Republika Srbija
MINISTARSTVO UNUTRAŠNJIH POSLOVA

PROCENA UTICAJA OBRADE NA ZAŠTITU PODATAKA O LIČNOSTI UPOTREBOM SAVREMENIH TEHNOLOGIJA VIDEO NADZORA U OKVIRU PROJEKTA „SIGURNO DRUŠTVO" U BEOGRADU

U Beogradu, mart 2020. godine

UVOD

Unapređivanje javne bezbednosti je jedan od ključnih prioriteta u radu Ministarstva, na osnovu identifikovanih rizika i pretnji koje su definisane u „Strateškoj proceni javne bezbednosti za period 2017 – 2021. Godine“, a odnosi se na sprovođenje osam strateških prioriteta:

1. Sprečavanje i suzbijanje organizovanog kriminala sa posebnim osvrtom na Nacionalnu procenu pretnje od teškog i organizovanog kriminala (SOCTA) za period 2020 – 2024. godine, a na osnovu definisanih prioriteta sa najvećim stepenom rizika i pretnji, a to su: Neovlašćena proizvodnja i stavljanje u promet opojnih droga; Pranje novca; Krijumčarenje ljudi; Trgovina ljudima; Visokotehnološki kriminal; Akcizne robe; Falsifikovanje novca; Krijumčarenje ljudi i Imovinski kriminal;

2. Sprečavanje i suzbijanje proizvodnje marihuane i sintetičkih droga u ilegalnim laboratorijama, kao jednom od dominantnih i najprofitabilnijih oblika kriminala u Republici Srbiji;

3. Sprečavanje i suzbijanje svih oblika korupcije kroz sprovođenje mera i aktivnosti iz Akcionog plana Nacionalne strategije za borbu protiv korupcije;

4. Sprečavanje i suzbijanje terorizma i nasilnog ekstremizma koji vodi ka terorizmu sprovođenjem mera širokog spektra, počev od ispunjenja strateških pretpostavki i unapređivanje sistema za borbu protiv finasiranja terorizma u Republici Srbiji, do unapređivanja operativnih, stručnih i materijalnih kapaciteta organizacione jedinice koja se bavi suzbijanjem terorizma i ekstremizma;

5. Unapređivanje stanja javnog reda i mira suprostavljanjem nasilju, s posebnim osvrtom na nasilje na sportskim priredbama, u školama i na javnim mestima, primenom proaktivnih modela policijskog rada „policija u zajednici”, podrškom širih društvenih aktivnosti usmerenih na unapređivanje ljudskih i manjinskih prava i jačanju tolerancije, uključujući i punu primenu Zakona o privatnom obezbeđenju;

6. Unapređivanje stanja bezbednosti saobraćaja na državnim putevima, uključujući i prolaske državnih puteva kroz naselje, kroz primenu novih modaliteta rada saobraćajne policije i jačanju kadrovskih i materijalnih kapaciteta;

7. Zaštitu nacionalnih granica od iregularnih migracija, krijumčarenja ljudi i drugih nezakonitih radnji, uz obezbeđivanje legalnog prometa ljudi i robe što je od ključnog značaja za nacionalnu bezbednost;

8. Sprečavanje i suzbijanje nasilja u porodici i partnerskim odnosima.

Takođe, jedan od prioriteta Ministarstva je i približavanje policije građanima i bolja međusobna saradnja zarad unapređivanja sigurnosti. Naime, građani sa pravom očekuju odlučan i adekvatan odgovor na pretnje savremenog oblika ugrožavanja javne bezbednosti i zakonom priznatih sloboda i prava. Imajući to u vidu, osnovni zadatak Ministarstva je da se angažuju svi potrebni resursi počev od prikupljanja podataka i informacija, preko procene, obrade i analize.

Ukoliko takav odgovor izostane, rizikujemo poverenje građana i temelje same demokratije. Izazov je veliki, jer se savremeni oblici ugrožavanja javne bezbednosti neprestano menjaju, posebno usled ubrzanog razvoja informacionih tehnologije i sredstava komunikacije.

Primena savremenih informaciono-komunikacionih tehnologija predstavlja neizostavni činilac unapređivanja bezbednosne zaštite građana. Istovremeno, razvoj i dostupnost savremenih komunikacionih i informacionih tehnologija je uticao na usložnjavanje bezbednosnih pretnji usled mogućnosti njihove zloupotrebe, kako za komunikaciju, propagandu, vrbovanje, finansiranje i obuku, tako i za sajber-terorističke napade. Sa druge strane, u oblasti informaciono-komunikacionih tehnologija izazovi se odnose na probleme vezane za dostupnost, uvezanost i kompatibilnost relevantnih evidencija različitih institucija, kao i obezbeđivanje potrebnog nivoa znanja i razmene iskustava sa predstavnicima zemalja članica Evropske unije. Takođe, izazovi obuhvataju i nemogućnost implementacije novih tehnologija u postojeće resurse, odnosno zaostajanje u tehnološkom razvoju, što izaziva nekompatibilnost sa partnerima sa kojima Ministarstvo ostvaruje saradnju. S tim u vezi neophodno je omogućiti pristup Ministarstva najnovijim tehnološkim rešenjima baziranim na najboljim svetskim iskustvima, a koje u svom radu primenjuju policije savremenih zemalja.

Uvođenjem savremenih tehnologija, stiču se uslovi za obavljanje policijskih poslova (propisanih članom 30. Zakona o policiji), primenom modela 3E (efikasniji, efektivniji i ekonomičniji način), neposrednim (on line) uvidom u događaj ili istoriju događaja, brzom i efikasnom reakcijom policije, izlaskom na mesto događaja i hapšenjem učinilaca krivičnih dela i procesuiranjem prekršaja, pronalaskom lica ili hapšenjem lica za kojima se traga, povećanja bezbednosti ljudi i imovine, granične kontrole i sprovođenje provere na graničnim prelazima, nadzor državne granice van graničnog prelaza, održavanje javnog reda i mira, obezbeđivanje javnih skupova, ličnosti, objekata i prostora, bezbednosne zaštite određenih ličnosti i objekata, identifikacije i pronalaska izvršilaca krivičnih dela i nestalih lica na osnovu biometrijskih podataka o licu, obezbeđivanje dokaza za podnošenje prekršajnih i krivičnih prijava, sprovođenje poslova unutrašnje kontrole, praćenja zakonitosti i unapređivanja rada Ministarstva, pokretanje i vođenje disciplinskih postupaka, kao i preduzimanje drugih mera i radnji propisanih Zakonom o policiji, Zakonikom o krivičnom postupku, Zakonom o prekršajima, Zakonom o javnom redu i miru, Zakonom o javnom okupljanju, Zakonom o sprečavanju nasilja i nedoličnog ponašanja na sportskim priredbama, Zakonom o bezbednosti saobraćaja na putevima, Zakonom o organizaciji i nadležnosti državnih organa u suzbijanju organizovanog kriminala, terorizma i korupcije i dr.

Uvođenjem savremenog video nadzora, sa brojnim mogućnostima primene softverskih rešenja za analitičku obradu video materijala, prepoznavanja registarskih i drugih oznaka na vozilima, detekcijom lika lica, upoređivanjem prikupljenih podataka sa raspoloživim podacima, te inicijalnom, kao i kasnijom identifikacijom lica u proceduri utvrđenoj zakonom, uočavanja prekršaja i krivičnih dela i identifikovanja njihovih učesnika, uočavanja tragova predmeta i sredstava izvršenja krivičnih dela, kao i bržeg i bezbednijeg prenosa podatka, izuzetno će doprineti efikasnosti rada policije i povećanju bezbednosti u zajednici.

Uvođenje ovakvog sistema u gradu Beogradu u značajnoj meri će unaprediti rad na poslovima potražne delatnosti i pomoći policiji kod pronalaska lica za kojima se traga, bilo da su u pitanju lica za kojima su raspisane poternice i policijske potrage ili objave za nestalim licem.

Такође, time će se doprineti efikasnijem otkrivanju nepoznatih učinilaca teških krivičnih dela (KD Ubistvo, Teško ubistvo, Silovanje, Otmica, Razbojništvo, itd), pre svega analizom video materijala neposredno pre i nakon izvršenja krivičnih dela, te na pravcima dolaska i odlaska sa mesta događaja, kao i razvoju kvalitetnije analize svih informacija o kretanju žrtve ili izvršioca u cilju utvrđivanja pripremnih radnji za izvršenje određenog krivičnog dela.[1]

Takođe, primena savremenih tehnologija omogućiće praćenje saobraćajnog toka, pojave zastoja i eventualno preusmeravanje saobraćaja na alternativne pravce, efikasno otkrivanje izvršilaca krivičnih dela i prekršaja u saobraćaju, smanjen broj angažovanih policijskih službenika saobraćajne policije, jer će se određeni saobraćajni prekršaji automatski detektovati, te će omogućiti praćenje rada saobraćajnih policajaca u realnom vremenu, što će ograničiti i mogućnost korupcije. Primena savremenih tehnologija omogućiće brzo i efikasno rasvetljavanje saobraćajnih nezgoda (prepoznavanje registarskih i drugih oznaka vozila, kao i utvrđivanje okolnosti koje su dovele do nastanka saobraćajnih nezgoda (određivanje putanje kretanja vozila pre, za vreme i nakon saobraćajne nezgode). U poslednjih nekoliko godina postoji tendencija smanjenja broja poginulih lica u saobraćajnim nezgodama na teritoriji Republike Srbije, a naročito nakon uvođenja sistema za automatsko detektovanje pojedinih saobraćajnih prekršaja (korišćenja saobraćajne trake namenjene za kretanje vozila za javni prevoz, prolazak na crveno svetlo, merenje brzine, merenje prosečne brzine kretanja vozila na auto putevima). Novi savremeni sistem video nadzora znatno bi doprineo smanjenju broja nezgoda, što direktno utiče i na smanjenje indirektnih troškova nastalih kao posledica saobraćajnih nezgoda (troškovi vršenja uviđaja, hitnog medicinskog zbrinjavanja, bolničkog lečenja, nastalog invaliditeta, izdržavanja zatvorske kazne, sudskih postupaka, veštačenja i slično), a koji padaju na teret svih poreskih obaveznika.

