Република Србија
МИНИСТАРСТВО УНУТРАШЊИХ ПОСЛОВА

ПРОЦЕНА УТИЦАЈА ОБРАДЕ НА ЗАШТИТУ ПОДАТАКА О ЛИЧНОСТИ УПОТРЕБОМ САВРЕМЕНИХ ТЕХНОЛОГИЈА ВИДЕО НАДЗОРА У ОКВИРУ ПРОЈЕКТА „СИГУРНО ДРУШТВО" У БЕОГРАДУ

У Београду, март 2020. године

УВОД

Унапређивање јавне безбедности је један од кључних приоритета у раду Министарства, на основу идентификованих ризика и претњи које су дефинисане у „Стратешкој процени јавне безбедности за период 2017 – 2021. Године", а односи се на спровођење осам стратешких приоритета:

1. Спречавање и сузбијање организованог криминала са посебним освртом на Националну процену претње од тешког и организованог криминала (SOCTA) за период 2020 – 2024. године, а на основу дефинисаних приоритета са највећим степеном ризика и претњи, а то су: Неовлашћена производња и стављање у промет опојних дрога; Прање новца; Кријумчарење људи; Трговина људима; Високотехнолошки криминал; Акцизне робе; Фалсификовање новца; Кријумчарење људи и Имовински криминал;

2. Спречавање и сузбијање производње марихуане и синтетичких дрога у илегалним лабораторијама, као једном од доминантних и најпрофитабилнијих облика криминала у Републици Србији;

3. Спречавање и сузбијање свих облика корупције кроз спровођење мера и активности из Акционог плана Националне стратегије за борбу против корупције;

4. Спречавање и сузбијање тероризма и насилног екстремизма који води ка тероризму спровођењем мера широког спектра, почев од испуњења стратешких претпоставки и унапређивање система за борбу против финасирања тероризма у Републици Србији, до унапређивања оперативних, стручних и материјалних капацитета организационе јединице која се бави сузбијањем тероризма и екстремизма;

5. Унапређивање стања јавног реда и мира супростављањем насиљу, с посебним освртом на насиље на спортским приредбама, у школама и на јавним местима, применом проактивних модела полицијског рада „полиција у заједници", подршком ширих друштвених активности усмерених на унапређивање људских и мањинских права и јачању толеранције, укључујући и пуну примену Закона о приватном обезбеђењу;

6. Унапређивање стања безбедности саобраћаја на државним путевима, укључујући и проласке државних путева кроз насеље, кроз примену нових модалитета рада саобраћајне полиције и јачању кадровских и материјалних капацитета;

7. Заштиту националних граница од ирегуларних миграција, кријумчарења људи и других незаконитих радњи, уз обезбеђивање легалног промета људи и робе што је од кључног значаја за националну безбедност;

8. Спречавање и сузбијање насиља у породици и партнерским односима.

Такође, један од приоритета Министарства је и приближавање полиције грађанима и боља међусобна сарадња зарад унапређивања сигурности. Наиме, грађани са правом очекују одлучан и адекватан одговор на претње савременог облика угрожавања

јавне безбедности и законом признатих слобода и права. Имајући то у виду, основни задатак Министарства је да се ангажују сви потребни ресурси почев од прикупљања података и информација, преко процене, обраде и анализе. Уколико такав одговор изостане, ризикујемо поверење грађана и темеље саме демократије. Изазов је велики, јер се савремени облици угрожавања јавне безбедности непрестано мењају, посебно услед убрзаног развоја информационих технологије и средстава комуникације.

Примена савремених информационо-комуникационих технологија представља неизоставни чинилац унапређивања безбедносне заштите грађана. Истовремено, развој и доступност савремених комуникационих и информационих технологија је утицао на усложњавање безбедносних претњи услед могућности њихове злоупотребе, како за комуникацију, пропаганду, вербовање, финансирање и обуку, тако и за сајбер-терористичке нападе. Са друге стране, у области информационо-комуникационих технологија изазови се односе на проблеме везане за доступност, увезаност и компатибилност релевантних евиденција различитих институција, као и обезбеђивање потребног нивоа знања и размене искустава са представницима земаља чланица Европске уније. Такође, изазови обухватају и немогућност имплементације нових технологија у постојеће ресурсе, односно заостајање у технолошком развоју, што изазива некомпатибилност са партнерима са којима Министарство остварује сарадњу. С тим у вези неопходно је омогућити приступ Министарства најновијим технолошким решењима базираним на најбољим светским искуствима, а које у свом раду примењују полиције савремених земаља.

Увођењем савремених технологија, стичу се услови за обављање полицијских послова (прописаних чланом 30. Закона о полицији), применом модела 3Е (ефикаснији, ефективнији и економичнији начин), непосредним (on line) увидом у догађај или историју догађаја, брзом и ефикасном реакцијом полиције, изласком на место догађаја и хапшењем учинилаца кривичних дела и процесуирањем прекршаја, проналаском лица или хапшењем лица за којима се трага, повећања безбедности људи и имовине, граничне контроле и спровођење провере на граничним прелазима, надзор државне границе ван граничног прелаза, одржавање јавног реда и мира, обезбеђивање јавних скупова, личности, објеката и простора, безбедносне заштите одређених личности и објеката, идентификације и проналаска извршилаца кривичних дела и несталих лица на основу биометријских података о лицу, обезбеђивање доказа за подношење прекршајних и кривичних пријава, спровођење послова унутрашње контроле, праћења законитости и унапређивања рада Министарства, покретање и вођење дисциплинских поступака, као и предузимање других мера и радњи прописаних Законом о полицији, Закоником о кривичном поступку, Законом о прекршајима, Законом о јавном реду и миру, Законом о јавном окупљању, Законом о спречавању насиља и недоличног понашања на спортским приредбама, Законом о безбедности саобраћаја на путевима, Законом о организацији и надлежности државних органа у сузбијању организованог криминала, тероризма и корупције и др.

Увођењем савременог видео надзора, са бројним могућностима примене софтверских решења за аналитичку обраду видео материјала, препознавања регистарских и других ознака на возилима, детекцијом лика лица, упоређивањем прикупљених података са расположивим подацима, те иницијалном, као и каснијом

идентификацијом лица у процедури утврђеној законом, уочавања прекршаја и кривичних дела и идентификовања њихових учесника, уочавања трагова предмета и средстава извршења кривичних дела, као и бржег и безбеднијег преноса података, изузетно ће допринети ефикасности рада полиције и повећању безбедности у заједници.

Увођење оваквог система у граду Београду у значајној мери ће унапредити рад на пословима потражне делатности и помоћи полицији код проналаска лица за којима се трага, било да су у питању лица за којима су расписане потернице и полицијске потраге или објаве за несталим лицем. Такође, тиме ће се допринети ефикаснијем откривању непознатих учинилаца тешких кривичних дела (КД Убиство, Тешко убиство, Силовање, Отмица, Разбојништво, итд), пре свега анализом видео материјала непосредно пре и након извршења кривичних дела, те на правцима доласка и одласка са места догађаја, као и развоју квалитетније анализе свих информација о кретању жртве или извршиоца у циљу утврђивања припремних радњи за извршење одређеног кривичног дела.[1]

Такође, примена савремених технологија омогућиће праћење саобраћајног тока, појаве застоја и евентуално преусмеравање саобраћаја на алтернативне правце, ефикасно откривање извршилаца кривичних дела и прекршаја у саобраћају, смањен број ангажованих полицијских службеника саобраћајне полиције, јер ће се одређени саобраћајни прекршаји аутоматски детектовати, те ће омогућити праћење рада саобраћајних полицајаца у реалном времену, што ће ограничити и могућност корупције. Примена савремених технологија омогућиће брзо и ефикасно расветљавање саобраћајних незгода (препознавање регистарских и других ознака возила, као и утврђивање околности које су довеле до настанка саобраћајних незгода (одређивање путање кретања возила пре, за време и након саобраћајне незгоде). У последњих неколико година постоји тенденција смањења броја погинулих лица у саобраћајним незгодама на територији Републике Србије, а нарочито након увођења система за аутоматско детектовање

---

[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.

