

OCENA UČINKOV
V ZVEZI Z VARSTVOM OSEBNIH
PODATKOV V SKLADU S 35. ČLENOM
SPLOŠNE UREDBE EU O VARSTVU
PODATKOV (ang. GDPR)

ZA VIDEONADZORNI SISTEM V OBČINI MEŽICA



December 2021

Povzetek

Občina Mežica namerava vzpostaviti videonadzorni sistem z napravami na območju občine. Ker so kamere nameščene na javnih površinah, lahko ta poseg predstavlja tveganje za pravice in svoboščine posameznikov, zaradi tega je Občina Mežica pred obdelavo v skladu z veljavno zakonodajo in priporočili Informacijskega pooblaščenca RS izvedla Oceno učinkov predvidenih dejanj obdelave na varstvo osebnih podatkov.

V oceni učinka smo natančno preučili pravne podlage za obdelavo osebnih podatkov ter njihovo zakonitost. Konkretizirali smo cilje in prednosti, ki jih zagotavlja predvidena obdelava podatkov v okviru izvajanja videonadzora. Prav tako smo analizirali ukrepe za zaščito podatkov, opredelili predvidene roke shranjevanja ter načine ustrezne obvestitve vseh skupin zadevnih posameznikov. Podrobno smo prikazali in razdelali snemalno območje videonadzornega sistema z grafičnim prikazom vseh kamer, ki so vključene v sistem snemanja na predvidenem območju. Preverili smo potrebnost in sorazmernost obdelave podatkov, ter preučili predvidena tveganja za varstvo osebnih podatkov in jih zmanjšali, če ne popolnoma odpravili.

Ugotavljamo, da je uvedba videonadzornega sistema z vidika varstva osebnih podatkov in pravic posameznika ustrezna.

KAZALO

UVOD	4
1 POTREBA PO IZVEDBI OCENE UČINKOV	4
2 OPIS PREDVIDENIH DEJANJ OBDELAVE IN NAMENOV OBDELAVE	6
2.1 OBMOČJE SNEMANJA KAMER - PRIKAZ SNEMALNEGA OBMOČJA VIDEONADZORNEGA SISTEMA	6
2.2 CILJI	6
2.3 PREDNOSTI	7
2.4 NABOR OSEBNIH PODATKOV, KI BODO ZAJETI, SHRANJENI ALI KAKOR KOLI DRUGAČE OBDELANI	7
3 POSTOPEK POSVETOVANJA	7
4 POTREBNOST IN SORAZMERNOST OBDELAVE.....	8
4.1 ZAKONITOST	9
4.2 ZBIRANJE INFORMACIJ	9
5 SNEMANJE	9
5.1 ALI SISTEMI OMOGOČAJO SNEMANJE?	9
5.2 KAKŠEN NAČIN PRENOSA SE UPORABLJA ZA PREDMET NAMESTITVE?.....	10
5.3 NAVEDITE, KATERE VARNOSTNE FUNKCIJE OBSTAJAJO ZA ZAŠČITO PODATKOV OB PRENOSU (NPR. ŠIFRIRANJE).	10
5.4 IZ KATERIH POVRŠIN SE BODO INFORMACIJE ZBIRALE?.....	11
5.5 O KOM SE BODO ZBIRALI OSEBNI PODATKI?	11
5.6 INFORMACIJE SE UPORABLJAJO ZA ODZIVANJE NA NEZAKONITE DEJAVNOSTI.	11
5.7 S KATERIMI ZUNANJIMI AGENCIJAMI/ORGANI SE ŠE LAHKO DELIJO INFORMACIJE/POSNETKI?	11
5.8 KAKO SE INFORMACIJE RAZKRIJEJO V PREJŠNJI TOČKI NAŠTETIM OSEBAM?	12
5.9 ALI OBSTAJA PISEN DOKUMENT, KI DOLOČA NASLEDNJE:	12
5.10 ALI OPERATIVNO OSEBJE PREJME USTREZNO USPOSABLJANJE, KI VKLJUČUJE NASLEDNJE?	12
5.11 S KOM STE SE POSVETOVALI? (ČE JE POTREBNO, OZNAČITE VEČ MOŽNOSTI)	12
6 PREGLEDNOST	13
7 SORAZMERNOST - NAJMANJŠI OBSEG PODATKOV	14
8 TOČNOST IN AŽURNOST.....	14
9 OMEJITEV SHRANJEVANJA	14
10 INFORMACIJSKA VARNOST	14
11 PREDVIDENA TVEGANJA VARNOSTI OSEBNIH PODATKOV (VERJETNOST IN RESNOST)	14
11.1 TVEGANJE NEDOVOLJENEGA DOSTOPANJA DO OSEBNIH PODATKOV S STRANI ZAPOSLENIH.....	15
11.2 TVEGANJE IZGUBE, KRAJE, NEDOVOLJENE ODSTRANITVE OSEBNIH PODATKOV TER NEPOOBLAŠČENE ALI NENAMERNE SPREMEMBE OSEBNIH PODATKOV.....	16
11.3 TVEGANJE NEUPOŠTEVANJA POSAMEZNIKOVIH PRAVIC PRI OBDELAVI OSEBNIH PODATKOV.....	16
11.4 TVEGANJE OBDELAVE OSEBNIH PODATKOV BREZ USTREZNE PRIVOLITVE ALI VEDNOSTI POSAMEZNIKA O TEM	16
11.5 TVEGANJE POSREDOVANJA OSEBNIH PODATKOV TRETJIM OSEBAM ALI V TRETJE DRŽAVE BREZ USTREZNE PRAVNE PODLAGE 16	
11.6 TVEGANJE HRAMBE OSEBNIH PODATKOV PREKO DOVOLJENIH ROKOV	17
11.7 TVEGANJE UPORABE OSEBNIH PODATKOV V NASPROTJU Z NAMENOM.....	17
12 UKREPI ZA ZMANJŠANJE TVEGANJA VARNOSTI OSEBNIH PODATKOV	17
12.1 OSNOVNI UKREPI ZA ZMANJŠANJE TVEGANJ.....	17
12.2 DODATNI UKREPI	21
13 ZAKLJUČEK.....	21

UVOD

Občina Mežica (v nadaljevanju: občina) želi uvesti videonadzor na področju javnih površin občine.