Problem sa kojim se Ministarstvo suočavalo u dosadašnjem radu je da su kamere, koje snimaju javna mesta uglavnom veoma lošeg kvaliteta, što je predstavljalo problem u

[1] **1**.Током 2018. године у Београду, у пролазу између зграда, извршено је кривично дело Убиство из члана 113. КЗ а у вези члана 35. КЗ, од стране три осумњичена лица. Након извршеног кривичног дела један НН извршилац је протрчао између два стуба и изашао из пролаза, где га је сачекао други осумњичени, који је управљао скутером италијанских регистарских ознака и након извршеног кривичног дела заједно су се на поменутом скутеру удаљили са места догађаја-Трећи НН извршилац се ПМВ непознатих регистарских ознака удаљио у непознатом правцу. Наведено возило које је коришћено приликом извршења овог кривичног дела, идентификовано је управо коришћењем материјала изузетог са видео надзора и представљао је један од кључних трагова у истрази и расветљавању овог кривичног дела. **2**.Дана 25.07.2014. године у Београду, на коловозу Бранковог моста дошло је до повређивања пешака од стране НН возила којим је управљао НН возач. На основу материјалних доказа пронађених на месту догађаја, пре свега делова који су отпали са НН возила које је изазвало саобраћајну незгоду, вештачењем је утврђено да исти припадају возилу марке „Мини“ модел „Кантримен”. Оперативним радом полиције и прегледом материјала прикупљеног путем видео надзора камера које су се налазиле на траси кретања предметног возила полиција је дошла до сазнања да је саобраћајну незгоду изазвало возило којим је управљао М.М., против кога је поднета кривична пријава надлежном тужилаштву за кривична дела Тешко дело против безбедности јавног саобраћаја из члана 297. КЗ и Непружање помоћи лицу повређеном у саобраћајној незгоди из члана 296. КЗ. 3.У Београду је 2018. године, у експозитури банке „Поштанска штедионица”, извршено кривично дело Разбојништво из члана 206. КЗ, којом приликом су три осумњичена. од радника „Поштанске штедионице” одузели новац у укупном износу од 11.500.000 динара а 2019. године је такође у Београду на штету привредног друштва НИС А.Д. Нови Сад извршено кривично дело Разбојништво из члана 206. КЗ, којом приликом су осумњичени извршили напред наведено кривично дело и оштетили ово привредно друштво за око 18.500.000 динара. Оба кривична дела су расветљена на основу доказа прикупљених анализом видео снимака сачињених употребом система видео надзора.

dokazivanju krivičnih dela i prekršaja. Iskustva u radu Ministarstva i kroz analizu prikupljenog video materijala koji potiče iz sistema video nadzora drugih državnih organa, institucija, poslovnih kompanija, građana i dr, potvrđuju da je kvalitet video materijala loš, usled čega je rad policije često nedovoljno efikasan, odnosno znatno otežan zbog procedura pribavljanja video materijala i količine tog materijal, njegove dalje obrade i analize. Količina video materijala je često ogromna i zahteva puno vremena za analizu. Najčešće je video nadzor postavljen tako da ne pokriva lokaciju koja je potrebna policiji. Zbog svega navedenog, bilo je potrebno je angažovati veliki broj zaposlenih na pribavljanju i analizi video materijala, a sama analiza se sprovodila na više lokacija te se tako trošio značajan broj radnih sati, što iscrpljuje zaposlene i utiče na kvalitet rada. Prema policijskim izveštajima, najveći broj lica ili vozila za kojima se tragalo, pronađen je prilikom redovne kontrole – legitimisanja (proverom identiteta) od strane policijskih službenika, odnosno kontrole učesnika u saobraćaju, a ne uvidom u video zapise.

Svrha i cilj primene savremene tehnologije usmeren je na sprovođenje zakonom utvrđenih poslova policije, koji se ogledaju u tome da je imperativ da policija preduzme potrebne mere i radnje da se pronađe učinilac krivičnog dela ili prekršaja da se učinilac ili saučesnik ne sakrije ili ne pobegne, da se otkriju i obezbede tragovi krivičnog dela i predmeti koji mogu poslužiti kao dokaz, kao i da se prikupe sva obaveštenja koja bi mogla biti od koristi za uspešno vođenje krivičnog i drugog postupka.

Cilj Ministarstva je da uvođenjem savremenih tehnologija u okviru projekta „Sigurno društvo" doprinese podizanju kapaciteta u radu policije, a samim tim i podizanju poverenja u rad policije radi smanjenja ukupnog kriminala na području grada Beograda i unapređenja bezbednosti svih građana.

Imajući u vidu bezbednosne izazove i potrebu za efikasnijim radom policije kao i sve prednosti koje nude savremene tehnologije, Ministarstvo je procenilo da su se stekli uslovi za uvođenje savremenih tehnologija u radu Ministarstva kroz sprovođenje projekta „Sigurno društvo" na teritoriji grada Beograda, a koji obuhvata unapređenje sistema video nadzora, uspostavljanje inteligentne video analitike i izgradnju eLTE bežične širokopojasne radio mreže, bazirane na LTE (LongTermEvolution) tehnologiji.

U prethodnom periodu u okviru ovog projekta na opredeljenim lokacijama montirane su pokretne (PTZ) kamere rezolucije fullHD (2Mpix) sa 30x optičkim zumom, fiksne kamere rezolucije fullHD (2Mpix) namenjene za opšti video nadzor i fiksne kamere rezolucije 4K (8Mpix), Sve kamere su opremljene sa IR diodama čime im je omogućen rad u noćnim uslovima i lošim vremenskim uslovima. Takođe kamere imaju slot za memorijske kartice kapaciteta 32 GB koje se koriste kao „backup" za snimanje u vanrednim situacijama kada dođe do prekida u prenosnom/komunikacionom putu od kamere do servera na kome se, u normalnom režimu rada, snima video signal sa kamera. Fiksne kamere su sa motorizovanim varifokalnim objektivom koji pruža mogućnost podešavanja vidnog polja kamere, koje je uslovljeno vrstom objektiva koji se koristi. Kamere su povezane na sistem koji radi na softverskoj platformi sa naprednim analitičkim alatima za obradu video materijala.

Do kraja projekta Ministarstvo će proširiti funkcionalnost video analitike uvođenjem nove funkcionalnosti - automatsko detektovanje lika lica iz kontinualnog video materijala. Ova funkcionalnost aktiviraće se softverski, dodeljivanjem licence određenoj kameri na sistemu.

Kamere, na kojima će se aktivirati licenca za detekciju lika, biće instalirane na prethodno precizno definisanim bezbednosno interesantnim lokacijama na teritoriji grada Beograda. Neophodno je da ove kamere budu postavljene na odgovarajućoj visini i usmerene u skladu sa tehničkim zahtevima i ograničenjima proizvođača opreme, odnosno, na visini od oko 4 metra sa uglom gledanja usmerenim ka zoni od interesa za policiju. Statistika detekcije lika iz kontinualnog video materijala, zavisiće od različitih faktora, kao što su: količina svetla, pozicija lica u zoni kamere, vremenskih prilika i dr. Softver za detekciju lika iz kontinualnog video materijala, automatski detektuje lik svih lica koja prolaze zonu nadzora kamera i izdvaja ih u vidu fotografije i kratkog video zapisa (trenutka kada je fotografija sačinjena), na sistemu za skladištenje po vremenski hronološkom kriterijumu.

Imajući u vidu da je Ministarstvo radi uvođenja savremenih tehnologija u obradi podataka o ličnosti dužno da izvrši procenu uticaja obrade na zaštitu podataka o ličnosti, u nastavku ovog teksta su navedeni svi bitni elementi te procene koje propisuje Zakon o zaštiti podataka o ličnosti iz 2018. Procena uticaja izrađena je na osnovu metodologije koju je u vezi sa procenom uticaja standardizovao EDPB.

PROCENA UTICAJA OBRADE NA ZAŠTITU PODATAKA O LIČNOSTI UPOTREBOM SAVREMENIH TEHNOLOGIJA VIDEO NADZORA U OKVIRU PROJEKTA „SIGURNO DRUŠTVO" U BEOGRADU

I SVEOBUHVATAN OPIS OBRADE PODATAKA

1. Pravni režim obrade

1.1. Podaci prikupljeni putem sistema video nadzora javnog mesta obrađuju se prvenstveno u posebnom pravnom režimu koji se primenjuje u slučajevima propisanim u čl. 1, st. 2. Zakona o zaštiti podataka o ličnosti (u daljem tekstu : Zakon).

