Ocena učinka na varstvo osebnih podatkov (DPIA) za sistem avtomatske prepoznave registrskih tablic na Železniški cesti

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

Podrobnosti o upravljavcu	
Upravljavec	Občina Ankaran, Jadranska cesta 66, 6280 Ankaran
Direktor:	Gregor Strmčnik
Pooblaščena oseba za varstvo podatkov	DATAINFO.SI, d.o.o. e-pošta: dpo@datainfo.si

Povzetek:

Ta DPIA dokument ocenjuje učinke stalnega (24/7/365) sistema avtomatskega prepoznavanja registrskih tablic (ANPR) na območju Železniške ceste v Občini Ankaran, namenjenega nadzoru tovornih vozil. Sistem omogoča samodejno prepoznavo registrskih tablic, beleženje časa in datuma prehoda ter uporabo podatkov za odkrivanje in sankcioniranje kršitev prometnih predpisov. Ocena potrjuje, da je obdelava osebnih podatkov zakonita, nujna in sorazmerna ter skladna z GDPR in ZVOP-2.

1. korak: Ugotovite potrebo po DPIA

Cilj uvedbe video nadzornega sistema z avtomatskim prepoznavanjem registrskih tablic je zagotoviti višjo stopnjo prometne varnosti ter zaščito občinske infrastrukture (predvsem mosta), zlasti zaradi ponavljajočih se kršitev prometne omejitve (vožnja tovornih vozil nad 3,5 t po občinski cesti, kjer je to prepovedano).

Na podlagi dosedanjih izkušenj in izvedenih ukrepov (sodelovanje s policijo in občinskim redarstvom, dodatna prometna signalizacija ipd.) je bilo ugotovljeno, da namenov iz prejšnjega odstavka ni mogoče učinkovito doseči z milejšimi ali manj invazivnimi ukrepi. Videonadzorni sistem predstavlja sorazmeren in učinkovit ukrep za zagotavljanje spoštovanja cestnoprometnih predpisov ter zaščito javne infrastrukture.

Lokacija: Železniška cesta

Razlogi:
- varovanje občinske infrastrukture – cesta in most
- zagotavljanje varnosti v cestnem prometu
- zagotavljanje spoštovanja cestno prometnih predpisov

Lokacija in usmeritev videonadzora:
- dve kameri na drogu javne razsvetljave, ki pokrivata obe smeri ceste

Snemanje:

- pasivno snemanje s prepoznavanjem vozil nad 3,5 tone in registrskih tablic

- snemalnik v občinskem objektu v komunikacijski omarici, objekt je varovan z alarmnim in videonadzorom sistemom
- omrežni dostop do snemalnika iz občinskega objekta na Železniški cesti 1

Grafični prikaz videonadzorih kamer, snemalnika in opozorilnih tabel

V skladu s členom 35 Splošne uredbe (GDPR)[1] je treba izvesti oceno učinkov, kadar vrsta obdelave, zlasti v primeru sistematičnega spremljanja javno dostopnih območij, lahko povzroči veliko tveganje za pravice in svoboščine posameznikov. Videonadzor z avtomatskim prepoznavanjem registrskih tablic predstavlja obliko sistematičnega nadzora javno dostopnega območja 24/7, pri katerem se posameznik ne more izogniti obdelavi svojih osebnih podatkov (registrske tablice, posnetki vozila), zato je izvedba DPIA obvezna.

Tudi Informacijski pooblaščenec RS v svojih smernicah in na seznamu primerov obdelav, za katere je DPIA obvezna, kot tipičen primer navaja videonadzorne sisteme, zlasti kadar gre za trajno in avtomatizirano spremljanje prometa na javnih površinah[2].

---

[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

Zaradi navedenega je občina kot upravljavec skladno s členom 35 Splošne uredbe izvedla Oceno učinkov v zvezi z varstvom podatkov za predvideni sistem ANPR.

Pri pripravi ocene učinkov so bili uporabljeni naslednji viri in metodološke podlage:

- Smernice o oceni učinka v zvezi z varstvom podatkov (WP248 rev.01) – Evropski odbor za varstvo podatkov (EDPB)[3],
- Smernice 1/2020 o obdelavi osebnih podatkov v okviru povezanih vozil in aplikacij, povezanih z mobilnostjo (EDPB)[4],
- Smernice Informacijskega pooblaščenca RS: Uporaba GPS sledilnih naprav in varstvo osebnih podatkov[5],
- Smernice Informacijskega pooblaščenca RS: Ocene učinkov na varstvo podatkov[6],
- Smernice Informacijskega pooblaščenca RS: Presoje vplivov na zasebnost pri projektih eUprave[7],
- Standard ISO/IEC 29134:2017 – *Guidelines for privacy impact assessment*[8],
- Smernice britanskega ICO: *Data Protection Impact Assessments (DPIAs) guidance*[9].
- Metodologijo PECB: Data Protection Impact Assessment Process[10]

2. korak: Opišite obdelavo

2.1 Narava obdelave

Videonadzorni sistem z avtomatskim prepoznavanjem registrskih tablic bo stalno spremljal določen cestni odsek, kjer velja omejitev vožnje za vozila nad 3,5 tone. Kamera zajema slike vozil, sistem pa avtomatsko prepozna registrsko številko, datum, čas in lokacijo prehoda in zajema le vozila nad 3,5 tone. Ostala vozila niso predmet nadzora in jih sistem ne obravnava.

Tehnični opis delovanja ANPR sistema

Sistem avtomatskega prepoznavanja registrskih tablic (ANPR) temelji na uporabi digitalne kamere, nameščene na vnaprej določenem cestnem odseku, ter programske opreme za obdelavo slik. Kamera je konfigurirana tako, da zajema izključno območje vozišča in vozila, ki fizično prečkajo nadzorovani cestni odsek.

Ob zaznavi prehoda vozila sistem samodejno zajame slikovni posnetek. Zajeta slika se v realnem času obdela s programsko opremo ANPR, ki izvede:

- zaznavo vozila na sliki,
- lokalizacijo registrske tablice,
- optično prepoznavanje znakov (OCR) in pretvorbo registrske oznake v strojno berljiv zapis.

Prepoznana registrska številka se uporabi za nadaljnje avtomatsko preverjanje, ali vozilo sodi v kategorijo vozil, za katera velja prometna omejitev (vozila z dovoljeno maso nad 3,5 tone). Sistem deluje kot orodje

---

[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

za zaznavo in dokumentiranje potencialnih kršitev ter sam po sebi ne sprejema dokončnih odločitev o obstoju prekrška.

