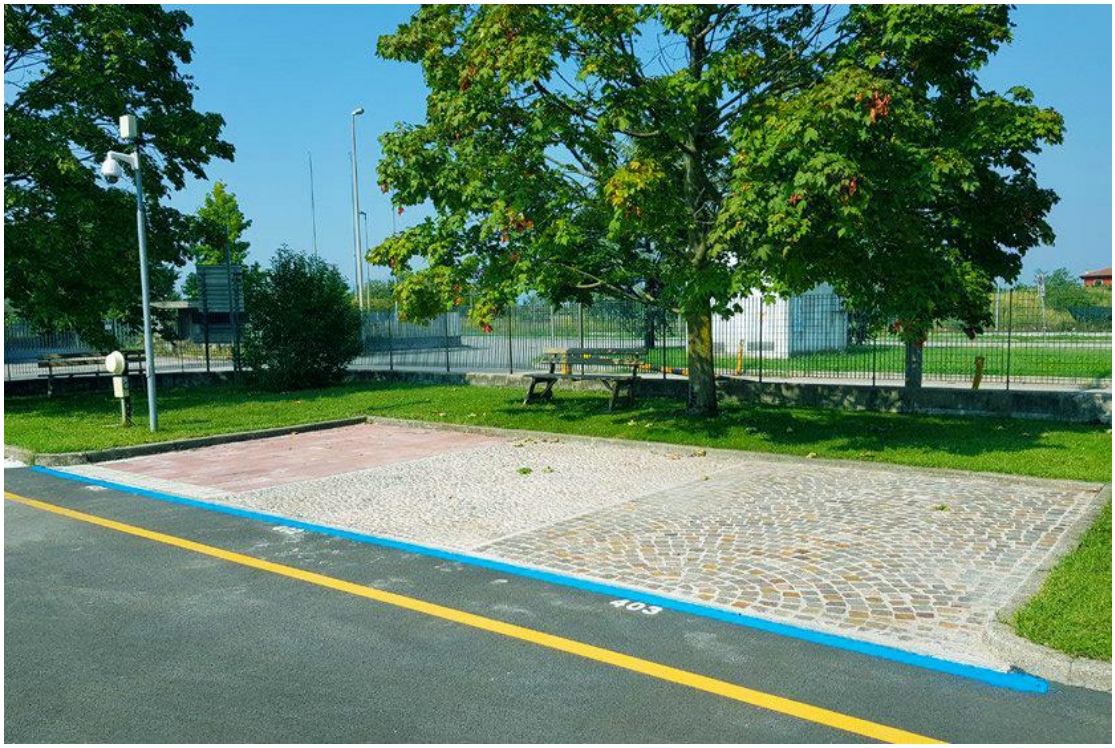


(vir: smartparkingsystems.com)

Vzpostavitev pametnih parkirišč v Tržiču – DPIA (Izvedba ocene učinka v zvezi z varstvom osebnih podatkov)

»PROJEKTI ZA PAMETNA MESTA IN SKUPNOSTI«

Dominik Gruškovnjak | Občina Tržič | 9.3.2020 (v1.10)

Uvod

Ocena učinka v zvezi z varstvom podatkov (v nadaljevanju: DPIA) je izvedena po potrebi in v primeru sprememb, ki bi lahko imele učinek na osebne podatke. Splošno mnenje strokovnjakov iz GDPR je takšno, da nove tehnologije že privzeto (*by default*) spadajo v kategorijo visokega tveganja, še posebej, če tehnologija vključuje umetno inteligenco, strojni vid, prepoznavanje obraza, internet stvari, avtonomna vozila, droni ipd.

Projekt "*Vzpostavitev pametnih parkirišč v Tržiču*" se uvršča med I. stopnjo »*inteligentne video analitike*«, kjer je cilj prepoznanje objekta in ne identifikacija posameznikov.

DPIA se izvede le z namenom, da s zagotovi skladnost z GDPR v delu, ki se nanaša na anonimizacijo osebnih podatkov.

Poznamo več vrst DPIA. V konkretnem primeru se izvede t.i. začetna oz. osnovna DPIA, v kateri se predvidijo ukrepi, ki jih mora izvajati upravljavec oz. morebitni zunanji subjekt, za zagotavljanje ustrezne stopnje anonimizacije.