појединих саобраћајних прекршаја (коришћења саобраћајне траке намењене за кретање возила за јавни превоз, пролазак на црвено светло, мерење брзине, мерење просечне брзине кретања возила на ауто путевима). Нови савремени систем видео надзора знатно би допринео смањењу броја незгода, што директно утиче и на смањење индиректних трошкова насталих као последица саобраћајних незгода (трошкови вршења увиђаја, хитног медицинског збрињавања, болничког лечења, насталог инвалидитета, издржавања затворске казне, судских поступака, вештачења и слично), а који падају на терет свих пореских обавезника.

Проблем са којим се Министарство суочавало у досадашњем раду је да су камере, које снимају јавна места углавном веома лошег квалитета, што је представљало проблем у доказивању кривичних дела и прекршаја. Искуства у раду Министарства и кроз анализу прикупљеног видео материјала који потиче из система видео надзора других државних органа, институција, пословних компанија, грађана и др, потврђују да је квалитет видео материјала лош, услед чега је рад полиције често недовољно ефикасан, односно знатно отежан због процедура прибављања видео материјала и количине тог материјал, његове даље обраде и анализе. Количина видео материјала је често огромна и захтева пуно времена за анализу. Најчешће је видео надзор постављен тако да не покрива локацију која је потребна полицији. Због свега наведеног, било је потребно је ангажовати велики број запослених на прибављању и анализи видео материјала, а сама анализа се спроводила на више локација те се тако трошио значајан број радних сати, што исцрпљује запослене и утиче на квалитет рада. Према полицијским извештајима, највећи број лица или возила за којима се трагало, пронађен је приликом редовне контроле – легитимисања (провером идентитета) од стране полицијских службеника, односно контроле учесника у саобраћају, а не увидом у видео записе.

Сврха и циљ примене савремене технологије усмерен је на спровођење законом утврђених послова полиције, који се огледају у томе да је императив да полиција предузме потребне мере и радње да се пронађе учинилац кривичног дела или прекршаја да се учинилац или саучесник не сакрије или не побегне, да се открију и обезбеде трагови кривичног дела и предмети који могу послужити као доказ, као и да се прикупе сва обавештења која би могла бити од користи за успешно вођење кривичног и другог поступка.

Циљ Министарства је да увођењем савремених технологија у оквиру пројекта „Сигурно друштво" допринесе подизању капацитета у раду полиције, а самим тим и подизању поверења у рад полиције ради смањења укупног криминала на подручју града Београда и унапређења безбедности свих грађана.

Имајући у виду безбедносне изазове и потребу за ефикаснијим радом полиције као и све предности које нуде савремене технологије, Министарство је проценило да су се стекли услови за увођење савремених технологија у раду Министарства кроз спровођење пројекта „Сигурно друштво" на територији града Београда, а који обухвата унапређење система видео надзора, успостављање интелигентне видео аналитике и изградњу eLTE бежичне широкопојасне радио мреже, базиране на LTE (LongTermEvolution) технологији.

У претходном периоду у оквиру овог пројекта на опредељеним локацијама монтиране су покретне (PTZ) камере резолуције fullHD (2Mpix) са 30x оптичким зумом, фиксне камере резолуције fullHD (2Mpix) намењене за општи видео надзор и фиксне камере резолуције 4К (8Mpix), Све камере су опремљене са IR диодама чиме им је омогућен рад у ноћним условима и лошим временским условима. Такође камере имају слот за меморијске картице капацитета 32 GB које се користе као „backup" за снимање у ванредним ситуацијама када дође до прекида у преносном/комуникационом путу од камере до сервера на коме се, у нормалном режиму рада, снима видео сигнал са камера. Фиксне камере су са моторизованим варифокалним објективом који пружа могућност подешавања видног поља камере, које је условљено врстом објектива који се користи. Камере су повезане на систем који ради на софтверској платформи са напредним аналитичким алатима за обраду видео материјала.

До краја пројекта Министарство ће проширити функционалност видео аналитике увођењем нове функционалности - аутоматско детектовање лика лица из континуалног видео материјала. Ова функционалност активираће се софтверски, додељивањем лиценце одређеној камери на систему. Камере, на којима ће се активирати лиценца за детекцију лика, биће инсталиране на претходно прецизно дефинисаним безбедносно интересантним локацијама на територији града Београда. Неопходно је да ове камере буду постављене на одговарајућој висини и усмерене у складу са техничким захтевима и ограничењима произвођача опреме, односно, на висини од око 4 метра са углом гледања усмереним ка зони од интереса за полицију. Статистика детекције лика из континуалног видео материјала, зависиће од различитих фактора, као што су: количина светла, позиција лица у зони камере, временских прилика и др. Софтвер за детекцију лика из континуалног видео материјала, аутоматски детектује лик свих лица која пролазе зону надзора камера и издваја их у виду фотографије и кратког видео записа (тренутка када је фотографија сачињена), на систему за складиштење по временски хронолошком критеријуму.

Имајући у виду да је Министарство ради увођења савремених технологија у обради података о личности дужно да изврши процену утицаја обраде на заштиту података о личности, у наставку овог текста су наведени сви битни елементи те процене које прописује Закон о заштити података о личности из 2018. Процена утицаја израђена је на основу методологије коју је у вези са проценом утицаја стандардизовао EDPB.

ПРОЦЕНА УТИЦАЈА ОБРАДЕ НА ЗАШТИТУ ПОДАТАКА О ЛИЧНОСТИ УПОТРЕБОМ САВРЕМЕНИХ ТЕХНОЛОГИЈА ВИДЕО НАДЗОРА У ОКВИРУ ПРОЈЕКТА „СИГУРНО ДРУШТВО" У БЕОГРАДУ

I СВЕОБУХВАТАН ОПИС ОБРАДЕ ПОДАТАКА

1. Правни режим обраде

1.1. Подаци прикупљени путем система видео надзора јавног места обрађују се првенствено у посебном правном режиму који се примењује у случајевима прописаним у чл. 1, ст. 2. Закона о заштити података о личности (у даљем тексту : Закон).

1.2. У осталим случајевима подаци прикупљени системом видео надзора обрађују се у општем правном режиму заштите података о личности прописаном Законом.

2. Примена правног режима обраде

2.1. Подаци прикупљени у систему видео надзора увек се обрађују на аутоматизовани начин, што значи да се обрађују у оквиру збирки података, и то путем следећих електронских уређаја:

а) 2.500 видео камера (фиксних и покретних) постављених на стубовима на јавним површинама, односно на објектима у јавној употреби;
б) 3500 уређаја за снимање аудио-видео записа који представљају саставни део опреме полицијских службеника. (еЛТЕ терминали).
в) 600 фискних видео камера монтираних на возилима полиције.
г) 1500 камера (body камере) као део опреме полицијских службеника.

2.2. Подаци се прикупљају системом видео-акустичког снимања (систем видео надзора), и то видео и аудио-видео надзором јавних места на територији града Београда, у оквиру пројекта "Сигуран град".

