ПРОЦЕНА УТИЦАЈА РАДЊИ ОБРАДЕ ПОДАТАКА О ЛИЧНОСТИ УПОТРЕБОМ СОФТВЕРА ЗА ОБРАДУ БИОМЕТРИЈСКИХ ПОДАТАКА У СИСТЕМУ ВИДЕО НАДЗОРА МИНИСТАРСТВА УНУТРАШЊИХ ПОСЛОВА НА ЗАШТИТУ ПОДАТАКА О ЛИЧНОСТИ

I ОПИС ОБРАДЕ ПОДАТАКА

У складу са законским овлашћењима полиције, полицијски службеници предузимају потребне мере у циљу утврђивања идентитета лица.

На основу података из видео записа добијеног употребом система видео надзора Министарства унутрашњих послова, идентификација лица се, у складу са важећим Законом о полицији, без обраде биометријских података, може извршити:

- препознавањем у току снимања, од стране овлашћеног полицијског службеника или
- препознавањем, накнадним прегледом снимљеног материјала од стране овлашћеног полицијског службеника, или од стране другог лица коме је, у складу са законом омогућен увид у видео запис.

Сходно Нацрту Закона о унутрашњим пословима, мере које се предузимају у циљу идентификације лица, могу да обухвате и обраду биометријских података употребом софтвера за препознавање лица у систему видео надзора.

Правни основ за обраду биометријских података је закон, а не пристанак лица, а биометријски подаци се обрађују на основу закона којим је уређена обрада података у области унутрашњих послова.

У циљу заштите интереса јавне и националне безбедности, спречавања нереда (јавни ред и мир) или криминала као и у циљу и заштите права и слобода других. (чл. 8 ст. 2 Европске конвенција о људским правима)[1] на основу израђеног профила безбедносног проблема[2] односно профила безбедносно интересантног лица[3], односно на основу процене безбедносно интересантних догађаја применом полицијско-обавештајног

[1] ЧЛАН 8 **Право на поштовање приватног и породичног живота** 1. Свако има право на поштовање свог приватног и породичног живота, дома и преписке. 2. Јавне власти неће се мешати у вршење овог права сем ако то није у складу са законом и неопходно у демократском друштву у интересу националне безбедности, јавне безбедности или економске добробити земље, ради спречавања нереда или криминала, заштите здравља или морала, или ради заштите права и слобода других.

[2] Скуп података и информација прикупљених у циљу сагледавања, разјашњења и бољег разумевања постојећих и нових појавних облика криминала, како би се иницирала или подржала полицијска активност према њима.- Извор: МУП (2016): Приручник: "Полицијско-обавештајни модел", доступно на сајту: www.mup.gov.rs.

[3] Скуп података и информација о безбедносно интересантним лицима, криминалним групама, жртвама и сведоцима кривичних дела, којим се иницира или подржава оперативно-полицијска активност према њима.- Извор: МУП (2016): Приручник: "Полицијско-обавештајни модел", доступно на сајту: www.mup.gov.rs.

модела опредељују се локације и време коришћења камера, повезаних са софтвером за препознавање лица.

Обрада биометријских података врши се детектовањем лица у току снимања, уз истовремено креирање фотографије/приказа лика из видео записа и издвајање биометријских података из такве фотографије у облику биометријског шаблона/дигиталног кода.

Сврха обраде биометријских података о личности је спречавање, истрага и откривање кривичних дела, гоњење учинилаца кривичних дела, као и спречавање и заштита од претњи јавној и националној безбедности. Нацртом Закона о унутрашњим пословима дата је могућност овлашћеном полицијском службенику да користи софтвер за препознавање лица у систему видео надзора, приликом провере идентитета, ради:

1) проналажења извршиоца кривичног дела за које се гоњење предузима по службеној дужности;
2) проналажење лица за које се основано сумња да припрема извршење кривичног дела тероризма и са њим повезаних кривичних дела;
3) проналажења лица за којим се трага.

Оправданост сврхе обраде заснива се на потреби остваривања законом одређених циљева обраде имајући у виду да је Министарство унутрашњих послова надлежни орган који је законом овлашћен да обрађује биометријске податке о личности у циљу јединствене идентификације лица као и да се обрада биометријских података о личности као посебне врсте података о личности може вршити и у циљу заштите животно важних интереса лица на које се подаци односе или другог физичког лица.

У складу са начелом минимизације, употребом софтвера за препознавање лица врши се прикупљање података о личности, у складу са законским овлашћењима полиције, а даље се обрађују подаци о личности који су примерени и битни за утврђивање идентитета само оних лица у односу на конкретну сврху обраде и не обрађују се у друге сврхе.

У циљу јединствене идентификације само одређених лица, биометријски подаци прикупљени употребом софтвера за препознавање лица се могу упоређивати са биометријским подацима из постојећих евиденција, прикупљеним у неке друге сврхе (нпр. са биометријским подацима који су садржани у евиденцији форензички регистрованих лица).