Namen videonadzornega sistema je, da se zagotovi optimalna stopnja za varovanje premoženja in ljudi, prepreči odklonska ravnanja posameznikov, da se olajša pojasnjevanje razlogov morebitnih incidentov, ter da se s tem zagotovi varno in kakovostno okolje za bivanje občanov občine. Naprave za izvajanje videonadzora se nahajajo na izbranem območju občine oziroma upravljavca.

Na podlagi člena 35 Splošne uredbe o varstvu podatkov (v nadaljevanju: Splošna uredba),¹ je potrebno v primerih, 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. Videonadzorni sistem lahko predstavlja tveganja, zato smo skladno s 35. členom Splošne uredbe izvedli oceno učinkov v zvezi z varstvom podatkov (angl. Data Protection Impact Assessment ali DPIA) za videonadzorni sistem. Namen predmetne ocene učinkov je preveritev vseh ukrepov z namenom ocene dejanj obdelave na varstvo osebnih podatkov.

V postopku priprave te ocene učinkov v zvezi z varstvom osebnih podatkov smo preučili cilje, prednosti, nabor osebnih podatkov, zakonitost pravne podlage obdelave, ukrepe in zaščite podatkov, potrebne roke shranjevanja ter načine obvestitve vseh skupin posameznikov. V tej oceni so opisani podatkovni tokovi, udeleženi subjekti in sredstva obdelave.

Izvedli smo ukrepe, ki prispevajo k upoštevanju nujnosti in sorazmernosti ter spoštovanju temeljnih načel. Med slednje spadajo določeni, izrecni in zakoniti nameni obdelave (člen 5(1b) Splošne uredbe), sama zakonitost obdelave (člen 6 Splošne uredbe) in upoštevanje omejitve shranjevanja - roki hrambe (člen 5(1e) Splošne uredbe). Preverili smo tudi, ali je obdelava ustrezna, relevantna in omejena na to, kar je potrebno za uresničitev namenov (člen 5(1c) Splošne uredbe).

Izvedeni so bili ukrepi, ki prispevajo k varstvu pravic posameznika. Vsem posameznikom so na voljo informacije o obdelavi podatkov (posameznik je na ustrezen način obveščen o izvajanju videonadzora, kdo je upravljavec podatkov, kam se lahko obrne za pridobitev informacij o hrambi posnetkov). Posameznikom je zagotovljena pravica do seznanitve in prenosljivosti podatkov, do popravka in izbrisa podatkov ter pravico do ugovora in omejitve obdelave.

Podatki se ne bodo prenašali v tretje države.

Občina ima že sprejet Pravilnik o zavarovanju osebnih podatkov, ki opredeljuje osnova načela zavarovanja osebnih podatkov. Po potrditvi te ocene učinkov v zvezi z varstvom osebnih podatkov namerava pred uvedbo videonadzornega sistema sprejeti še nov Pravilnik o videonadzoru, s katerim se podrobneje ureja namen in način uporabe videonadzornega sistema, način odrejanja snemanja, ravnanje z videoposnetki ter nadzor nad delovanjem videonadzornega sistema in uporabo videoposnetkov. Pred uvedbo videonadzora bodo o tem pisno obveščeni vsi zaposleni pri upravljavcu.

1 POTREBA PO IZVEDBI OCENE UČINKOV

V členu 35 Splošne uredbe 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

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), 2016. L 119/1.

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 sistematičnega in obsežnega vrednotenja osebnih vidikov v zvezi s posamezniki, ki temelji na avtomatizirani obdelavi, vključno z oblikovanjem profilov, in je osnova za odločitve, ki imajo pravne učinke v zvezi s posameznikom ali nanj na podoben način znatno vplivajo.

Ravno tako Informacijski pooblaščenec Republike Slovenije v kriterijih glede Ocena učinka v zvezi z varstvom podatkov² predlaga, da je smiselna izvedba Ocene učinka v primeru sistematičnega nadzora, zlasti v primerih, kjer se posameznik ne more izogniti obdelavi njegovih podatkov ali se obdelave sploh ne zaveda, kot je npr. videonadzor javnih površin.

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

Pri delu smo za metodologijo izvedbe upoštevali naslednje smernice oziroma dokumentacijo:

- Smernice 3/2019 o obdelavi osebnih podatkov prek videonaprav European Data protection Board,³
- Smernice Informacijskega pooblaščenca Republike Slovenije, predvsem z vidika Presoje vplivov na zasebnost pri projektih eUprave,⁴
- Standard ISO/IEC 29134,⁵
- Smernice angleškega informacijskega pooblaščenca pri PIA (Privacy impact assesment),⁶
- Metodologijo PECB: Data Protection Impact Assessment Process.⁷

Obseg ocene učinkov zajema procese in informacijske rešitve v zvezi z uvedbo videonadzornega sistema. V postopku priprave te ocene učinka smo konkretizirali ukrepe, ki se bodo izvedli z namenom prispevanja k upoštevanju nujnosti in sorazmernosti ter spoštovanju temeljnih načel v zvezi z obdelavo osebnih podatkov. Med slednje spadajo določeni, izrecni in zakoniti nameni obdelave (člen 5(1b) Splošne uredbe), sama zakonitost (pravna podlaga) obdelave (člen 6 Splošne uredbe) in upoštevanje omejitve shranjevanja - roki hrambe (člen 5(1e) Splošne uredbe). Preverili smo tudi, ali je obdelava ustrezna, relevantna in omejena na to, kar je potrebno za uresničitev namenov (člen 5(1c) Splošne uredbe).

Izvedeni so bili ukrepi, ki prispevajo k varstvu pravic posameznika. Vsem posameznikom bodo na voljo informacije o obdelavi podatkov, posameznikom bo zagotovljena pravica do seznanitve in prenosljivosti podatkov, do popravka in izbrisa podatkov ter pravico do ugovora in omejitve obdelave. Ustrezno smo uredili odnose s pogodbenimi obdelovalci tj. pooblaščenimi zunanji izvajalci, ki namestijo in tehnično vzdržujejo videonadzorni sistem, ter imajo za opravljanje dejavnosti vsa ustrezna dovoljenja in licence.