1.2. U ostalim slučajevima podaci prikupljeni sistemom video nadzora obrađuju se u opštem pravnom režimu zaštite podataka o ličnosti propisanom Zakonom.

2. Primena pravnog režima obrade

2.1. Podaci prikupljeni u sistemu video nadzora uvek se obrađuju na automatizovani način, što znači da se obrađuju u okviru zbirki podataka, i to putem sledećih elektronskih uređaja:

a) 2.500 video kamera (fiksnih i pokretnih) postavljenih na stubovima na javnim površinama, odnosno na objektima u javnoj upotrebi;
b) 3500 uređaja za snimanje audio-video zapisa koji predstavljaju sastavni deo opreme policijskih službenika. (eLTE terminali).
v) 600 fisknih video kamera montiranih na vozilima policije.
g) 1500 kamera (body kamere) kao deo opreme policijskih službenika.

2.2. Podaci se prikupljaju sistemom video-akustičkog snimanja (sistem video nadzora), i to video i audio-video nadzorom javnih mesta na teritoriji grada Beograda, u okviru projekta "Siguran grad".

2.3. Lokacije na kojima se postavljaju kamere iz 2.1 a opredeljene su na osnovu izvršene analize potreba Ministarstva unutrašnjih poslova u cilju ostvarivanja svrhe video nadzora i to prema sledećim kriterijumima:
-Učestalost izvršenja krivičnih dela i prekršaja
-Učestalost saobraćajnih nezgoda
-Protočnost saobraćaja, saobraćajni koridori
-Mesta javnog okupljanja
-Objekti i lica koja obezbeđuje Ministarstvo unutrašnjih poslova

3. Podaci koji se obrađuju

3.1. Putem sistema video nadzora prikupljaju se sledeći podaci o fizičkim licima: lik, što uključuje i biometrijske podatke u slučaju nadzora kamerom koja stvara biometrijske podatke lika, izgled, što uključuje i telesne karakteristike lica, kao i učešće lica u događaju.

3.2. Putem sistema video nadzora u izuzetnim slučajevima prikupljaju se i podaci o zdravlju lica (na primer kod povređivanja izazvanog saobrađajnom nezgodom, u požaru i sl.), kao i podaci o pružanju zdravstvenih usluga u vezi sa tim podacima.

3.3. Putem sistema video nadzora prikupljaju se i sledeći podaci o vozilima: registarske i druge oznake vozila, boja vozila, drugi karakteristični znaci (na primer reklamni natpisi, oznaka proizvođaća vozila isl.).

3.4. Putem sistema video nadzora prikupljaju se i podaci o drugim predmetima (naprimer: ostavljeni koferi, torbe i sl. na javnom mestu);

3.5. Sistem video nadzora automatski generiše podatke o vremenu i mestu prikupljanja podataka.

4. Radnje obrade podataka

4.1. Obrada podataka u sistemu video nadzora obuhvata sledeće radnje obrade: prikupljanje, razvrstavanje, grupisanje, pohranjivanje, uvid, upotreba, otkrivanje prenosom, odnosno dostavljanjem, umnožavanje, upoređivanje, ograničavanje, brisanje odnosno uništavanje na drugi način.

4.2. Prikupljanje podataka se vrši stvaranjem video zapisa, fotografije, odnosno audio-video zapisa u digitalnom obliku putem video kamera i uređaja koji omogućavaju audio i video snimanje.

4.3. Video kamere imaju mogućnost zumiranja u skladu sa potrebom ovlašćenog lica rukovaoca. Pokretne video kamere uz mogućnost zumiranja mogu da se okreću u skladu sa potrebom ovlašćenog lica rukovaoca.

4.5. Video i audio-video zapisi se razvrstavaju odnosno grupišu na sledeći način:

a) automatski , prema lokaciji kamere, kao i datumu i vremenu stvaranja zapisa.
b) na osnovu odluke ovlašćenog lica rukovaoca, prema licu, vozilu, odnosno događaju koji se nadzire.

4.6. Audio i video zapisi se pohranjuju na čvrstu memoriju (hard diskovi, memorijske kartice, cd, usb memorije).

4.7. Uvid u audio i video zapise ima ovlašćeno lice koje rukuje kamerama na daljinu iz korisničkog centra, policijski službenik koji obavlja policijske poslove nadzorom javnog mesta i drugo ovlašćeno lice rukovaoca.

4.8. Upotreba audio i video zapisa je ograničena na svrhu i ciljeve prikupljanja i dalje obrade.

4.9. Audio i video zapisi se u pojedinačnim slučajevima mogu preneti ovlašćenim primaocima.

4.10. Zapisi lika se upoređuju sa drugim zapisima u cilju identifikacije lica, na osnovu biometrijskih podataka, kao i bez njih, dok se podaci o vozilu upoređuju sa drugim podacima o vozilima u cilju identifikacije vlasnika, odnosno korisnika vozila.

4.11. Identifikacija lica se može vršiti u toku snimanja ili pregledom snimljenog materijala.

4.12. Obrada podataka prikupljenih putem audio i video snimanja se može ograničiti, u skladu sa odredbama Zakona.

4.13. Audio i video zapisi se trajno brišu odnosno uništavaju nakon proteka zakonskog roka za njihovo čuvanje, odnosno proteka roka određenog odlukom rukovaoca koji je kraći od zakonskog roka, u skladu sa Zakonom.

4.14. Prilikom obrade podataka koristi se i profilisanje i to u slučaju obrade podataka koji nisu zasnovani na ličnoj oceni, kao i u slučaju obrade podataka koji su zasnovani na ličnoj oceni policijskog službenika.

4.15. Prilikom obrade podataka primenjuju se mere kriptozaštite.

5. Rukovalac, obrađivač i primalac

5.1. Rukovalac podacima koji se obrađuju putem sistema video nadzora je Ministarstvo unutrašnjih poslova Republike Srbije (dalje: Ministarstvo).

5.2. Ministarstvo samostalno obrađuje podatke u sistemu video nadzora, i to angažovanjem stručnih i ovlašćenih lica zaposlenih u okviru posebnih organizacionih jedinica Ministarstva korišćenjem opreme koja se nalazi u posedu Ministarstva.

5.3. Primalac podataka koji se obrađuju u posebnom režimu može biti samo nadležni organ, u smislu čl. 4, tač. 26. Zakona.

5.4. Primalac podataka koji se obrađuju u opštem režimu mogu biti organi javne vlasti, kao i pravna i fizička lica, u skladu sa Zakonom.

5.5. Podaci se mogu preneti primaocu u drugoj državi, odnosno međunarodnoj organizaciji, u skladu sa Zakonom.

6. Zakonitost obrade, poštenje i transparentnost

6.1. Pravni osnov za obradu podataka je isključivo zakon. Podaci se ne obrađuju na osnovu pristanka lica na koje se odnose.

6.2. U slučajevima obrade podataka u posebnom pravnom režimu, osnov za obradu su:
a) Zakon, čl. 13;
b) Zakon o policiji, čl.30,47, 50, 52, 59. 64 i77;
v) Zakon o evidencijama i obradi podataka u oblasti unutrašnjih poslova, čl. 13, 39, 47. 49, i 50;

g) Zakon o bezbednosti saobraćaja na putevima čl. 278. i 286;
d) Zakonik o krivičnom postupku, čl. 286.

6.3. U slučajevima obrade podataka u opštem pravnom režimu osnov za obradu su:
a) Zakon, čl. 12, st. 1, tač. 4. i 5;
b) Zakon o policiji, čl.30-33, čl. 35,42, 45, 131-134,;
v) Zakon o evidencijama i obradi podataka u oblasti unutrašnjih poslova čl. 3. t. 26,29,31,36 i 37.
g) Zakon o bezbednosti saobraćaja na putevima čl. 286.

6.4. Podaci se obrađuju pošteno i transparentno, u skladu sa Zakonom, što uključuje i primenu zakonskih odredbi o dopuštenim ograničenjima prava lica koja se odnose na ostvarivanje i zaštitu načela poštenja i transparentnosti obrade.

7. Svrha obrade

7.1. Svrha obrade podataka je u svakom konkretnom slučaju precizno određena, izričita, opravdana i zakonita, a podaci se dalje ne obrađuju na način koji nije u skladu sa tom svrhom.

7.2. Svrha obrade podataka u posebnom režimu je sprečavanje, istraga i otkrivanje krivičnih dela, gonjenje učinilaca krivičnih dela, odnosno obezbeđivanje izvršenja krivičnih sankcija. Svrha obrade je i sprečavanje i zaštita od pretnji javnoj i nacionalnoj bezbednosti.

7.3. Opravdanost svrhe obrade podataka u posebnom režimu neposredno se zasniva na potrebi ostvarivanja zakonom precizno određenih ciljeva obrade, i to:

a) Identifikovanje lica protiv kojih postoji osnovi sumnje da su izvršila ili nameravaju da izvrše krivično delo, odnosno prekršaj;
b) Identifikovanje lica protiv kojih postoji osnovana sumnja da su izvršila krivično delo, odnosno prekršaj;
v) Identifikovanje lica koja su oštećena krivičnim delom, odnosno prekršajem, ili za koja se pretpostavlja da bi mogla biti oštećena krivičnim delom, odnosno prekršajam;
g) Identifikovanje drugih lica koja su u vezi sa krivičnim delom, odnosno prekršajem, kao što su svedoci, lica koja mogu da obezbede informacije o krivičnom delu, odnosno prekršaju, kao i povezana lica ili saradnici lica navedenih pod a), b) i v).