Sistem je zasnovan tako, da omogoča takojšnje filtriranje podatkov: zajeti podatki o vozilih, pri katerih ni ugotovljena relevantnost za nadzor (npr. vozila, ki ne sodijo v nadzorovano kategorijo), se ne shranjujejo oziroma se samodejno izbrišejo v najkrajšem tehnično možnem času.

Obseg in način obdelave osebnih podatkov

- **Zbiranje:** podatki se samodejno zajamejo ob prehodu vozila mimo kamere.
- **Uporaba:** podatki se uporabijo izključno za preverjanje, ali vozilo presega dovoljeno težo oziroma krši prometno omejitev.
- **Shranjevanje:** posnetki in prepoznane registrske tablice, pri katerih ni ugotovljene kršitve, se ne beležijo.
- Podatki o ugotovljenih kršitvah se hranijo do zaključka prekrškovnega postopka v zavarovanem informacijskem sistemu.
- **Brisanje:** po preteku roka hrambe se podatki samodejno izbrišejo.
- **Vir podatkov:** vozila, ki fizično prečkajo nadzorovani cestni odsek.
- **Delitev podatkov:** Osebni podatki, pridobljeni z uporabo ANPR sistema, so dostopni izključno pooblaščenim osebam upravljavca ter se posredujejo pristojnim organom (občinsko redarstvo in policija) na podlagi zakonskih pooblastil. Druge osebe do osebnih podatkov nimajo dostopa.
- **Podatkovni tok (poenostavljen):** Zajem slike → prepoznava registrske tablice → preverjanje kršitve → shranjevanje podatkov o kršitvah → posredovanje pooblaščenim organom → izbris po zaključenem postopku.

Vrste obdelave, ki predstavljajo visoko tveganje:

- sistematično spremljanje javno dostopnega območja,
- avtomatizirano prepoznavanje registrskih tablic (OCR),
- obdelava podatkov posameznikov, ki se nadzoru ne morejo izogniti,
- možnost povezovanja s podatki iz uradnih evidenc za namen prekrškovnega postopka.

2.2 Obseg obdelave

Vrsta podatkov: registrska številka vozila, čas in lokacija prehoda, posnetek vozila, ki presega 3,5 tone. Sistem ne obdeluje podatkov posebnih kategorij (npr. zdravstveni, politični, verski ipd.). Podatki o kršitvah se lahko štejejo za podatke, povezane s prekrški, zato se z njimi ravna z ustreznimi varnostnimi in pravnimi zaščitnimi ukrepi.

Količina in pogostost: zajem se izvaja stalno (24/7/365); shranijo se le podatki o zaznanih kršitvah, pričakovano v majhnem številu. Vozila, ki ne izpolnjujejo pogojev za zaznavo kršitve, niso zajeta v obdelavo in zanje se ne ustvarjajo ali hranijo posnetki.

Rok hrambe: do zaključka prekrškovnega postopka za podatke o kršitvah.

Število posameznikov: odvisno od prometne obremenitve odseka, ocenjuje se nekaj sto vozil dnevno; podatke se pridobiva in hrani le za manjši delež (vozila nad 3,5 t, ki kršijo omejitev).

Geografsko območje: točno določen cestni odsek na območju občine, kjer je postavljena prometna signalizacija o omejitvi.

2.3 Kontekst obdelave

Upravljavec je občina, ki izvaja obdelavo v okviru svojih zakonskih pristojnosti na področju varnosti in urejanja prometa (Zakon o lokalni samoupravi – ZLS, Uradni list RS, št. 94/07 – uradno prečiščeno besedilo, 76/08, 79/09, 51/10, 40/12 – ZUJF, 11/14 – popr., 14/15 – ZUUJFO, 11/18 – ZSPDSLS-1, 30/18, 61/20 – ZIUZEOP-A, 80/20 – ZIUOOPE, 62/24 – odl. US, 102/24 – ZLV-K in 83/25 – ZOUL; Zakon o pravilih cestnega prometa – ZPrCP, Uradni list RS, št.156/21 – uradno prečiščeno besedilo, 161/21 – popr., 22/25 in 86/25 – odl. US; Zakon o cestah – ZCes-2, Uradni list RS, št. 132/22, 140/22 – ZSDH-1A, 29/23 in 78/23 –

ZUNPEOVE; Zakon o občinskem redarstvu – ZORed, Uradni list RS, št. 139/06 in 9/17). Posamezniki (vozniki vozil) so v javnem prostoru, kjer lahko upravičeno pričakujejo določen nadzor prometa, zlasti kadar gre za območja z izrecno prometno omejitvijo. Posamezniki nimajo možnosti, da bi se obdelavi izognili, vendar so o njej jasno obveščeni s prometno signalizacijo in obvestili.

Obdelava ne vključuje otrok ali drugih ranljivih skupin. Trenutna tehnologija ANPR je zrela, široko uporabljena in preverjena v praksi. Varnostni mehanizmi vključujejo šifrirano komunikacijo, omejen dostop, nadzor dostopov in redno tehnično vzdrževanje. Ni znanih preteklih zlorab ali incidentov pri podobnih sistemih, vendar obstaja potencialno tveganje za zlorabo podatkov (npr. neupravičen vpogled), ki ga obvladujemo z ustreznimi tehničnimi in organizacijskimi ukrepi.

Občina ni vključena v noben certificiran kodeks ravnanja ali certifikacijsko shemo, vendar se pri izvajanju obdelave opira na smernice in priporočila Informacijskega pooblaščenca RS ter dobre prakse iz standarda ISO/IEC 29134.

2.4 Nameni obdelave

Namen uvedbe sistema ANPR je:

- preprečiti in zmanjšati število prekrškov (vožnja tovornih vozil nad 3,5 t po občinski cesti, kjer je to prepovedano),
- zaščititi občinsko infrastrukturo in povečati prometno varnost,
- zagotoviti učinkovitejše izvajanje pristojnosti občinskega redarstva, kadar drugi ukrepi niso bili uspešni.

Predvideni učinki na posameznike:

- na zakonite uporabnike cest se vpliv ne pričakuje,
- za kršitelje pomeni obdelava možnost uvedbe prekrškovnega postopka,
- sistem ne ustvarja profilov posameznikov niti ne uporablja avtomatiziranega odločanja brez človeškega nadzora.

Prednosti obdelave:

- večja prometna varnost in varnost prebivalcev ter udeležencev v prometu,
- zmanjšanje stroškov vzdrževanja občinskih cest,
- učinkovitejše izvajanje zakonodaje in preprečevanje ponavljajočih se kršitev.

