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 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

[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: http://www.mup.gov.rs/wps/wcm/connect/23a0498f-e93a-4fd3-a507-6ebc568cd10e/Prirucnik+POM+sajt+7.10.2016.pdf?MOD=AJPERES&CVID=mC0sR8O

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:

- проналажења извршиоца кривичног дела за које се гоњење предузима по службеној дужности;
- проналажење лица за које се основано сумња да припрема извршење кривичног дела тероризма и са њим повезаних кривичних дела;
- 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.

[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.

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 критеријумима 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.

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 податаке 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 о евиденцијама и обради података у области унутршњих посова („Сл. глсник РС“ бр.24/18), 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.

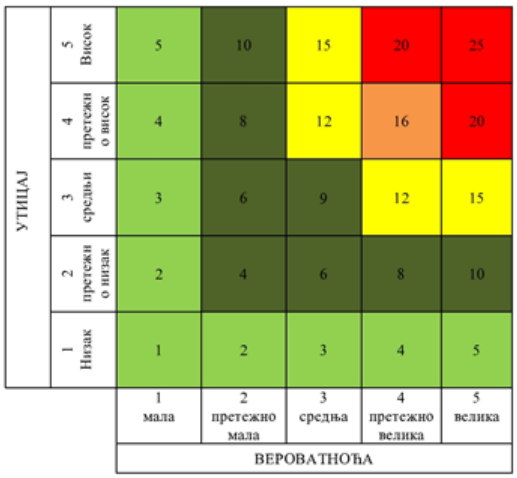
Копирани подаци се у појединачним случајевима могу пренети овлашћеним примаоцима/другим надлежним органима (тужилаштво, суд) или лицу на које се подаци односе и то достављањем на носачу података.

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 након чега је оцењен резидуални ризик. 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 5x5.



Укупна изложеност ризику представљена је као производ рангираног утицаја и вероватноће те се добијени резултати изложености ризику могу представити као:

1-5 НЕЗНАТНА (не захтева се никаква активност)
6-10 ДОПУСТИВА (нема потребе за додатним активностима, потребно је пратити ситуацију)
11-15 УМЕРЕНА (потребно је у наређеном периоду планирати и друге мере, пратити поједине активности и дефинисати начин контроле)
16-20 ЗНАТНА (потребни су ефикасни механизми контроле примене мера за смањења ризика)
21-25 НЕДОПУСТИВА (обраду података не би требало вршити док се ризик не умањи)

ПРЕПОЗНАТИ РИЗИЦИ

- **<u>Обрада биометријских података неодређеног броја лица – неселективна употреба софтвера за препознавање лица</u>**

Овај ризик се везује за употребу софтвера за прикупљање и чување биометријских података неодређеног броја лица која се затекну у зони снимања, ради претраге подударања њихових података са расположивим подацима знатно мањег броја лица, било у тренутку њиховог прикупљања или накнадног претраживања.

Оваквом обрадом података није могуће направити неопходну разлику између појединих врста лица (чл. 9. Закона о заштити података о личности) односно софтвер за препознавање лица прикупља податке сваког лица које се затекне у зони снимања, и у случају „препознавања“ то лице третира као „потенцијалног осумњиченог“.

Обрада података сваког „пролазника“ озбиљно утиче на разумна очекивања лица да буду анонимна на јавном простору што је предуслов за многе аспекте демократског процеса, као што су на пример: слободна одлука о удруживању са другима, посећивање скупова и упознавање људи из других друштвених и културних средина, учествовању у политичком протесту и слично.

Употребом софтвера за препознавање лица приликом вршења надзора на јавном простору код лица се ствара осећај да су подвргнути константном надзору, а да притом нису ни сигурни да ли је стварно тако. Овакав осећај може утицати на понашање појединаца што даље утиче и на карактер друштва. Додатни аспект оваквог осећаја код појединаца је и одвраћање од сусрета или виђања у јавности са одређеним лицима (рођацима, пријатељима) за које се претпоставља да су имали или могу имати „проблем“ са полицијом. Код употребе софтвера за препознавање лица на јавном простору немогуће је ограничити његову примену на начин да се обезбеди поверљив контакт са одређеним лицима (као што је например контакт са новинарима, адвокатима, свештенством, лекарима и сл.). Такође, од употребе овог софтвера на јавном простору немогуће је „заштити“ посебно осетљиве групе лица као што су на пример деца. Неселективна употреба технологије за препознавање лица, где сва лица која се затекну на одређеном простору могу бити предмет обраде, поред поменутих угрожава и право на претпоставку невиности.

Ниво утицаја повреда права и слободе лица је: претежно висок (4)
Ниво вероватноће повреда права и слободе лица је: велик (5)
Изложеност ризику повреда права и слободе је: недопустива (20)

Контролу ризика врши се употребом организационих и техничких мера.

Употреба софтвера за препознавање лица мора се вршити на основу израђеног профила безбедносног проблема односно профила безбедносно интересантног лица, те се локације и време коришћења камера, повезаних са софтвером за препознавање лица морају одредити на основу процене безбедносно интересантних догађаја применом полицијско-обавештајног модела и то: ради проналажења извршиоца кривичног дела за које се гоњење предузима по службеној дужности; проналажење лица за које се основано сумња да припрема извршење кривичног дела тероризма и са њим повезаних кривичних дела; проналажења лица за којим се трага.