7.4. Svrha obrade podataka u opštem režimu je zaštita životno važnih interesa lica (život i zdravlje), na koje se podaci odnose ili drugog lica, u smislu čl. 12, st. 1, tač. 4. Zakona. Takođe, svrha obrade podataka u opštem režimu je obavljanje zakonom propisanih poslova u javnom interesu, odnosno izvršenje zakonom propisanih ovlašćenja rukovaoca, u smislu čl. 12, st. 1, tač. 5. Zakona.

7.5. Opravdanost svrhe obrade podataka u opštem režimu neposredno se zasniva na potrebi ostvarivanja zakonom precizno određenih ciljeva obrade, i to:

a) Identifikovanje lica čiji je život ili zdravlje ugroženo u saobraćanoj nezgodi ili na drugi način (u slučaju nestanka deteta ili dementnog lica i sl.), odnosno lica čija je identifikacija neophodna u cilju zaštite života ili zdravlja drugih lica (u cilju sprečavanja širenja zaraze na druga lica i sl.);
b) Ostvarivanje uvida u stanje saobraćaja;
v) Informisanje javnosti o događajima koji su od značaja za život u gradu;
g) Obezbeđivanje materijala koji se koristi u školovanju, obuci, odnosno stručnom usavršavanju policijskih službenika;
d) Obezbeđivanje materijala koji se koristi za potrebe analize efekata obrade, daljeg razvoja i unapređivanja sistema video nadzora, kao i za statističke potrebe.

8. Minimizacija podataka

8.1. Obrađuju se samo oni podaci koji su primereni svrsi obrade, bitni za ostvarivanje svrhe obrade i ograničeni na ono što je neophodno u odnosu na svrhu obrade.

8.2. Na osnovu prikupljenih podataka putem sistema video nadzora vrši se identifikacija samo onih lica bez čije identifikacije nije moguće ostvariti svrhu obrade u konkretnom slučaju, i to:
a) Lica navedenih pod 7.3;
b) Lica navedenih pod 7.5.a).

8.3. Identitet lica koja ne pripadaju grupama lica navedenih pod 8.2. se ne utvrđuje na osnovu podataka prikupljenih u sistemu video nadzora.

9. Tačnost podataka

9.1. U sistemu video nadzora prikupljaju se podaci na osnovu kojih se upotrebom novih tehnologija može identifikovati lice sa veoma visokim stepenom pouzdanosti.

9.2. Ako fotografija odnosno video zapis sadrži i biometrijske podatke lika, identifikacija lica se vrši korišćenjem ovih podataka. U tom slučaju sistem video nadzora automatski generiše i podatke o stepenu pouzdanosti identifikacije za svako lice ponaosob.

9.3 Identifikaciju lica moguće je izvršiti i bez korišćenja biometrijskih podataka lika, upoređivanjem podataka prikupljenih u sistemu video nadzora sa drugim podacima kojima raspolaže rukovalac, u skladu sa čl. 77. Zakona o policiji.

9.4. Pouzdanost identifikacije lica u svakom konkretnom slučaju proverava ovlašćeno lice rukovaoca vršenjem službenih radnji propisanih zakonom. Ako se proverom utvrdi da se lice ne može identifikovati na osnovu podataka prikupljenih u sistemu video nadzora, ti podaci se brišu nakon isteka roka iz tačke 10.3.

10. Čuvanje podataka

10.1. Podaci prikupljeni u sistemu video nadzora na osnovu kojih je utvrđen identitet lica čuvaju se u roku koji je neophodan za ostvarivanje svrhe obrade, i to:

a) Podaci o identifikovanim licima navedenim pod 7.3. u zakonom propisanom roku od pet godina od dana nastanka zapisa, u smislu čl. 47, st. 3. Zakona o evidencijama i obradi podataka u oblasti unutrašnjih poslova, odnosno od dana okončanja postupka u smislu čl. 47, st 4. istog zakona.
b) Podaci o identifikovanim licima navedenim pod 7.5.a) u roku koji je neophodan za ostvarivanje svrhe obrade koja se odnosi na zaštitu života i zdravlja lica u smislu čl. 7, st. 2. Zakona o evidencijama i obradi podataka u oblasti unutrašnjih poslova.

10.2. Podaci prikupljeni u sistemu video nadzora na osnovu kojih se ne utvrđuje identitet lica čuvaj se najmanje 30 dana od dana nastanka zapisa. Rok od 30 dana propisan čl. 47. st. 3 Zakona o evidencijama i obradi podataka u oblasti unutrašnjih poslova, uslovljen je tehničkim ograničenjima pohranjivanja podataka prikupljenih u sistemu video nadzora i kraći je od roka koji je određen Zakonom o policiji, čl. 52. Sistem automatski ciklično briše najstarije podatke novijim kada se popuni memorijski prostor arhive(tzv. kružno snimanje).

10.3. Rukovalac proverava da li se lice navedeno pod 7.3. može identifikovati na osnovu podataka prikupljenih u sistemu video nadzora u roku od jedne godine od dana nastanka zapisa. Ako je proverom iz 9.4. utvrđeno da se lice ne može identifikovati na osnovu podataka

prikupljenih u sistemu video nadzora u navedenom roku, podaci se uništavaju, u skladu sa Zakonom o policiji, čl. 52, st. 7.

11. Integritet i poverljivost podataka

11.1. Bezbednost podataka se osigurava primenom odredbi o dopuštenoj obradi podataka, odredbi koje se odnose na prava lica, kao i primenom tehničkih, organizacionih i kadrovskih mera propisanih Zakonom.

11.2. Poseban cilj primene odredbi i mera kojima se osigurava bezbednost podataka jeste eliminasanje rizika od obrade podataka po prava i slobode fizičkih lica, i to u potpunosti, odnosno u najvećoj meri.

12. Obrada u druge svrhe

12.1. Podaci koji se obrađuju u posebnom režimu u cilju identifikacije lica navedenih pod 7.3. i 7.5a rukovalac ne obrađuje u druge svrhe.

12.2. U cilju identifikacije lica navedenih pod 7.3. i 7.5.a) podaci prikupljeni u sistemu video nadzora se mogu upoređivati sa podacima koji su prikupljeni u druge svrhe, a posebno u slučaju kad se upoređivanje vrši sa podacima, uključujući i biometrijske podatke, koji su sadržani u evidenciji ličnih isprava fizičkih lica.

12.3. Ako se u cilju identifikacije lica navedenih pod 7.3. i 7.5.a) podaci prikupljeni u sistemu video nadzora upoređuju sa podacima koji su prvobitno prikupljeni od strane nadležnih organa u druge posebne svrhe iz čl. 1, st. 2. Zakona, utvrđivanje identiteta lica se zasniva na čl. 7, st. 1. i 2. Zakona, kao i na odredbama zakona navedenih pod 6.2.

12.4. Ako se u cilju identifikacije lica navedenih pod 7.3. i 7.5.a) podaci prikupljeni u sistemu video nadzora upoređuju sa podacima koji su prvobitno prikupljeni u druge svrhe koje nisu navedene pod 12.3, utvrđivanje identiteta lica se zasniva na čl. 6, st. 1. i čl. 40, st. 1, tač. 1. do 6, 9. i 10. Zakona, kao i na odredbama zakona navedenih pod 6.3.

13. Razlikovanje vrsta lica i podataka

13.1. Prilikom identifikacije lica na osnovu podataka prikupljenih u sistemu video nadzora, rukovalac razvrstava podatke o licima navedenim pod 7.3. i 7.5.a) u posebne grupe podataka.

13.2. Razvrstavanje podataka o sledećim grupama lica navedenim pod 7.3. zasnovano je na ličnoj oceni:
a) Lica protiv kojih postoji osnovi sumnje da su izvršila ili nameravaju da izvrše krivično delo, odnosno prekršaj;
b) Lica protiv kojih postoji osnovana sumnja da su izvršila krivično delo, odnosno prekršaj;
v) Lica za koja se pretpostavlja da bi mogla biti oštećena krivičnim delom, odnosno prekršajam;
g) Lica koja su u vezi sa krivičnim delom, odnosno prekršajem, kao što su svedoci, lica koja mogu da obezbede informacije o krivičnom krivičnom delu, odnosno prekršaju, kao i povezana lica ili saradnici lica navedenih pod 7.3.

14. Obrada posebnih vrsta podataka o ličnosti

14.1. Identifikacija lica navedenih pod 7.3. može se vršiti na osnovu obrade biometrijskih podataka lika lica, a u skladu sa zakonskim ovlašćenjima rukovaoca, u smislu čl. 18, tač. 1. Zakona.

14.2. Identifikacija lica navedenih pod 7.5.a) može se vršiti na osnovu obrade biometrijskih podataka lika. Prilikom identifikacije ovih lica obrađuju se i podaci o njihovom zdravstvenom stanju. Obrada podataka o ovim licima zasniva se na zakonskim ovlašćenjima rukovaoca, u smislu čl. 17, st. 2, tač. 3. Zakona.

15. Obrada koja ne zahteva identifikaciju

15.1. Na osnovu podataka prikupljenih u sistemu video nadzora utvrđuje se samo identitet lica navedenih pod 7.3. i 7.5.a), a ne i drugih lica, i o tome rukovalac informiše lica obuhvaćena video nadzorom putem medija, drugih sredstava javnog obaveštavanja (internet prezentacije i sl.), i na drugi pogodan način.