Upravljavec se zaveda možnosti zlorab in zato deluje popolnoma transparentno: o uvedbi sistema in namenih obdelave bo redno obveščal javnost prek spletne strani Občine Ankaran (https://obcina-ankaran.si/pravila-varstva-zasebnosti-in-piskotkov/#s-1) in občinskega glasila *Amfora*, na lokaciji bo nameščena ustrezna prometna in informacijska tabla v skladu z določbami ZVOP-2, Splošno uredbo o varstvu podatkov (GDPR) ter smernicami Informacijskega pooblaščenca RS o izvajanju videonadzora, obveščanju posameznikov in uporabi naprednih nadzornih tehnologij izvajanju videonadzora v skladu s smernicami IP RS.

3. korak: Postopek posvetovanja

3.1 Posvetovanje z javnostjo in posamezniki

Upravljavec se zaveda pomena transparentnosti pri uvedbi sistemov videonadzora na javnih površinah. Ker se obdelava izvaja na javni cesti, kjer posamezniki nimajo neposrednega odnosa z upravljavcem in se obdelava izvaja v okviru zakonskih pristojnosti občine, ni izvedljivo zbirati individualnih mnenj posameznikov.

Kljub temu bo občina zagotovila ustrezno obveščanje javnosti o uvedbi sistema ANPR in njegovih namenih, in sicer:

- z objavo informacij na spletni strani Občine Ankaran,
- z obvestilom v občinskem glasilu *Amfora*,
- z jasno označitvijo območja videonadzora na lokaciji s prometno in informacijsko tablo v skladu z določbami ZVOP-2, Splošno uredbo o varstvu podatkov (GDPR) ter smernicami Informacijskega pooblaščenca RS o izvajanju videonadzora, obveščanju posameznikov in uporabi naprednih nadzornih tehnologij v skladu s smernicami Informacijskega pooblaščenca RS.

Na ta način bo zagotovljena preglednost in možnost seznanitve vseh prebivalcev ter udeležencev v prometu z namenom in obsegom obdelave.

3.2 Notranje posvetovanje znotraj organizacije

Pri pripravi in izvedbi projekta so vključene naslednje notranje službe oziroma odgovorne osebe:

- Pooblaščena oseba za varstvo podatkov (DPO) – svetovanje glede skladnosti z GDPR in ZVOP-2,
- oddelek za javno varnost in zaščito – določitev lokacije in tehničnih zahtev,
- oddelek za razvoj in investicije – tehnične in varnostne rešitve ter upravljanje sistema,
- občinsko redarstvo – določitev postopkov pri obravnavi prekrškov.

DPO je sodeloval pri pripravi DPIA in podal priporočila glede minimizacije obsega obdelave, roka hrambe, dostopov in obveščanja javnosti.

3.3 Posvetovanje z zunanjimi deležniki

Občina se bo po potrebi posvetovala tudi z:

- izvajalcem sistema ANPR (pogodbeni obdelovalec) glede tehničnih in varnostnih ukrepov,
- strokovnjakom za informacijsko varnost v fazi testiranja in nastavitve sistema,
- policijo in občinskim redarstvom glede usklajenosti postopkov pri ugotavljanju prekrškov in uporabe dokazov.

Če se bo izkazalo, da bi obdelava lahko povzročila prekomerno tveganje za pravice posameznikov, ki ga ni mogoče z ustreznimi ukrepi zmanjšati, bo občina pred uvedbo sistema zaprosila za mnenje Informacijskega pooblaščenca RS (v skladu s 36. členom GDPR).

4. korak: Ocenite nujnost in sorazmernost

Zakonita podlaga za obdelavo

Zakonita podlaga v tem delu pomeni pravno podlago za obdelavo osebnih podatkov, ne (samo) občinskega pravnega akta, temveč sklop zakonskih določb, ki omogočajo, da občina kot upravljavec osebne podatke obdeluje zakonito.

Gre torej za splošno pravno podlago v smislu člena 6 Splošne uredbe o varstvu podatkov (GDPR), ki se dopolnjuje s področnimi predpisi, ki urejajo izvajanje videonadzora in varnost javne infrastrukture na občinskem območju.

Zakonitost

Upravljavec ugotavlja, da uvaja projekt v skladu z veljavno zakonodajo na področju varstva osebnih podatkov.

Pravna podlaga za zbiranje, hrambo in druge vrste obdelav osebnih podatkov je utemeljena na naslednjih pravnih temeljih:

- Splošna uredba o varstvu podatkov (GDPR), zlasti člen 6(1)(e) – obdelava je potrebna za opravljanje naloge v javnem interesu ali pri izvajanju javne oblasti, ki je dodeljena upravljavcu;
- Zakon o varstvu osebnih podatkov (ZVOP-2) – ureja splošne pogoje za zakonito obdelavo osebnih podatkov in videonadzor; določbe ZVOP-2 o videonadzoru se pri ANPR sistemu ne uporabljajo, vendar ostajajo pomembne za splošne pogoje obdelave osebnih podatkov. ki ureja pogoje za izvajanje videonadzora;
- Zakon o celostnem prometnem načrtovanju (ZCPN), 25. člen – neposredno ureja uporabo ANPR sistema v cestnem prometu in posredovanje podatkov o kršiteljih redarstvu, kot javnemu organu z nalogami v javnem interesu.
- Zakon o občinskem redarstvu (ZORed-1) in Zakon o cestah (ZCes-1) – ki določata pristojnosti občine glede zagotavljanja prometne varnosti in varstva občinskega premoženja.

V konkretnem primeru se obdelava osebnih podatkov izvaja v okviru izvirnih nalog občine, kot jih določata Zakon o lokalni samoupravi (ZLS, Uradni list RS, št. 94/07 in 27/18) ter področna prometna zakonodaja (Zakon o cestah – ZCes-2, Uradni list RS, št. 84/04 in 19/19 ter Zakon o občinskem redarstvu – ZORed, Uradni list RS, št. 65/13 in 103/23), pri čemer Zakon o varstvu osebnih podatkov (ZVOP-2, Uradni list RS, št. 94/07, 59/11 in 71/21) predstavlja splošni pravni okvir za zakonito obdelavo osebnih podatkov, ne pa samostojne materialne podlage za uvedbo ukrepa. V konkretnem primeru je pravno podlago za obdelavo osebnih podatkov mogoče utemeljiti na zgoraj navedenih predpisih.

Ali obdelava dejansko doseže vaš namen?

Da. V primeru izrednega dogodka bo z obdelavo dosežen namen. Doslej pridobljene izkušnje občine kažejo, da obdelava podatkov iz video nadzornega sistema v primerih izrednih dogodkov (npr. vandalizem, prometne kršitve) omogoča ugotovitev odgovorne osebe in varovanje občinskega premoženja. Tako obdelava dejansko prispeva k doseganju cilja – povečanju varnosti in zmanjšanju kršitev.