Фотографије детектованих лица, са издвојеним биометријским подацима у облику шаблона/дигиталног кода, могу се похрањивати на чврсту меморију централног система за складиштење података (data centar) и чувати најдуже 72 сата од момента креирања фотографије. Увид у ове фотографије може бити омогућен само овлашћеним полицијским службеницима у корисничком центру са посебном дозволом односно одобрењем. Претраживање похрањених фотографија и њихово издвајање мора се ограничити на сврху и циљеве обраде биометријских података и њихова даља обрада се може вршити само у складу са овлашћењима полицијских службеника (налог тужилаштва или суда, предмет оперативне обраде и сл). Само 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. Идентитет лица се неће утврђивати искључиво на основу аутоматизоване обраде података, односно неће се примењивти тзв. аутоматско препознавање лица већ ће у сваком конкретном случају бити неопходна улога полицијског службеника у смислу одређивања сврхе и начина примене конкретне радње обраде.

Поступање полицијских службеника приликом употребе софтвера за препознавање лица мора бити засновано на организационој структури у систему подељених улога у погледу вршења појединачних радњи обраде и одлучивања о потреби појединачне идентификације лица, чиме ће се омогућити идентификација само оних лица без чије обраде података није могуће остварити сврху обраде података.

Корисници овог система су полицијски службеници који морају бити бити 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 приликом употребе овог система. Сваком полицијском службенику додељени су налози за приступ систему који се при промени послова или престанка радног односа укидају, односно нивои приступа се ажурирају. Сваки приступ систему се аутоматски бележи (системски журнал). Подаци се на централном систему за складиштење чувају најдуже 72 сата након чега се аутоматски бришу.

Применом организационих и техничких мера, резидуални ризик се умањује али је изложеност ризику знатна која се даље умањује ефикасним механизмима контроле примене свих мера заштите и благовременим извештавањем.

Ниво утицаја повреда права и слободе лица је: претежно висок (4)
Ниво вероватноће повреда права и слободе лица је: претежно висок (4)
Изложеност ризику повреда права и слободе је: знатна (16)

- **<u>Ризик недовољне транспаретности</u>**

Ризик недовољне транспарентности се везује за начин остваривања права на информисаност лица чији се подаци обрађују употребом софтвера за препознавање лица, односно за недовољну информисаност лица о томе да ли су и у којим све ситуацијама били или су и даље предмет надзора.

Употреба овакве технологије на јавном простору, код лица се ствара осећај да су подвргнути константном надзору, а да при том нису сигурни да ли је стварно тако, услед чега се код њих може јавити осећај несигурности, односно неизвесности остваривања

људских права и слобода и то не само права која су им зајемчена прописима о заштити података о личности.

Изостанак или недовољна информисаност лица о употреби софтвера за препознавање лица додатно продубљује осећај несигурности, односно нелагодности.

Ниво утицаја повреда права и слободе лица је: средњи (3)
Ниво вероватноће повреда права и слободе лица је: средњи (3)
Изложеност ризику повреда права и слободе је: допустива (9)

Контрола ризика врши се употребом предвиђених организационих и техничких мера.

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

У складу са Правилником о начину снимања на јавном месту и начину саопштавања намере о том снимању (Сл. гласник РС, 111/20), о употреби софтвера за препознавање лица, Министарство путем медија, других средстава јавног обавештавања (средство јавног информисања, интернет презентације и сл.) обавестиће јавност а самим тим и сва лица која могу бити обухваћена видео надзором који је повезан за софтвером за препознавање лица.

Локација камера (стадиони, гранични прелази и друга места са великом фрекфенцијом људи) на којима ће бити функционалан софтвер за препознавање лица које се врши истовременим-аутоматизованим упоређивањем биометријских података у тренутку детекције лица, морају бити јасно обележене како би се свим лицима који се затекну на тој локацији омогућило да се упознају са чињеницом да ће доласком на одређену локацију заправо бити под надзором који подразумева обраду њихових биометријских података.

Лицима се поред оваквог информисања мора омогућити и конкретно остваривање права у вези са обрадом података о личности (право на увид, копију, брисање или друга права у скаду са законом). Информисање мора да садржи и обавештавање о начину остваривања права код руковаоца (нпр. подношењем захтева Министарству унутрашњих послова територијално надлежној полицијској управи, по месту локације камера).
Уз примену мера за умањење ризка умањује се и вероватноћа повреде права и слободе лица али се мора имати у виду да ће и поред свих предузетих мера увек постојати лица која неће бити обавештена или неће довољно јасно разумети обавештење које им је пружено, те резидуални ризик, односно је изложеност ризику самњена али остаје допустива и може се контролисати ефикасним поступањем по захтевима грађана за остваривање права у вези са обрадом података о личнсоти.

Ниво утицаја повреда права и слободе лица је: средњи (3)
Ниво вероватноће повреда права и слободе лица је: претежно мали (2)
Изложеност ризику повреда права и слободе је: допустива (6)

- **<u>Профилисање лица</u>**

Ризик по права и слободе лица везује се за могућност профилисања лица. Софтвер за препознавање лица, као облик аутоматизоване обраде података, се може користити да би се оценило одређено својство личности, посебно у циљу анализе или предвиђања понашања, локација, кретања или личних сколоности (на основу стварне или претпостављене припадности удружењу, односно верској заједници, политичког или другог мишљења, сексуалног опредељења или другог стварног или претпостављеног личног својства). Обавеза је руковаоца је да лице на које се подаци односе информише о могућности профилисања лица и пружи додатне информације које могу да буду неопходне да би се обезбедила поштена и транспарентна обрада.