Pomembno je, da s tem, ko se zagotovijo ustrezni tehnični ukrepi za ananomizacijo, drugih zahtev v skladu z določili GDPR in ZVOP-1 Občini Tržič ni potrebno izpolnjevati, ker v primeru zagotovitve popolne anonimizacije, ne gre za dejavnost obdelave osebnih podatkov.

Namen projekta

Namen projekta je opisan v dokumentu "*Vsebinska-tehnična dokumentacija*", ki je priložen kot priloga k DPIA.

Opis tehnologije

Inteligentna video analitika temelji na algoritmih, ki omogočajo prepoznavo vzorcev na video posnetkih v realnem času. Namenska programska oprema obdeluje živo sliko, pridobljeno iz IP video kamere (v nadaljevanju: video senzorji) in iz nje izlušči določene vzorce, ki naj bi ustrezali človeku, obrazom ali drugim objektom. Odvisno od sofisticiranosti sistema, algoritmi lahko zaznajo, ali se pred video kamero nahaja oseba ali predmet, sledi pojavu, mirovanju in gibanju osebe ali predmeta. Za delovanje sistema ni potrebno shranjevanje posnetkov, saj tovrstna video analitika deluje v realnem času, prav tako nihče ne gleda žive slike, ker za doseganje ciljev to ni potrebno. Cilj tehnologije je ugotoviti oziroma zaznati, ali se pred kamero nahaja oseba, objekt ali pa iz osebe prepoznati določene lastnosti (emocija, starost, spol). **Njen cilj ni v tem, da ugotovi oz. prepozna (identificira) osebo. Inteligentna video analitika deluje na t.i. metapodatkih (tip objekta, smer gibanja in hitrost gibanja objekta) in omogoča zaznavo, ne pa prepoznave v smislu identifikacije.** Nekateri uporabljajo tudi pojem anonimna video analitika (*anonymous video analytics - AVA*), a tovrstnega izraza ni možno uporabiti, ker zaradi avtomatizirane obdelave še vedno obstaja možnost določljivosti osebe.

Spodaj opisana tehnološka oprema (video senzorji) tvori pametno parkirišče:

Kamera (video senzor) zajame območje parkirišča, programska oprema pa omogoči, da se slika (iz katere posameznik ni določljiv – zamegljeno – posameznik ni določljiv preko zaznavanja podobe ali podatkov o vozilu) iz te kamere razdeli po točkah oz. posameznih parkirnih mestih (mapiranje, metode računalniškega vida itd.). Tehnologija v teh kamerah zazna stanje točke, ki so lahko zakrite (zasedeno) ali odkrite (prosto). Za prenos podatkov iz video senzorja potrebujemo zanesljivo LTE mobilno omrežje in pripadajočo opremo (router) ali pa optično povezavo med kamerami in anteno, ki potem dostopa do interneta in ustrezne programske opreme. Programska oprema obdela podatke in jih pošilja v obliki odprtih podatkov naprej do informacijskih tabel in drugih naprav.

Pravna podlaga

V konkretnem primeru naročnik oz. Občina Tržič vzpostavlja sistem obdelave, ki ne omogoča identifikacije posameznika. Popolna anonimizacija pomeni, da je živa slika pred obdelavo **zamegljena do te mere**, da je nemogoče določiti osebo ali prepoznati registrsko tablico vozila. V primeru popolne anonimizacije, pravne podlage v skladu z določili 6. člena GDPR in določili 9. člena ZVOP-1, ni potrebno zagotoviti.

Metodologija in izvedba DPIA

KONTEKST

"**Nabor podatkov**"

Podatki, ki jih za delovanje sistema obdelujemo, shranjujejo in potrebujemo so:

- oznaka parkirnega mesta,
- stanje zasedenosti določenega parkirnega mesta (da, ne),
- datum in čas zajema in obdelave podatkov.

Nadaljnja obdelava podatkov pomeni, da se izračuna, koliko je prostih parkirnih mest na posameznem parkirišču. Številčni podatki, ki predstavljajo število prostih parkirnih mest na parkirišču se pošljejo do informacijske table in prikažejo na RGB / LED display-u.

Navedeni podatki bodo preko API javno dostopni v obliki odprtih podatkov in ne vsebuje nobenih podatkov ali indikacij, ki bi lahko na kakršenkoli način določili posameznika ali pa njegove aktivnosti.