Ali obstaja drug način za dosego enakega rezultata?

Ne. Okrepitev nadzora s strani policije, redarske službe ali dodatne prometne signalizacije ne predstavlja zadostnega ukrepa za zagotavljanje enake stopnje varnosti. Fizični nadzor (policija ali redarstvo) ni izvedljiv kontinuirano ter ne omogoča stalnega in objektivnega evidentiranja kršitev. Dodatna prometna signalizacija sama po sebi ne zagotavlja spoštovanja prometne omejitve, temveč ima zgolj preventivni učinek.
Z uporabo drugih, milejših načinov enakega rezultata ni mogoče doseči, saj nadzor brez tehničnega snemanja ne omogoča pravočasnega in dokazanega ukrepanja.

Kako boste preprečili »lezenje funkcije«?

Upravljavec bo to tveganje preprečil z naslednjimi ukrepi:

- namen uporabe ANPR sistema je natančno določen (nadzor in prepoznava registrskih tablic zaradi varnosti in preprečevanja kršitev),
- sistem bo tehnično omejen tako, da ne omogoča uporabe za druge namene (npr. prepoznavanje obrazov ali sledenje vozilom izven določenega območja),
- vse spremembe namena obdelave bodo možne le po predhodnem soglasju DPO in izvedbi nove ocene učinkov,
- vsi dostopi in vpogledi v sistem se bodo beležili in revizijsko preverjali.

Dodatne omejitve vključujejo:

- stalno fiksno usmeritev kamere izključno na nadzorovani cestni odsek,
- programsko onemogočeno povezovanje podatkov z drugimi evidencami, razen v zakonsko določenih primerih,
- časovno omejeno hrambo podatkov in avtomatsko brisanje,
- prepoved uporabe sistema za splošno spremljanje gibanja vozil ali posameznikov.

Kako boste zagotovili kakovost podatkov in minimizacijo podatkov?
Sistem bo nastavljen tako, da:

- zajema le registrske tablice vozil, brez snemanja okolice ali oseb,
- ne zajema zvoka,
- bo deloval le na lokaciji, kjer obstajajo dokazana tveganja prometnih kršitev,
- dostop do posnetkov bo možen le na podlagi prijave pri pristojnih organih pregona.

V primerih, ko sistem zaradi slabega vremena (sneg, dež, megla ipd.) ali nepopolnih oziroma neberljivih slik ne prepozna registrske tablice, se tak posnetek ne beleži kot uspešna prepoznava in se ne shranjuje kot podatek o registrski tablici, temveč se obravnava kot nepopolna oziroma zavržena informacija.

Po 4. odstavku 25. člena Zakona o celostnem prometnem načrtovanju (ZCPN, Uradni list RS, št. 130/22) morajo upravljavci voditi evidenco samodejno zaznanih registrskih oznak vozil in samodejno prepoznanih vozil. Priporočamo, da se ta evidenca vodi tudi za primere neprepoznanih oziroma nepopolnih posnetkov, da se zagotovi preglednost in sledljivost delovanja sistema.

Za popolne in pravilno prepoznane registrske tablice se vodi redna evidenca za namene preverjanja kršitev, za neprepoznane pa se evidentira, da je bil poskus prepoznave neuspešen.

V vseh sistemih bo zagotovljeno pasivno snemanje (ni sprotnega spremljanja). Posnetki se bodo redno preverjali in brisali po preteku roka hrambe.

Katere informacije boste dali posameznikom?
Videoposnetki se posredujejo na zahtevo posameznikov, na katere se posnetki nanašajo, ob izpolnjevanju pogojev, določenih v pravilih o varstvu osebnih podatkov, ki veljajo pri upravljavcu.
Posamezniki bodo o izvajanju videonadzora obveščeni:

- z obvestilnimi tablami na mestih snemanja,
- s politiko varstva osebnih podatkov, objavljeno na spletni strani občine (https://obcina-ankaran.si/pravila-varstva-zasebnosti-in-piskotkov/#s-1).

Kako boste pomagali podpreti njihove pravice?
Upravljavec posameznikom omogoča uveljavljanje vseh pravic po GDPR (dostop, izbris, omejitev obdelave, ugovor). V kolikor posameznik izpolnjuje pogoje, se mu posreduje izpis ali kopija posnetka, na katerem je prepoznaven.
Upravljavec posameznikom omogoča uveljavljanje pravic v skladu z Uredbo (EU) 2016/679 (GDPR), in sicer pravice do dostopa do osebnih podatkov, pravice do popravka, pravice do izbrisa, kadar so za to izpolnjeni zakonski pogoji, pravice do omejitve obdelave ter pravice do ugovora o obdelavi, kadar je ta pravica dopustna glede na pravno podlago obdelave.

Obdelava osebnih podatkov z uporabo sistema samodejnega prepoznavanja registrskih tablic (ANPR) temelji na členu 6(1)(c) in členu 6(1)(e) GDPR, saj je potrebna za izpolnjevanje zakonskih obveznosti ter za izvajanje nalog v javnem interesu oziroma pri izvrševanju javne oblasti, skladno z Zakonom o pravilih

cestnega prometa (ZPrCP), Zakonom o cestah (ZCes-2), Zakonom o prekrških (ZP-1) ter predpisi, ki urejajo delovanje medobčinskih redarstev.

V primeru, da sistem ANPR zazna tovorno vozilo z največjo dovoljeno maso nad 3,5 t na cestnem odseku, kjer velja omejitev, se zajeti podatki posredujejo medobčinskemu redarstvu. Medobčinsko redarstvo izvede preverjanje zaznave in opravi človeško presojo dejanskega stanja. Prekrškovni postopek se sproži izključno na podlagi človeškega pregleda in ne temelji zgolj na avtomatizirani obdelavi, zato se ne izvaja avtomatizirano sprejemanje odločitev v smislu člena 22 GDPR.

V okviru pravice do dostopa se posamezniku, če izpolnjuje pogoje in to ne posega v pravice in svoboščine drugih oseb ali v zakonitost prekrškovnega postopka, posreduje izpis osebnih podatkov ali kopija posnetka, na katerem je prepoznaven. Po potrebi se osebni podatki tretjih oseb ustrezno anonimizirajo ali zameglijo.

Posameznikom je zagotovljena tudi pravica do vložitve pritožbe pri nadzornem organu, Informacijskem pooblaščencu Republike Slovenije.

Katere ukrepe izvajate za zagotovitev skladnosti obdelave?
Sistem videonadzora z avtomatskim prepoznavanjem registrskih tablic vzpostavi in upravlja občina kot formalni upravljavec sistema. Občina je odgovorna za tehnične in organizacijske ukrepe za varovanje infrastrukture in podatkov pred nepooblaščenim dostopom, uničenjem ali zlorabo.