Забрањено је доношење одлуке искључиво на основу аутоматизоване обраде коју министарство врши као надлежни органи у посебне сврхе, укључујући и профилисање, ако таква одлука може да произведе штетне правне последице по лице на које се подаци односе или значајно утиче на положај тог лица, осим ако је доношење те одлуке засновано на закону и ако су тим законом прописане одговарајуће мере заштите права и слобода лица на које се подаци односе, а најмање право да се обезбеди учешће физичког лица под контролом руковаоца у доношењу одлуке. Забрањено је профилисање које доводи до дискриминације физичких лица на основу посебних врста података о личности.

Ризик по права и слободе лица представља недозвољено профилисање које би подразумевало доношење одлуке на основу аутоматизоване обраде без примене одговарајућих мера заштите права и слобода лица, односно до било каквог облика дискриминације на основу посебних врста података и које нема за циљ анализу или предвиђање понашања, локације, кретање извршиоца кривичног дела за које се гоњење предузима по службеној дужности, проналажење лица за које се основано сумња да припрема извршење кривичног дела тероризма и са њим повезаних кривичних дела, проналажење лица за којим се трага,

Ниво утицаја повреда права и слободе лица је: висок (5)
Ниво вероватноће повреда права и слободе лица је: велик (5)
Изложеност ризику повреда права и слободе је: недопустива (25)

Контрола ризика врши се употребом предвиђених организационих и техничких мера.

Обрада података коју врше надлежни органи у посебне сврхе, којом се открива расно или етничко порекло, политичко мишљење, верско или филозофско уверење или чланство у синдикату, као и обрада генетских података, биометријских података у циљу јединствене идентификације физичког лица, података о здравственом стању или података о сексуалном животу или сексуалној оријентацији физичког лица, допуштена је само ако је то неопходно, уз примену одговарајућих мера заштите права лица на које се подаци односе, у случајевима када је надлежни орган законом овлашћен да обрађује посебне врсте података о личности; када се обрада посебних врста података о личности врши у циљу заштите животно важних интереса лица на које се подаци односе или другог физичког лица или када се обрада односи на посебне врсте података о личности које је лице на које се они односе очигледно учинило доступним јавности.

Доношење било какве одлуке која производи правне последице, односно која утиче на положај лица на које се подаци односе мора бити засновано на закону и морају се предузети одговарајуће мере заштите права и слобода лица а најмање права да се обезбеди учешће физичког лица (овлашћеног полицијског службеника) у доношењу одлуке.

Овлашћени полицијски службеник дужан је да за свако лице понаособ доносе одлуку о предузимању мера и радњи или примене полицијских овлашћења у циљу јединствне идентификације тог лица. Дакле, идентитет лица се не утврђује искључиво на основу аутоматизоване обраде података већ је у сваком конкретном случају неопходна улога полицијског службеника код одређивања сврхе и начина примене конкретне радње обраде. Тек након такве идентификације лица, могу се предузети радње или донети одлуке које производе правне последице по то лице, односно које утичу на положај лица.

Поступање полицијских службеника 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 недозвољеног профилисања.

Овакво дозвољено профилисање мора се вршити уз примену адекватних организационих мера заштите података као што су управљање корисничким налозима, софтверско генерисање налога за претрагу, двоструки приступ систему, ограничено чување шаблона биометријских података.

Обрада података може се вршити само уз примену и одговарајућих техничких мера заштите података као што су: 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.

Корисници овог система могу бити само оспособљени и едуковани полицијски службеници. Полицијски службеници морају бити едуковани о законским условима за профилисање као и начину примене полицијских овлашћења, мера и радњи, о утврђеним стандардима полицијског рада и о правном режиму заштите података о личности. Додатна мера заштите од ризика који настају при промени послова или престанка радног односа полицјских службеника је укидање налога за приступ систему се односно нивои приступа се морају ажурирати. Механизам утврђивања дисциплинске одговорности је истовремено превентивна и реактивна мера заштите података која се мора примењивати

Уз примену наведених мера за умањење ризка резидуални ризик је умањен али је и даље знатан и да би се контролисао неопходни су ефикасни механизми контроле изложености ризику.

Ниво утицаја повреда права и слободе лица је: претежно висок (4)
Ниво вероватноће повреда права и слободе лица је: претежно велика (4)
Изложеност ризику повреда права и слободе је: знатна (16)

- **<u>Биометријски подаци из евиденција за упоређивање нису тачни</u>**

Одабиром одређене похрањене фотографије са издвојеним биометријским податком у облику шаблона/дигиталног кода из те фотографије и постављањем упита ка софтверу за препознавање лица од стране овлашћеног полицијског службеника проверава се подударност са биометријским подацима из других евиденција који се за потребе тог поређења повезују са софтвером за препознавање лица. Такође, аутоматизовано (истовремено) упоређивање биометријских података у тренутку детекције лица и издвајања биометријских података, вршиће се повезивањем софтвера за препознавање лица са биометријским подацима који су похрањени у другим евиденцијама, које Министарство води у складу са законом (евиденције форензички регистрованих лица).
Ризик по слободе и права лица који може настати употребом софтвера за препознавање лица везује се за обраду биометријских података садржаних у евиденцијама који служе за упоређивање, а који нису тачни. Обрада таквих нетачних података довела би до погрешне идентификације, односно идентификације „погрешног“ лица. Оваква обрада би за последицу могла имати неосновано идентификовање лица односно неосновано поступање полицијских службеника према том лицу јер се за њега везују нетачни биометријски подаци из других евиденција, чиме би се повредило његово право на приватност и достојанство.