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>

³ https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-32019-processing-personal-data-through-video_en

⁴ https://www.ip-rs.si/fileadmin/user_upload/Pdf/smernice/Presoje_vplivov_na_zasebnost.pdf

⁵ <https://www.iso.org/obp/ui/#iso:std:iso-iec:29134:ed-1:v1:en>

⁶ <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/>

⁷ www.pecb.com

Osební podatki se v nobenem primeru ne bodo prenašali v tretje države izven EU, saj se vsi podatki hranijo lokalno, varnostne kopije ostajajo znotraj EU.

2 OPIS PREDVIDENIH DEJANJ OBDELAVE IN NAMENOV OBDELAVE

Upravljaev bo na javnih površinah občine uvedel videonadzorni sistem, v katerega bo vključenih skupno 18 kamer, z namenom zavarovanja premoženja in varovanja posameznikov.

2.1 OBMOČJE SNEMANJA KAMER - PRIKAZ SNEMALNEGA OBMOČJA VIDEONADZORNEGA SISTEMA

Območje snemanja kamer obsega tri glavna področja Občine Mežica:

1. Stavba Narodni dom in njena okolica:
 - kopališče, v smeri balinišča (ena kamera)
 - kopališče, v smeri pumptrack steze (ena kamera)
 - kopališče, v smeri skate parka (ena kamera)
 - glavni vhod v Narodni dom (ena kamera)
 - oder pri Narodnem domu (ena kamera)
 - službeni vhod v Narodni dom (ena kamera)
 - vhod v knjižnico (ena kamera)
 - stadion, v smeri parkirišča pri Narodnem domu (ena kamera)
 - stadion, v smeri proti stopnicam (ena kamera)
2. Stavba Občine Mežica in njena okolica
 - vhod v Občino Mežica (ena kamera)
 - ekološki otok Stržovo (ena kamera)
 - tržnica (dve kameri)
 - ekološki otok Leška cesta (ena kamera)
3. Okolice stavbe Osnovne šole Mežica
 - ekološki otok pri Osnovni šoli Mežica (ena kamera)
 - parkirišče pri Osnovni šoli Mežica (ena kamera)
 - vhod v Osnovno šolo Mežica (ena kamera)
 - plato pri Osnovni šoli Mežica (ena kamera)

Podroben seznam kamer s slikami kamer in zaslonskimi slikami kamer ter pojasnili je dodan v posebni prilogi, ki je del tega dokumenta.

Nameščene kamere so znamke Dahua IPC-HFW2531T-ZS-S2, z resolucijo 2592x1944 (5MP), z motorizirano lečo 100°-26° in IR LED dometom do 60m. Kamere niso opremljene z mikrofonom, tako da se zvoka ne snema, kamere tudi niso opremljene s termo senzorji, imajo pa senzor za gibanje.

2.2 CILJI

Cilji, ki jih zasledujemo ob uvedbi videonadzornega sistema, so:

- zagotavljanje varovanja premoženja in ljudi,
- varovanje premičnega in nepremičnega premoženja,

- zagotovitev dokazov, ki lahko pripomorejo k pojasnjevanju okoliščin incidentov v okolici stavb in pripomorejo k prijetju in pregonu storilcev,
- odvracanje in preprečevanje kriminala, vandalizma in/ali psihičnega ali fizičnega nasilja.

2.3 PREDNOSTI

Pričakujemo, da bodo predmetni ukrepi naši občini, posameznikom ali tretjim osebam, zagotovili naslednje prednosti:

- Preprečevanje fizičnega in psihičnega nasilja,
- zmanjšanje škode na opremi in objektih,
- bolj kakovostno in varno delovno okolje in
- zmanjšanje strahu pred nasiljem.

2.4 NABOR OSEBNIH PODATKOV, KI BODO ZAJETI, SHRANJENI ALI KAKOR KOLI DRUGAČE OBDELANI

	DA	NE
Fotografije posameznikov	X	
Video posnetki posameznikov	X	
Živa slika na monitorju uslužbenca		X
Audio posnetki posameznikov		X
Registrske tablice avtomobilov ali drugih vozil posameznikov	X	
Sistematičen nadzor javnih površin		X
Posebne vrste osebnih podatkov (občutljivi osebni podatki)		X
Drugi podatki o posameznikih (<i>navedi</i>): _____		

3 POSTOPEK POSVETOVANJA

Ob pripravi te Ocene učinkov smo se posvetovali s pooblaščen osebo za varstvo podatkov Občine Mežica, ki je dodano kot priloga tej oceni učinka.

Občina Mežica ima imenovano pooblaščen osebo za varstvo podatkov, ki je dostopna na naslovu: dpo@mezica.si.

Za vzpostavitev in vzdrževanje videonadzornega sistema skrbi družba ODZIV d.o.o. s sedežem na Prevaljah.

Ker pri pripravi te ocene učinka ne gre za takšne postopke, ki bi zahtevali predhodno posvetovanje z Informacijskim pooblaščencom po postopku iz 36. člena Splošne uredbe, tega dokumenta Informacijskemu pooblaščenču nismo posredovali.

Dokumentacija

Ali obstaja pisen dokument, ki določa naslednje:

- | | |
|---------------------------------|--|
| Kdo ima dostop do podatkov? | ☐ DA ☒ NE |
| Kako se obdelujejo informacije? | ☐ DA ☒ NE |
| Ali so ti postopki objavljeni? | ☐ DA ☒ NE (samo zaposlenim) |

Občina ima sprejet dokument Pravilnik o varstvu osebnih podatkov iz leta 2018. Pred uvedbo videonadzornega sistema namerava občina sprejeti nov Pravilnik o videonadzoru, ki bo podrobneje uredil obdelavo in varovanje osebnih podatkov, zbranih z izvajanjem videonadzora. Zaposleni bodo pred uvedbo videonadzora pisno seznanjeni z vsebino Pravilnika o videonadzoru. Občina bo z uvedbo videonadzora, pričela voditi tudi Evidenco uporabe videonadzora z namenom vodenja evidence nad dostopom do posnetkov, prekinitvijo snemanj, ter posredovanj posnetkov tretjim osebam.

Izobraževanje

Ali operativno osebje prejme ustrezno usposabljanje, ki vključuje naslednje?