У складу са одредбама Закона о заштити података о личности, Министарство унутрашњих послова Републике Србије је руковалац подацима који се обрађују у систему видео надзора, односно употребом софтвера за препознавање лица. Министарство самостално обрађује податке, ангажовањем сопствених ресурса.

Прималац података које Министарство обрађује, може бити само други надлежни орган, у смислу чл. 4, тач. 26. Закона о заштити података о личности. Подаци се могу пренети и примаоцу (надлежном органу) у другој држави, односно међународној организацији, у складу са законом.

О употреби софтвера за препознавање лица, Министарство путем медија, других средстава јавног обавештавања (средство јавног информисања, интернет презентације и сл.) обавештава лица обухваћена видео надзором који је повезан за софтвером за препознавање лица.

ПОДАЦИ О ЛИЧНОСТИ КОЈИ СЕ ОБРАЂУЈУ

Употребом видео надзора обрађују се следећи подаци о физичким лицима: видео запис догађаја у којем учествује лице, време и место настанка видео записа и ГПС локација камере, регистарске и друге ознаке возила, употребом појединих камера из система видео надзора које су повезане са софтвером за препознавање лица обрађује се и **приказ лика физичког лица (фотографија лица)** са издвојеним **биометријским подацима у облику *шаблона/дигиталног кода***.

РАДЊЕ ОБРАДЕ

Обрада биометријских података у систему видео надзора обухвата следеће радње обраде: **прикупљање, разврставање, похрањивање, увид, претраживање, издвајање, копирање, преношење, упоређивање, ограничавање, чување** и **брисање** односно **уништавање** на други начин.

Подаци из видео записа односно видео записи се аутоматски **генеришу и разврставају по** времену настанка видео записа и месту снимања/ГПС локација камере.

Прикупљање биометријских података врши се детектовањем лица у току снимања, креирањем фотографије лица/приказа лика из видео записа и издвајањем биометријских података из такве фотографије у облику шаблона/дигиталног кода.

Детектована лица односно фотографије лица/приказ лика које су издвојене из видео записа као и биометријски подаци издвојени у облику шаблона/дигиталног кода се аутоматски генеришу **и разврставају по** времену детектовања лица/стварања фотографије односно шаблона/дигиталног кода и месту детектовања лица/ГПС локацији камере.

Видео записи са камера се **похрањују** на чврсту меморију (хард дискови, меморијске картице) централног система за складиштење података (*data centar*) и **чувају** се по систему кружног снимања, тј.систем аутоматски циклично брише најстарије податке када се попуни меморијски простор али не пре истека 30 дана од дана снимања.

Фотографије детектованих лица, са издвојеним биометријским подацима у облику шаблона/дигиталног кода, похрањују се на чврсту меморију истог централног система за складиштење података *(data centar)* али одвојено од видео записа и **чувају** се најдуже 72 сата од момента креирања фотографије.

Увид у податке из видео записа у реалном времену (*live stream*), омогућен је овлашћеном полицијском службенику[4] непосредним посматрањем, у корисничком центру.

Увид у похрањене податке из видео записа у корисничком центру врши се **претраживањем** и **издвајањем** одабраног видео записа на "радној станици" ради његове репродукције.

Претраживање похрањених видео записа се врши према критериујмима за претраживање као што су: локација односно назив камере/камерног места, датум и време настанка видео записа, а претраживање је, употребом посебних аналитичких алата, могуће и на основу других критеријума.

Претраживање и увид у похрањене податке из видео записа омогућен је само овлашћеним полицијским службеницима у корисником центру са посебном дозволом односно одобрењем. Претраживање и вршење увида **ограничено је** на сврху и циљеве прикупљања података а њихова даља обрада врши се у складу са овлашћењима полицијских службеника (налог тужилаштва или суда, предмет оперативне обраде и сл.).

Увид у фотографије/приказ лика детектованих лица у тренутку детектовања омогућен је само овлашћеним полицијским службеницима у корисничком центру са посебном дозволом односно одобрењем.

Претраживање похрањених фотографија и њихово издвајање ради вршења увида на радној станици, врши се према критериујмима за претраживање као што су: локација односно назив камере/камерног места, датум и време креирања фотографије.

Ово претраживање и вршење увида у фотографије детектованих лица/лика **ограничено је** на сврху и циљеве обраде биометријских података и њихова даља обрада се врши у складу са овлашћењима полицијских службеника (налог тужилаштва или суда, предмет оперативне обраде и сл).

Претраживање похрањених издвојених биометријских података у облику шаблона/дигиталног кода врши се употребом посебних алата, полуаутоматизовано или аутоматизовано.