Zunanji IT sodelavec, imenovan kot operater sistema po sklepu župana in Pravilniku o izvajanju videonadzora, deluje izključno po navodilih upravljavca sistema kot obdelovalec osebnih podatkov v smislu člena 28 GDPR. Ne odloča samostojno o namenu ali sredstvih obdelave osebnih podatkov. Z obdelovalcem je sklenjena pogodba o obdelavi osebnih podatkov, ki določa pravice in obveznosti obeh strani ter zagotavlja skladnost z GDPR.

Dostop do osebnih podatkov je omejen na pooblaščene osebe, vzpostavljeno je beleženje dostopov in uvedeni tehnični ter organizacijski ukrepi za zagotavljanje varnosti osebnih podatkov.

Kako varujete morebitne mednarodne prenose?
Avtomatski sistem zazna zgolj kršitve cestnoprometnih predpisov in podatke o kršiteljih samodejno posreduje medobčinskemu redarstvu, ki v okviru svojih zakonskih pristojnosti deluje kot samostojen upravljavec podatkov za vodenje prekrškovnega postopka. Posredovanje podatkov redarstvu se izvaja na podlagi 7. odstavka 25. člena ZNCP, ki določa pošiljanje podatkov redarstvu.

V primeru, da gre za tujega državljana, redarski organ potrebne podatke pridobi prek Policije, upravljavec sistema pa ne izvaja neposrednih mednarodnih prenosov osebnih podatkov.

Podatki se obdelujejo in hranijo izključno znotraj EU, brez prenosa v tretje države. Morebitni prenosi bi bili izvedeni le skladno s členi 46–49 GDPR, pri čemer bi bili posamezniki ustrezno obveščeni.

Ločitev odgovornosti med upravljavcem sistema in upravljavcem podatkov
Za namen vodenja prekrškovnih postopkov je upravljavec podatkov redarski prekrškovni organ.
Občina ostaja upravljavec sistema, odgovoren za infrastrukturo, tehnične ukrepe in varovanje sistema, ne pa za odločitve ali postopke, ki jih izvaja redarski organ.
Ta ločitev zagotavlja, da:

- občina nadzoruje varnost sistema,
- redarski organ samostojno upravlja osebne podatke za prekrškovni postopek,

- odgovornosti in nameni obdelave niso premešani, kar je skladno s prakso IP RS.

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,
- obdobje hrambe osebnih podatkov ali merila za določitev tega obdobja,
- obstoj pravic posameznika (dostop, popravek, izbris, omejitev, ugovor, prenosljivost),
- pravico do vložitve pritožbe pri nadzornem organu,
- obstoj avtomatiziranega sprejemanja odločitev, če obstaja, in smiselne informacije o razlogih zanj.

Dopustno je, da upravljavec osnovne informacije navede na vidnem mestu pred vstopom na območje snemanja.
Podrobne informacije so dostopne v Politiki varstva osebnih podatkov na spletni strani občine (https://obcina-ankaran.si/pravila-varstva-zasebnosti-in-piskotkov/#s-1).

Osnutek obvestila, ki se namesti:

POZOR – ANPR VIDEONADZOR
Na tem območju se izvaja videonadzor z avtomatskim prepoznavanjem registrskih tablic vozil (ANPR) zaradi nadzora nad spoštovanjem prometnih omejitev (prepoved vožnje vozil nad 3,5 t) in zagotavljanja varnosti.

Upravljavec 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.

ATTENZIONE – VIDEOSORVEGLIANZA ANPR
In quest'area è attivo un sistema di videosorveglianza con riconoscimento automatico delle targhe dei veicoli (ANPR) per il controllo del rispetto delle limitazioni al traffico (divieto di transito ai veicoli oltre 3,5 t) e per garantire la sicurezza.
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.

Korak 5: Prepoznava in ocena tveganj

Za oceno tveganj pri obdelavi osebnih podatkov v okviru uvedbe sistema ANPR smo uporabili metodologijo, opisano v dokumentu PECB Data Protection Impact Assessment, z manjšimi prilagoditvami.

Namen tega koraka je prepoznati in oceniti tveganja za pravice in svoboščine posameznikov, na katere se nanašajo osebni podatki, ki se obdelujejo v okviru izvajanja tehničnega nadzora cestnega prometa z uporabo ANPR sistema.

Ocena tveganj je bila izvedena ob predpostavki, da ne obstajajo nobeni tehnični, organizacijski ali drugi varovalni ukrepi, kot to zahtevajo usmeritve Informacijskega pooblaščenca. Rezultati te ocene so podlaga za opredelitev ustreznih ukrepov za zmanjševanje tveganj v nadaljnjem koraku DPIA.

A. Identifikacija scenarijev tveganj

Scenariji tveganj so bili identificirani na podlagi:

- analize namena in načina delovanja sistema ANPR,
- pregleda pravnih podlag za obdelavo osebnih podatkov,
- interakcije z relevantnimi deležniki (upravljavec, IT skrbnik sistema, DPO, uporabniki rezultatov obdelave – medobčinsko redarstvo),
- izkušenj z izvajanjem videonadzora in prekrškovnih postopkov.

Sistem ANPR je namenjen zaznavi kršitev omejitve vožnje vozil nad 3,5 t na lokalni cesti. Sistem je zasnovan tako, da omogoča tehnično filtriranje in obdelavo izključno podatkov o vozilih, pri katerih obstaja sum kršitve, medtem ko se podatki o ostalih vozilih ne shranjujejo in se ne obdelujejo. Odločitev o obstoju prekrška je vedno predmet človeškega pregleda s strani medobčinskega redarstva, zato avtomatizirano odločanje v smislu 22. člena GDPR ni prisotno.

B. Analiza tveganj

Vsako identificirano tveganje je bilo analizirano z vidika:

- verjetnosti realizacije tveganja in
- potencialnega vpliva na pravice in svoboščine posameznikov (npr. poseg v zasebnost, napačna sankcija, omejevanje pravic, ugled, pravni položaj).

C. Ocena verjetnosti tveganja

Verjetnost posameznega tveganja je bila ocenjena ob upoštevanju:

- narave in obsega obdelave,
- izkušenj iz primerljivih sistemov,
- možnosti zlorab ali napak.

Uporabljena je bila naslednja lestvica:

Ocena	Verjetnost dogodka	Povzetek
1,2	Malo verjetno	Tveganje bi se lahko realiziralo, pa se verjetno ne bo.
3,4	Možno	Tveganje je bolj verjetno, da se zgodi kot ne (med nizkim in visokim).