- | | |
|---|--|
| Zakonodajna vprašanja | ☐ DA ☒ NE |
| Spremljanje, ravnanje, razkrivanje, shranjevanje in brisanje informacij | ☐ DA ☒ NE |
| Postopke v zvezi z incidenti | ☐ DA ☒ NE |
| Omejitve uporabe sistema | ☐ DA ☒ NE |
| Operativno osebje se enkrat letno udeležijo usposabljanj. | ☐ DA ☒ NE |
| Postopke glede uresničevanja pravic posameznikov. | ☐ DA ☒ NE |

4 POTREBNOST IN SORAZMERNOST OBDELAVE

Izvedli smo ukrepe, ki prispevajo k upoštevanju nujnosti in sorazmernosti ter spoštovanju temeljnih načel. Med slednje spadajo določeni, izrecni in zakoniti nameni obdelave (člen 5(1b) Splošne uredbe), sama zakonitost obdelave (člen 6 Splošne uredbe), ki mora biti izpolnjena, da je obdelava podatkov zakonita in upoštevanje načela omejitve shranjevanja (rokov hrambe), ki določa, da morajo biti osebni podatki hranjeni v obliki, ki dopušča identifikacijo posameznikov, na katere se nanašajo osebni podatki, le toliko časa, kolikor je potrebno za namene, za katere se osebni podatki obdelujejo (člen 5(1e) Splošne uredbe). Preverili smo tudi, ali je obdelava ustrezna, relevantna in omejena na to, kar je potrebno za uresničitev namenov, za katere se osebni podatki obdelujejo (člen 5(1c) Splošne uredbe).

Izvedeni so bili ukrepi, ki prispevajo k varstvu pravic posameznika. Vsem posameznikom so na voljo informacije o obdelavi osebnih podatkov. V skladu z določilom 37. člena Splošne uredbe smo imenovali

pooblaščen osebo za varstvo podatkov, ki je dostopna na naslovu: dpo@mezica.si, na katero se lahko posamezniki obrnejo v zvezi z vsemi vprašanji, ki se nanašajo na obdelavo osebnih podatkov. Posameznikom je zagotovljena pravica do seznanitve in prenosljivosti podatkov, do popravka in izbrisa podatkov ter pravica do ugovora in omejitve obdelave. Več informacij o obdelavi osebnih podatkov je dostopnih v Politiki zasebnosti, objavljeni na <https://www.mezica.si/gdpr>. Ustrezno ima urejene odnose s pogodbenimi obdelovalci.

4.1 ZAKONITOST

Obdelava poteka v skladu z veljavno zakonodajo na področju varstva osebnih podatkov.

Pravna podlaga za zbiranje, hrambo ali drugo vrsto obdelave osebnih podatkov v zvezi z uvedenim videonadzornim sistemom je utemeljena na naslednjem pravnem temelju:

Obdelava osebnih podatkov v primeru videonadzornega sistema je potrebna zaradi uveljavljanja zakonitih interesov, za katere si prizadeva upravljavec ali tretja oseba, razen kadar nad takimi interesi prevladajo interesi ali temeljne pravice in svoboščine posameznika, na katerega se nanašajo osebni podatki, ki zahtevajo varstvo osebnih podatkov.

Zakoniti interesi, za katere si v konkretnem primeru prizadeva upravljavec (občino) so zlasti varovanje ljudi in premoženja ter nepremičnega premoženja na območju izvajanja videonadzora.

Na omenjenih območjih ima občina tudi evidentirane incidente in poškodovanje lastnine, ki jih zaradi pomanjkanja slikovnega materiala ni mogla razrešiti oziroma preprečiti. Podrobneje je to opisano v seznamu kamer.

4.2 ZBIRANJE INFORMACIJ

Informacije se zbirajo s pomočjo:

- ☐ Kamera CCTV
- ☐ Samostojne kamere
- ☒ IP kamere
- ☐ Prenos v živo
- ☐ drugo _____

5 SNEMANJE

5.1 ALI SISTEMI OMOGOČAJO SNEMANJE?

- ☒ DA
- ☐ NE

Vsi snemalniki so znamke DHI-NVR5216-4KS2 z vgrajenimi pomnilniki 6TB, kar zadostuje za največ 90 dni snemalnih dni, kar je odvisno tudi od razmer: več kot je gibanja pred kamero, več je posnetkov. Npr., če se pred objektivom ponoči vidi pajčevina, je teh posnetkov zelo veliko, kar skrajša celotni čas.

Diski v snemalni enoti niso kriptirani, ampak ustrezno fizično varovani in omejeno dostopni samo pooblaščenim osebam na lokacijah:

- Občina – v zaklenjeni komunikacijski omari v prostoru jedilnica, ki se redno zaklepa;
- Narodni dom – v zaklenjeni komunikacijski omari v prostorih društva invalidov, ki se redno zaklepajo;
- Osnovna šola – v zaklenjeni kovinski omari v prostoru hišnika, ki se redno zaklepa.

Vse snemalne enote so zaklenjene z uporabniškim imenom in geslom. Dostop je omogočen samo pooblaščenim osebam, ki jo pooblasti odgovorna oseba občine. Do sistemov se lahko dostopa lokalno, oziroma preko programske opreme Dahua SmartPSS.

Vsi sistemi snemajo 24/7, snemajo pa, ko zaznajo gibanje, možno je določiti časovno omejeno snemanje oziroma urnike.

5.2 KAKŠEN NAČIN PRENOSA SE UPORABLJA ZA PREDMET NAMESTITVE?

- ☒ Optična vlakna
- ☐ Brezžična povezava
- ☐ Širokopasovni dostop
- ☐ Koaksialni kabel
- ☒ UTP kabel
- ☐ drugo _____

Za prenos podatkov se uporablja fizično ločeno omrežje. Od kamer do snemalnih enot je nameščen klasičen UTP kabel. Vsaka kamera je posebej zaščitena z uporabniškim imenom in geslom, ki ni javno. Podatki se do snemalne naprave prenašajo v šifriranem https načinu, s čimer se preprečuje, da bi se kdorkoli priklopil na signal in ga mimo sistema prestregel.