А) Полуаутоматизовано претраживање (ради поређења) похрањених биометријских података врши се од стране овлашћеног полицијског службеника, одабиром одређене похрањене фотографије/приказа лика са издвојеним биометријским податком у облику шаблона/дигиталног кода из те фотографије и постављањем упита ка софтверу за препознавање лица који проверава њихову подударност са биометријским подацима из других евиденција који се за потребе тог поређења повезују са софтвером за препознавање лица.

[4] Под овлашћеним полицијским службеником за потребе израде ове процене подразумева се полицијски службеник који је распоређен на радно место чији опис послова подразумева руковање системом видео надзора. Ови полицијски службеници су едуковани и одобрена су им права приступа систему видео надзора. Немају сви полицијски службеници исти ниво приступа. Под овлашћеним полицијским службеником се такође подразумева и полицијски службеник који је у конкретном случају задужен за рад на утврђивању идентитета извршиоца и других неопходних чињеница у вези неког кривичног дела. Овај полицијски службеник налог за поступање добија од свог руководиоца.

Оваква провера подударности биометријских података користи се у случајевима када треба идентификовати непознатог извршиоца кривчног дела чије лице је детектовала нека од камера која је повезана на софтвер за препознавање лица. У таквим случајевима се биометријски подаци пореде са подацима из на пример евиденције форензички регистрованих лица, где софтвер за препознавање лица врши поређење у циљу утврђивања подударности биометријских података из фотографије са биометријским подацима из друге евиденције. У оваквим случајевима примењује се принцип поступности и сразмерности односно неопходности обраде података и то на следећи начин: Ако је на пример извршено кривчно дело разбојништва од стране лица мушког пола, из евиденције форензички регистрованих лица се ради проналаска подударних биометријских података прво издвајају биометријски подаци регистрованих извршилаца кривичног дела разбојништва мушког пола. Ако таква претрага нема резултата онда се издвајају и биометријски подаци регистрованих учинилаца других кривичних дела. Ако ни ова претрага нема резулата онда се користе и биометријски подаци из других евиденција.

Полуаутоматизовано претраживање похрањених биометријских података могуће је и у ситуацијама када се ради о познатом учиниоцу кривичног дела или на пример лицу за којим се трага а чије биометријске податке Министарство већ има у својим евиденцијама или је за потребе трагања прибавило. У таквим случајевима се, на упит овлашћеног полицијског службеника, расположиви/прибављени биометријски подаци тог лица повезују са софтвером за препознавање лица, који врши претрагу похрањених података ради проналаска биометријких података који се подударају са прибављеним подацима. Оваква провера подударности биометријских података врши се у случајевима када је потребно утврдити да ли је нека од камера које су повезане са софтвером за препознавање лица детектовала лице које полиција тражи.

Такође, се из похрањених видео записа са неке од камера која није повезана са софтвером за препознавање лица, употребом одговарајућих алата, може издвојити фотографија а софтвер за препознавање лица ће из такве фотографије издвојити биометријске податке у облику шаблона/дигиталног кода, који се на већ описан начин може користи за претраживање односно поређење подударности са расположивим биометријским подацима.

Б) Аутоматизовано (истовремено) упоређивање биометријских података у тренутку детекције лица и издвајања биометријских података могуће је само повезивањем биометријских података који су похрањени у другим евиденцијама, које Министарство води у складу са законом, са софтвером за препознавање лица (на пример база података која садржи податке о терористима/екстремистима, база података лица за којима се трага, база нестале деце, база података лица којима је изречена забрана присуствовања спротским манифестацијама, база података лица која су осуђена за кривична против полне слободе извршена над малолетницима и сл). Софтвер врши аутоматизовано упоређивање биометријских података уз могућност креирања различитих врста аларма у случају подударања. Уколико приликом аутоматизованог упоређивања биометријских података софтвер пронађе подударне податке резултат упоређивања се бележи на

систему, приказује кориснику на радној станици у облику извештаја са резултатом подударности, уз могућност креирања различитих врста аларма.

Аутоматизовано упоређивање биометријских података је ограничено и може се примењивати само на одређеним локацијама у складу са израђеним профилом безбедносног проблема и трајати само одређени временски период. Оваква обрада података ограничена је и само на лица за која је, на основу претходно израђеног профила безбедносно интересантног лица, неопходна у циљу анализе или предвиђања његовог понашања, или локације кретања. Оваква обрада је у складу са начелима законитости, легитимности, неопходности и сразмерности.Овлашћени полицијски службеник у циљу јединствне идентификације, доноси одлуку о предузимању других мера и радњи и примене полицијских овлашћења и то за свако лице понаособ. То значи да се идентитет лица не утврђује искључиво на основу аутоматизоване обраде података, односно не примењује тзв.аутоматско препознавање лица.

