ПРОЦЕНА УТИЦАЈА НАМЕРАВАНИХ РАДЊИ ОБРАДЕ БИОМЕТРИЈСКИХ ПОДАТКА О ЛИЧНОСТИ НА ЗАШТИТУ ПОДАТАКА О ЛИЧНОСТИ

I ОПИС ОБРАДЕ ПОДАТАКА

На основу Закона о полицији („Службени гласник РС”, бр. 6/16, 24/18 и 87/18), полиција врши надзор и снимање јавног места и врши обраду података о личности у складу са Законом о евиденцијама и обради података у области унутрашњих послова („Службени гласник РС”, бр. 24/18).

У претходном периоду Министарство унутрашњих послова (у даљем тексту: Министарство) је на основу израђеног профила безбедносног проблема[1] односно на основу процене безбедносно интересантних догађаја, применом полицијско-обавештајног модела, определило локације и поставило камере за снимање на јавном месту. Такође, у циљу унапређења стања јавне безбедности, пратећи развој савремених информационих технологија, у Министарству је у току увођење и eLTE технологије, односно савремених радио станица последње генерације опремљених видео камерама, која функционише у оквиру 4Г мреже на *андроид* платформи. Поред тога, један број „полицијских“ возила је опремљен камерама за „видео надзор у покрету“, а у плану је и опремање једног броја полицијских службеника камерама које се носе на униформи.

Такође, полиција има увид и у видео записе који настају вршењем послова приватног обезбеђења. Наиме, према одредбама чл. 32. Закона о приватном обезбеђењу („Службени гласник РС”, бр. 104/13, 42/15 и 87/18) када се послови заштите објекта или простора који се користе за јавну употребу врше уз употребу уређаја за снимање слике, корисник услуга је обавезан да архивиране снимке, стави на увид овлашћеном полицијском службенику.

На основу доступних видео записа или фотографија без обраде биометријских података Министарство врши идентификацију лица: препознавањем од стране полицијског службеника у току снимања или накнадним прегледом снимљеног материјала, такође препознавањем од стране полицијског службеника или другог лица коме је ради идентификације лица са снимака или фотографије, омогућен увид у видео запис у складу са законом.

Полицијски службеници приликом овакавог начина идентификације лица, морају да изврше анализу видео надзора да би утврдили локације камера односно објеката на којима постоји видео надзор и које су све камере могле да забележе извршење кривичног дела или учиниоца кривичног дела, време извршења кривичног дела, време непосредно пре и након извршења кривичног дела. Након овакве анализе полицијски службеници врше преглед снимљеног материјала, издвајају одређене сегменте видео записа ради њихове репродукције, а све у циљу идентификације одређеног лица са видео записа.

[1] 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.

Код оваквог начина идентификације лица, неопходно је додатно ангажовање полицијских службеника који морају да прегледају целокупан видео материјал, односно видео записе чије трајање често може да траје неколико десетина или стотина сати. С тим у вези, намера Министарства је да унапреди могућности претраживања, односно обраде видео записа или фотографија, уз могућност да се идентификација лица из видео записа или фотографија врши обрадом биометријских података о личности. Оваква обрада видео записа или фотографија, ради издвајања биометријских података и њиховог поређења са биометријским подацима које Министарство већ обрађује у другим евиденцијама би полицијским службеницима омогућила знатно бржу идентифиакцију лица са видео записа или фотографије.

Код оваквог начина обраде биометријских података о личности, мора се имати у виду да се према одредбама Закона о заштити података о личности („Сл.гласник РС",87/2018) ради о посебној врсти података о личности, чија је обрада у циљу јединствене идентфикације лица од стране надлежних органа у „посебне сврхе“[2] допуштена ако је то неопходно уз примену одговарајућих мера заштите права лица на које се подаци односе, у случајевима када:

1) је надлежни орган законом овлашћен да обрађује посебне врсте података о личности;
2) се обрада посебних врста података о личности врши у циљу заштите животно важних интереса лица на које се подаци односе или другог физичког лица;
3) се обрада односи на посебне врсте података о личности које је лице на које се они односе очигледно учинило доступним јавности.

Дакле, неопходно је законско овлашћење Министарства, као основни предуслов за обраду биометријских података у посебне сврхе. С тим у вези, код овакве намераване обраде података, неопходно је размотрити законски оквир за обраду биометријских података.

Сва питања која се односе на законитост обраде биометријских података о личности од стране Министарства као надлежног органа у смислу члана. 4. тачка 26) Закона о заштити података о личности, морају се разматрити у контексту члана 8. Европске конвенције о људским правима (Конвенција) којом се јемчи право на поштовање приватног и породичног живота (право на приватност).

Право на поштовање приватног и породичног живота, припада групи такозваних релативних (квалификованих) права и слобода, за које су прописана легитимна ограничења у њиховом остваривању: а) у интересу националне безбедности; б) у интересу јавне безбедности или економске добробити земље; ц) ради спречавања нереда или криминала; д) ради заштите здравља или морала, или е) ради заштите права и слобода других (чл. 8. ст. 2. Конвенције)[3].

[2] Обрада података коју врше надлежни органи у сврхе спречавања, истраге и откривања кривичних дела, гоњења учинилаца кривичних дела или извршења кривичних санкција, укључујући спречавање и заштиту од претњи јавној и националној безбедности

[3] Чл. 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.