2.3. Локације на којима се постављају камере из 2.1 а опредељене су на основу извршене анализе потреба Министарства унутрашњих послова у циљу остваривања сврхе видео надзора и то према следећим критеријумима:
-Учесталост извршења кривичних дела и прекршаја
-Учесталост саобраћајних незгода
-Проточност саобраћаја, саобраћајни коридори
-Места јавног окупљања
-Објекти и лица која обезбеђује Министарство унутрашњих послова

3. Подаци који се обрађују

3.1. Путем система видео надзора прикупљају се следећи подаци о физичким лицима: лик, што укључује и биометријске податке у случају надзора камером која ствара биометријске податке лика, изглед, што укључује и телесне карактеристике лица, као и учешће лица у догађају.

3.2. Путем система видео надзора у изузетним случајевима прикупљају се и подаци о здрављу лица (на пример код повређивања изазваног саобраћајном незгодом, у пожару и сл.), као и подаци о пружању здравствених услуга у вези са тим подацима.

3.3. Путем система видео надзора прикупљају се и следећи подаци о возилима: регистарске и друге ознаке возила, боја возила, други карактеристични знаци (на пример рекламни натписи, ознака произвођача возила исл.).

3.4. Путем система видео надзора прикупљају се и подаци о другим предметима (например: остављени кофери, торбе и сл. на јавном месту);

3.5. Систем видео надзора аутоматски генерише податке о времену и месту прикупљања података.

4. Радње обраде података

4.1. Обрада података у систему видео надзора обухвата следеће радње обраде: прикупљање, разврставање, груписање, похрањивање, увид, употреба, откривање преносом, односно достављањем, умножавање, упоређивање, ограничавање, брисање односно уништавање на други начин.

4.2. Прикупљање података се врши стварањем видео записа, фотографије, односно аудио-видео записа у дигиталном облику путем видео камера и уређаја који омогућавају аудио и видео снимање.

4.3. Видео камере имају могућност зумирања у складу са потребом овлашћеног лица руковаоца. Покретне видео камере уз могућност зумирања могу да се окрећу у складу са потребом овлашћеног лица руковаоца.

4.5. Видео и аудио-видео записи се разврставају односно групишу на следећи начин:

а) аутоматски , према локацији камере, као и датуму и времену стварања записа.
б) на основу одлуке овлашћеног лица руковаоца, према лицу, возилу, односно догађају који се надзире.

4.6. Аудио и видео записи се похрањују на чврсту меморију (хард дискови, меморијске картице, цд, усб меморије).

4.7. Увид у аудио и видео записе има овлашћено лице које рукује камерама на даљину из корисничког центра, полицијски службеник који обавља полицијске послове надзором јавног места и друго овлашћено лице руковаоца.

4.8. Употреба аудио и видео записа је ограничена на сврху и циљеве прикупљања и даље обраде.

4.9. Аудио и видео записи се у појединачним случајевима могу пренети овлашћеним примаоцима.

4.10. Записи лика се упоређују са другим записима у циљу идентификације лица, на основу биометријских података, као и без њих, док се подаци о возилу упоређују са другим подацима о возилима у циљу идентификације власника, односно корисника возила.

4.11. Идентификација лица се може вршити у току снимања или прегледом снимљеног материјала.

4.12. Обрада података прикупљених путем аудио и видео снимања се може ограничити, у складу са одредбама Закона.

4.13. Аудио и видео записи се трајно бришу односно уништавају након протека законског рока за њихово чување, односно протека рока одређеног одлуком руковаоца који је краћи од законског рока, у складу са Законом.

4.14. Приликом обраде података користи се и профилисање и то у случају обраде података који нису засновани на личној оцени, као и у случају обраде података који су засновани на личној оцени полицијског службеника.

4.15. Приликом обраде података примењују се мере криптозаштите.

5. Руковалац, обрађивач и прималац

5.1. Руковалац подацима који се обрађују путем система видео надзора је Министарство унутрашњих послова Републике Србије (даље: Министарство).

5.2. Министарство самостално обрађује податке у систему видео надзора, и то ангажовањем стручних и овлашћених лица запослених у оквиру посебних организационих јединица Министарства коришћењем опреме која се налази у поседу Министарства.

5.3. Прималац података који се обрађују у посебном режиму може бити само надлежни орган, у смислу чл. 4, тач. 26. Закона.

5.4. Прималац података који се обрађују у општем режиму могу бити органи јавне власти, као и правна и физичка лица, у складу са Законом.

5.5. Подаци се могу пренети примаоцу у другој држави, односно међународној организацији, у складу са Законом.

6. Законитост обраде, поштење и транспарентност

6.1. Правни основ за обраду података је искључиво закон. Подаци се не обрађују на основу пристанка лица на које се односе.

6.2. У случајевима обраде података у посебном правном режиму, основ за обраду су:
а) Закон, чл. 13;
б) Закон о полицији, чл.30,47, 50, 52, 59. 64 и77;
в) Закон о евиденцијама и обради података у области унутрашњих послова, чл. 13, 39, 47. 49, и 50;
г) Закон о безбедности саобраћаја на путевима чл. 278. и 286;
д) Законик о кривичном поступку, чл. 286.

6.3. У случајевима обраде података у општем правном режиму основ за обраду су:
а) Закон, чл. 12, ст. 1, тач. 4. и 5;
б) Закон о полицији, чл.30-33, чл. 35,42, 45, 131-134,;
в) Закон о евиденцијама и обради података у области унутрашњих послова чл. 3. т. 26,29,31,36 и 37.
г) Закон о безбедности саобраћаја на путевима чл. 286.

6.4. Подаци се обрађују поштено и транспарентно, у складу са Законом, што укључује и примену законских одредби о допуштеним ограничењима права лица која се односе на остваривање и заштиту начела поштења и транспарентности обраде.

7. Сврха обраде

7.1. Сврха обраде података је у сваком конкретном случају прецизно одређена, изричита, оправдана и законита, а подаци се даље не обрађују на начин који није у складу са том сврхом.

7.2. Сврха обраде података у посебном режиму је спречавање, истрага и откривање кривичних дела, гоњење учинилаца кривичних дела, односно обезбеђивање извршења кривичних санкција. Сврха обраде је и спречавање и заштита од претњи јавној и националној безбедности.

7.3. Оправданост сврхе обраде података у посебном режиму непосредно се заснива на потреби остваривања законом прецизно одређених циљева обраде, и то:

а) Идентификовање лица против којих постоји основи сумње да су извршила или намеравају да изврше кривично дело, односно прекршај;
б) Идентификовање лица против којих постоји основана сумња да су извршила кривично дело, односно прекршај;
в) Идентификовање лица која су оштећена кривичним делом, односно прекршајем, или за која се претпоставља да би могла бити оштећена кривичним делом, односно прекршајам;
г) Идентификовање других лица која су у вези са кривичним делом, односно прекршајем, као што су сведоци, лица која могу да обезбеде информације о кривичном делу, односно прекршају, као и повезана лица или сарадници лица наведених под а), б) и в).

7.4. Сврха обраде података у општем режиму је заштита животно важних интереса лица (живот и здравље), на које се подаци односе или другог лица, у смислу чл. 12, ст. 1, тач. 4. Закона. Такође, сврха обраде података у општем режиму је обављање законом прописаних послова у јавном интересу, односно извршење законом прописаних овлашћења руковаоца, у смислу чл. 12, ст. 1, тач. 5. Закона.

