ustrezno obvladovana.

Pojasnilo glede sodelovanja zunanjega svetovalca / DPO

Izdelava, dokončanje, sprejem ocene učinka ter izvajanje predvidenih ukrepov za obvladovanje tveganj je v celoti odgovornost upravljavca. To izrecno določa 35. člen Uredba (EU) 2016/679 – Splošna uredba o varstvu podatkov.

Upravljavec je odgovoren za zagotovitev, da so vse navedbe v oceni učinka resnične. DATAINFO.SI, d.o.o. zagotavlja le vzorce, možne oz. tipične primere, običajne rešitve, smernice za pripravo osnutka ocene učinka, podaja mnenja na določena vprašanja oz. dokumente in ne pripravi končnega dokumenta.
Zakonita obdelava osebnih podatkov in upoštevanje veljavne zakonodaje je vedno odgovornost upravljavca.

V Ankaranu: 31.3.2026
Številka: 240-0001/2023 -14

OBČINA ANKARAN - COMUNE DI ANCARANO
1
ŽUPAN - IL SINDACO

Gregor Strmčnik
ŽUPAN