5.3 NAVEDITE, KATERE VARNOSTNE FUNKCIJE OBSTAJAJO ZA ZAŠČITO PODATKOV OB PRENOSU (NPR. ŠIFRIRANJE).

Dostop snemalne naprave in do programa za vpogled v posnetke imajo le pooblaščen osebe. Seznam in upravljanje dostopov bo podrobneje opredeljen v Pravilniku o videonadzoru. Tudi podeljevanje dostopov se ustrezno beleži v dnevniških zapisih. Dostop do programske opreme za pooblaščen osebe uredi služba za informatiko. Dostopi za pooblaščen osebe so zavarovani:

- z uporabniškimi imeni in gesli, ki so jih prejele pooblaščen osebe,
- s požarno pregrado, ki onemogoča zagon programske opreme nepooblaščenim uporabnikom.

Videonadzorni sistem je namestila in ga administrira gospodarska družba ODZIV d.o.o. , ki ima za opravljanje dejavnosti vsa ustrezna dovoljenja in licence.

5.4 IZ KATERIH POVRŠIN SE BODO INFORMACIJE ZBIRALE?

- ☒ Javnih površin
- ☒ Parkirišč
- ☒ Zunanjih delov stavb/prostorov
- ☐ Notranjih delov stavb/prostorov
- ☐ drugo: _____

Podroben seznam vseh kamer skupaj z zaslonskimi slikami kamer bo sestavni del Pravilnika o videonadzoru, prav tako pa je podroben seznam kamer opredeljen v 2.1 točki te ocene učinka (Območje snemanja kamer - prikaz snemalnega območja videonadzornega sistema), zaslonske slike kamer pa so med drugim dodane tudi v posebni prilogi, ki je del tega dokumenta.

Pri pregledu zaslonskih slik kamer se ugotavlja, da so lokacije kamer, njihova usmeritev skladne z namenom, pri ukrepih pa so dodane nekatere možne izboljšave.

5.5 O KOM SE BODO ZBIRALI OSEBNI PODATKI?

- ☒ Splošni javnosti na nadzorovanih območjih
- ☒ Vozilih
- ☒ Obiskovalcih
- ☒ Zaposlenih
- ☐ drugo: _____

5.6 INFORMACIJE SE UPORABLJAJO ZA ODZIVANJE NA NEZAKONITE DEJAVNOSTI.

Na prenosne medije (npr. USB ključ, SD kartica, DVD, omrežni disk) se shranjujejo posnetki posameznih incidenčnih oz. izrednih dogodkov, kadar odgovorna oseba družbe oziroma pooblaščen oseba oceni, da je potrebno posnetek takega dogodka shraniti zaradi zagotovitve dokaznega gradiva v pritožbenem, odškodninskem, disciplinskem ali kazenskem postopku. Ti posnetki se hranijo do zaključka postopka oz. do predaje pooblaščenim organom. Posnetki na prenosnih medijih se hranijo v ustreznem spisu, tako kot ostali osebni podatki.

5.7 S KATERIMI ZUNANJIMI AGENCIJAMI/ORGANI SE ŠE LAHKO DELIJO INFORMACIJE/POSNETKI?

- ☒ Državno tožilstvo in policija
- ☒ Pravni zastopniki
- ☒ Posamezniki, na katere se nanašajo podatki, na zahtevo
- ☐ Drugo: _____

5.8 KAKO SE INFORMACIJE RAZKRIJEJO V PREJŠNJI TOČKI NAŠTETIM OSEBAM?

- ☒ Ob obisku na kraju samem ob prisotnosti pooblaščen osebe za videonadzorni sistem
- ☒ Izročitev kopije posnetkov ob prisotnosti pooblaščen osebe za videonadzorni sistem
- ☐ Z oddaljenega strežnika
- ☐ Drugo: _____

5.9 ALI OBSTAJA PISEN DOKUMENT, KI DOLOČA NASLEDNJE:

- | | |
|--------------------------------|--|
| Kdo ima dostop | ☒ DA ☐ NE |
| Kako se podatki razkrijejo | ☒ DA ☐ NE |
| Kako se obdelujejo informacije | ☒ DA ☐ NE |
| Ali so ti postopki objavljeni? | ☒ DA ☐ NE |

Vse navedene zahteve bodo podrobneje urejene v Pravilniku o videonadzoru.

5.10 ALI OPERATIVNO OSEBJE PREJME USTREZNO USPOSABLJANJE, KI VKLJUČUJE NASLEDNJE?

- | | |
|---|--|
| Zakonodajna vprašanja | ☒ DA ☐ NE |
| Spremljanje, ravnanje, razkrivanje, shranjevanje in brisanje informacij | ☒ DA ☐ NE |
| Disciplinske postopke | ☒ DA ☐ NE |
| Postopke v zvezi z incidenti | ☒ DA ☐ NE |
| Omejitve uporabe sistema | ☒ DA ☐ NE |
| Drugo _____ | |

Operativno osebje se letno udeleži usposabljanja v zvezi z upravljanjem videonadzornega sistema.

5.11 S KOM STE SE POSVETOVALI? (ČE JE POTREBNO, OZNAČITE VEČ MOŽNOSTI)

- ☒ Pooblaščen osebo za varstvo osebnih podatkov
- ☒ Inženirji, razvijalci in inštalaterji
- ☐ Obdelovalci podatkov

☐ Zaposlenimi

☐ Sindikatom

☒ Drugo: Podjetje z ustreznimi referencami pri svetovanju na področju varstva osebnih podatkov

Ob pripravi te Ocene učinkov smo se posvetovali s pooblaščen osebo za varstvo podatkov Občine Mežica, ki je dodano kot priloga tej oceni učinka.

Ob pripravi te Ocene učinkov smo se posvetovali z DATAINFO.SI, d.o.o., ki je podjetje z ustreznimi referencami pri svetovanju na področju varstva osebnih podatkov, ki je priloženo.