"**Namen obdelave**"

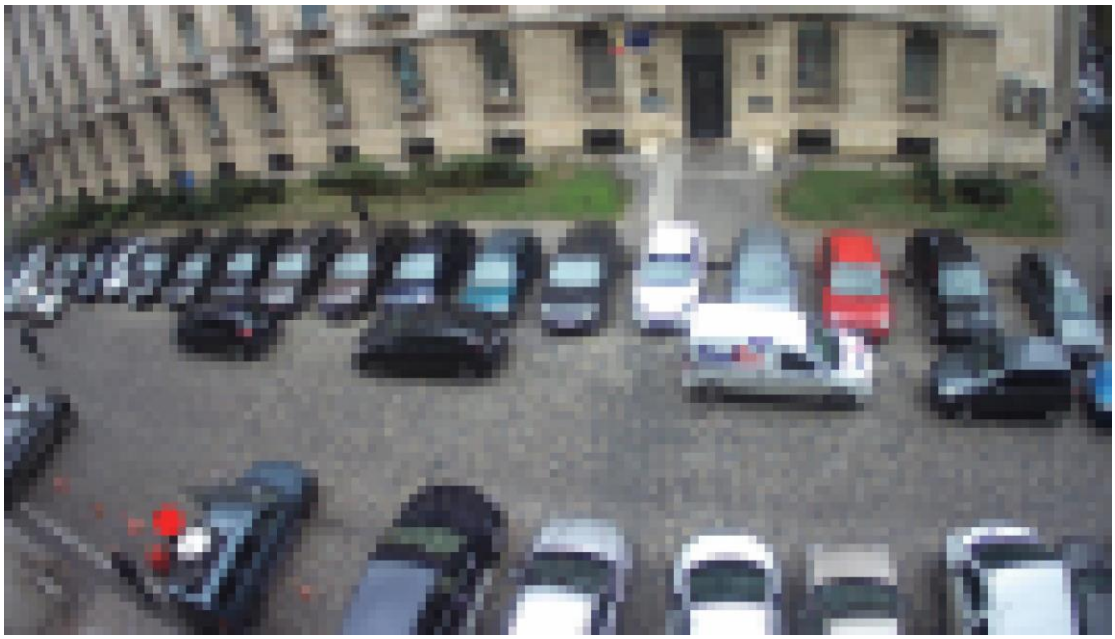
Stanje zasedenosti parkirišča (oz. število prostih parkirnih mest) se v obliki informacije pošlje do informacijske (usmerjevalne) table oz. bo prikazano na RGB / LED display-u.

Voznik s tem dobi ažurno informacijo o zasedenosti željenega oz. najbližjega parkirišča, kar pomeni, da mu informacija pomaga pri odločitvi ali bo zapeljal na parkirišče ali ne.

"**Podatkovni tok**"

V nadaljevanju je obrazloženo, kako se podatki zajamejo, pošiljajo in obdelajo za namen.

- Video senzorji na vsakih 5 - 15 sekund (oz. odvisno od nastavitve) zajamejo živo sliko parkirišča (živa slika zagotavlja popolno anonimizacijo – posameznika ni možno identificirati preko njegove podobe ali registrske tablice oz. vozila – »zameglitev«).
- Zajeta slika se preko šifriranega video »streama« (*encrypted traffic*) pošlje na statični IP naslov strežnika, ki se nahaja v varovanih prostorih (server soba) Občine Tržič ali pa pri ponudniku programske opreme (*cloud oz. računalniški oblak*).
- Komunikacija med video senzorji in strežnikom poteka preko mobilnega 4G / LTE omrežja, kjer je zelo težko prestreči promet, dešifriranje pa je zaradi zavarovanega komunikacijskega protokola HTTPS praktično nemogoče.
- Zajeta in posredovana slika se **pred** obdelavo s pomočjo programske opreme in nastavitev strežnika zamegli (anonimizacija).
- Video analitika s pomočjo algoritmov iz zamegljene slike obdela in shrani podatke, ki so navedeni v poglavju "Nabor podatkov". Live video stream zaradi anonimizacije torej ni mogoč.



Sliki prikazujeta anonimizacijo osebnih podatkov. Zaradi zamegljene slik, voznikov in registrskih tablic ni mogoče določiti, povezati osebo.

"**Način pridobivanja podatkov**"

Proces pridobivanja in obdelave podatkov s pomočjo video analitike je opisan v uvodnem poglavju "*Opis tehnologije*".

Proces obdelave podatkov je popolnoma avtomatiziran, niti ne obstaja potreba po ročni obdelavi pridobljenih podatkov.