7.5. Оправданост сврхе обраде података у општем режиму непосредно се заснива на потреби остваривања законом прецизно одређених циљева обраде, и то:

а) Идентификовање лица чији је живот или здравље угрожено у саобраћаној незгоди или на други начин (у случају нестанка детета или дементног лица и сл.), односно лица чија је идентификација неопходна у циљу заштите живота или здравља других лица (у циљу спречавања ширења заразе на друга лица и сл.);
б) Остваривање увида у стање саобраћаја;
в) Информисање јавности о догађајима који су од значаја за живот у граду;
г) Обезбеђивање материјала који се користи у школовању, обуци, односно стручном усавршавању полицијских службеника;
д) Обезбеђивање материјала који се користи за потребе анализе ефеката обраде, даљег развоја и унапређивања система видео надзора, као и за статистичке потребе.

8. Минимизација података

8.1. Обрађују се само они подаци који су примерени сврси обраде, битни за остваривање сврхе обраде и ограничени на оно што је неопходно у односу на сврху обраде.

8.2. На основу прикупљених података путем система видео надзора врши се идентификација само оних лица без чије идентификације није могуће остварити сврху обраде у конкретном случају, и то:
а) Лица наведених под 7.3;
б) Лица наведених под 7.5.а).

8.3. Идентитет лица која не припадају групама лица наведених под 8.2. се не утврђује на основу података прикупљених у систему видео надзора.

9. Тачност података

9.1. У систему видео надзора прикупљају се подаци на основу којих се употребом нових технологија може идентификовати лице са веома високим степеном поузданости.

9.2. Ако фотографија односно видео запис садржи и биометријске податке лика, идентификација лица се врши коришћењем ових података. У том случају систем видео

надзора аутоматски генерише и податке о степену поузданости идентификације за свако лице понаособ.

9.3 Идентификацију лица могуће је извршити и без коришћења биометријских података лика, упоређивањем података прикупљених у систему видео надзора са другим подацима којима располаже руковалац, у складу са чл. 77. Закона о полицији.

9.4. Поузданост идентификације лица у сваком конкретном случају проверава овлашћено лице руковаоца вршењем службених радњи прописаних законом. Ако се провером утврди да се лице не може идентификовати на основу података прикупљених у систему видео надзора, ти подаци се бришу након истека рока из тачке 10.3.

10. Чување података

10.1. Подаци прикупљени у систему видео надзора на основу којих је утврђен идентитет лица чувају се у року који је неопходан за остваривање сврхе обраде, и то:

а) Подаци о идентификованим лицима наведеним под 7.3. у законом прописаном року од пет година од дана настанка записа, у смислу чл. 47, ст. 3. Закона о евиденцијама и обради података у области унутрашњих послова, односно од дана окончања поступка у смислу чл. 47, ст 4. истог закона.
б) Подаци о идентификованим лицима наведеним под 7.5.а) у року који је неопходан за остваривање сврхе обраде која се односи на заштиту живота и здравља лица у смислу чл. 7, ст. 2. Закона о евиденцијама и обради података у области унутрашњих послова.

10.2. Подаци прикупљени у систему видео надзора на основу којих се не утврђује идентитет лица чувај се најмање 30 дана од дана настанка записа. Рок од 30 дана прописан чл. 47. ст. 3 Закона о евиденцијама и обради података у области унутрашњих послова, условљен је техничким ограничењима похрањивања података прикупљених у систему видео надзора и краћи је од рока који је одређен Законом о полицији, чл. 52. Систем аутоматски циклично брише најстарије податке новијим када се попуни меморијски простор архиве(тзв. кружно снимање).

10.3. Руковалац проверава да ли се лице наведено под 7.3. може идентификовати на основу података прикупљених у систему видео надзора у року од једне године од дана настанка записа. Ако је провером из 9.4. утврђено да се лице не може идентификовати на основу података прикупљених у систему видео надзора у наведеном року, подаци се уништавају, у складу са Законом о полицији, чл. 52, ст. 7.

11. Интегритет и поверљивост података

11.1. Безбедност података се осигурава применом одредби о допуштеној обради података, одредби које се односе на права лица, као и применом техничких, организационих и кадровских мера прописаних Законом.

11.2. Посебан циљ примене одредби и мера којима се осигурава безбедност података јесте елиминасање ризика од обраде података по права и слободе физичких лица, и то у потпуности, односно у највећој мери.

12. Обрада у друге сврхе

12.1. Подаци који се обрађују у посебном режиму у циљу идентификације лица наведених под 7.3. и 7.5а руковалац не обрађује у друге сврхе.

12.2. У циљу идентификације лица наведених под 7.3. и 7.5.а) подаци прикупљени у систему видео надзора се могу упоређивати са подацима који су прикупљени у друге сврхе, а посебно у случају кад се упоређивање врши са подацима, укључујући и биометријске податке, који су садржани у евиденцији личних исправа физичких лица.

12.3. Ако се у циљу идентификације лица наведених под 7.3. и 7.5.а) подаци прикупљени у систему видео надзора упоређују са подацима који су првобитно прикупљени од стране надлежних органа у друге посебне сврхе из чл. 1, ст. 2. Закона, утврђивање идентитета лица се заснива на чл. 7, ст. 1. и 2. Закона, као и на одредбама закона наведених под 6.2.

12.4. Ако се у циљу идентификације лица наведених под 7.3. и 7.5.а) подаци прикупљени у систему видео надзора упоређују са подацима који су првобитно прикупљени у друге сврхе које нису наведене под 12.3, утврђивање идентитета лица се заснива на чл. 6, ст. 1. и чл. 40, ст. 1, тач. 1. до 6, 9. и 10. Закона, као и на одредбама закона наведених под 6.3.

13. Разликовање врста лица и података

13.1. Приликом идентификације лица на основу података прикупљених у систему видео надзора, руковалац разврстава податке о лицима наведеним под 7.3. и 7.5.а) у посебне групе података.

13.2. Разврставање података о следећим групама лица наведеним под 7.3. засновано је на личној оцени:
а) Лица против којих постоји основи сумње да су извршила или намеравају да изврше кривично дело, односно прекршај;
б) Лица против којих постоји основана сумња да су извршила кривично дело, односно прекршај;
в) Лица за која се претпоставља да би могла бити оштећена кривичним делом, односно прекршајам;
г) Лица која су у вези са кривичним делом, односно прекршајем, као што су сведоци, лица која могу да обезбеде информације о кривичном кривичном делу, односно прекршају, као и повезана лица или сарадници лица наведених под 7.3.

14. Обрада посебних врста података о личности

14.1. Идентификација лица наведених под 7.3. може се вршити на основу обраде биометријских података лика лица, а у складу са законским овлашћењима руковаоца, у смислу чл. 18, тач. 1. Закона.

14.2. Идентификација лица наведених под 7.5.а) може се вршити на основу обраде биометријских података лика. Приликом идентификације ових лица обрађују се и подаци о њиховом здравственом стању. Обрада података о овим лицима заснива се на законским овлашћењима руковаоца, у смислу чл. 17, ст. 2, тач. 3. Закона.

15. Обрада која не захтева идентификацију

15.1. На основу података прикупљених у систему видео надзора утврђује се само идентитет лица наведених под 7.3. и 7.5.а), а не и других лица, и о томе руковалац информише лица обухваћена видео надзором путем медија, других средстава јавног обавештавања (интернет презентације и сл.), и на други погодан начин.

15.2. За остваривање сврхе обраде није неопходно потребно утврдити идентитет других лица лица који не припадају групама лица наведеним под 7.3. и 7.5.а) на основу података прикупљених у систему видео надзора. Због тога овлашћено лице руковаоца не прибавља

и не обрађује додатне податке у циљу идентификације тих других лица, у смислу чл. 20, ст. 1. Закона.