6 PREGLEDNOST

O zbiranju osebnih podatkov bomo posameznike in javnost obveščali na naslednje načine:

☐ letaki (npr. pri dogodkih zaprtega tipa)	☐ druga tiskana gradiva (npr. vstopnice, brošure)	☐ obvestila v tiskanih medijih	☐ informacije v naših organizacijskih enotah
☒ informacije na naši spletni strani	☒ fiksna obvestila (table)	☐ obvestila na spletnih medijih	☐ Drugo (navedite): _____ _____ _____ _____

Posamezniki so o obdelavi podatkov ustrezno obveščeni, informacije o obdelavi osebnih podatkov so navedene v Politiki zasebnosti, objavljeni na <https://www.mezica.si/gdpr>. Posamezniki bodo ob vstopu v območje videonadzora obveščeni s pomočjo ustreznih opozoril, ki bodo nameščena na vidnih mestih in sicer na način, se bodo z vsebino obvestila seznanili najkasneje takrat, ko se bo nad njimi začel izvajati videonadzor. Na opozorilu je zapisano:

Objekt in okolica je pod videonadzorom (oziroma fotografija kamere: 

Občina Mežica

Telefon: 02 82 79 350

E-pošta: info@mezica.si



7 SORAZMERNOST - NAJMANJŠI OBSEG PODATKOV

Za zmanjšanje obsega zbranih osebnih podatkov se uporabi naslednje postopke in ukrepe (*označiti ustrezno*):

- ☒ izbor samo nujnih senzorjev (brez zajema avdio posnetkov, ker to ni potrebno);
- ☒ prostovoljno časovno omejevanje zajema podatkov
- ☐ uporaba tehnologij za anonimizacijo (npr. zameglitev obrazov, registrskih tablic);
- ☒ sprotno in naknadno pregledovanje/urejanje posnetkov in zajetih podatkov ter čimprejšnje naknadno izločanje oz. brisanje nepotrebnih osebnih podatkov.

8 TOČNOST IN AŽURNOST

- ☒ Predvidene imamo postopke za dopolnitev, brisanje ali popravek netočnih in neažurnih podatkov.
- ☐ Zaradi narave zbranih podatkov ali okoliščin zbiranja podatkov točnost in ažurnost podatkov ni relevantna.

Vse navedene zahteve bodo urejene v Pravilniku o videonadzoru.

9 OMEJITEV SHRANJEVANJA

Prilagodili smo čas hrambe osebnih podatkov na najkrajši možni čas, da lahko dosežemo zasledovane namene; rok hrambe osebnih podatkov je 3 mesece. Najdaljši dovoljen čas hrambe po zakonodaji je 12 mesecev. Po predlogu ZVOP-2 se bo maksimalni rok hrambe posnetkov predvidoma skrajšal na 6 mesecev.

10 INFORMACIJSKA VARNOST

Osební podatki morajo biti med obdelavo ustrezno zavarovani s postopki in ukrepi, s katerimi preprečujemo, da bi podatki bili dostopni nepooblaščenim osebam, bili uničeni, spremenjeni ali na drug način zlorabljeni.

Sprejeli smo naslednje ukrepe za obvladovanje *splošnih tveganj* v povezavi z varnostjo podatkov:

- ☒ sprejete imamo interne akte o varnosti osebnih podatkov,
- ☒ imenovali smo pooblaščenca osebe za varstvo podatkov,
- ☒ opredeljene in vzdrževane so pravice uporabnikov za dostop do podatkov,
- ☒ udeležene osebe smo ozavestili glede zakonodaje o varstvu osebnih podatkov,
- ☐ drugo (*navedite*): _____.

11 PREDVIDENA TVEGANJA VARNOSTI OSEBNIH PODATKOV (VERJETNOST IN RESNOST)

Za oceno tveganj smo pri izdelavi učinka ocene uporabili naslednjo metodologijo.

Za posamezna tveganja se določi:

- pojavnost tveganja/grožnje, učinek tveganja/grožnje in

- skupna stopnja tveganja/grožnje, ki predstavlja zmnožek pojavnosti/frekvence in učinka.

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

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

Učinek 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.

- Za 4 (zelo visoka stopnja) je značilno pomembna škoda, večja od 25.000 EUR, večji negativni medijski odziv daljši čas ali krajša odsotnost s trga, kazenski pregon vodstva, velike kazni ali odškodnine, samoprijava pri IP RS, obvestilo strankam o kršitvi, razkritje podrobnosti znanih osebnosti ali strogo zaupnih podatkov ali tajnih podatkov po zakonu ter spodkopana dolgoročna poslovna strategija organizacije.
- Za stopnjo 3 (visoka stopnja) je značilna znatna škoda nad 5.000 EUR, pomembni negativni medijski odziv krajši čas, več civilnih tožb ali civilna tožba velike vrednosti, samoprijava pri IP RS, verjetno obvestilo strankam o kršitvi, javno razkritje informacij o strankah ter spodkopana pomembna poslovna strategija.
- Za stopnjo 2 (srednja stopnja) je značilna manjša škode na 1.000 EUR, negativni medijski odziv ali več pritožb strank, odškodnina po zakonu, samoprijava pri IP RS, možno obvestilo strankam o kršitvi, razkritje informacij v organizaciji o strankah ali osebjem ter spodkopana poslovna strategija.
- Za stopnjo 1 (nizka stopnja) je značilna škoda pod 1.000 EUR, pritožba nekaj strank, odškodnina pod 1.000 EUR, vpliva na tajnost podatkov ter pa poslovno delovanje podjetja pa ni oz. je vpliv zanemarljiv.

Skupna ocena tveganja predstavlja zmnožek ocene Pojavnosti oziroma frekvence tveganja/grožnje in Učinka tveganja/grožnje in ocene. 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.

11.1 TVEGANJE NEDOVOLJENEGA DOSTOPANJA DO OSEBNIH PODATKOV S STRANI ZAPOSLJENIH

Tveganje zajema zlorabo (npr. krajo identitete) s strani zaposlenih. Posledica je lahko od neupravičene seznanitve s podatki, do dejanske materialne škode (npr. odtujitve sredstev).

Pojavnost tveganja/grožnje	Učinek tveganja/grožnje	Skupna stopnja tveganja/grožnje
2	4	8

11.2 TVEGANJE IZGUBE, KRAJE, NEDOVOLJENE ODSTRANITVE OSEBNIH PODATKOV TER NEPOOBLAŠČENE ALI NENAMERNE SPREMEMBE OSEBNIH PODATKOV

Tveganje obsega izgubo, krajo, nedovoljeno odstranitev osebnih podatkov ter nepooblaščno ali nenamerno spremembo osebnih podatkov. Splošna uredba določa realizacijo tega tveganja kot verjetno podlago za samoprijavo pri Informacijskem pooblaščenču in verjetno zahteva še obvezno obvestilo posamezniku.