"**Način in sredstva obdelave podatkov**"

Sredstva v sistemu za obdelavo podatkov so:

- strojna oprema: namenska IP video kamera (video senzorji),
- mrežna oprema: oprema za 4G/LTE (router),
- strežniška oprema: sprejem in obdelava podatkov, nameščena programska oprema za video analitiko; baza podatkov;
- človeški viri: ogled poročil in analize.

"**Udeleženi subjekti**"

- ponudnik: postavitev, konfiguracija sistema,
- naročnik (Občina Tržič): administracija, nadzor nad delovanjem, analize,

- uporabniki: vozniki, ki iščejo najbližje prosto, brezplačno parkirno mesto na javnih parkiriščih v občini Tržič,
- rok hrambe: v podatkovni bazi največ 1 leto. Po tem času se podatki iz podatkovne baze avtomatično zbrišejo.

Tveganja in ukrepi

V tem poglavju smo identificirali možna tveganja in določili oceno tveganja. Ocena tveganja se izvede po temeljnih načelih varstva osebnih podatkov tako kot jih določa 5. člen GDPR.

V naši analizi so tveganja povezana z verjetnostjo nastanka: visoka, srednja, nizka. Resnost tveganja predstavlja težo posledic, ki jih bo imela uresničitev tveganja: visoka, srednja, nizka. Raven tveganja torej predstavlja vsoto: **verjetnost** + **resnost** = **raven tveganja**.

Pri vsakem tveganju naštejemo še ukrepe, ki jih moramo storiti, da se tem identificiranim tveganjem v celoti izognemo ali jih vsaj znižamo na sprejemljivo raven.

Vsa našteta tveganja veljajo za programsko opremo, ki je nameščena pri naročniku (*on-premise*) in za opremo, ki je nameščena pri ponudniku (*cloud provider*).

TVEGANJA, POVEZANA S TEMELJNIM NAČELOM CELOVITOSTI IN ZAUPNOSTI (INFORMACIJSKA VARNOST)

Št.	Tveganje	Verjetnost	Resnost	Raven tveganja	Ukrepi in omilitve
1	Nesreča (požar, kraja, poplava), ki v server sobi uniči strežniško infrastrukturo	Nizka	Nizka	Nizka	UREJENO: Ni nevarnosti poplave, server soba ustrezno zavarovana (protivlomna, protipožarna vrata), ustrezno hlajenje. Backup podatkov na drugih lokacijah (on-site in off-site).
2	Nove tehnologije in posebna privlačnost za hekerske napade, ki vodijo do manipulacije z videom, nedelovanjem sistema ipd.	Srednja	Visoka	Visoka	Zaradi tega tveganja obstaja možnost nezakonite obdelave osebnih podatkov. REDNO: spremljanje delovanja sistema, preverjanje .log datotek in izrednih dogodkov, nameščanje varnostnih

					popravkov v programski (patches, updates) in strojni opremi (firmware). UREJENO: Promet do strežnika šifriran z ustreznimi kriptografskimi protokoli.
3	Zaradi napačne konfiguracije / nepazljivosti, pomanjkljivega nadzora živa slika ni zamegljena; osebni podatki so dostopni	Nizka	Visoka	Srednja	Zaradi tega tveganja obstaja možnost nezakonite obdelave osebnih podatkov. REDNO: spremljanje delovanja sistema, preverjanje .log datotek in izrednih dogodkov.
4	Pridobitev administratorskega gesla za dostop do programske opreme preko različnih oblik napadov na sistem s strani tretje (nepooblaščene) osebe.	Nizka	Visoka	Srednja	REDNO: spremljanje delovanja sistema, preverjanje .log datotek in izrednih dogodkov. UREJENO: Ravnanje z gesli določeno v Priloga 5.11 Informacijska varnostna politika Občine Tržič (Pravilnik o varstvu osebnih podatkov) Možnost vpeljave dvostopenjske avtentikacije.