16. Аутоматизовано доношење одлука

16.1. Идентификација лица наведених под 7.3. и 7.5.а) у сваком конкретном случају се врши на основу одлуке овлашћених лица руковаоца, и то без обзира на то да ли се идентификација врши у току стварања записа или накнадним прегледом записа. То значи да се у систему видео надзора идентитет лица не утврђује искључиво на основу аутоматизоване обраде података, у смислу чл. 38. и 39. Закона, односно да се не примењује тзв. аутоматско препознавање лица.

16.2. Након идентификације лица наведених под 7.3. и 7.5.а), могу се предузети радње или донети одлуке које производе правне последице по лице, односно утичу на положај лица. Ове радње и одлуке се не примењују на лице искључиво на основу аутоматизоване обраде података, већ се у сваком конкретном случају захтева посредовање овлашћених лица руковаоца у смислу одређивања сврхе и начина примене радње, односно одлуке. Правни основ за предузимање радње или доношење одлуке о идентификованом лицу је у сваком конкретном садржан у закону који се примењују на поступање полиције.

II ПРОЦЕНА РИЗИКА ПО ПРАВА И СЛОБОДЕ ЛИЦА

1. Ризик који се односи на идентификацију лица без правног основа

1.1. Догађај који подразумева ризик по права и слободе лица везује се за идентификацију лица на основу података прикупљених у систему видео надзора јавних површина у циљу који није обухваћен тачкама 7.3. и 7.5.а) из првог дела документа ("Свеобухватан опис обраде података"). При томе, за потребе процене ризика у одређеној мери је од значаја разлог за противправну идентификацију, односно чињеница да је идентификација мотивисана разлозима личне или друге природе.

1.2. Услед догађаја наведеног под 1.1. могле би наступити следеће последице по права и слободе лица:
а) Повреда права на приватан живот и то посматрањем активности активности лица које је идентификовано у систему видео надзора, као и похрањивањем и другим радњама обраде података о овим активностима, без обзира на чињеницу да се активности предузимају на јавним површинама;
б) Повреда слободе удруживања, окупљања и изражавања, односно права на миран протест, као и слободе кретања, и то идентификовањем и даљом обрадом података лица која се на јавним површинама окупљају, као чланови удружења или без обзира на чланство у удружењу, изражавају своје мишљење, идеје и ставове, мирно протестују, односно крећу се на јавним површинама као део поворке, протестног скупа и сл, у складу са законом који уређује услове за вршење наведених слобода и права;
в) Повреда слободе вероисповести и то идентификовањем и даљом обрадом података лица која улазе у или излазе из верских објеката или учествују у вршењу верских обреда на јавним површинама;
г) Повреда принципа забране дискриминације у случајевима повреде слобода и права наведених под 1.2. б) и в), и то путем профилисања идентификованих лица на основу стварне или претпостављене припадности удружењу, односно верској заједници, политичког или другог мишљења, сексуалног опредељења или другог личног својства.

1.3. Ниво извесности наступања догађаја наведеног под 1.1. је низак. Приликом процене нивоа извесности посебно се узимају о обзир следеће околности, односно чињенице:
а) Идентификација лица на основу података прикупљених у систему видео надзора темељи се у сваком конкретном случају на организационој структури у систему подељених улога у погледу вршења радњи обраде, одлучивања о потреби идентификације и контроле, што у највећој мери онемогућава евентуални индивидуални покушај злоупотребе полицијских овлашћења;
б) Свака радња обраде података прикупљених у систему видео надзора, укључујући и идентификацију лица, бележи се у циљу омогућавања ефикасне контроле вршења полицијских овлашћења, што у највећој мери одвраћајуће делује на потенцијалне прекршиоце полицијских овлашћења;
в) Број случајева злоупотребе, односно кршења полицијских овлашћења је годинама уназад веома мали у односу на број предузетих радњи овлашћених лица руковаоца, што указује на изузетну дисциплинованост и савесност полицијских службеника.
г) Овлашћена лица руковаоца су већ едукована о правном режиму заштите личних података, што указује на висок ниво свести о неопходности поштовања начела законитости и других начела Закона у погледу вршења полицијских овлашћења приликом обраде података, а посебно у систему видео надзора.

1.4. Процена озбиљности могуће повреде права и слобода лица наведених под 1.2. се одређује на следећи начин:
а) Право на приватност лица обухваћеног системом видео надзора би нужно било повређено услед догађаја наведеног под 1.1, а с обзиром на то да лице оправдано претпоставља да у односу према другим људима задржава своју анонимност иако активности предузима на јавној површини;
б) Друга права лица обухваћеног системом видео надзора која су наведена под 1.2. не би нужно била повређена услед догађаја наведеног под 1.1. Наступање повреде права би у сваком конкретном случају зависило од намере прекршиоца полицијских овлашћења, односно циља недопуштеног профилисања и других радњи обраде.
в) На процену озбиљности могуће повреде права и слобода лица наведених под 1.2. утиче и степен развијености свести грађана о висини ризика по њихова права и слободе. Ако у јавности преовлађује свест о томе да је ниво ризика по права и слободе лица обухваћених видео надзором висок, онда се може претпоставити да би та околност могла произвести негативан ефекат у погледу уживања појединих права и слобода (например стварање осећања оправдане бојазни за свој приватан живот или уздржавање од учешћа у јавном окупљању, изражавању мишљења и сл.).

2. Ризик који се односи на снимање приватног простора

2.1. Догађај који подразумева ризик по права и слободе лица везује се за снимање приватног простора, као што је унутрашњост станова, кућа и окућница, канцеларија и других пословних простора, коришћењем видео камера које су постављене на стубовима и зградама у јавној употреби. При томе, за потребе процене ризика у одређеној мери је од значаја разлог за противправно снимање, односно чињеница да је снимање мотивисано разлозима личне или друге природе.

2.2. Услед догађаја наведеног под 2.1. могла би наступити последица која се састоји у повреди права на приватност и то увидом у активности лица које се налази у простору који се снима, као и похрањивањем и другим радњама обраде података о овим активностима.

2.3. Ниво извесности наступања догађаја наведеног под 2.1. је низак. Приликом процене нивоа извесности посебно се узимају о обзир следеће околности, односно чињенице:

а) Фиксне камере су физички постављене тако да снимају само јавни простор, док се покретне камере могу користити за снимање приватног простора и то само у оним изузетним случајевима кад снимање није ограничено физичким препрекама (например камера је постављена на нижем положају у односу на приватан простор или на положају који је веома удаљен од приватног простора или је приватан простор заклоњен дрвећем, завесама, ролетнама, оградама и сл), што у највећој мери ограничава могућност праћења активности лица у приватном простору;
б) Праћење активности лица употребом покретних видео камера темељи се у сваком конкретном случају на организационом систему подељених улога у погледу вршења радњи обраде, одлучивања о потреби праћења и контроле, што у највећој мери онемогућава евентуални индивидуални покушај злоупотребе полицијских овлашћења;
в) Податак о окретању камере у сваком конкретном случају може утврдити у циљу омогућавања ефикасне контроле вршења полицијских овлашћења, што у највећој мери одвраћајуће делује на потенцијалне прекршиоце полицијских овлашћења;
г) Број случајева злоупотребе, односно кршења полицијских овлашћења је годинама уназад веома мали у односу на број предузетих радњи овлашћених лица Министарства, што указује на изузетну дисциплинованост и савесност полицијских службеника.
д) Овлашћена лица руковаоца су већ едукована о правном режиму заштите личних података, што указује на висок ниво свести о неопходности поштовања начела законитости и других начела Закона у погледу вршења полицијских овлашћења приликом обраде података, а посебно у систему видео надзора.