5	Zelo verjetno	Obstaja velika verjetnost, da se tveganje lahko realizira.

Utemeljitev dodelitve stopnje tveganja je potrebno dokumentirati in hraniti kot dokaz za prihodnjo uporabo.

D. Ocena vpliva

Vpliv tveganja je ocenjen glede na **resnost posledic za posameznike**, na katere se nanašajo osebni podatki, zlasti z vidika:

- posega v zasebnost,
- pravnega in finančnega položaja posameznika,
- ugleda,
- možnosti neupravičene ali napačne sankcije.

Uporabljena je bila naslednja lestvica:

Ocena	Opis	Povzetek
1,2	Zmerno	To predstavlja manjšo težavo, ki ne povzroči večje škode.
3,4	Resno	To bo povzročilo znatno škodo majhnemu številu posameznikov, na katere se osebni podatki nanašajo, ali manjšo škodo velikemu številu posameznikov, na katere se osebni podatki nanašajo.
5	Kritično	To bo povzročilo znatno škodo velikemu številu posameznikov, na katere se nanašajo osebni podatki.

Utemeljitev dodelitve vpliva je potrebno dokumentirati in hraniti kot dokaz za prihodnjo uporabo.

Za določitev stopnje tveganja na podlagi naslednje matrike tveganja je treba uporabiti oceno verjetnosti tveganja in razvrščanje vpliva:

	Posledice	Majhne posledice		Srednje posledice		Visoke posledice
Verjetnost		**1**	**2**	**3**	**4**	**5**
Zelo verjetno	**5**	5	10	15	20	25
	4	4	8	12	16	20
Možno	**3**	3	6	9	12	15
	2	2	4	6	8	10
Malo verjetno	**1**	1	2	3	4	5

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

- Od 10 do 25 je tveganje visoko oz. kritično in predstavlja nesprejemljivo tveganje,
- Od 3 do 9 predstavlja srednje (oz. resno) in sprejemljivo tveganje
- Od 1 do 2 predstavlja zmerno (oz. nizko) in sprejemljivo tveganje.

Skupna ocena 9 je največja sprejemljiva raven tveganj.

Rezultati postopka ocene tveganj se uporabijo za naslednjo fazo v DPIA – ukrepe za zmanjšanje tveganj.

Pri oceni tveganja smo identificirali najpogostejša tveganja in opredelili verjetnost in učinek (ter skupno oceno) na način, kot da ne bi izvajali nobenih varovalnih ali organizacijskih ukrepov.

1. Zakonitost, poštenost in preglednost

	Opišite vir tveganja in naravo možnega vpliva na posameznike. Po potrebi vključite povezana tveganja skladnosti.	**Verjetnost tveganja/ grožnje**	**Škoda (učinek tveganja/grožnje)**	**Skupna ocena tveganja**
1	**Tveganje neupoštevanja posameznikovih pravic pri obdelavi osebnih podatkov** Tveganje zajema neupoštevanje pravic posameznika, ki izhajajo iz Splošne uredbe, predvsem pa pravico do informiranja, seznanitve, popravka, prenosa, ugovora in omejitve obdelave itd. kot jih zahtevajo 12. do 21. člen GDPR.	4	3	**12**
2	**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.	4	3	**12**
3	**Tveganja, povezana z neustreznimi načini informiranja posameznikov** Tveganje, da informacije za posameznike ne bodo podane v jedrnati, pregledni, razumljivi in lahko dostopni obliki ter jasnem in preprostem jeziku in skladno z zahtevami 12. člena GDPR.	3	3	**9**
4	**Tveganja, povezana s pomanjkljivim informiranjem posameznikov** Tveganje, da informacije za posameznike ne bodo celovite, skladno z zahtevami 12./14. člena GDPR, npr. pomanjkljiva objava kontaktnih podatkov DPO, časa hrambe osebnih podatkov, možnosti prenosov v tretje države ipd.	3	3	**9**

2. Omejitev namena

	Opišite vir tveganja in naravo možnega vpliva na posameznike. Po potrebi vključite povezana tveganja skladnosti.	**Verjetnost tveganja/ grožnje**	**Škoda (učinek tveganja/grožnje)**	**Skupna ocena tveganja**
5	**Tveganje uporabe osebnih podatkov v nasprotju z namenom** Uporaba osebnih podatkov v namene, ki niso povezani z izvajanjem prekrškovnega nadzora	3	3	**9**
6	**Tveganje možnosti nenamenske uporabe podatkov z vidika pogodbenih obdelovalcev** Tveganje zajema situacije, ko se podatki, ki so sicer pravilno pridobljeni, s strani oseb, ki so z upravljavcem v pogodbenem razmerju (pogodbeni obdelovalci), uporabijo za namene, za katere ni pravne podlage.	3	3	**9**

3. Najmanjši obseg podatkov

	Opišite vir tveganja in naravo možnega vpliva na posameznike. Po potrebi vključite povezana tveganja skladnosti.	Verjetnost tveganja/ grožnje	Škoda (učinek tveganja/grožnje)	Skupna ocena tveganja
7	**Tveganje prekomerne obdelave osebnih podatkov in povezovanje** Tveganje zajema npr. primere, ki predstavljajo kršitev načela najmanjšega obsega podatkov, ki določa, da morajo biti osebni podatki ustrezni, relevantno in omejeni na to, kar je potrebno za namene, za katere se obdelujejo. Zakonska podlaga namreč natančno opredeljuje nabor osebnih podatkov, ki se lahko pridobivajo in povezujejo.	3	4	**12**

4. Točnost

	Opišite vir tveganja in naravo možnega vpliva na posameznike. Po potrebi vključite povezana tveganja skladnosti.	Verjetnost tveganja/ grožnje	Škoda (učinek tveganja/grožnje)	Skupna ocena tveganja
8	**Tveganje pridobivanja zastarelih, netočnih ali neustreznih podatkov** Pridobivanje netočnih ali neustreznih podatkov (npr. napačna zaznava kršitve), kar lahko vodi v neupravičen postopek	3	4	**12**

5. Omejitve shranjevanja

	Opišite vir tveganja in naravo možnega vpliva na posameznike. Po potrebi vključite povezana tveganja skladnosti.	Verjetnost tveganja/ grožnje	Škoda (učinek tveganja/grožnje)	Skupna ocena tveganja
9	**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. Podatki niso izbrisani oz. anonimizirani po poteku roka hrambe.	5	3	**15**

6. Celovitost in zaupnost

	Opišite vir tveganja in naravo možnega vpliva na posameznike. Po potrebi vključite povezana tveganja skladnosti.	Verjetnost tveganja/ grožnje	Škoda (učinek tveganja/grožnje)	Skupna ocena tveganja