Ниво вероватноће повреде права и слобода лица одређен је обрадом нетачних података којом се могу угрозити право на приватност и достојанство лица чији се подаци обрађују. Могућнст да нису тачни биометријски подаци који су похрањени у евиденцијама Министарства се не може занемарити, пре свега из разлога што су биометријски подаци у претходном периоду прикупљани и обрађивани употребом другачије технологије. Такође постоје могућности да је например фотографија једног лица повезана са подацима другог лица јер је начињена грешка приликом ручног уноса података у евиденције (приликом преноса података из евиденција које су се раније водиле у папирној форми)

Ниво утицаја повреда права и слободе лица је: претежно низак (2)
Ниво вероватноће повреда права и слободе лица је: мала (1)
Изложеност ризику повреда права и слободе је: незнатна (2)

Контрола ризика врши се употребом предвиђених организационих и техничких мера.

Примена полицијских овлашћења, мера и радњи које укључују употребу софтвера за препознавање лица мора се вршити професионално и у складу са утврђеним стандардима полицијског рада што подразумева да полицијски службеник у случају очигледне нетачности податка мора извршити додатне провере пре доношења одлуке о даљем поступању према лицу које је софтвер препознао. Спровођењем континуриане едукације и контролно-инструктивнним делатностима омогућиће се и ефикасан механизам управљања подацима који подразумева начин вођења евиденција и увид у поступање полицијских службеника.

Поступање полицијских службеника приликом вођења евиденција мора бити засновано на организационој структури у систему подељених улога у погледу вршења појединачних радњи обраде, чиме је умањена могућност грешке односно нетачног или неажурног вођења евиденција што подразумева унос, ажурирање, измену или исправљање података садржаних у тим евиденцијама.

Применом одређених техничких мера заштите као што су: 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, такође се обезбеђује ефикасан механизам управљања подацима.

И код евентуалног настанака овог ризка се мора имати у виду је „човек“ карика која предствља највећу претњу за нетачно или неажурно вођење евиденција када је у питању ручни унос података. Међутим, не може се занемарити ни чињеница да није увек људска грешка или несавестан рад разлог нетачно унетих података у евиденције, јер постоји могућност да например подаци који су од другог руковаоца достављени министарству ради уноса у евидеције нису тачни или да је податак измењен приликом преноса. Применом ефикасних контролних механизама може се обезбедити висок ниво тачности података, те се и резидуални ризк може успешно контролисати односно остати на ниову незнатног.

Ниво утицаја повреда права и слободе лица је: претежно низак (2)
Ниво вероватноће повреда права и слободе лица је: мала (1)
Изложености ризику повреда права и слободе је: незнатна (2)

- **<u>Снимање лица у приватном простору</u>**

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.
Снимањем, похрањивањем и другим радњама обраде података о активности лица која се налазе у приватном простору може се угрозити право на приватност лица.
Лице оправдано очекује да су активности које предузима у приватном простору заштићене од погледа других људи;
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.
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.
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.

Ниво утицаја повреда права и слободе лица је: претежно низак (2)
Ниво вероватноће повреда права и слободе лица је: претежно мала (2)
Изложеност ризику повреда права и слободе је: незнатна (4)

Контрола ризика врши се употребом предвиђених организационих и техничких мера.

Уз периодично преиспитивање видног поља камера, као и спровођењем контролно-инструктивне делатности омогућен је увид у начин руковања камерама и поступања полицијских службеника Корисници система/камера су полицијски службеници који

морају бити оспособљени и едуковани за руковање камерама као и о законским условима и начину употребе система видео надзора односно софтвера за препознавање лица. Поступање полицијских службеника приликом руковања камерама засновано је на организационој структури у систему подељених улога.

Уз примену техничких мера заштите као што су :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 обезбеђује се ефикасан механизам управљања подациам.

Употреба софтера за препознавање лица у систему видео надзора јавног простора у урбаним (градским срединама) је додатни изазов за Министарство као руковаоца. Јер јавни простор који је предмет видео надозра подразумева и велики број стамбених, пословних и других објеката у којима лица бораве те је немогуће вршити видео надзор на начин да се не посматрају и ови објекти односно лица која у њима бораве. Пројектовање система видео надзора мора бити усклађено са постојећом или планирнаном инфраструктуром, али треба имати у виду да је готово немогуће да видео надзор не обухвати и одређене објекте који нису предмет надзора. Употребом одговарајућих филтера, видео надзор се може користити на начин да не угрожава приватност нечијег дома или пословног простора, односно на начин да не изазва нелагодност код грађана због бојазни да су предмет надзора док бораве у том простору. Применом адкватних мера заштите и механизама контроле њихове примене може се обезбедити да ниво резидуалног ризика буде низак до занемраљивог.

Ниво утицаја повреда права и слободе лица је: претежно низак (2)
Ниво вероватноће повреда права и слободе лица је: мали (1)
Изложеност ризику повреда права и слободе је: незнатна (2)

- Грешка софтвера

Постојање овог ризика везује се за чињеницу да се препознавање биометријских карактеристика не може посматрати као стопостотно тачна технологија, већ да се заснива на „подешавању нивоа осетљивости“ у односу на „лажне негативне“ и „лажне позитивне резултате“. Лажни резултати (негативни или позитивни) носе значајне ризике за појединца (лице може бити погрешно препознато/идентификовано као извршилац кривичног дела и обрнуто да систем за препознавање лица уопште не препозна извршиоца кривичног дела или се извршиоцу кривчног дела услед грешке софтвера обезбеђује алиби).