15.2. Za ostvarivanje svrhe obrade nije neophodno potrebno utvrditi identitet drugih lica lica koji ne pripadaju grupama lica navedenim pod 7.3. i 7.5.a) na osnovu podataka prikupljenih u sistemu video nadzora. Zbog toga ovlašćeno lice rukovaoca ne pribavlja i ne obrađuje dodatne podatke u cilju identifikacije tih drugih lica, u smislu čl. 20, st. 1. Zakona.

16. Automatizovano donošenje odluka

16.1. Identifikacija lica navedenih pod 7.3. i 7.5.a) u svakom konkretnom slučaju se vrši na osnovu odluke ovlašćenih lica rukovaoca, i to bez obzira na to da li se identifikacija vrši u toku stvaranja zapisa ili naknadnim pregledom zapisa. To znači da se u sistemu video nadzora identitet lica ne utvrđuje isključivo na osnovu automatizovane obrade podataka, u smislu čl. 38. i 39. Zakona, odnosno da se ne primenjuje tzv. automatsko prepoznavanje lica.

16.2. Nakon identifikacije lica navedenih pod 7.3. i 7.5.a), mogu se preduzeti radnje ili doneti odluke koje proizvode pravne posledice po lice, odnosno utiču na položaj lica. Ove radnje i odluke se ne primenjuju na lice isključivo na osnovu automatizovane obrade podataka, već se u svakom konkretnom slučaju zahteva posredovanje ovlašćenih lica rukovaoca u smislu određivanja svrhe i načina primene radnje, odnosno odluke. Pravni osnov za preduzimanje radnje ili donošenje odluke o identifikovanom licu je u svakom konkretnom sadržan u zakonu koji se primenjuju na postupanje policije.

II PROCENA RIZIKA PO PRAVA I SLOBODE LICA

1. Rizik koji se odnosi na identifikaciju lica bez pravnog osnova

1.1. Događaj koji podrazumeva rizik po prava i slobode lica vezuje se za identifikaciju lica na osnovu podataka prikupljenih u sistemu video nadzora javnih površina u cilju koji nije obuhvaćen tačkama 7.3. i 7.5.a) iz prvog dela dokumenta (”Sveobuhvatan opis obrade podataka”). Pri tome, za potrebe procene rizika u određenoj meri je od značaja razlog za protivpravnu identifikaciju, odnosno činjenica da je identifikacija motivisana razlozima lične ili druge prirode.

1.2. Usled događaja navedenog pod 1.1. mogle bi nastupiti sledeće posledice po prava i slobode lica:
a) Povreda prava na privatan život i to posmatranjem aktivnosti aktivnosti lica koje je identifikovano u sistemu video nadzora, kao i pohranjivanjem i drugim radnjama obrade podataka o ovim aktivnostima, bez obzira na činjenicu da se aktivnosti preduzimaju na javnim površinama;
b) Povreda slobode udruživanja, okupljanja i izražavanja, odnosno prava na miran protest, kao i slobode kretanja, i to identifikovanjem i daljom obradom podataka lica koja se na javnim

površinama okupljaju, kao članovi udruženja ili bez obzira na članstvo u udruženju, izražavaju svoje mišljenje, ideje i stavove, mirno protestuju, odnosno kreću se na javnim površinama kao deo povorke, protestnog skupa i sl, u skladu sa zakonom koji uređuje uslove za vršenje navedenih sloboda i prava;
v) Povreda slobode veroispovesti i to identifikovanjem i daljom obradom podataka lica koja ulaze u ili izlaze iz verskih objekata ili učestvuju u vršenju verskih obreda na javnim površinama;
g) Povreda principa zabrane diskriminacije u slučajevima povrede sloboda i prava navedenih pod 1.2. b) i v), i to putem profilisanja identifikovanih lica na osnovu stvarne ili pretpostavljene pripadnosti udruženju, odnosno verskoj zajednici, političkog ili drugog mišljenja, seksualnog opredeljenja ili drugog ličnog svojstva.

1.3. Nivo izvesnosti nastupanja događaja navedenog pod 1.1. je nizak. Prilikom procene nivoa izvesnosti posebno se uzimaju o obzir sledeće okolnosti, odnosno činjenice:
a) Identifikacija lica na osnovu podataka prikupljenih u sistemu video nadzora temelji se u svakom konkretnom slučaju na organizacionoj strukturi u sistemu podeljenih uloga u pogledu vršenja radnji obrade, odlučivanja o potrebi identifikacije i kontrole, što u najvećoj meri onemogućava eventualni individualni pokušaj zloupotrebe policijskih ovlašćenja;
b) Svaka radnja obrade podataka prikupljenih u sistemu video nadzora, uključujući i identifikaciju lica, beleži se u cilju omogućavanja efikasne kontrole vršenja policijskih ovlašćenja, što u najvećoj meri odvraćajuće deluje na potencijalne prekršioce policijskih ovlašćenja;
v) Broj slučajeva zloupotrebe, odnosno kršenja policijskih ovlašćenja je godinama unazad veoma mali u odnosu na broj preduzetih radnji ovlašćenih lica rukovaoca, što ukazuje na izuzetnu disciplinovanost i savesnost policijskih službenika.
g) Ovlašćena lica rukovaoca su već edukovana o pravnom režimu zaštite ličnih podataka, što ukazuje na visok nivo svesti o neophodnosti poštovanja načela zakonitosti i drugih načela Zakona u pogledu vršenja policijskih ovlašćenja prilikom obrade podataka, a posebno u sistemu video nadzora.

1.4. Procena ozbiljnosti moguće povrede prava i sloboda lica navedenih pod 1.2. se određuje na sledeći način:
a) Pravo na privatnost lica obuhvaćenog sistemom video nadzora bi nužno bilo povređeno usled događaja navedenog pod 1.1, a s obzirom na to da lice opravdano pretpostavlja da u odnosu prema drugim ljudima zadržava svoju anonimnost iako aktivnosti preduzima na javnoj površini;
b) Druga prava lica obuhvaćenog sistemom video nadzora koja su navedena pod 1.2. ne bi nužno bila povređena usled događaja navedenog pod 1.1. Nastupanje povrede prava bi u svakom konkretnom slučaju zavisilo od namere prekršioca policijskih ovlašćenja, odnosno cilja nedopuštenog profilisanja i drugih radnji obrade.
v) Na procenu ozbiljnosti moguće povrede prava i sloboda lica navedenih pod 1.2. utiče i stepen razvijenosti svesti građana o visini rizika po njihova prava i slobode. Ako u javnosti preovlađuje svest o tome da je nivo rizika po prava i slobode lica obuhvaćenih video nadzorom visok, onda se može pretpostaviti da bi ta okolnost mogla proizvesti negativan efekat u pogledu uživanja pojedinih prava i sloboda (naprimer stvaranje osećanja opravdane bojazni za svoj privatan život ili uzdržavanje od učešća u javnom okupljanju, izražavanju mišljenja i sl.).

2. Rizik koji se odnosi na snimanje privatnog prostora

2.1. Događaj koji podrazumeva rizik po prava i slobode lica vezuje se za snimanje privatnog prostora, kao što je unutrašnjost stanova, kuća i okućnica, kancelarija i drugih poslovnih prostora, korišćenjem video kamera koje su postavljene na stubovima i zgradama u javnoj upotrebi. Pri tome, za potrebe procene rizika u određenoj meri je od značaja razlog za protivpravno snimanje, odnosno činjenica da je snimanje motivisano razlozima lične ili druge prirode.

2.2. Usled događaja navedenog pod 2.1. mogla bi nastupiti posledica koja se sastoji u

povredi prava na privatnost i to uvidom u aktivnosti lica koje se nalazi u prostoru koji se snima, kao i pohranjivanjem i drugim radnjama obrade podataka o ovim aktivnostima.

2.3. Nivo izvesnosti nastupanja događaja navedenog pod 2.1. je nizak. Prilikom procene nivoa izvesnosti posebno se uzimaju o obzir sledeće okolnosti, odnosno činjenice:
a) Fiksne kamere su fizički postavljene tako da snimaju samo javni prostor, dok se pokretne kamere mogu koristiti za snimanje privatnog prostora i to samo u onim izuzetnim slučajevima kad snimanje nije ograničeno fizičkim preprekama (naprimer kamera je postavljena na nižem položaju u odnosu na privatan prostor ili na položaju koji je veoma udaljen od privatnog prostora ili je privatan prostor zaklonjen drvećem, zavesama, roletnama, ogradama i sl), što u najvećoj meri ograničava mogućnost praćenja aktivnosti lica u privatnom prostoru;
b) Praćenje aktivnosti lica upotrebom pokretnih video kamera temelji se u svakom konkretnom slučaju na organizacionom sistemu podeljenih uloga u pogledu vršenja radnji obrade, odlučivanja o potrebi praćenja i kontrole, što u najvećoj meri onemogućava eventualni individualni pokušaj zloupotrebe policijskih ovlašćenja;
v) Podatak o okretanju kamere u svakom konkretnom slučaju može utvrditi u cilju omogućavanja efikasne kontrole vršenja policijskih ovlašćenja, što u najvećoj meri odvraćajuće deluje na potencijalne prekršioce policijskih ovlašćenja;
g) Broj slučajeva zloupotrebe, odnosno kršenja policijskih ovlašćenja je godinama unazad veoma mali u odnosu na broj preduzetih radnji ovlašćenih lica Ministarstva, što ukazuje na izuzetnu disciplinovanost i savesnost policijskih službenika.
d) Ovlašćena lica rukovaoca su već edukovana o pravnom režimu zaštite ličnih podataka, što ukazuje na visok nivo svesti o neophodnosti poštovanja načela zakonitosti i drugih načela Zakona u pogledu vršenja policijskih ovlašćenja prilikom obrade podataka, a posebno u sistemu video nadzora.