10	**Tveganje izgube, kraje, nedovoljene odstranitve osebnih podatkov ter nepooblaščene ali nenamerne spremembe osebnih podatkov** Splošna uredba določa realizacijo tega tveganja kot verjetno podlago za samoprijavo pri Informacijskem pooblaščencu in verjetno zahteva še obvezno obvestilo posamezniku. Običajno gre za zlonamerne zunanje napade na informacijski sistem, kot npr. phising napadi, ransomware napadi, izsiljevanja, zlonamerna objava celotne baze podatkov, izkoriščanje za nadaljnje napade na druge informacijske sisteme RS ipd.	5	4	**20**
11	**Tveganja povezana z nedelovanjem sistema** Gre za tveganja ob nedelovanju sistema in nebeleženju podatkov ali beleženju napačnih podatkov zaradi neizvajanja varnostnih posodobitev ali zaradi napačnega vzdrževanja ali drugih primerih.	4	3	**12**
12	**Tveganje naravnih nesreč** Gre za tveganja naravnih nesreč oz. katastrofičnih dogodkov, kot je npr. potres ali poplava.	2	5	**10**

7. Odgovornost

	Opišite vir tveganja in naravo možnega vpliva na posameznike. Po potrebi vključite povezana tveganja skladnosti.	**Verjetnost tveganja/ grožnje**	**Škoda (učinek tveganja/grožnje)**	**Skupna ocena tveganja**
13	**Tveganja povezana s pogodbenimi obdelovalci** Gre za tveganja, kot izhajajo v primeru, da z pogodbenimi obdelovalci niso sklenjene pogodbe in se ne izvajajo na način kot jih zahteva 28. člen GDPR.	3	4	**12**
14	**Tveganja iz naslova možnih kršitev določb 33. in 34. Splošne uredbe** Gre za tveganja glede nespoštovanja kratkih rokov, ko je potrebno v primeru kršitve varstva osebnih podatkov, kadar so s kršitvijo ogrožene pravice in svoboščine posameznikov, v roku 72 ur obveščati nadzorni organ (IP). Kadar pa je verjetno, da kršitev varstva osebnih podatkov povzroči veliko tveganje za pravice in svoboščine posameznikov, je upravljavec brez nepotrebnega odlašanja to dolžan sporočiti posamezniku, na katerega se nanašajo osebni podatki.	3	4	**12**

8. Varstvo pravic posameznika

	Opišite vir tveganja in naravo možnega vpliva na posameznike. Po potrebi vključite povezana tveganja skladnosti.	**Verjetnost tveganja/ grožnje**	**Škoda (učinek tveganja/grožnje)**	**Skupna ocena tveganja**
15	**Tveganja povezana z zagotavljanjem pravic posameznikov** Gre za tveganja, da posamezniki ne bodo ustrezno obveščeni o obdelavi osebnih podatkov, da jim bo oteženo uveljavljanje pravice do seznanitve in prenosljivosti, popravka in izbrisa, ugovora in omejitve obdelave podatkov, da ne bodo zagotovljene varovalke glede prenosa podatkov v tretje države ter da ne bo opravljeno ustrezno predhodno povezovanje.	3	3	**9**

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	Dostop omogočen samo pooblaščenim osebam z individualnim uporabniškim imenom in geslom. Redno preverjanje pooblastil in revizijska sled dostopov. Redno izobraževanje zaposlenih. Interna pravila za določitev pravic IT skrbnikov.	9	2	2	**4**	Zmanjšano, sprejemljivo tveganje
2	Tveganje izgube, kraje, nedovoljene odstranitve osebnih podatkov ter nepooblaščene ali nenamerne spremembe osebnih podatkov	Interna pravila za varnostno kopiranje in hrambo podatkov. Izbran zanesljiv ponudnik za hrambo z dokazano visoko stopnjo varnosti. Revizijska sled in zaščita avtentikacijskih mehanizmov.	20	2	2	**4**	Zmanjšano, sprejemljivo tveganje
3	Tveganje prekomernega zbiranja, združevanja in povezovanja osebnih podatkov	Redno preverjanje pravnih podlag in sporazumov z obdelovalci. Omejen dostop na pooblaščene osebe. Usklajeni roki hrambe na najkrajši možni čas za dosego namena.	12	2	2	4	Zmanjšano, sprejemljivo tveganje
4	Tveganje neupoštevanja posameznikovih pravic pri obdelavi osebnih podatkov	Priprava in objava politike zasebnosti s postopki uveljavljanja pravic. Aktivno vključevanje DPO. Interni postopki za obravnavo zahtev posameznikov.	12	2	2	4	Zmanjšano, sprejemljivo tveganje
5	Tveganje obdelave osebnih podatkov brez ustrezne pravne podlage ali vednosti posameznika o tem	Obvezna vidna obvestila o videonadzoru (z opisom, kontaktom, QR kodo in povezavo na politiko zasebnosti). Redni testni vpogledi v revizijsko sled. Interna navodila za pooblaščene uporabnike. Pravilnik o delovanju videonadzornega sistema.	9	2	2	4	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 vseh obdelovalcev in sklenitev pogodb o obdelavi. Letno preverjanje skladnosti pogodbenih obdelovalcev.	3	1	2	2	Zmanjšano, sprejemljivo tveganje
7	Tveganje hrambe osebnih podatkov preko dovoljenih rokov	Interna pravila z jasno določenimi roki hrambe. Avtomatiziran izbris po izteku roka hrambe. Redno preverjanje Evidence dejavnosti obdelave.	15	2	2	4	Zmanjšano, sprejemljivo tveganje
8	Tveganje uporabe osebnih podatkov v nasprotju z namenom	Dostop omejen na pooblaščene osebe z individualnimi prijavami. Revizijska sled in nivojski dostopi po nalogah. Redno usposabljanje zaposlenih s področja varstva podatkov.	12	2	2	4	Zmanjšano, sprejemljivo tveganje
9	Tveganja povezana z avtomatiziranim odločanjem	Informiranje posameznikov o avtomatizirani obdelavi (v politiki zasebnosti). Notranji postopki za uveljavljanje pravic glede avtomatiziranega odločanja. Revizijska sled in nadzor funkcionalnosti sistema.	3	1	2	2	Zmanjšano, sprejemljivo tveganje
10	Tveganja povezana z nedelovanjem sistema	Interna pravila glede vzdrževanja. Sklenjena vzdrževalna pogodba z zunanjim izvajalcem. Redno izdelovanje varnostnih kopij.	4	1	2	2	Zmanjšano, sprejemljivo tveganje
11	Tveganja naravnih nesreč	Lokacija opreme ustrezno zaščitena pred naravnimi nesrečami, redno preverjanje stanja in pripravljenost načrta za izredne razmere.	10	2	4	8	Zmanjšano, sprejemljivo tveganje