Одлуке овлашћених полицијских службеника се у односу на лице не примењују искључиво на основу аутоматизоване обраде, већ је у сваком конкретном случају неопходна улога полицијског службеника у смислу одређивања сврхе и начина примене конкретне радње обраде. Након идентификације лица могу се предузети радње или донети одлуке које производе правне последице по то лице, односно утичу на положај лица

Издвојени видео записи и фотографије се ради вршења увида и других радњи обраде ван корисничког центра могу **пренети копирањем,** у складу са законом, са радне станице на други носач података (меморијске картице, цд/двд, усб меморије и сл). Фотографије се осим копирања на други носач података могу копирати/умножавати штампањем на папиру.

Копирани подаци се у појединачним случајевима могу **пренети** овлашћеним примаоцима/другим надлежним органима (тужилаштво, суд) или лицу на које се подаци односе и то достављањем на носачу података.

Похрањени подаци се у систему видео надзора аутоматски трајно **бришу** на централном систему за складиштење. Подаци на основу којих се не утврђује идентитет лица **чувају** се најмање 30 дана од дана прикупљања. 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.).

Код издвајања и преношења података ради вршења увида ван корисничког центра, подаци се чувају у складу са законом.

Подаци на основу којих је утврђен идентитет лица преносе се на носач информација и чувају се у законом прописаном року који је неопходан за остваривање сврхе обраде.

II ПРОЦЕНА РИЗИКА ПО ПРАВА И СЛОБОДЕ ЛИЦА

Након анализе радњи обраде података идентификовани су и оцењени ризици по права и слободе лица до којих може довести употреба софтвера за препознавање лица.

Дефинисане су мере за контролу и смањење ризика.

Министарство ће као руковалац података о личности периодично ажурирати анализу ризика у складу са појављивањем претњи.

Рангирање ризика је извршено укрштањем утицаја и вероватноће, а за мерење ризика коришћена је матрица ризика 4x4.

УТИЦАЈ					
	4 Висок	4	8	12	16 неприхватљиви ризици
	3 Средњ	3	6	9	12
	2 Уме	2	4	6	8
	1 Мали	1 прихватљиви ризици	2	3	4
		1 Мала	2 Умерена	3 Средња	4 Висока
		ВЕРОВАТНОЋА			

Укупна изложеност ризику добијена је множењем бодова за утицај с бодовима за вероватноћу. Укупна изложеност ризику може бити:

- ниска (оцена 1 и 2) - ти ризици се сматрају занемарљивим,
- умерена (оцене 3 и 4) – прихватљиви ризици,
- средња (оцене 6, 8 и 9) – те ризике је потребно надгледати и управљати њима, и
- висока (оцене 12 и 16) - за такве ризике је потребно предузимање додатних мера и активности како би се последице њиховог деловања свеле на најмању меру.

1) Идентификација лица без правног основа

Опис ризика:
Ризик по права и слободе лица везује се за њихову идентификацију без правног основа, на основу података прикупљених видео надзором.

Ниво утицаја на повреде права и слобода лица одређен је према следећим показатељима:
а) Снимањем активности и идентификацијом лица, као и похрањивањем и другим радњама обраде података о овим активностима, без обзира на чињеницу да се активности предузимају на јавним површинама угрожавају се права на приватан живот, слободу удруживања, слободу окупљања, слободу изражавања, као и слободу кретања;

б) Снимањем активности и идентификацијом лица, као и даљом обрадом података лица која улазе у или излазе из верских објеката или учествују у вршењу верских обреда угрожава се слобода вероисповести;

в) Профилисањем идентификованих лица на основу стварне или претпостављене припадности удружењу, односно верској заједници, политичког или другог мишљења, сексуалног опредељења или другог личног својства угрожава се принцип забране дискриминације.

Ниво вероватноће повреде права и слобода лица одређен је према следећим показатељима:

а) Снимање лица употребом видео надзора угрожава се право на приватан живот, право слободе удруживања, слободу окупљања, слободе изражавања, слободе кретања, слобода вероисповести као и принцип забране дискриминације, имајући у виду да лица оправдано очекују да задрже своју анонимност иако активности предузимају на јавној површини;

б) Идентификација лица без правног основа представља повреду права и слобода лица.

Мере за смањење ризика:
Организационе мере: поступање полицијских службеника приликом употребе видео надзора засновано је на организационој структури у систему подељених улога у погледу вршења појединачних радњи обраде и одлучивања о потреби идентификације лица и профилисања идентификованих лица, чиме је умањена могућност идентификације лица без правног основа и омогућено утврђивање индивидуалне одговорности полицијских службеника.

Техничке мере: контрола приступа опреми, контрола носача података, контрола чувања података, контрола корисника, контрола приступа подацима, контрола преноса, контрола транспорта, опоравак система, обезбеђивање интегритета система, управљање корисничким налозима, системски журнал, физичка и техничка заштита објеката и опреме, заштита од оштећења и крађе средстава која чине систем видео надзора.