Вероватноћа грешке мора се посматрати у односу на околности употребе софтвера. Наиме, употребом софтвера за препознавање лица на местима која посећује велики број људи (аеродроми, стадиони, железничке станице и сл.) и мали процент грешке софтвера доводи до погрешне идентификације великог броја лица. Например грешка софтвера чији је процанат ефикасности 99 %, ипак укључује грешку од 1% што у односу на 100 000 људи чије податке ће софтвер обрађивати у току једног дана на аеродрому је чак 1000 погрешно идентификованих људи.

За разлику од ових условно речено „контролисаних окружења“, где је проценат грешке мали, свакако да проценат грешке софтвера расте када се користи на јавном простору

(на пример Трг Републике), где се услед различитих околности (ответљење, временске прилике, удаљеност камере, коришћење различитих средстава за избегавање видео надзора попут наочара за сунце, капе, шала или маске преко лица) повећава и ризик од грешке.

Тачност-поузданост софтвера за препознавње лица одређује се на основу податка произвођача али мора постојати и независно оцењивање уз периодично преиспитивање нивоа тачности.

Ниво утицаја грешке софтвера на повреде права на приватност и достојанство лица, одређен је применом полицијских овлашћења, мера и радњи којима се угрожавају права 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 потребне провере резултата упоређивања биометријских података повећава ризк повреде права на приватност и достојанство лица.

Ниво утицаја повреда права и слободе лица је: претежно висок (4)
Ниво вероватноће повреда права и слободе лица је: средњи (3)
Изложеност ризику повреда права и слободе је: умерен (12)

Контрола ризика врши се употребом предвиђених организационих и техничких мера. 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. 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 је превентивна и реактивна мера која у великој мери умањује овај ризик. Независно оцењивање и периодично преиспитивање нивоа тачности софтвера је неопходно како би се ценила његова поузданост.

Применом техничких и организационих мера као што су: контрола корисника, контрола приступа подацима, контрола чувања 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 обезбеђују се неопходни предуслови за употребу софтвера односно поуздану обраду података о личности.

Мора се имати у виду чињеница и да се упркос убрзаном развоју софтвера, развоју вештачке интелигенције и применом предвиђенх мера заштите резидуални ризик не може умањити и он ће остати на нивоу умереног.

Ниво утицаја повреда права и слободе лица је: претежно висок (4)
Ниво вероватноће повреда права и слободе лица је: средњи (3)
Изложеност ризику повреда права и слободе је: умерен (12)

- **<u>Ризик од приступања подацима од стране неовлашћених лица</u>**

Постојање овог ризика везује се за приступ/могућност приступа подацима од стране неовлашћених лица.

Различити нивои приступа одобравају се полицијским службенцима у односу на организациону структуру у систему подељених улога и то у погледу вршења појединачних радњи обраде. Ниво утицаја на повреде права на приватност и достојанство лица, одређен је употребом софтвера од стране овлашћених лица/овлашћених полицијских службеника, где ниво утицаја повреде права расте уколико постоји било каква могућност да неовлашћена лица приступају софтверу односно подацима који се обрађују његовом применом.

Ниво вероватноће повреде права на приватност и достојанство лица одређен је у односу на могућност приступа подацима од стране неовлашћених лица и то неовлашћеним приступом опреми или носачима података. Сама чињеница да таква могућност постоји изазива додатни осећај несигурности код грађана те се она применом мера заштите мора у потпуности елиминисати или макар свести на најмању могућу меру.

Ниво утицаја повреда права и слободе лица је: претежно висок (4)
Ниво вероватноће повреда права и слободе лица је: претежно мали (2)
Изложеност ризику повреда права и слободе је: допустив (8)

Контрола ризика врши се употребом предвиђених организационих и техничких мера.

Уређаји и опрема за аутоматску обраду података и носачи информација (ЦД, ДВД, екстерни хард дискови итд) на које су подаци у оквиру система снимљени морају бити обезбеђени, чувани у посебним просторијама које се закључавају, обезбеђене системом контроле приступа, видео-надзором, уз примеу мера заштите од пожара, поплава струјног удара и других инцидената, енкриптовани. Носачи информација се не смеју износити из просторија осим за јасно дефинисане потребе, као што је рецимо израда резевних копија или опоравак система из резервних копија. У случају инцидента морају се обезбедити интегритет података у оквиру система и обнова функционалности система, што се постиже редовном израдом резервних копија података (дневни, месечни, годишњи ниво) којима могу приступати само овлашћени запослени (систем администратори) и само у случају инцидента када је неопходно извршити опоравак система. Применом техничких и организационих мера као што су 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 као и чување шаблона биометријских података у року од 72 сата, обезеђује поуздан систем управљања

подацима. Поред наведених мера ризик се може контролистати и укидањем или ажурианьем права приступа при промени послова или престанка радног односа, као и континуираном едукцијом запослених у вези са извештавањем и реаговањем у случају инцидената.

Готово је немогуће у потпуности елиминисати ризик неовлашћеног приступа подацима али се ефикасном применом мера зашите резидуални ризик може значајно умањити.