Nujni skupni ukrepi

Da se ohrani dolgoročna skladnost in zaupnost sistema ANPR, se izvajajo naslednji stalni ukrepi:

1. Določitev internih pravil glede uporabe sistema (pooblastila, dopustnost vpogledov, revizijska sled, roki hrambe, anonimizacija ipd.).
2. Redni letni pregled DPO, vključno s preverjanjem pogodbenih obdelovalcev, pri čemer se prva revizija izvede v roku 3–6 mesecev po začetku uporabe sistema ANPR, nadaljnje pa najmanj enkrat letno oziroma ob vsaki pomembni spremembi sistema, namena obdelave ali zakonodaje.
3. Ponovno preverjanje in posodobitev DPIA vsaj enkrat letno oziroma ob vsaki spremembi zakonodaje ali namena obdelave.
4. Preverjanje vpogledov v sistem in priprava letnega poročila o izvajanju nadzora.
5. Redno letno izobraževanje zaposlenih na področju varstva osebnih podatkov in informacijske varnosti.

7. korak: Zaključek in povzetek rezultatov

Preverjanje elementov, ki jih mora vsebovati ocena učinkov

Element presoje po 35 GDPR in smernicah EDPB	Ugotovitev	Opomba / Sklep
Sistematičen opis obdelave (člen 35(7a))	✔	Opis obdelave je podan: vključuje naravo, obseg, okoliščine in namen obdelave; opredeljeni so nabori podatkov (registrske tablice, metapodatki), roki hrambe, uporabniki, upravljavec in pogodbeni obdelovalci. Vključen je opis podatkovnih tokov, sredstev obdelave (strojna, programska in komunikacijska sredstva) ter upoštevani so elementi skladnosti s priporočili IP RS in EDPB.
Ocena nujnosti in sorazmernosti (člen 35(7b))	✔	Ocena nujnosti in sorazmernosti obdelave je izvedena. Utemeljena je pravna podlaga (člen 6(1)(e) – izvajanje javne naloge v javnem interesu; ZVOP-1 in področna zakonodaja). Opredeljeni so nameni obdelave (varnost, zaščita premoženja), čas hrambe, minimalen obseg podatkov, informiranje posameznikov ter upoštevanje načela omejitve hrambe.
Ukrepi za spoštovanje temeljnih načel (člen 5 GDPR)	✔	Določeni, izrecni in zakoniti nameni obdelave; načelo najmanjšega obsega podatkov; omejitev hrambe in sorazmernost obdelave so ustrezno zagotovljeni.
Ukrepi za varstvo pravic posameznika	✔	Posamezniki so ustrezno informirani (člena 12–14 GDPR), zagotovljene so pravice do dostopa, popravka, izbrisa, omejitve obdelave, prenosljivosti in ugovora. Vzpostavljeni so postopki za uveljavljanje pravic, opredeljeni v politiki zasebnosti.
Odnosi z obdelovalci (člen 28 GDPR)	✔	Z izbranimi pogodbenimi obdelovalci so sklenjene pogodbe o obdelavi, ki vključujejo ustrezne tehnične in organizacijske ukrepe ter obveznost zaupnosti. Vodi se seznam obdelovalcev.
Prenosi v tretje države (Poglavje V GDPR)	✔	Podatki se ne prenašajo v tretje države. Izvajalci uporabljajo strežnike znotraj EU. V primeru spremembe je predvidena uporaba standardnih pogodbenih klavzul.

Element presoje po 35 GDPR in smernicah EDPB	Ugotovitev	Opomba / Sklep
Ocena tveganj za pravice in svoboščine posameznikov (člen 35(7c))	✔	Ocena izvora, narave, verjetnosti in resnosti tveganj je izvedena. Tveganja so ocenjena kvantitativno (verjetnost × škoda), upoštevajoč vpliv na posameznike. Identificiranih je 10 vrst tveganj.
Ukrepi za obvladovanje tveganj (člen 35(7d))	✔	Za vsako prepoznano tveganje so določeni konkretni ukrepi. Po izvedbi ukrepov so vsa tveganja ocenjena kot zmanjšana in sprejemljiva (končna ocena ≤ 4).
Vključenost zainteresiranih strani (člena 35(2) in 35(9))	✔	Pridobljeno je mnenje DPO. Javnost bo obveščena o uvedbi sistema preko spletne strani občine in občinskega glasila. Posvetovanje z Informacijskim pooblaščencem ni potrebno, saj tveganja po izvedbi ukrepov niso ocenjena kot visoka.

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 je sorazmerna in skladna z namenom zagotavljanja varnosti in zaščite premoženja,
- ukrepi skladnosti so ustrezno določeni, vključno z rednim preverjanjem pooblaščene osebe za varstvo podatkov in letnim pregledom izvajanja.

Priporočila za nadaljnje ukrepanje:

1. Izvesti posodobitev DPIA ob vsaki večji spremembi sistema ANPR.
2. Nadaljevati z rednim usposabljanjem zaposlenih glede varstva osebnih podatkov.
3. Izvajati letne notranje revizije dostopov in revizijskih sledi.
4. Zagotoviti transparentno obveščanje javnosti o delovanju sistema.
5. Spremljati spremembe zakonodaje (ZVOP-2, GDPR, področne uredbe) in po potrebi prilagoditi ukrepe.

IZJAVA O PREVERITVI IN SPREJEMLJIVOSTI TVEGANJ

Ocena učinkov v zvezi z varstvom osebnih podatkov

Sistem avtomatske prepoznave registrskih tablic (ANPR) – nadzor prometa vozil nad 3,5 t na občinski cesti

Na podlagi izvedene ocene učinkov v zvezi z varstvom osebnih podatkov (v skladu s 35. členom Uredbe (EU) 2016/679 – GDPR) je bila za predvideno obdelavo osebnih podatkov s sistemom videonadzora z avtomatskim prepoznavanjem registrskih tablic (ANPR) 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 – preprečevanje nezakonite vožnje tovornih vozil (>3,5 t) po občinski cesti.
2. Vsa prepoznana tveganja za pravice in svoboščine posameznikov so bila ustrezno ocenjena in zmanjšana na sprejemljivo raven z uvedbo določenih ukrepov.
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 v primeru sprememb sistema ali zakonodaje.

Na podlagi izvedene presoje se ocenjuje, da je obdelava osebnih podatkov v okviru sistema ANPR 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: 10.3.2026
Številka: 224-0001/2026 -1

OBČINA ANKARAN - COMUNE DI ANCARANO
2
ŽUPAN - IL SINDACO

Gregor Strmčnik
ŽUPAN