Кадровске мере: корисници система су полицијски службеници. Сви корисници су оспособљени и едуковани. Предузимају се мере заштите од ризика који настају при промени послова или престанка радног односа. Полицијски службеници су едуковани о законским условима и начину примене полицијских овлашћења, мера и радњи, о утврђеним стандардима полицијског рада и о правном режиму заштите података о личности. Утврђивање дисциплинске одговорности.

Ниво утицаја повреда права и слободе лица је: висок **(4)**
Ниво вероватноће повреда права и слободе лица је: мала **(1)**

Ниво ризика повреда права и слободе је: умерен **(4)**

2) <u>Профилисање лица без правног основа</u>

Опис ризика:
Ризик по права и слободе лица везује се за профилисање лица без правног основа, на основу стварне или претпостављене припадности удружењу, односно верској заједници,

политичког или другог мишљења, сексуалног опредељења или другог стварног или претпостављеног личног својства.

Ниво утицаја на повреде права и слобода лица одређује се према профилисању идентификованих лица у циљу анализе личних склоности, понашања и кретања којим се угрожава право на приватан живот, слободу удруживања, слободу окупљања, слободу изражавања, слободу вероисповести, сексуално опредељење, слободу кретања, политичког или другог мишљења и другог личног својства.

Ниво вероватноће одређује се према профилисању лица без правног основа, у циљу анализе личних склоности, понашања и кретања чиме се угрожава право на приватан живот, слободу удруживања, слободу окупљања, слободу изражавања, слободу вероисповести, сексуално опредељење, слободу кретања, политичког или другог мишљења и другог личног својства, имајући у виду забрану дискриминације лица по било ком основу.

Мере за смањење ризика:
Организационе мере: Поступање полицијских службеника приликом профилисања лица засновано је на организационој структури у систему подељених улога у погледу вршења појединачних радњи обраде и одлучивања о циљу анализе склоности, понашања и кретања лица, чиме је умањена могућност профилисања лица супротно принципу забране дискриминације; Мере усмерене контроле и примена полицијских овлашћења, мера и радњи према профилисаним лицима врше се професионално и у складу са утврђеним стандардима полицијског рада.

Техничке мере: контрола приступа опреми, контрола носача података, контрола чувања података, контрола корисника, контрола приступа подацима, контрола преноса, контрола транспорта, опоравак система, обезбеђивање интегритета система, управљање корисничким налозима, системски журнал, физичка и техничка заштита објеката и опреме, заштита од оштећења и крађе средстава која чине систем видео надзора

Кадровске мере: корисници система су полицијски службеници. Сви корисници су оспособљени и едуковани. Предузимају се мере заштите од ризика који настају при промени послова или престанка радног односа. Полицијски службеници су едуковани о законским условима и начину примене полицијских овлашћења, мера и радњи, о утврђеним стандардима полицијског рада и о правном режиму заштите података о личности. Утврђивање дисциплинске одговорности.

Ниво утицаја повреда права и слободе лица је: средњи **(3)**
Ниво вероватноће повреда права и слободе лица је: средња **(3)**

Ниво ризика повреда права и слободе је: средњи **(9)**

3) <u>Биометријски подаци из евиденција за упоређивање нису тачни</u>

Опис ризика:

Ризик по слободе и права везује се за обраду нетачних биометријских податак садржаних у евиденцијама за упоређивање које ово Министарство води у складу са законом.

Ниво утицаја на повреде права и слобода лица одређен је према следећим показатељима: Обрада нетачних података довела би до упоређивања са нетачним подацима из евиденција што би могло имати за последицу неосновано поступање полицијских службеника према лицу за које се везују нетачни биометријски подаци чиме би се повредило његово право на приватност и достојанство.

Ниво вероватноће повреде права и слобода лица одређен је обрадом нетачних података могу се угрозити право на приватност и достојанство лица чији се подаци обрађују.

Мере за смањење ризика:
Организационе мере: Поступање полицијских службеника приликом вођења евидењнција засновано је на организационој структури у систему подељених улога у погледу вршења појединачних радњи обраде и одлучивања о циљу анализе склоности, понашања и кретања лица, чиме је умањена могућност нетачног и неажурног вођења евиденција.

Техничке мере: контрола приступа опреми, контрола носача података, контрола чувања података, контрола корисника, контрола приступа подацима, контрола преноса, контрола транспорта, опоравак система, обезбеђивање интегритета система, управљање корисничким налозима, системски журнал, физичка и техничка заштита објеката и опреме, заштита од оштећења и крађе средстава која чине систем видео надзора.

Кадровске мере: Примена полицијских овлашћења, мера и радњи према лицима из евиденције врше се професионално и у складу са утврђеним стандардима полицијског рада. Подразумева се да ће полицијски службеник у случају очигледне нетачности податка извршити додатне провере пре доношења одлуке о даљем поступању према лицу; спровођењем контролно-инструктивне делатности омогућен је увид у начин вођења евиденција и поступање полицијских службеника.