Pojavnost tveganja/grožnje	Učinek tveganja/grožnje	Skupna stopnja tveganja/grožnje
2	4	8

11.3 TVEGANJE NEUPOŠTEVANJA POSAMEZNIKOVIH PRAVIC PRI OBDELAVI OSEBNIH PODATKOV

Tveganje zajema kršenje pravic posameznika, ki izhajajo iz Splošne uredbe, predvsem pravice do informiranja, seznanitve, popravka itd.

Pojavnost tveganja/grožnje	Učinek tveganja/grožnje	Skupna stopnja tveganja/grožnje
2	2	4

11.4 TVEGANJE OBDELAVE OSEBNIH PODATKOV BREZ USTREZNE PRIVOLITVE ALI VEDNOSTI POSAMEZNIKA O TEM

Tveganje zajema kršitev pravice do seznanjenosti z obdelavo osebnih podatkov, npr. da posamezniki pred vstopom v z videonadzorom nadzorovano območje, o izvajanju videonadzora niso ustrezno obveščeni (npr. z opozorilno tablo).

Pojavnost tveganja/grožnje	Učinek tveganja/grožnje	Skupna stopnja tveganja/grožnje
2	2	4

11.5 TVEGANJE POSREDOVANJA OSEBNIH PODATKOV TRETJIM OSEBAM ALI V TRETJE DRŽAVE BREZ USTREZNE PRAVNE PODLAGE

Tveganje zajema nezakonito posredovanje osebnih podatkov tretjim osebam ali v tretje države brez ustreznih pravnih podlag in brez ustreznih zaščitnih ukrepov.

Pojavnost tveganja/grožnje	Učinek tveganja/grožnje	Skupna stopnja tveganja/grožnje
2	4	8

11.6 TVEGANJE HRAMBE OSEBNIH PODATKOV PREKO DOVOLJENIH ROKOV

Tveganje zajema situacije, po katerih se podatki lahko hranijo in obdelujejo dlje, kot dopušča zakonodaja, kar pa lahko ima za posameznika negativne posledice, npr. podatki niso izbrisani oz. anonimizirani po poteku roka hrambe.

Pojavnost tveganja/grožnje	Učinek tveganja/grožnje	Skupna stopnja tveganja/grožnje
1	2	2

11.7 TVEGANJE UPORABE OSEBNIH PODATKOV V NASPROTJU Z NAMENOM

Tveganje zajema obdelavo osebnih podatkov o stranki, ki so sicer pravilno pridobljeni, a se uporabljajo v namene, za katere ni pravne podlage. Tveganje zajema tudi uporabo osebnih podatkov oseb, ki z občino niso v pogodbenem ali predpogodbenem razmerju. Tveganje zajema tudi prekomerno zbiranje osebnih podatkov, združevanje in povezovanja osebnih podatkov brez pravne podlage oz. s preseganjem namenov.

Pojavnost tveganja/grožnje	Učinek tveganja/grožnje	Skupna stopnja tveganja/grožnje
2	4	8

12 UKREPI ZA ZMANJŠANJE TVEGANJA VARNOSTI OSEBNIH PODATKOV

12.1 OSNOVNI UKREPI ZA ZMANJŠANJE TVEGANJ

Tveganje	Ukrepi za zmanjšanje ali odpravo tveganja
1 Tveganje nedovoljenega dostopanja do osebnih podatkov s strani zaposlenih (opis pri 11.1.)	UKREP: Skrbnik IT sistema mora biti pooblaščen za dostop do podatkov UKREP: Letna redna verifikacija ustreznosti dodeljenih pooblastil UKREP: Dostop je omogočen le z individualnim uporabniškim imenom in geslom, ki je dodeljeno izključno pooblaščenemu zaposlenemu UKREP: Revizijska sled UKREP: Letno izobraževanje zaposlenih UKREP: Ustrezno varovanje mehanizmov za avtentikacijo UKREP: Interna pravila, ki določajo pravice IT skrbnika, pravice pooblaščenih oseb za dostop do posnetkov.

	UKREP: Vodenje Evidence uporabe videonadzora, v katero se vpisuje vsakršen dostop do posnetkov, prekinitev snemanja in posredovanje posnetkov tretjim osebam. UKREP: Ustrezno ozaveščanje strank Dostop do snemalne naprave in podatkov sistema je omejen na določeno osebo iz področja IT-ja. Vpeljano je vodenje evidence zahtevkov oziroma vpogledov v posamezne snemalne enote. Za izvajanje revizijske sledi na aplikativnem delu je poskrbljeno na ravni programa samega. Zaposleni so seznanjeni z beleženjem vpogledov, kar zmanjšuje možnost neupravičenih vpogledov. V pravilniku o videonadzoru bo določeno, katere pooblaščen osebe upravljajo s sistemom in katere so upravičene dostopati do posnetkov.
--	---

Vpliv ukrepov na tveganje	Preostalo tveganje	Ukrepi so odobreni (da/ne)
Tveganje je zmanjšano.	1 x 4 = 4	Da

Tveganje	Ukrepi za zmanjšanje ali odpravo tveganja
2 Tveganje izgube, kraje, nedovoljene odstranitve osebnih podatkov ter nepooblaščen ali nenamerne spremembe osebnih podatkov. (opis pri 11.2.)	UKREP: Interna pravila z opredeljenimi postopki varnostnega kopiranja in hranjenja podatkov UKREP: Za ponudnika hrambe podatkov je izbran priznani in zanesljiv ponudnik, ki lahko izkaže visok nivo varnosti. Snemalne naprave vključno s pomnilniki so ustrezno zavatovane. Dostop do programa za vpogled v posnetke imajo le pooblaščen osebe. Seznam in upravljanje dostopov bo urejen v Pravilniku o videonadzoru. Tudi podeljevanje dostopov se ustrezno beleži v dnevniških zapisih. Dostop do programske opreme za pooblaščen osebe uredi služba za informatiko. Dostopi za pooblaščen osebe so zavarovani z uporabniškimi imeni in gesli, ki so jih prejele pooblaščen osebe in s požarno pregrado, ki onemogoča zagon programske opreme nepooblaščenim uporabnikom.