2.4. Procena ozbiljnosti moguće povrede prava na privatnost lica se određuje na sledeći način:
a) Pravo na privatnost lica obuhvaćenog sistemom video nadzora bi nužno bilo povređeno usled događaja navedenog pod 2.1, a s obzirom na to da lice opravdano pretpostavlja da su aktivnosti koje preduzima u privatnom prostoru zaštićene od pogleda drugih ljudi;
b) Na procenu ozbiljnosti moguće povrede prava na privatnost lica utiče i stepen razvijenosti svesti građana o visini rizika po ovo njihovo pravo. Ako u javnosti preovlađuje svest o tome da je nivo rizika koji se vezuje za video snimanje privatnih prostora visok, onda se može pretpostaviti da bi ta okolnost mogla proizvesti negativan efekat u pogledu uživanja prava na privatnost (naprimer stvaranje osećanja opravdane bojazni za svoj privatan život).

3. Rizik koji se odnosi na povredu bezbednosti podataka

3.1. Događaj koji podrazumeva rizik po prava i slobode lica vezuje se za povredu bezbednosti podataka prikupljenih u sistemu video nadzora usled pristupa opremi koja se koristi u svrhu video nadzora (naprimer preuzimanje kontrole nad kamerama), odnosno kopiranja, otkrivanja, odnosno prenošenja podataka i to od strane trećeg lica, u smislu čl. 4, tač. 11. Zakona. Pri tom, za potrebe procene rizika nije od značaja razlog za povredu bezbednosti, odnosno činjenica da je povreda bezbednosti motivisana razlozima lične ili druge prirode.

3.2. Usled događaja navedenog pod 3.1. mogla bi nastupiti posledica koja se sastoji u
povredi prava na zaštitu podataka o ličnosti lica, na koje se odnose podaci čija je bezbednost povređena.

3.3. Nivo izvesnosti nastupanja događaja navedenog pod 3.1. je nizak. Prilikom procene nivoa izvesnosti posebno se uzimaju o obzir sledeće okolnosti, odnosno činjenice:
a) Oprema i podaci su obezbeđeni tehničkim merama zaštite na najvišem nivou, a posebno u pogledu softverske zaštite, zaštita mreže za prenos podataka, zaštite podataka sistemom

kriptozaštie, kao i fizičke zaštite kamera, vodova, opreme za skladištenje podataka i sl, što u najvećoj meri efikasno sprečava povredu bezbednosti podataka od strane trećeg lica;
b) Oprema i podaci su obezbeđeni sveobuhvatnim organizacionim merama zaštite, a posebno primenom sistema podeljenih uloga u pogledu vršenja radnji obrade, što u najvećoj meri efikasno sprečava povredu bezbednosti podataka od strane trećeg lica, a u saradnji sa policijskim službenicima;
v) Ovlašćena lica rukovaoca su putem edukacije već osposobljena za preduzimanje tehničkih i organizacionoih mera zaštite podataka o ličnosti, što u najvećoj meri efikasno sprečava povredu bezbednosti podataka od strane trećeg lica;
g) Godinama unazad nije dolazilo do povrede bezbednosti podataka od strane trećeg lica, što ukazuje na delotvornost preduzetih mera zaštite kad se radi o obradi podataka koju vrši rukovaoc.

3.4. Procena ozbiljnosti moguće povrede prava na privatnost lica se određuje na sledeći način:
a) Pravo na zaštitu podataka koji se odnose na lice obuhvaćeno sistemom video nadzora bi nužno bilo povređeno usled događaja navedenog pod 3.1, a s obzirom na to da je rukovalac po Zakonu dužan da obezbedi podatke koje obrađuje od povrede;
b) Na procenu ozbiljnosti moguće povrede prava na zaštitu podataka o ličnosti utiče i stepen razvijenosti svesti građana o visini rizika po ovo njihovo pravo. Ako u javnosti preovlađuje svest o tome da je nivo rizika koji se vezuje za povredu bezbednosti podataka od strane trećeg lica visok, onda se može pretpostaviti da bi ta okolnost mogla proizvesti negativan efekat u pogledu uživanja prava na zaštitu podataka o ličnosti (naprimer stvaranje osećanja opravdane bojazni za podatke koje rukovalac o njemu obrađuje).

4. Rizik koji se odnosi na javno objavljivanje podataka

4.1. Događaj koji podarazumeva rizik po prava i slobode lica vezuje se za pravno nedopušteno javno objavljivanje podataka prikupljenih u sistemu video nadzora putem medija, društvenih mreža ili korišćenjem drugih sredstava komunikacije. Pri tome, za potrebe procene rizika u određenoj meri je od značaja razlog za javno objavljivanje, odnosno činjenica da je javno objavljivanje motivisano razlozima lične ili druge prirode.

4.2. Usled događaja navedenog pod 4.1. mogle bi nastupiti sledeće posledice po prava i slobode lica:
a) Povreda prava na privatan život i to uvidom u aktivnosti lica koje je obuhvaćeno sistemom video nadzora od strane javnosti, odnosno primaoca informacija koje se objavljuju u medijima, u okviru društvenih mreža ili se šire putem drugih sredstava komunikacije;
b) Povreda prava na identitet, u slučajevima kad je lice koje je obuhvaćeno sistemom video nadzora pogrešno identifikovano u javnosti;
v) Povreda ličnog moralnog integriteta, u slučajevima kad je usled javnog objavljivanja informacije koja se odnosi na privatan život lica povređen ugled, čast ili pijetet tog lica;
g) Povreda prava navedenih pod 1.2. b) od g), u slučajevima kad je usled javnog objavljivanja informacije koja se odnosi na privatan život lica povređeno neko od navedenih prava.

4.3. Nivo izvesnosti nastupanja događaja navedenog pod 4.1. je nizak. Prilikom procene nivoa izvesnosti posebno se uzimaju o obzir sledeće okolnosti, odnosno činjenice:
a) Obrada podataka prikupljenih u sistemu video nadzora temelji se u svakom konkretnom slučaju na organizacionom sistemu podeljenih uloga u pogledu vršenja radnji obrade, što u najvećoj meri onemogućava nedopušteno javno objavljivanje podataka;
b) Svaka radnja obrade podataka prikupljenih u sistemu video nadzora, beleži se u cilju omogućavanja efikasne kontrole vršenja policijskih ovlašćenja, što u najvećoj meri odvraćajuće deluje na neovlašćeno dostavljanje podataka medijima, odnosno prenos podataka u cilju njihovog javnog objavljivanja;

v) Broj slučajeva nedopuštenog javnog objavljivanja podataka koje rukovalac obrađuje se iz godine u godinu smanjuje i veoma je mali u odnosu na broj preduzetih radnji ovlašćenih lica rukovaoca, što ukazuje na izuzetnu disciplinovanost i savesnost policijskih službenika.
g) Ovlašćena lica rukovaoca su već edukovana o pravnom režimu zaštite ličnih podataka, što ukazuje na visok nivo svesti o neophodnosti poštovanja načela zakonitosti i drugih načela Zakona u pogledu vršenja policijskih ovlašćenja prilikom obrade podataka, a posebno u vezi sa sprečavanjem nedopuštenog javnog objavljivanja podataka.

4.4. Procena ozbiljnosti moguće povrede prava i sloboda lica navedenih pod 4.2. se određuje na sledeći način:
a) Pravo na privatnost lica obuhvaćenog sistemom video nadzora bi nužno bilo povređeno usled događaja navedenog pod 4.1, a s obzirom na to da je nužno pretpostaviti da usled javnog objavljivanja podataka prikupljenih sistemom video nadzora dolazi do identifikacije lica.
b) Druga prava lica obuhvaćenog sistemom video nadzora koja su navedena pod 4.2. ne bi nužno bila povređena usled događaja navedenog pod 4.1. Nastupanje povrede prava bi u svakom konkretnom slučaju zavisilo od objektivnih okolnosti koje se odnose na tačnost identifikacije, odnosno podobnost javno objavljenih podataka iz privatnog života da prouzrokuju povredu ličnog moralnog integriteta lica, kao i subjektivnih okolnosti koje se odnose na nameru povredioca prava, odnosno cilj nedopuštenog profilisanja i drugih radnji obrade.
v) Na procenu ozbiljnosti moguće povrede prava i sloboda lica navedenih pod 4.2. utiče i stepen razvijenosti svesti građana o visini rizika po njihova prava i slobode. Ako u javnosti preovlađuje svest o tome da je nivo rizika po prava i slobode lica obuhvaćenih video nadzorom visok, onda se može pretpostaviti da bi ta okolnost mogla proizvesti negativan efekat u pogledu uživanja pojedinih prava i sloboda (naprimer stvaranje osećanja opravdane bojazni za svoj privatan život, identitet, odnosno lični moralni integritet ili uzdržavanje od vršenja prava i sl.).