Ниво утицаја повреда права и слободе лица је: висок **(4)**
Ниво вероватноће повреда права и слободе лица је: мала **(1)**

Ниво ризика повреда права и слободе је: умерен **(4)**

4) <u>Снимање лица у приватном простору</u>

Опис ризика:
Ризик по права и слободе лица постоји у ситуацијама када се снимањем камерама које су повезане са софтвером за препознавање лица, сними и део приватног простора.

Ниво утицаја на повреде права и слобода лица одређен је према следећим показатељима:

а) Снимањем, похрањивањем и другим радњама обраде података о активности лица која се налазе у приватном простору може се угрозити право на приватност лица.

б) Лице оправдано очекује да су активности које предузима у приватном простору заштићене од погледа других људи;

в) Транспарентном употребом видео надзора умањује се субјективни осећај угрожености права на приватност лица, чиме се подиже свест грађана о висини ризика по ово њихово право.

Ниво вероватноће повреде права и слобода лица одређен је према следећим показатељима:

а) Употреба наведених камера има за циљ снимање јавног простора, те постоји могућност да се сними приватни или пословни простор на оним местима на којим не постоје физичке препреке чиме се може угрозити право на приватност.

б) Уколико је наведена камера веома удаљена од приватног или пословног простора, односно уколико се у односу на приватни простор налази под неодговарајућим углом, или је такав простор заклоњен дрвећем, завесама, ролетнама, оградама и сл., квалитет прикупљених података је лош, а могућност повреде права је занемарљива.

Мере за смањење ризика:
Организационе мере: Поступање полицијских службеника приликом руковања камерама засновано је на организационој структури у систему подељених улога. Спровођењем контролно-инструктивне делатности омогућен је увид у начин руковања камерама и поступање полицијских службеника.

Техничке мере: Контрола приступа опреми, контрола носача података, контрола чувања података, контрола корисника, контрола приступа подацима, контрола преноса, контрола транспорта, обезбеђивање интегритета система, управљање корисничким налозима, системски журнал.

Кадровске мере: корисници система/камера су полицијски службеници. Сви корисници су оспособљени и едуковани за руковање камерама као и о законским условима и начину примене полицијских овлашћења, мера и радњи, о утврђеним стандардима полицијског рада и о правном режиму заштите података о личности. Утврђивање дисциплинске одговорности.

Ниво утицаја повреда права и слободе лица је: висок **(4)**
Ниво вероватноће повреда права и слободе лица је: мала **(1)**

Ниво ризика повреда права и слободе је: умерен **(4)**

5) <u>Повреда безбедности података</u>

Опис ризика:
Ризик по права и слободе лица постоји у погледу могућности повреде безбедности података прикупљених системом видео надзора.

Ниво утицаја на повреде права и слобода лица одређен је према следећим показатељима:

а) Догађај који подразумева ризик по права и слободе лица везује се за повреду безбедности података прикупљених у систему видео надзора услед неовлашћеног приступа опреми (за складиштење и пренос података), копирања, откривања, преношења, неовлашћеног уношења, измена и брисања података о личности чиме се угрожавају права и слободе лица;

б) Злоупотребом права приступа систему видео надзора од стране овлашћеног лица угрозиће се права и слободе лица.

Ниво вероватноће повреде права и слобода лица одређен је према следећим показатељима:

а) Неовлашћеним приступом опреми (за складиштење и пренос података), копирањем, откривањем, преношењем, неовлашћеним уношењем, изменом и брисањем података о личности угрожава се безбедност података.

б) Злоупотребом права приступа од стране овлашћеног лица и то копирањем, откривањем, преношењем, неовлашћеним уношењем, изменом и брисањем података о личности угрожава се безбедност података.

Мере за смањење ризика:
Организационе мере: поступање полицијских службеника приликом примене мера заштите безбедности података у систему видео надзора засновано је на организационој структури у систему подељених улога. У Министарству унутрашњих послова, посебна организациона јединица се бави пословима информационе безбедности, Одељење за информациону безбедност као и Одељење за серверску инфраструктуру. Министарство у свом саставу има и Центар за реаговање на нападе на информациони систем (ЦЕРТ). Посебна организациона јединица у саставу Секретаријата министарства обавља послове спровођења организационих, техничких и кадровских мера заштите података о личности (Контролна листа КЛ 001 од 25.10.2019. године).