Ниво утицаја повреда права и слободе лица је: претежно висок (4)
Ниво вероватноће повреда права и слободе лица је: мала (1)
Изложеност ризику повреда права и слободе је: незнатна (4)

- **<u>Ризик од злоупотреба које могу извршити овлашћена лица.</u>**

Постојање овог ризика односи се на могућности злоупотребе податка од стране овлашћених лица/полицијских службеника којима је одобрен приступ подацима. Злопотребе су могуће у тренутку прикупљања података или током њихове даље обраде (овлашћени полицијски службеник може иврши идентификцију лица без правог основа, односно искористити софтвер за препознавње лица у сврхе за које није намењен где је најчешће овај ризик мотивисан разлозима личне природе).

Овлашћени полицијски службеник може вршити увид у похрањене податке без правног основа или похрањене податке може издвојити, копирати и пренети неовлашћеном лицу ради даље употребе што може подразумевати и недопуштено објављивање података. Такође се овај ризик везује и за могућност да овлашћени полицијски службеник пропусти да додатно провери резултат подударности упоређених података који добија употребом софтвера услед чега може донети погрешну одлуку о предузимању других мера и радњи према лицу и на тај начин угрозити његова права.

Ниво утицаја повреда права и слободе лица је: претежно висок (4)
Ниво вероватноће повреда права и слободе лица је: средњи (3)
Изложености ризику повреда права и слободе је: умерен (12)

Контрола ризика врши се употребом предвиђених организационих и техничких мера.
Ради правилне употребе софтвера за препознавње лица и обраде података прикупљених системом видео надзора неопходно је обезбедити да се приликом сваког приступа снимљеном материјалу бележи дигитални запис о том приступу који би требало да садржи најмање следеће информације: име и презиме полицијског службеника, број службене легитимације или матични број полицијског службеника, ИД уређаја са кога је приступљено, податке о трајању сваке сесије, као и податке о активностима. Дигитални записи о приступу се трајно чувају у системском журналу.

Приликом приступања информационом систему, за све додељене корисничке налоге мора бити подешена додатна (двострука) аутентификација приликом приступа снимљеним материјалима, која би се остваривала нпр. путем службене легитимације.

Препорука је да се приликом приступа систему у просторије не уносе било какви уређаји са могућношћу снимања аудио или видео записа, као што су мобилни телефони, камере,

диктафони и слично као и да се ограничи могућност преноса података на носаче података (УСБ или ЦД)

Дефинисањем привилегија и рола за сваког полицијског службеника са овлашћењем да приступа снимљеном материјалу неопходно је утврдити одговарајући ниво приступа у складу са радним местом, тј. позицијом у оквиру организационе јединице. На пример, само одређени службеници (систем администратори) имају администраторски приступ информационом систему, који омогућава напредније опције попут креирања и брисања налога за друге службенике. Само одређени полицијски службеници могу добити улогу која им омогућава да прегледају снимке, без могућности преузимања, измене или брисања материјала, док други полицијски службеници имају могућност преузимања података. Свако преузимање података се евидентира уз означавање броја израђених копија, разлога изузимања и сл. Потребно је обезбедити да се софтверски дефинише одговарајући приступни захтев, како би приликом сваког приступа било евидентирано на основу ког захтева се поступа

Након престанка радног односа или премештаја на друго радно место у оквиру министарства, кориснички налози за приступ систему којима је истекло овлашћење морају бити деактивирани и архивирани, тј. мора бити онемогућен приступ систему са тих налога у најкраћем могућем року.

Уз примену ефикасних мера за умањење ризка мора се имати у виду чињеница да се „човек“ увек појављује као најслабија карика те могућност злоупотребе увек постоји а која увек за собом повлачи и одређене последице за лице на које се подаци односе али се ефикасном применом мера резидуални ризк може умањити да постане допустив.

Ниво утицаја повреда права и слободе лица је: претежно висок (4)
Ниво вероватноће повреда права и слободе лица је: претежно мали (2)
Изложености ризику повреда права и слободе је: допустива (8)

- **<u>Ризик од губитка, уништења или измене података или изостанак надзора</u>**

Постојање овог ризика везује се за губитак, уништење и измену података од стране овлашћених или неовлашћених лица. Постојање овог ризика везује се и за изостанак адекватног надзора и обавештавања и реакције у случају инцидената који могу довести до губитка измене или уништења података. Наступање ризика је могуће како у тренутку прикупљања података, тако и приликом њихове даље обраде. Овлашћени полицијски службеник може извршити измену или уништење података без правног основа (злоупотребом овлашћења или одобреног нивоа проступа). Неодговорно поступање са подацима доводи до губитка података (нпр. приликом преноса, транспорта носача података, неадекватно чување података такође доводи до губитка података)

Ниво утицаја повреда права и слободе лица је: претежно висок (4)
Ниво вероватноће повреда права и слободе лица је: претежно мали (2)
Изложености ризику повреда права и слободе је: допустива (8)

Контрола ризика врши се употребом предвиђених организационих и техничких мера.

Контрола носача података, контрола чувања података,, контрола приступа подацима, контрола преноса, контрола транспорта, системски журнал, заштита од злонамерног софтвера, обезбеђивање исправног и безбедног функционисања система, чување података о догађајима који могу бити од значаја за безбедност система, је неопходна ради успостављања ефикасног механизма управљања подацима.