2.4. Процена озбиљности могуће повреде права на приватност лица се одређује на следећи начин:
а) Право на приватност лица обухваћеног системом видео надзора би нужно било повређено услед догађаја наведеног под 2.1, а с обзиром на то да лице оправдано претпоставља да су активности које предузима у приватном простору заштићене од погледа других људи;
б) На процену озбиљности могуће повреде права на приватност лица утиче и степен развијености свести грађана о висини ризика по ово њихово право. Ако у јавности преовлађује свест о томе да је ниво ризика који се везује за видео снимање приватних простора висок, онда се може претпоставити да би та околност могла произвести негативан ефекат у погледу уживања права на приватност (например стварање осећања оправдане бојазни за свој приватан живот).

3. Ризик који се односи на повреду безбедности података

3.1. Догађај који подразумева ризик по права и слободе лица везује се за повреду безбедности података прикупљених у систему видео надзора услед приступа опреми која се користи у сврху видео надзора (например преузимање контроле над камерама), односно копирања, откривања, односно преношења података и то од стране трећег лица, у смислу чл. 4, тач. 11. Закона. При том, за потребе процене ризика није од значаја разлог за повреду безбедности, односно чињеница да је повреда безбедности мотивисана разлозима личне или друге природе.

3.2. Услед догађаја наведеног под 3.1. могла би наступити последица која се састоји у повреди права на заштиту података о личности лица, на које се односе подаци чија је безбедност повређена.

3.3. Ниво извесности наступања догађаја наведеног под 3.1. је низак. Приликом процене нивоа извесности посебно се узимају о обзир следеће околности, односно чињенице:
а) Опрема и подаци су обезбеђени техничким мерама заштите на највишем нивоу, а посебно у погледу софтверске заштите, заштита мреже за пренос података, заштите података системом криптозаштие, као и физичке заштите камера, водова, опреме за

складиштење података и сл, што у највећој мери ефикасно спречава повреду безбедности података од стране трећег лица;
б) Опрема и подаци су обезбеђени свеобухватним организационим мерама заштите, а посебно применом система подељених улога у погледу вршења радњи обраде, што у највећој мери ефикасно спречава повреду безбедности података од стране трећег лица, а у сарадњи са полицијским службеницима;
в) Овлашћена лица руковаоца су путем едукације већ оспособљена за предузимање техничких и организационоих мера заштите података о личности, што у највећој мери ефикасно спречава повреду безбедности података од стране трећег лица;
г) Годинама уназад није долазило до повреде безбедности података од стране трећег лица, што указује на делотворност предузетих мера заштите кад се ради о обради података коју врши руковаоц.

3.4. Процена озбиљности могуће повреде права на приватност лица се одређује на следећи начин:
а) Право на заштиту података који се односе на лице обухваћено системом видео надзора би нужно било повређено услед догађаја наведеног под 3.1, а с обзиром на то да је руковалац по Закону дужан да обезбеди податке које обрађује од повреде;
б) На процену озбиљности могуће повреде права на заштиту података о личности утиче и степен развијености свести грађана о висини ризика по ово њихово право. Ако у јавности преовлађује свест о томе да је ниво ризика који се везује за повреду безбедности података од стране трећег лица висок, онда се може претпоставити да би та околност могла произвести негативан ефекат у погледу уживања права на заштиту података о личности (например стварање осећања оправдане бојазни за податке које руковалац о њему обрађује).

4. Ризик који се односи на јавно објављивање података

4.1. Догађај који подаразумева ризик по права и слободе лица везује се за правно недопуштено јавно објављивање података прикупљених у систему видео надзора путем медија, друштвених мрежа или коришћењем других средстава комуникације. При томе, за потребе процене ризика у одређеној мери је од значаја разлог за јавно објављивање, односно чињеница да је јавно објављивање мотивисано разлозима личне или друге природе.

4.2. Услед догађаја наведеног под 4.1. могле би наступити следеће последице по права и слободе лица:
а) Повреда права на приватан живот и то увидом у активности лица које је обухваћено системом видео надзора од стране јавности, односно примаоца информација које се објављују у медијима, у оквиру друштвених мрежа или се шире путем других средстава комуникације;
б) Повреда права на идентитет, у случајевима кад је лице које је обухваћено системом видео надзора погрешно идентификовано у јавности;
в) Повреда личног моралног интегритета, у случајевима кад је услед јавног објављивања информације која се односи на приватан живот лица повређен углед, част или пијетет тог лица;
г) Повреда права наведених под 1.2. б) од г), у случајевима кад је услед јавног објављивања информације која се односи на приватан живот лица повређено неко од наведених права.

4.3. Ниво извесности наступања догађаја наведеног под 4.1. је низак. Приликом процене нивоа извесности посебно се узимају о обзир следеће околности, односно чињенице:
а) Обрада података прикупљених у систему видео надзора темељи се у сваком конкретном случају на организационом систему подељених улога у погледу вршења

радњи обраде, што у највећој мери онемогућава недопуштено јавно објављивање података;
б) Свака радња обраде података прикупљених у систему видео надзора, бележи се у циљу омогућавања ефикасне контроле вршења полицијских овлашћења, што у највећој мери одвраћајуће делује на неовлашћено достављање података медијима, односно пренос података у циљу њиховог јавног објављивања;
в) Број случајева недопуштеног јавног објављивања података које руковалац обрађује се из године у годину смањује и веома је мали у односу на број предузетих радњи овлашћених лица руковаоца, што указује на изузетну дисциплинованост и савесност полицијских службеника.
г) Овлашћена лица руковаоца су већ едукована о правном режиму заштите личних података, што указује на висок ниво свести о неопходности поштовања начела законитости и других начела Закона у погледу вршења полицијских овлашћења приликом обраде података, а посебно у вези са спречавањем недопуштеног јавног објављивања података.

4.4. Процена озбиљности могуће повреде права и слобода лица наведених под 4.2. се одређује на следећи начин:
а) Право на приватност лица обухваћеног системом видео надзора би нужно било повређено услед догађаја наведеног под 4.1, а с обзиром на то да је нужно претпоставити да услед јавног објављивања података прикупљених системом видео надзора долази до идентификације лица.
б) Друга права лица обухваћеног системом видео надзора која су наведена под 4.2. не би нужно била повређена услед догађаја наведеног под 4.1. Наступање повреде права би у сваком конкретном случају зависило од објективних околности које се односе на тачност идентификације, односно подобност јавно објављених података из приватног живота да проузрокују повреду личног моралног интегритета лица, као и субјективних околности које се односе на намеру повредиоца права, односно циљ недопуштеног профилисања и других радњи обраде.
в) На процену озбиљности могуће повреде права и слобода лица наведених под 4.2. утиче и степен развијености свести грађана о висини ризика по њихова права и слободе. Ако у јавности преовлађује свест о томе да је ниво ризика по права и слободе лица обухваћених видео надзором висок, онда се може претпоставити да би та околност могла произвести негативан ефекат у погледу уживања појединих права и слобода (например стварање осећања оправдане бојазни за свој приватан живот, идентитет, односно лични морални интегритет или уздржавање од вршења права и сл.).