Техничке мере: контрола приступа опреми, контрола носача података, контрола чувања података, контрола корисника, контрола приступа подацима, контрола преноса, контрола транспорта, опоравак система, обезбеђивање интегритета система, управљање корисничким налозима, системски журнал, заштита од злонамерног софтвера, физичка и техничка заштита објеката и опреме, заштита од оштећења и крађе средстава која чине систем видео надзора**.**

Кадровске мере: корисници система су полицијски службеници. Сви корисници су оспособљени и едуковани. Предузимају се мере заштите од ризика који настају при промени послова или престанка радног односа. Полицијски службеници су едуковани о примени мера заштите и безбедности података и обучени за правилну употребу видео надзора. Утврђивање дисциплинске одговорности и иницирање за утврђивање кривичне и прекршајне одговорности од стране надлежног органа.

Ниво утицаја повреда права и слободе лица је: висок **(4)**
Ниво вероватноће повреда права и слободе лица је: мала **(1)**

Ниво ризика повреда права и слободе је: умерен **(4)**

6) Недопуштено објављивање података

Опис ризика:
Недопуштено објављивање података прикупљених системом видео надзора, путем медија, друштвених мрежа или коришћењем других средстава комуникације угрозиће права и слободе лица чији се подаци обрађују.

Ниво утицаја на повреде права и слобода лица одређен је према следећим показатељима:

а) Увидом у активности лица које је обухваћено видео надзором од стране јавности, односно примаоца информација које се објављују у медијима, у оквиру друштвених мрежа или се шире путем других средстава комуникације угрозиће се право на приватан живот;

б) Објављивањем информације која се односи на приватан живот лица угрозиће се углед, част, достојанство, лични и морални интегритет лица чији се подаци обрађују видео надзором.

Ниво вероватноће повреде права и слобода лица одређен је према следећим показатељима:

а) Недопуштено објављивање података прикупљених видео надзором, путем медија, друштвених мрежа или коришћењем других средстава комуникације повредиће права и слободе лица чији се подаци обрађују.

б) Број евидентираних случајева недопуштеног објављивања података, од стране запослених у министарству, је занемарљив.

Мере за смањење ризика:
Организационе мере: поступање полицијских службеника приликом употребе видео надзора засновано је на организационој структури у систему подељених улога у погледу вршења појединачних радњи обраде, чиме је умањена могућност недопуштеног објављивања података и омогућено утврђивање индивидуалне одговорности полицијских службеника**.**

Техничке мере: контрола приступа опреми, контрола носача података, контрола чувања података, контрола корисника, контрола приступа подацима, контрола преноса, контрола транспорта, опоравак система, обезбеђивање интегритета система, управљање корисничким налозима, системски журнал, заштита од злонамерног софтвера, физичка и техничка заштита објеката и опреме, заштита од оштећења и крађе средстава која чине систем видео надзора.

Кадровске мере: Примена полицијских овлашћења, мера и радњи, употребом система видео надзора, врше се професионално и у складу са утврђеним стандардима полицијског рада. Предузимају се мере заштите од ризика који настају при промени послова или престанка радног односа. Запослени у министарству су едуковани о правном режиму заштите података о личности. Утврђивање дисциплинске одговорности и иницирање за утврђивање кривичне одговорности од стране надлежног органа.

Ниво утицаја повреда права и слободе лица је: висок **(4)**
Ниво вероватноће повреда права и слободе лица је: умерена **(2)**

Ниво ризика повреда права и слободе је: средњи **(8)**

7) <u>Грешка софтвера</u>

Опис ризика:
Ризик по слободе и права везује се за предузимање полицијских мера и радњи према лицу чији се подаци обрађују употребом софтвера за препознавање лица.

Ниво утицаја на повреде права на приватност и достојанство лица, одређен је применом полицијских овлашћења, мера и радњи, којима се угрожава право на приватност и достојанство тог лица.

Ниво вероватноће повреде права на приватност и достојанство лица, одређен је на начин што овлашћени полицијски службеник у циљу идентификације лица, чији се подаци обрађују употребом софтвера за препознавање лица, увек додатно проверава резултат упоређивања биометријских података и доноси одлуку о предузимању других мера и радњи према лицу. Изостанак провере резултата упоређивања биометријских података, повредиће право на приватност и достојанство лица.

Мере за смањење ризика:
Организационе мере: поступање полицијских службеника приликом употребе видео надзора засновано је на организационој структури у систему подељених улога у погледу вршења неопходних провера резултата упоређивања биометријских података, чиме је умањена могућност предузимања других мера и радњи према лицу, без вршења неопходне провере.

Техничке мере: контрола носача података, контрола чувања података, контрола корисника, контрола приступа подацима, контрола преноса, контрола транспорта, опоравак система, обезбеђивање интегритета софтвера и оперативних система, системски журнал, заштита од злонамерног софтвера, обезбеђивање исправног и безбедног функционисања система, чување података о догађајима који могу бити од значаја за безбедност система, обезбеђивање да активности на ревизији система имају што мањи утицај на његово функционисање и обезбеђивање континуитета обављања послова у ванредним околностима.