III OPIS PRIMENJENIH MERA I MEHANIZAMA U ODNOSU NA RIZIK PO PRAVA I SLOBODE LICA

1. Mere zaštite bezbednosti podataka i mehanizmi zaštite prava lica

1.1. Predstavljeni rizici po prava i slobode lica efikasno se uklanjaju, odnosno svode na najmanju meru putem primene opštih organizacionih, kadrovskih i tehničkim mera zaštite bezbednosti podataka, odnosno mehanizama zaštite prava i sloboda lica u vezi sa obradom podataka o ličnosti. Ove mere i mehanizmi propisani su Zakonom i drugim propisima, kao što je Zakon o informacionoj bezbednosti, Zakon o policiji, Zakon o evidencijama i obradi podataka u oblasti unutrašnjih poslova i podzakonski akti doneti od strane Ministarstva.

1.2. Mere zaštite bezbednosti podataka i mehanizmi zaštite prava lica primenjuju se na specifičan način u sistemu video nadzora. Pojedine od ovih mera i mehanizama primenjuju se u odnosu na više različitih rizika i to na isti ili različit način, dok se druge mere i mehanizmi primenjuju samo u odnosu na pojedinačno određen rizik.

2. Sistem podeljenih uloga u obradi podataka

2.1. Sistem video nadzora je kreiran tako da može da bude funkcionalan samo u sistemu podeljenih uloga. To znači da u prikupljanju i daljoj obradi podataka u sistemu video nadzora nije moguće organizaciono, tehnički i pravno zamisliti situaciju u kojoj se odluka o preduzimanju radnji obrade koje imaju za cilj identifikaciju lica, odnosno praćenje aktivnosti lica, a u kontekstu procene nivoa izvesnosti nastupanja rizika navedene pod II 1.3. a), 2.3. b), 3.3. b) i 4.3. a) (”Procena rizika po prava i slobode lica”), donosi izvan sistema podeljenih uloga.

2.2. Primenom ove organizacione mere zaštite efikasno se sprečava eventualni individualni pokušaj zloupotreba policijskih ovlašćenja, i to zbog toga što ovlašćeno službeno lice rukovaoca nikada ne može samo, bez učešća drugih ovlašćenih službenih lica, da preduzme radnje obrade na koje upućuju rizici navedeni pod 2.1. Na taj način se u najvećoj meri minimizuje verovatnoća nastupanja rizika.

2.3. Sistem podele uloga u sistemu video nadzora zasniva se na Pravilniku o unutrašnjem uređenju i sistematizaciji radnih mesta u Ministarstvu. Ovim aktom uređuje se nadležnost pojedinih organizacionih jedinica Ministarstva, kao i opis poslova i zadataka za svako pojedinačno radno mesto, što uključuje i propisivanje opštih i posebnih uslova za raspoređivanje na radno mesto.

2.4. Zaposleni raspoređeni na pojedinim radnim mestima u sistemu video nadzora sa ovlašćenjima da prikupljaju i dalje obrađuju podatke, imaju status ovlašćenih službenih lica. U vršenju svojih poslova i zadataka u sistemu video nadzora oni su raspoređeni po organizacionim jedinicama Ministarstva.

2.5. U svakoj od organizacionih jedinica za svako ovlašćeno službeno lice vezuje se unapred određeni nivo odlučivanja, odnosno ovlašćenje za preduzimanje pojedinih radnji obrade. Takođe, za pojedina ovlašćena službena lica vezuje se i funkcija kontrole izvršenja poslova i zadataka u sistemu video nadzora.

2.5. U sistemu video nadzora kojim rukuje Ministarstvo svaku radnju obrade vrši lice koje je ovlašćeno za preduzimanje te radnje. Pri tome, nijedno od lica angažovanih u sistemu video nadzora nema ovlašćenje za preduzimanje svih radnji obrade, te se naprimer ovlašćenje za prikupljanje podataka vezuje za lice koje je raspoređeno u okviru jedne organizacione jedinice, dok se ovlašćenja za korišćenje drugih podataka na osnovu kojih je moguće identifikovati lice na koje se odnose prikupljeni podaci, kao i za odlučivanje o neophodnosti identifikacije tog lica, vezuju za druga službena lica koja su raspoređena u više različitih organizacionih jedinica.

2.6. Kontrolu zakonitosti, odnosno pravilnosti vršenja ovlašćenja navedenih pod 2.5. neposredno vrše ovlašćena službena lica koja rukovode pojedinim organizacionim jedinicama u sistemu video nadzora, Sektor unutrašnje kontrole, kao i organiizaciona jedinica nadležna za poslove kontrole rada. Ova kontrola se, između ostalog, obezbeđuje evidentiranjem svake radnje obrade, odnosno tehničkim omogućavanjem utvrđivanja činjenica koje se odnose na korišćenje kamera i druge opreme u sistemu video nadzora u svakom konkretnom slučaju.

2.7. Primena tehničkih mera zaštite u sistemu video nadzora takođe je zasnovana na sistemu podeljenih uloga i to prema nadležnostima različitih organizacionih jedinica.

2.8. Primena navedenih organizacionih mera zaštite podataka u sistemu video nadzora, i sa njima povezanih tehničkih i kadrovskih mera zaštite, uređuje se Zakonom o evidencijama i obradi podataka u oblasti unutrašnjih poslova, Uputstvom o merama informacione bezbednosti u informaciono-komunikacionom sistemu Ministarstva unutrašnjih poslova i Uputstvom o uslovima izgradnje, korišćenja i održavanja sistema video nadzora u Ministarstvu unutrašnjih poslova i Uputstvom o načinu vođenja evidencija u oblasti video-akustičkog snimanja.

3. Tehnički aspekti obezbeđivanja sistema video nadzora

3.1. Izgradnja sistema video nadzora vrši se na obrazloženi predlog Direkcije policije a na osnovu odluke ministra, odnosno lica koje on ovlasti za donošenje ove odluke. U svrhu donošenja odluke o izgradnji sistema video nadzora ili dela ovog sistema vrši se analiza potreba postavljanja kamera na pojedinim kamernim mestima, a prema kriterijumima navedenim pod I 2.3. (”Sveobuhvatan opis radnji obrade”). Pri tome se u kontekstu procene nivoa izvesnosti

nastupanja rizika navedene pod II 2.3. a) (”Procena rizika po prava i slobode lica”), posebno vodi računa o ostvarenju svrhe video nadzora, odnosno o tome da se postavljanjem kamera na adekvatne položaje u najvećoj meri onemogući snimanje privatnog prostora.

3.2. Sistem video nadzora predstavlja sastavni deo informaciono-komunikacionog sistema (IKT), kojim rukuje Ministarstvo. Ovaj sistem se efikasno štiti, između ostalog, odgovarajućim tehničkim merama informacione bezbednosti koje se primenjuju prema podacima i opremi koja se koristi. U kontekstu procene nivoa izvesnosti nastupanja rizika navedene pod II 3.3. a) i g) (”Procena rizika po prava i slobode lica”), tehničkim merama se efikasno štite podaci i oprema, posebno uzimajući u obzir činjenicu da godinama unazad nije zabeležen nijedan slučaj povrede bezbednosti podataka od strane trećih lica usled nedostataka vezanih za ove mere zaštite.

3.3. Tehničke mere zaštite koje se koriste u sistemu video nadzora naročito obuhvataju sledeće:
- Postizanje bezbednosti rada na daljinu i upotrebe mobilnih uređaja;
- Zaštita nosača podataka;
-Upotreba kriptozaštite radi zaštite tajnosti, autentičnosti odnosno integriteta podataka;
- Fizička zaštita objekata, prostora, prostorija, odnosno zona u kojima se nalaze sredstva i dokumenti IKT sistema i obrađuju podaci u IKT sistemu;
- Zaštita od gubitka, oštećenja, krađe ili drugog oblika ugrožavanja bezbednosti sredstava koja čine IKT sistem;
- Obezbeđivanje ispravnog i bezbednog funkcionisanja IKT sistema;
- Zaštita podataka i sredstva za obradu podataka od zlonamernog softvera;
- Zaštita od gubitka podataka;
- Čuvanje podataka o događajima koji mogu biti od značaja za bezbednost IKT sistema;
- Obezbeđivanje integriteta softvera i operativnih sistema;
- Zaštita od zloupotrebe tehničkih bezbednosnih slabosti IKT sistema;
- Zaštita podataka u komunikacionim mrežama uključujući uređaje i vodove;
- Osiguranje bezbednosti podataka koji se prenose unutar IKT sistema, kao i između IKT sistema MUP-a i drugih IKT sistema;
- Prevencija i reagovanje na bezbednosne incidente u okviru IKT sistema, što podrazumeva adekvatnu razmenu informacija o bezbednosnim slabostima, incidentima i pretnjama u okviru IKT sistema.

3.4. Tehničkim merama zaštite se posebno obezbeđuje evidentiranje svake radnje obrade, odnosno tehnička mogućnost utvrđivanja činjenica koje se odnose na korišćenje kamera i druge opreme u sistemu video nadzora u svakom konkretnom slučaju. Na ovaj način se obezbeđuje efikasna kontrola nad radnjama obrade, što u najvećoj meri odvraćajuće deluje na potencijalne prekršioce službenih ovlašćenja i to u kontekstu procene nivoa izvesnosti nastupanja rizika navedene pod II 1.3. b), 2.3. v) i 4.3. b) (”Procena rizika po prava i slobode lica”).