III ОПИС ПРИМЕЊЕНИХ МЕРА И МЕХАНИЗАМА У ОДНОСУ НА РИЗИК ПО ПРАВА И СЛОБОДЕ ЛИЦА

1. Мере заштите безбедности података и механизми заштите права лица

1.1. Представљени ризици по права и слободе лица ефикасно се уклањају, односно своде на најмању меру путем примене општих организационих, кадровских и техничким мера заштите безбедности података, односно механизама заштите права и слобода лица у вези са обрадом података о личности. Ове мере и механизми прописани су Законом и другим прописима, као што је Закон о информационој безбедности, Закон о полицији, Закон о евиденцијама и обради података у области унутрашњих послова и подзаконски акти донети од стране Министарства.

1.2. Мере заштите безбедности података и механизми заштите права лица примењују се на специфичан начин у систему видео надзора. Поједине од ових мера и механизама

примењују се у односу на више различитих ризика и то на исти или различит начин, док се друге мере и механизми примењују само у односу на појединачно одређен ризик.

2. Систем подељених улога у обради података

2.1. Систем видео надзора је креиран тако да може да буде функционалан само у систему подељених улога. То значи да у прикупљању и даљој обради података у систему видео надзора није могуће организационо, технички и правно замислити ситуацију у којој се одлука о предузимању радњи обраде које имају за циљ идентификацију лица, односно праћење активности лица, а у контексту процене нивоа извесности наступања ризика наведене под II 1.3. а), 2.3. б), 3.3. б) и 4.3. а) ("Процена ризика по права и слободе лица"), доноси изван система подељених улога.

2.2. Применом ове организационе мере заштите ефикасно се спречава евентуални индивидуални покушај злоупотреба полицијских овлашћења, и то због тога што овлашћено службено лице руковаоца никада не може само, без учешћа других овлашћених службених лица, да предузме радње обраде на које упућују ризици наведени под 2.1. На тај начин се у највећој мери минимизује вероватноћа наступања ризика.

2.3. Систем поделе улога у систему видео надзора заснива се на Правилнику о унутрашњем уређењу и систематизацији радних места у Министарству. Овим актом уређује се надлежност појединих организационих јединица Министарства, као и опис послова и задатака за свако појединачно радно место, што укључује и прописивање општих и посебних услова за распоређивање на радно место.

2.4. Запослени распоређени на појединим радним местима у систему видео надзора са овлашћењима да прикупљају и даље обрађују податке, имају статус овлашћених службених лица. У вршењу својих послова и задатака у систему видео надзора они су распоређени по организационим јединицама Министарства.

2.5. У свакој од организационих јединица за свако овлашћено службено лице везује се унапред одређени ниво одлучивања, односно овлашћење за предузимање појединих радњи обраде. Такође, за поједина овлашћена службена лица везује се и функција контроле извршења послова и задатака у систему видео надзора.

2.5. У систему видео надзора којим рукује Министарство сваку радњу обраде врши лице које је овлашћено за предузимање те радње. При томе, ниједно од лица ангажованих у систему видео надзора нема овлашћење за предузимање свих радњи обраде, те се например овлашћење за прикупљање података везује за лице које је распоређено у оквиру једне организационе јединице, док се овлашћења за коришћење других података на основу којих је могуће идентификовати лице на које се односе прикупљени подаци, као и за одлучивање о неопходности идентификације тог лица, везују за друга службена лица која су распоређена у више различитих организационих јединица.

2.6. Контролу законитости, односно правилности вршења овлашћења наведених под 2.5. непосредно врше овлашћена службена лица која руководе појединим организационим јединицама у систему видео надзора, Сектор унутрашње контроле, као и органиизациона јединица надлежна за послове контроле рада. Ова контрола се, између осталог, обезбеђује евидентирањем сваке радње обраде, односно техничким омогућавањем утврђивања чињеница које се односе на коришћење камера и друге опреме у систему видео надзора у сваком конкретном случају.

2.7. Примена техничких мера заштите у систему видео надзора такође је заснована на систему подељених улога и то према надлежностима различитих организационих јединица.

2.8. Примена наведених организационих мера заштите података у систему видео надзора, и са њима повезаних техничких и кадровских мера заштите, уређује се Законом о евиденцијама и обради података у области унутрашњих послова, Упутством о мерама информационе безбедности у информационо-комуникационом систему Министарства унутрашњих послова и Упутством о условима изградње, коришћења и одржавања система видео надзора у Министарству унутрашњих послова и Упутством о начину вођења евиденција у области видео-акустичког снимања.

3. Технички аспекти обезбеђивања система видео надзора

3.1. Изградња система видео надзора врши се на образложени предлог Дирекције полиције а на основу одлуке министра, односно лица које он овласти за доношење ове одлуке. У сврху доношења одлуке о изградњи система видео надзора или дела овог система врши се анализа потреба постављања камера на појединим камерним местима, а према критеријумима наведеним под I 2.3. ("Свеобухватан опис радњи обраде"). При томе се у контексту процене нивоа извесности наступања ризика наведене под II 2.3. а) ("Процена ризика по права и слободе лица"), посебно води рачуна о остварењу сврхе видео надзора, односно о томе да се постављањем камера на адекватне положаје у највећој мери онемогући снимање приватног простора.

3.2. Систем видео надзора представља саставни део информационо-комуникационог система (ИКТ), којим рукује Министарство. Овај систем се ефикасно штити, између осталог, одговарајућим техничким мерама информационе безбедности које се примењују према подацима и опреми која се користи. У контексту процене нивоа извесности наступања ризика наведене под II 3.3. а) и г) ("Процена ризика по права и слободе лица"), техничким мерама се ефикасно штите подаци и опрема, посебно узимајући у обзир чињеницу да годинама уназад није забележен ниједан случај повреде безбедности података од стране трећих лица услед недостатака везаних за ове мере заштите.

3.3. Техничке мере заштите које се користе у систему видео надзора нарочито обухватају следеће:
- Постизање безбедности рада на даљину и употребе мобилних уређаја;
- Заштита носача података;
-Употреба криптозаштите ради заштите тајности, аутентичности односно интегритета података;
- Физичка заштита објеката, простора, просторија, односно зона у којима се налазе средства и документи ИКТ система и обрађују подаци у ИКТ систему;
- Заштита од губитка, оштећења, крађе или другог облика угрожавања безбедности средстава која чине ИКТ систем;
- Обезбеђивање исправног и безбедног функционисања ИКТ система;
- Заштита података и средства за обраду података од злонамерног софтвера;
- Заштита од губитка података;
- Чување података о догађајима који могу бити од значаја за безбедност ИКТ система;
- Обезбеђивање интегритета софтвера и оперативних система;
- Заштита од злоупотребе техничких безбедносних слабости ИКТ система;
- Заштита података у комуникационим мрежама укључујући уређаје и водове;
- Осигурање безбедности података који се преносе унутар ИКТ система, као и између ИКТ система МУП-а и других ИКТ система;

- Превенција и реаговање на безбедносне инциденте у оквиру ИКТ система, што подразумева адекватну размену информација о безбедносним слабостима, инцидентима и претњама у оквиру ИКТ система.

3.4. Техничким мерама заштите се посебно обезбеђује евидентирање сваке радње обраде, односно техничка могућност утврђивања чињеница које се односе на коришћење камера и друге опреме у систему видео надзора у сваком конкретном случају. На овај начин се обезбеђује ефикасна контрола над радњама обраде, што у највећој мери одвраћајуће делује на потенцијалне прекршиоце службених овлашћења и то у контексту процене нивоа извесности наступања ризика наведене под II 1.3. б), 2.3. в) и 4.3. б) ("Процена ризика по права и слободе лица").