Кадровске мере: Примена полицијских овлашћења, мера и радњи, употребом система видео надзора, врше се професионално и у складу са утврђеним стандардима

полицијског рада. Предузимају се мере заштите од ризика који настају при промени послова или престанка радног односа. Запослени у министарству су едуковани о правном режиму заштите података о личности. Утврђивање дисциплинске одговорности.

Ниво утицаја повреда права и слободе лица је: средњи **(3)**
Ниво вероватноће повреда права и слободе лица је: мала **(1)**
Ниво ризика повреда права и слободе је: умерен **(3)**

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

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 у складу са законом.

1. Мере заштите безбедности података и механизми заштите права лица

Представљени ризици по права и слободе лица ефикасно се уклањају, односно своде на најмању меру применом општих организационих, кадровских и техничких 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 о заштити података о личности и другим прописима, као што је Закон о информационој безбедности, Закон о полицији, Закон о евиденцијама и обради података у области унутрашњих послова и подзаконским актима донетим од стране Министарства.

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

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 у контексту процене нивоа извесности наступања ризика, једноставно није могуће организационо, технички и правно замислити ситуацију у којој се изван система подељених улога доноси одлука о предузимању радњи обраде које имају за циљ идентификацију лица.

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

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.

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.

У свакој од организационих јединица Министарства, сваком овлашћеном лицу додељује се унапред одређени ниво одлучивања, односно овлашћење за предузимање појединих радњи обраде. Тако појединa овлашћена лица имају и улогу контроле извршења послова и задатака у систему видео надзора.

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. Тако, на пример овлашћење за прикупљање података има само лице које је распоређено у оквиру једне организационе јединице, док овлашћења за коришћење података, на основу којих је могуће идентификовати лице на које се односе прикупљени подаци, као и за одлучивање о неопходности идентификације тог лица, имају друга службена лица која су распоређена у више различитих организационих јединица.

Контролу законитости, односно правилности вршења овлашћења, непосредно врше овлашћена лица која руководе појединим организационим јединицама у систему видео надзора, Сектор унутрашње контроле, као и организациона јединица надлежна за послове контроле законитости рада. Оваква контрола, између осталог, обезбеђена је 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 (системски журнал).

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

Примена наведених организационих мера заштите података у систему видео надзора, и са њима повезаних техничких и кадровских мера заштите, уређује се Законом о полицији, 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 и другим прописима који регулишу предметну материју.

3. Технички аспекти обезбеђивања система видео надзора

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 раније поменутим критеријумима. При томе се у контексту процене нивоа извесности наступања ризика, 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.

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.

Техничке мере заштите које се користе у систему видео надзора нарочито обухватају следеће:

- Заштита носача података;
- Употреба криптозаштите ради обезбеђивања тајности, аутентичности и интегритета података;
- Физичка заштита возила, објеката, простора, просторија, односно зона у којима се налазе средства и документи ИКТ 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;
- 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;
- Ограничење приступа подацима и средствима за обраду података;
- Одобравање овлашћеног приступа и спречавање неовлашћеног приступа ИКТ систему и систему и услугама које ИКТ систем пружа.

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

Дисциплинованост и савесност овлашћених полицијских службеника ангажованих у систему видео надзора обезбеђује се применом превентивних и реактивних мера заштите. Овим мерама се подиже ниво свести овлашћених полицијских службеника о неопходности заштите безбедности података и поштовања права и слобода лица.

Превентивне мере заштите подразумевају безбедносне провере кандидата за пријем у радни однос и запослених у Министарству, континуирану едукацију овлашћених полицијских службеника 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.

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 јединицама 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.

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.

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 Министарство унутрашњих послова, тужилаштво и суд. Четврту групу чине мере које примењује Повереник за слободан приступ информацијама од јавног значаја и заштиту података о личности, у складу са Законом.

5. Механизми заштите права лица

Свако лице чије податке обрађује Министарство 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.

У складу са Законом о полицији, о употреби софтвера за препознавања лица, Министарство информише лица чији се подаци обрађују употребом тог софтвера, као и о њиховим правима. Информисање лица врши се путем интернет странице Министарства, објављивањем информација у медијима, као и на други адекватан начин, у складу са подзаконским актом донетим у складу са законом.

Циљ информисања јесте и развијање свести код лица обухваћених системом видео надзора о допуштености примене софтвера за препознавање лица, веома ниском нивоу извесности повреде права употребом овог софтвера, као и о његовом значају и неопходности употребе са становишта заштите личне и имовинске безбедности грађана, односно ефикасности супротстављања свим облицима криминалитета који се могу ефикасно сузбијати коришћењем овог софтвера. На овај начин се ефикасно умањује бојазан лица, чији се подаци обрађују употребом софтвера, за своја права, чиме се подиже ниво поверења 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.

У Београду, дана_____2022. године.