Приликом сваког приступа подацима неопходно је бележити дигитални запис о том приступу (системски журнал). Приликом приступања информационом систему, за све додељене корисничке налоге мора бити подешена додатна/двострука аутентификација и дефинисање привилегија и рола за сваког полицијског службеника

Обрада података употребом система видео надзора мора се вршити професионално и у складу са утврђеним стандардима полицијског рада али је немогуће елиминисати ризик кад се има у виду да је овлашћено лице-полицијски службеник ипак само „човек“ који је као што је више пута већ констатовано најслабија карика и немогуће је допрети до свести сваког појединца, али се ефикасном применом превентивних и реактивних мера резидуални ризк може умањити.

Ефикасном применом наведених мера резидуални ризик може умањити да постане незнатан.

Ниво утицаја повреда права и слободе лица је: претежно висок (4)
Ниво вероватноће повреда права и слободе лица је: мали (1)
Изложености ризику повреда права и слободе је: незнатана (1)

- Недопуштено објављивање података

Постојање овог ризика односи се на могућности злоупотребе од стране овлашћених лица/полицијских службеника којима је одобрен приступ подацима. Злопотребе су могуће у тренутку прикупљања података или током њихове даље обраде (овлашћени полицијски службеник може извршити идентификцију лица без правог основа и податке пренети неовлашћеном примацу или накнадном обрадом похрањених података извршити њихово копирање и преношење неовлашћеном примаоцу, где је овај ризик најчешће мотивисан разлозима личне природе). Не искључује се могућност и да овлашћени полицијски службеник може вршити увид у похрањене податке и без правног основа издвојити, копирати и пренети неовлашћеном лицу самоиницијативно или на основу налога надређеног.
Мора се имати у виду да се ризик односи само на недопуштно објављивање података и и том смислу је неопходно направити јасну разлику од објављивања које је допуштено.

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.
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;

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.
Недопуштено објављивање података прикупљених видео надзором, путем медија, друштвених мрежа или коришћењем других средстава комуникације повредиће права и слободе лица чији се подаци обрађују.
Број евидентираних случајева недопуштеног објављивања података, од стране запослених у министарству, је мали.

Ниво утицаја повреда права и слободе лица је: претежно велик (4)
Ниво вероватноће повреда права и слободе лица је: претежно висок (4)
Изложеност ризику повреде права и слободе је: знатна (16)

Контрола ризика врши се употребом предвиђених организационих и техничких мера.

Ради правилне употребе софтвера за препознавње лица и обраде података прикупљених системом видое надзора неопходно је обезбедити да се приликом сваког приступа снимљеном материјалу бележи дигитални запис о том приступу који би требало да садржи најмање следеће информације: име и презиме полицијског службеника, број службене легитимације или матични број полицијског службеника, ИД уређаја са кога је приступљено, податке о трајању сваке сесије, као и податке о активностима. Дигитални записи о приступу се трајно чувају у системском журналу.

Приликом приступања информационом систему, за све додељене корисничке налоге мора бити подешена додатна (двострука) аутентификација приликом приступа снимљеним материјалима, која би се остваривала нпр. путем службене легитимације.

Препорука је да се приликом приступа систему у просторије не уносе било какви уређаји са могућношћу снимања аудио или видео записа, као што су мобилни телефони, камере, диктафони и слично као и да се ограничи могућност преноса података на носаче података (УСБ или ЦД)

Дефинисањем привилегија и рола за сваког полицијског службеника са овлашћењем да приступа снимљеном материјалу неопходно је утврдити одговарајући ниво приступа у складу са радним местом, тј. позицијом у оквиру организационе јединице. На пример, само одређени службеници (систем администратори) имају администраторски приступ информационом систему, који омогућава напредније опције попут креирања и брисања налога за друге службенике. Само одређени полицијски службеници могу добити улогу која им омогућава да прегледају снимке, без могућности преузимања, измене или брисања материјала, док други полицијски службеници имају могућност преузимања података. Свако преузимање података се мора евидентирати уз означавање броја израђених копија, разлоге изузимања и сл. Неопходно је обезбедити да се софтверски дефинише одговарајући приступни захтев, како би приликом сваког приступа било евидентирано на основу ког захтева се поступа. Након престанка радног односа или премештаја на друго радно место у оквиру министарства, кориснички налози за приступ систему морају бити деактивирани и архивирани, тј. мора бити онемогућен приступ систему са тих налога у најкраћем могућем року.

Мере заштите као што су 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, обезбеђују ефикасн и поуздан механизам управљања подацима.

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.

Уз примену ефикасних мера за умањење ризка мора се имати у виду чињеница да је и овде „човек“ најслабија карика те могућност злоупотребе у виду недопуштеног објављивања података увек постоји која као таква готово увек за собом повлачи и одређене последице за лице на које се подаци односе. Примена полицијских овлашћења, мера и радњи, употребом система видео надзора, врше се професионално и у складу са утврђеним стандардима полицијског рада а утврђивање дисциплинске одговорности и иницирање за утврђивање кривичне одговорности од стране надлежног органа такође су неопходни елементи ефикасног механизма управљања подацима којим се резидуални ризк може умањити до одређеног нивоа али ће остати умерен.

Ниво утицаја повреда права и слободе лица је: претежно велик (4)
Ниво вероватноће повреда права и слободе лица је: претежно висок (3)
Изложеност ризику повреде права и слободе је: умерена (12)

III ОПИС МЕРА И МЕХАНИЗАМА ЗАШТИТЕ У ОДНОСУ НА РИЗИК ПО ПРАВА И СЛОБОДЕ ЛИЦА - Мере заштите безбедности података и механизми заштите права 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.