TVEGANJA, POVEZANA S TEMELJNIM NAČELOM ZAKONITOSTI, PRAVIČNOSTI IN PREGLEDNOSTI

Št.	Tveganje	Verjetnost	Resnost	Raven tveganja	Ukrepi in omilitve
1	Če se ne zagotovi popolna anonimizacija, obstajajo tveganja glede zakonitosti obdelave osebnih podatkov (pravne podlaga v skladu z	Srednja	Srednja	Srednja	UREJENO: Zaradi zagotovljene anonimizacije (zameglitev žive slike) se smatra, da pravna podlaga ni potrebna. Osebni podatki se ne obdelujejo, niti se jih ne potrebuje.

	doočili 6. člena GDPR ni zagotovljene)				REDNO: Spremljati spremembe na področju zakonodaje.
2	Obvestila o izvajanju projekta so premalo vidna. Naročnik pozabi objaviti obvestila o izvajanju projektu na uradni spletni strani. Naročnik ne objavi obvestila o izvajanju projekta na parkiriščih.	Nizka	Srednja	Srednja	UREJENO: Za preprečevanje teh nesporazumov (pritožb) in visoki transparentnosti izvajanja projekta, bodo na vsakem drogu z video senzorji nalepljena obvestila o namenu projekta s povezavo do javnega DPIA dokumenta.
3	Tveganje, da se podatki obdelujejo na opremi, ki ne izpolnjuje zahtev za zaščito podatkov.	Srednja	Nizka	Nizka	UREJENO: Strojna in programska oprema sta skladni z GDPR. Zunanji izvajalec zagotavlja, da se zagotavlja anonimizacija. S ponudnikom se sklene storitvena pogodba. Naročnik v pogodbi o izvedbi storitev jasno zapiše zahteve glede zagotavljanja anonimizacije in ustreznega nivoja varnosti.

TVEGANJA, POVEZANA S TEMELJNIM NAČELOM OMEJITVE NAMENA OBDELAVE

Št.	Tveganje	Verjetnost	Resnost	Raven tveganja	Ukrepi in omilitve
1	Zloraba celotnega sistema za namen opravljanja standardnega videonadzora.	Nizka	Srednja	Srednja	REDNO: Preprečevanje nezakonitega nadzora, ker to vodi do visokih kazni, nezaupanje in zmanjšanje ugleda naročnika. UREJENO: Pravilnik o varstvu osebnih podatkov.

TVEGANJA, POVEZANA S TEMELJNIM NAČELOM TOČNOSTI

Št.	Tveganje	Verjetnost	Resnost	Raven tveganja	Ukrepi in omilitve
1	Zaradi nedelovanja sistema (različni vzroki) podatki, ki se obdelujejo, niso ne točni in ne ažurni. Z neažurnimi in netočnimi podatki dosežemo ravno nasprotne učinke namena projekta.	Nizka	Srednja	Nizka	REDNO: Dnevni pregled delovanja sistema. S ponudnikom sklenjena pogodba o vzdrževanju, kjer so opredeljeni odzivni časi, oddaljena podpora itd.

V času pred in med izvajanjem projekta bosta naročnik (upravljalec) in ponudnik (obdelovalec) po nasvetih DPO Občine Tržič upoštevala varnost obdelave podatkov, spremljala novosti, upoštevala ter redno izvajala ustrezne ukrepe za zagotavljanje varnosti obdelave, med katerimi se izpostavi:

- stalno zaupnost, celovitost, dostopnost in odpornost sistemov in storitev za obdelavo;
- zagotavljanje revizijske sledi;
- redno testiranje, ocenjevanje in vrednotenje učinkovitosti tehničnih in organizacijskih ukrepov, ki zagotavljajo varno obdelavo in zavarovanje pred kršitvami.

Zaključek

Iz dokumenta izhaja, da gre v konkretnem primeru za izdelavo t.i. začetne oz. osnovne DPIA z namenom, da se zagotovi skladnost z GDPR v delu, ki se nanaša na anonimizacijo osebnih podatkov.

Občina Tržič bo v skladu z ugotovitvami in identificiranimi tveganji nadzorovala vzpostavitev in konfiguracijo sistema, nadzorovala točnost in zanesljivost delovanja, skrbela za informacijsko varnost in popolno anonimizacijo podatkov ter spremljala novosti v zakonodaji, ki se nanaša na novo tehnologijo.

Končno poročilo DPIA bo izdelano po izvedbi projekta, ko bo dejansko preverjeno, če je zunanji izvajalec izvedel vse ukrepe za zagotavljanje anonimizacije in s tem zagotovil skladnost z določili GDPR.

Seznanitev

Z DPIA bodo seznanjeni:

- mag. Renata Zatler, DPO Občine Tržič
- mag. Borut Sajovic, župan Občine Tržič
- dr. Metka Knific Zaletelj, direktorica Občine Tržič
- Katarina Turk, svetovalka za javna naročila
- ponudniki, povabljeni k oddaji ponudbe

Priloge

- Vsebinska-tehnična dokumentacija »Vzpostavitev pametnih parkirišč v Tržiču«.