3.5. Primena navedenih tehničkih mera zaštite podataka i opreme u sistemu video nadzora, i sa njima povezanih organizacionih mera zaštite, uređuje se Zakonom o evidencijama i obradi podataka u oblasti unutrašnjih poslova, Uputstvom o merama informacione bezbednosti u informaciono-komunikacionom sistemu Ministarstva unutrašnjih poslova, Uputstvom o uslovima izgradnje, korišćenja i održavanja sistema video nadzora u Ministarstvu unutrašnjih poslova i Uputstvom o načinu vođenja evidencija u oblasti video-akustičkog snimanja.

4. Disciplinovanost i savesnost policijskih službenika

4.1. Disciplinovanost i savesnost ovlašćenih službenih lica angažovanih u sistemu video nadzora obezbeđuje se primenom preventivnih i reaktivnih mera zaštite. U kontekstu procene nivoa izvesnosti nastupanja rizika navedene pod II 1.3. v) i g), 2.3. g) i d), 3.3. v) i 4.3. v) i g) (”Procena rizika po prava i slobode lica”), ovim merama se podiže nivo svesti ovlašćenih službenih lica o

neophodnosti zaštite bezbednosti podataka i poštovanja prava i sloboda lica, što u najvećoj meri povratno deluje na minimizaciju verovatnoće nastupanja rizika.

4.2 Preventivne mere zaštite se prvenstveno sprovode putem kontinuirane edukacije ovlašćenih službenih lica i to u vezi sa primenom odredbi Zakona i drugih propisa koji se odnose na zaštitu podataka o ličnosti. Poslovi edukacije vrše se u skladu sa Uredbom o stručnom osposobljavanju i usavršavanju u Ministarstvu unutrašnjih poslova, na osnovu Programa stručnog usavršavanja policijskih službenika Ministarstva unutrašnjih poslova i Direktive o načinu obavljanja poslova u vezi sa zaštitom podataka o ličnosti u Ministarstvu unutrašnjih poslova.

4.3. U periodu nakon usvajanja Zakona održana su dva ciklusa edukacija. U periodu oktobar-novembar 2019. organizovano je osam treninga za trenere o zaštiti podataka o ličnosti u okviru Ministarstva. U aprilu 2020. organizovano je još četiri produbljena celodnevna seminara o zaštiti podataka o ličnosti za ovlašćena lica Ministarstva, sa posebnim akcentom na pitanja vezana za video nadzor.

4.4. Oba edukaciona ciklusa bila su namenjena ovlašćenim licima Ministarstva sa čitave teritorije Republike Srbije. Kroz edukaciju su, između ostalih, prošli i svi načelnici područnih policijskih uprava. Jednu od posebnih grupa polaznika činili su rukovodioci strateškog nivoa i ovlašćena službena lica Sektora unutrašnje kontrole. Oba edukaciona ciklusa bila su organizovana od strane Ministarstva, u partnerstvu sa Kancelarijom saveta za nacionalnu bezbednost i zaštitu tajnih podataka, Misijom OEBS u Srbiji, i organizacijama civilnog društva.

4.5. Uz edukaciju ovlašćenih lica, Ministarstvo takođe kontinuirano primenjuje i čitav paket drugih mera usmerenih ka zaštiti podataka o ličnosti. Direktiva o načinu obavljanja poslova u vezi sa zaštitom podataka o ličnosti u Ministarstvu unutrašnjih poslova propisuje sledeće oblike mera:
- Informisanje i davanje mišljenja organizacionim jedinicima i zaposlenima koji vrše radnje obrade o njihovim zakonskim obavezama u vezi sa zaštitom podataka o ličnosti, i to na zahtev organizacione jedinice;
- Sveobuhvatno praćenje primene odredbi Zakona i drugih propisa koji se odnose na zaštitu podataka o ličnosti u okviru Ministarstva;
- Davanje mišljenja o proceni uticaja obrade podataka na zaštitu podataka o ličnosti i praćenje postupanja po toj proceni;
- Ostvarivanje saradnje sa Poverenikom za slobodan pristup informacijama od javnog značaja i zaštitu podataka o ličnosti u vezi sa obradom podataka u okviru Ministarstva.

4.6. Reaktivne mere se primenjuju u slučaju povrede bezbednosti podataka, odnosno prava lica. Prva grupa ovih mera odnosi se na povredu bezbednosti podataka, i to bez obzira na to da li je u konkretnom slučaju na povredu bezbednosti reagovano drugim mehanizmom zaštite. Primena mera iz ove grupe propisana je Zakonom i Uputstvom o načinu vođenja evidencije i obaveštavanja o povredama podataka o ličnosti u Ministarstvu unutrašnjih poslova.

4.7. Druga grupa ovih mera jesu disciplinske mere i one su propisane Zakonom o policiji. Treću grupu mera koje su propisane Zakonom i Krivičnim zakonikom primenjuje Sektor unutrašnje kontrole, tužilaštvo i sud. Četvrtu grupu čine mere koje primenjuju Poverenik za slobodan pristup informacijama od javnog značaja i zaštitu podataka o ličnosti, u skladu sa Zakonom.

4.8. Prema podacima koji su sadržani u godišnjim izveštajima koje Ministarstvo dostavlja Povereniku, kao i u redovnim kvartalnim izveštajima koji se dostavljaju ministru, broj evidentiranih i procesuiranih povreda bezbednosti podataka i prava lica čiji se podaci obrađuju od strane ovlašćenih lica Ministarstva je izuzetno mali u odnosu na ukupan broj radnji obrade podataka koje se vrše u okviru nadležnosti Ministarstva, odnosno ukupan broj lica čije podatke Ministarstvo obrađuje. Među ovim povredama, najmanji broj se vezuje za obradu podataka koji

su prikupljeni u sistemu video nadzora. Takođe, iz raspoloživih podataka se nedvosmisleno zaključuje da se ukupan broj povreda već godinama smanjuje.

5. Mehanizmi zaštite prava lica

5.1. Svako lice čije podatke obrađuje Ministarstvo, uključujući i podatke prikupljene i dalje obrađivane u sistemu video nadzora, ovlašćeno je da se zahtevom za ostvarivanje, odnosno zaštitu prava obrati Ministarstvu, u skladu sa Zakonom. Mehanizam kontrole postupanja po zahtevima lica čiji se podaci obrađuju poverava se licu za zaštitu podataka o ličnosti u Ministarstvu, a oblici kontrole uređeni su Direktivom o načinu obavljanja poslova u vezi sa zaštitom podataka o ličnosti.

5.2. U skladu sa Zakonom i na temelju principa rada policije u zajednici (čl. 27. Zakona o policiji), Ministarstvo informiše najširu javnost o poslovima obrade podataka o ličnosti koje obavljaju službena lica Ministarstva, kao i o pravima lica čiji se podaci obrađuju. Informisanje javnosti vrši se putem internet stranice Ministarstva, objavljivanjem informacija u medijima, kao i na drugi adekvatan način.

5.3. Informisanje lica obuhvaćenih sistemom video nadzora vrši se u skladu sa Pravilnikom o načinu snimanja na javnom mestu i načinu saopštavanja namere o tom snimanju. Odredbe Pravilnika u delu koji se odnosi na informisanje lica odražavaju standarde informisanja u sistemu video nadzora koje je formulisao EDPB (European Data Protection Board), i primenjuju se u slučajevima kad se video nadzor vrši putem svih oblika snimanja navedenih pod I 2.1. (”Sveobuhvatan opis radnji obrade”).

5.4. Standardi navedeni pod 5.3. odnose se posebno na dvostepeno informisanje putem postavljanja odgovarajućih znakova na kamernom mestu i upućivanja na internet stranicu Ministarstva na kojoj su istaknute detaljne informacije o obradi podataka u sistemu video nadzora. Na internet stranici Ministarstva su, u skladu sa standardima navedenim pod 5.3, istaknute i ažurirane informacije o svakom od kamernih mesta.

5.5. Cilj informisanja jeste i razvijanje svesti u javnosti i kod lica obuhvaćenih sistemom video nadzora o dopuštenosti primene ovog sistema, veoma niskom nivou izvesnosti povrede prava u korišćenju ovog sistema, kao i o njegovom značaju sa stanovišta zaštite lične i imovinske bezbednosti građana, odnosno efikasnosti suprotstavljanja onim oblicima kriminaliteta koji se mogu efikasno suzbijati upravo korišćenjem ovog sistema. Na ovaj način se efikasno može umanjiti bojazan lica obuhvaćenih sistemom video nadzora za svoja prava (”Procena rizika po prava i slobode lica”, II 1.4. v), 2.4. b), 3.4. b) i 4.4. v), kao i doprineti izgradnji poverenja u osnosu građana prema Ministarstvu.

U skladu sa čl. 54. st. 3 Zakona, pribavljeno je mišljenje lica za zaštitu podataka o ličnosti u Ministarstvu koje je u prilogu ovog dokumenta.

Prilog: Mišljenje lica za zaštitu podataka o ličnosti u Ministarstvu unutrašnjih poslova na Procenu uticaja obrade na zaštitu podataka o ličnosti upotrebom savremenih tehnologija video nadzora u okviru projekta „Sigurno društvo“ u Beogradu.

U Beogradu

POTPREDSEDNIK VLADE I
MINISTAR UNUTRAŠNJIH POSLOVA

Dana_____2020. God.

dr Nebojša Stefanović