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.

Примена 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.

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

Контрола приступа опреми, контрола корисника, контрола приступа подацима, системски журнал као техничке мере подразумевају да је приликом сваког приступа снимљеном материјалу,неопходно бележити дигитални запис о том приступу који би требало да садржи најмање следеће информације: име и презиме полицијског службеника, број службене легитимације или значке полицијског службеника, матични број, ИД уређаја са кога је приступљено, податке о трајању сесије, као и податке о активностима(све операције које су вршене, претраге које су рађене итд.). Дигитални записи о приступу (логови) се морају трајно чувати у системском журналу.

Обавезна двострука потврда идентитета (2ФА) подразумева да приликом приступања информационом систему, за све додељене корисничке налоге мора бити подешена додатна аутентификација приликом приступа снимљеним материјалима, која се остварује путем службене легитимације полицијског службеника-корисника система.

Контрола носача података, контрола чувања података, физичка и техничка заштита објеката и опреме, заштита од оштећења и крађе средстава која чине систем видео надзора као техничке мере заштите подразумева да уређаји и носачи информација (ЦД, ДВД, екстерни хард дискови итд) на које су подаци у оквиру система снимљени морају бити енкриптовани, чувани у посебним просторијама које се закључавају и које су обезбеђене заштитом од пожара, поплаве, струјног удара и других инцидената, као и видео-надзором. За приступ носачима информација неопходан је исти ниво приступа као за приступање информационом систему. Носачи информација се не смеју износити из просторија осим за јасно дефинисане потребе, као што је израда копија или опоравак система из резервних копија. Приликом приступа систему у просторије се не смеју уносити било какви уређаји са могућношћу снимања аудио или видео записа, као што су мобилни телефони, камере, диктафони итд.

Опоравак система и обезбеђивање интегритета система подразумева да се у случају инцидента морају обезбедити интегритет података у оквиру система и обнова функционалности система, што се постиже редовном израдом резервних копија података (дневни, месечни, годишњи ниво) којима могу приступати само овлашћени запослени

(систем администратори) и само у случају инцидента када је неопходно извршити опоравак система. Резервне копије података морају бити заштићене савременим енкрипционим стандардима

Унапређење софтвера подразуемва редовно ажурирање софтвера ради побољшања перформанси система и применом вештачке интелигенције (машинско учење)

ОРГАНИЗАЦИОНЕ МЕРЕ ЗАШТИТЕ

Управљањекорисничкимналозима подразумева дефинисање привилегија и рола за сваког полицијскогслужбеника са овлашћењем да приступаснимљеном материјалу и неопходно је утврдити/прописати одговарајући ниво приступа у складу са радним местом, тј. позицијом у оквиру организационе јединице. На пример, само одређени службеници (систем администратори) би требало да имајуадминистраторски приступ информационом систему, који омогућава напредније опције попут креирањаи брисања налога за друге службенике, док осталимогу добити улогу која им омогућава да само прегледају снимке, односно налоге без могућности преузимања, измене или брисања материјала. Надређеним службеницима се мора омогућити софтверско генерисање корисничких налога за претрагу или креирање налога за претрагу.

Софтверско генерисање налога за претрагу подразумева софтверски дефинисан приступни захтев, како би приликом сваког приступа било видљиво/јасно на основу ког/чијег захтева/налога се поступа.

Мере заштите од ризика који настају при промени послова или престанка радног односа подаразумевају да након престанка радног односа или премештаја на друго радно место у оквиру МУП, кориснички налози за приступ систему којима је истекло овлашћење морају бити деактивирани и архивирани, тј.мора бити онемогућен приступ систему са тих налога у најкраћем могућем року

Мере ограниченог чувања шаблона биометријских података подразумевају софтверско решење да се шаблони биометријских података насталих употребом система чувају 72 сата од тренутка издвајања шаблона, односно након тог рока се бришу.

Систем подељених улога у обради података о личности подразумева да један полицијски службеник не може самостално, без учешћа других овлашћених службених лица, да предузме радње обраде података које би довеле до идентификације лица, чиме се у великој мери смањује могућност злоупотребе и вероватноћа наступања ризика. Прикупљање података обавља лице које је распоређено у оквиру једне организационе јединице, а даљу обраду и коришћење података врше друга службена лица која су распоређена у више различитих организационих јединица. Систем подељених улога као организациона мера приказана у талбели подразумева да систем видео надзора буде 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 злоупотребе 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 организационе јединице надлежне 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.

Информисање грађана подразумева да се лицима се поред информисања мора омогућити и конкретно остваривање права у вези са обрадом података о личности (право на увид, копију, брисање или друга права у скаду са законом). Информисање мора да садржи и обавештавање о начину остваривања права код руковаоца (нпр. подношењем захтева Министарству унутрашњих послова територијално надлежној полицијској управи, по месту локације камера

Дисциплинованост и савесност полицијских службеника Законито и професионално поступање полицијских службеника у примени видео надзора обезбеђује се применом проактивних и реактивних мера заштите којима се подиже ниво свести о неопходности

заштите безбедности података и поштовања права и слобода лица, што у највећој мери умањује вероватноћу наступања ризика. Превентивне мере 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. 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.

Механизми заштите права лица Свако лице чије податке обрађује Министарство, може 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 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.