3.5. Примена наведених техничких мера заштите података и опреме у систему видео надзора, и са њима повезаних организационих мера заштите, уређује се Законом о евиденцијама и обради података у области унутрашњих послова, Упутством о мерама информационе безбедности у информационо-комуникационом систему Министарства унутрашњих послова, Упутством о условима изградње, коришћења и одржавања система видео надзора у Министарству унутрашњих послова и Упутством о начину вођења евиденција у области видео-акустичког снимања.

4. Дисциплинованост и савесност полицијских службеника

4.1. Дисциплинованост и савесност овлашћених службених лица ангажованих у систему видео надзора обезбеђује се применом превентивних и реактивних мера заштите. У контексту процене нивоа извесности наступања ризика наведене под II 1.3. в) и г), 2.3. г) и д), 3.3. в) и 4.3. в) и г) ("Процена ризика по права и слободе лица"), овим мерама се подиже ниво свести овлашћених службених лица о неопходности заштите безбедности података и поштовања права и слобода лица, што у највећој мери повратно делује на минимизацију вероватноће наступања ризика.

4.2 Превентивне мере заштите се првенствено спроводе путем континуиране едукације овлашћених службених лица и то у вези са применом одредби Закона и других прописа који се односе на заштиту података о личности. Послови едукације врше се у складу са Уредбом о стручном оспособљавању и усавршавању у Министарству унутрашњих послова, на основу Програма стручног усавршавања полицијских службеника Министарства унутрашњих послова и Директиве о начину обављања послова у вези са заштитом података о личности у Министарству унутрашњих послова.

4.3. У периоду након усвајања Закона одржана су два циклуса едукација. У периоду октобар-новембар 2019. организовано је осам тренинга за тренере о заштити података о личности у оквиру Министарства. У априлу 2020. организовано је још четири продубљена целодневна семинара о заштити података о личности за овлашћена лица Министарства, са посебним акцентом на питања везана за видео надзор.

4.4. Оба едукациона циклуса била су намењена овлашћеним лицима Министарства са читаве територије Републике Србије. Кроз едукацију су, између осталих, прошли и сви начелници подручних полицијских управа. Једну од посебних група полазника чинили су руководиоци стратешког нивоа и овлашћена службена лица Сектора унутрашње контроле. Оба едукациона циклуса била су организована од стране Министарства, у партнерству са Канцеларијом савета за националну безбедност и заштиту тајних података, Мисијом ОЕБС у Србији, и организацијама цивилног друштва.

4.5. Уз едукацију овлашћених лица, Министарство такође континуирано примењује и читав пакет других мера усмерених ка заштити података о личности. Директива о начину

обављања послова у вези са заштитом података о личности у Министарству унутрашњих послова прописује следеће облике мера:
- Информисање и давање мишљења организационим јединицима и запосленима који врше радње обраде о њиховим законским обавезама у вези са заштитом података о личности, и то на захтев организационе јединице;
- Свеобухватно праћење примене одредби Закона и других прописа који се односе на заштиту података о личности у оквиру Министарства;
- Давање мишљења о процени утицаја обраде података на заштиту података о личности и праћење поступања по тој процени;
- Остваривање сарадње са Повереником за слободан приступ информацијама од јавног значаја и заштиту података о личности у вези са обрадом података у оквиру Министарства.

4.6. Реактивне мере се примењују у случају повреде безбедности података, односно права лица. Прва група ових мера односи се на повреду безбедности података, и то без обзира на то да ли је у конкретном случају на повреду безбедности реаговано другим механизмом заштите. Примена мера из ове групе прописана је Законом и Упутством о начину вођења евиденције и обавештавања о повредама података о личности у Министарству унутрашњих послова.

4.7. Друга група ових мера јесу дисциплинске мере и оне су прописане Законом о полицији. Трећу групу мера које су прописане Законом и Кривичним закоником примењује Сектор унутрашње контроле, тужилаштво и суд. Четврту групу чине мере које примењују Повереник за слободан приступ информацијама од јавног значаја и заштиту података о личности, у складу са Законом.

4.8. Према подацима који су садржани у годишњим извештајима које Министарство доставља Поверенику, као и у редовним кварталним извештајима који се достављају министру, број евидентираних и процесуираних повреда безбедности података и права лица чији се подаци обрађују од стране овлашћених лица Министарства је изузетно мали у односу на укупан број радњи обраде података које се врше у оквиру надлежности Министарства, односно укупан број лица чије податке Министарство обрађује. Међу овим повредама, најмањи број се везује за обраду података који су прикупљени у систему видео надзора. Такође, из расположивих података се недвосмислено закључује да се укупан број повреда већ годинама смањује.

5. Механизми заштите права лица

5.1. Свако лице чије податке обрађује Министарство, укључујући и податке прикупљене и даље обрађиване у систему видео надзора, овлашћено је да се захтевом за остваривање, односно заштиту права обрати Министарству, у складу са Законом. Механизам контроле поступања по захтевима лица чији се подаци обрађују поверава се лицу за заштиту података о личности у Министарству, а облици контроле уређени су Директивом о начину обављања послова у вези са заштитом података о личности.

5.2. У складу са Законом и на темељу принципа рада полиције у заједници (чл. 27. Закона о полицији), Министарство информише најширу јавност о пословима обраде података о личности које обављају службена лица Министарства, као и о правима лица чији се подаци обрађују. Информисање јавности врши се путем интернет странице Министарства, објављивањем информација у медијима, као и на други адекватан начин.

5.3. Информисање лица обухваћених системом видео надзора врши се у складу са Правилником о начину снимања на јавном месту и начину саопштавања намере о том снимању. Одредбе Правилника у делу који се односи на информисање лица одражавају

стандарде информисања у систему видео надзора које је формулисао ЕДПБ (European Data Protection Board), и примењују се у случајевима кад се видео надзор врши путем свих облика снимања наведених под I 2.1. ("Свеобухватан опис радњи обраде").

5.4. Стандарди наведени под 5.3. односе се посебно на двостепено информисање путем постављања одговарајућих знакова на камерном месту и упућивања на интернет страницу Министарства на којој су истакнуте детаљне информације о обради података у систему видео надзора. На интернет страници Министарства су, у складу са стандардима наведеним под 5.3, истакнуте и ажуриране информације о сваком од камерних места.

5.5. Циљ информисања јесте и развијање свести у јавности и код лица обухваћених системом видео надзора о допуштености примене овог система, веома ниском нивоу извесности повреде права у коришћењу овог система, као и о његовом значају са становишта заштите личне и имовинске безбедности грађана, односно ефикасности супротстављања оним облицима криминалитета који се могу ефикасно сузбијати управо коришћењем овог система. На овај начин се ефикасно може умањити бојазан лица обухваћених системом видео надзора за своја права ("Процена ризика по права и слободе лица", II 1.4. в), 2.4. б), 3.4. б) и 4.4. в), као и допринети изградњи поверења у односу грађана према Министарству.

У складу са чл. 54. ст. 3 Закона, прибављено је мишљење лица за заштиту података о личности у Министарству које је у прилогу овог документа.

Прилог: Мишљење лица за заштиту података о личности у Министарству унутрашњих послова на Процену утицаја обраде на заштиту података о личности употребом савремених технологија видео надзора у оквиру пројекта „Сигурно друштво" у Београду.

У Београду
01-1275/19-15
Дана 23.04. **2020. Год.**

ПОТПРЕДСЕДНИК ВЛАДЕ И
МИНИСТАР УНУТРАШЊИХ ПОСЛОВА

др Небојша Стефановић