Vpliv ukrepov na tveganje	Preostalo tveganje	Ukrepi so odobreni (da/ne)
Tveganje je zmanjšano	1 x 4 = 4	Da

Tveganje	Ukrepi za zmanjšanje ali odpravo tveganja
----------	---

3 Tveganje neupoštevanja posameznikovih pravic pri obdelavi osebnih podatkov (opis pri 11.3)	UKREP: Interni akti, kjer je opredeljeno uveljavljanje pravic posameznika UKREP: Letno izobraževanje zaposlenih UKREP: Objava ustreznega dokumenta z opisom pravic in postopkom uveljavljanja na spletni strani UKREP: 1x letno preverjanje DPIA DODATNI UKREP: Posvetovanje s podjetjem z ustreznimi referencami na področju varstva osebnih podatkov
--	---

Vpliv ukrepov na tveganje	Preostalo tveganje	Ukrepi so odobreni (da/ne)
Tveganje je zmanjšano.	1 x 4 = 4	Da

Tveganje	Ukrepi za zmanjšanje ali odpravo tveganja
4 Tveganje obdelave osebnih podatkov brez ustrezne privolitve ali vednosti posameznika o tem (opis pri 11.4)	UKREP: Obvezna namestitvev opozorilnih tabel in seznaniitev stranke pred vstopom v območje, ki je varovano z videonadzorom. UKREP: Letno izobraževanje zaposlenih UKREP: Izpis revizijske sledi vpogleda v zahtevek (kdo in kdaj je vpogledal) DODATNI UKREP: Interna navodila za zaposlene Vsa področja občine, na katerih se bo izvajal videonadzor, bodo ustrezno opremljena z opozorilnimi tablamami z zakonsko določenimi informacijami.

Vpliv ukrepov na tveganje	Preostalo tveganje	Ukrepi so odobreni (da/ne)
Tveganje je zmanjšano.	1 x 2 = 2	Da

Tveganje	Ukrepi za zmanjšanje ali odpravo tveganja
5 Tveganje nedovoljenega prenosa podatkov drugemu obdelovalcu ali v tretje države brez ustrezne pravne	UKREP: Pregled razmerij s pogodbeni obdelovalci in sklenitev ustreznih pogodb o obdelavi osebnih podatkov UKREP: Redno preverjanje pogodbenih (pod)obdelovalcev, najmanj enkrat letno Za prenose podatkov se uporablja fizično ločeno omrežje. Dostop do programa za vpogled v posnetke imajo le pooblaščen osebe. Seznam in upravljanje dostopov bo urejen v Pravilniku o videonadzoru. Tudi podeljevanje dostopov se ustrezno beleži v dnevniških zapisih. Dostop do programske opreme za pooblaščen osebe uredi

podlage (opis pri 11.5)	služba za informatiko. Dostopi za pooblaščen osebe so zavarovani z uporabniškimi imeni in gesli, ki so jih prejele pooblaščen osebe in s požarno pregrado, ki onemogoča zagon programske opreme nepooblaščenim uporabnikom.
--------------------------------	---

Vpliv ukrepov na tveganje	Preostalo tveganje	Ukrepi so odobreni (da/ne)
Tveganje je zmanjšano.	1 x 4 = 4	Da

Tveganje	Ukrepi za zmanjšanje ali odpravo tveganja
6 Tveganje hrambe osebnih podatkov preko dovoljenih rokov (opis 11.6)	UKREP: Interna pravila z opredelitvijo rokov hrambe UKREP: Avtomatiziran postopek za brisanje posnetkov in fizična omejitev pomnilnikov UKREP: Vodenje in redno preverjanje Evidence dejavnosti obdelave z opredelitvijo rokov hrambe Programska oprema je nastavljena tako, da se posnetki po poteku 3 mesecev izbrišejo. Posnetkov, ki so starejši od 3 mesecev na snemalni enoti ni.

Vpliv ukrepov na tveganje	Preostalo tveganje	Ukrepi so odobreni (da/ne)
Tveganje je zmanjšano.	1 x 2 = 2	Da

Tveganje	Ukrepi za zmanjšanje ali odpravo tveganja
7 Tveganje uporabe osebnih podatkov v nasprotju z namenom (opis 11.7)	UKREP: Omejena možnost dostopa do podatkov na pooblaščen zaposlene z dodeljenim uporabniškim imenom in geslo UKREP: Revizijska sled UKREP: Letno izobraževanje zaposlenih UKREP: Letno preverjanje DPIA UKREP: Posvetovanje s pooblaščen osebo za varstvo podatkov oziroma podjetjem z ustreznimi referencami na področju varstva osebnih podatkov v primeru vprašanj

Vpliv ukrepov na tveganje	Preostalo tveganje	Ukrepi so odobreni (da/ne)
---------------------------	--------------------	----------------------------

Tveganje je zmanjšano.	1 x 4 = 4	Da
------------------------	-----------	----

12.2 DODATNI UKREPI

Sprejeti so tudi naslednji dodatni ukrepi za zmanjšanje tveganja varnosti osebnih podatkov.

- Ob sprejemu in uveljavitvi novega Zakona o varstvu osebnih podatkov ZVOP-2 se ponovno preveri in po potrebi ustrezno dopolni Pravilnik o zavarovanju osebnih podatkov oz. druge dokumente v povezavi z varstvom osebnih podatkov.

Ustreznost ocene učinkov se ponovno preveri v roku 1 leta od sprejetja teh učinkov.

13 ZAKLJUČEK

V zaključku podajamo še nekatere informacije v zvezi z nastajanjem dokumenta ter postopkovnimi navodili glede ponovnega preverjanja na osnovi tega dokumenta.

Datum začetka priprave dokumenta: 15.9.2021

Datum potrditve dokumenta: 1.12.2021

Ukrepe je dne 1. 12. 2021 odobrili direktor občinske uprave in župan občine.

Preostalo tveganje ni tako visoko, da bi potrebovalo posvetovanje z Informacijskim pooblaščencom.

Predlog datum ponovnega revidiranja dokumenta: 1.12.2022.

Priloge:

- Seznam kamer s slikami kamer in zaslonskimi slikami
- Mnenje pooblaščenca osebe za varstvo podatkov (DPO) Občine Mežica