С тим у вези, у складу са начелима обраде података о личности прокламованих Законом о заштити података о личности, обрада биометријских података подразумевала би обраду података о личности у складу са законским овлашћењима полиције и то обраду података само оних лица чији подаци су неопходни за утврђивање идентитета лица у односу на конкретну сврху обраде, без непотребног задржавања (похрањива или архивирања) тих података.

У складу са одредбама Закона о заштити података о личности, Министарство би имало улогу руковаоца који самостално, ангажовањем сопствених ресурса, обрађује податке о личности уз примену адекватних мера заштите и механизама контроле свих радњи обраде. Прималац односно корисник ових података би могао бити само други надлежни орган и такви подаци би се могли пренети примаоцу у другој држави, односно међународној организацији, у складу са законом али само ако се ради о надлежном органу за обраду података у посебне сврхе.

II ПРОЦЕНА НЕОПХОДНОСТИ И СРАЗМЕРНОСТИ

Режим заштите обраде података о личности коју јемчи члан 8. Конвенције, се посматра и у контексту члана 17. Конвенције, којим се забрањује злоупотреба права. Наиме, чл. 17. прописује да се ниједна одредба Конвенције не може тумачити тако да подразумева право било које државе или лица, да се „упусте у неку делатност или изврше неки чин усмерен на поништавање било ког од наведених права и слобода или на њихово ограничавање у већој мери од оне која је предвиђена Конвенцијом“.

Такође, поред законског оквира у погледу обраде биометријских података о личности у посебне сврхе, узимају се у обзир и чињенице да обрада ове врсте података не може бити оправдана по сваку цену односно без пажљивог балансирања потенцијалне користи од њиховог коришћења и легитимног интереса појединца за заштитом његове приватности.

У складу са важећим Законом о полицији, идентификација лица коришћњем система видео надзора без обраде биометријских података врши се увидом у видео запис или фотографију и то непосредним препознавањем од стране овлашћеног полицијског службеника или од стране другог лица (оштећеног/жртве кривчног дела или сведока).

С тим у вези треба истаћи да је протеклих 5 година, на подручју 26 подручних полицијских управа, извршено укупно 7 убистава, од којих су 4 квалификована као тешка убиства, чије извршење или учиниоце тих дела су забележиле камере видео надзора, а која још увек нису расветљена. Полицијски службеници Одељења криминалистичке полиције подручних полицијских управа по налогу надлежног тужилаштва, односно по наредби суда, су предузимали све законом прописане мере и радње из своје надлежности, односно исцрпели су све расположиве ресурсе али учиниоци наведених кривичних дела нису идентификовани.

Анализом предузетих радњи и примењених овлашћења од стране полицијских службеника у вези са идентификовањем учиниоца само два кривична дело убиства која су 2017 године, извршена у Србији, може се оценити неопходност намераване

обраде биометријских подтака о личности у циљу унапређења ефикасности идентификације лица.

Наиме, кривично дело убиства које је 2017. године, извршено у централној Србији забележено је камерама видео надзора са објекта на којем су камере инсталиране као мера техничке заштите у складу са Законом о приватном обезбеђењу. Прегледом око 1000 сати видео записа са укупно 17 објеката, полицијски службенци нису успели да идентификују учиниоца овог кривичног дела.

Друго кривично дело убиства извршено 2017. године на југу Србије је такође забележено сигурносним камерама, али полицијски службеници прегледом више стотина сати видео записа са сигурносних камера са око 20 објеката, такође нису успели да идентификују учиниоца.

Поред прегледа видео записа, а у циљу идентификације учиниоца само ова два кривична дела, полицијски службеници су предузели низ полицијских мера и радњи и применили полицијска овлашћења према великом броју грађана, али још увек нису успели да идентификују учиниоца. Наиме, полицијски службеници су извршили:

- 60 претреса станова и других просторија,
- 64 полиграфска тестирања,
- 55 вештачења (балистичка, ДНК вештачења, запаљених возила и сл),
- 1809 анализа оствареног телекомуникационог саобраћаја са базних станица,
- сачилни 291 службену белешку о обавештењу примљеном од грађана,
- прегледали више од 80 снимака видео надзора са сигурносних камера чије трајање је дуже од 1000 сати.

Неопходност обраде биометријских података може се приказати и кроз друге видове идентификације лица од стране полицијских службеника, на пример, анализом коришћења „Ванредних обавешења“. Наиме поред прегледа видео записа или фотографија, полиција у свом раду у циљу идентификације лица користи и ванредна обавештења (распис) која се у папирној форми достављају свим подручним полицијским управама ради упознавања свих полицијских службеника који раде на терену како би помогли у идентификацији лица. Ова обавештења садрже кратку информацију о кривичним делу и фотографије лица које треба идентификовати. Такође, оваква обавештења се неретко јавно објављују и преко медија или других средстава јавног обавештавња, ради прикупљања информација о евентуалним сазнањима која полицији могу помоћи у идентификацији лица. На исти начин се поступа и у ситуацијама када полиција у циљу идентификације лица користи „фото-робот“ односно цртеж који је сачињен на основу описа лица од стране оштећених или других сведока.

Током претходне три године, Служба за сузбијање криминала, Управе криминалистичке полиције и подручне полицијске управе расписале су укупно 234 ванредних обавештења где је идентификовано само 35 лица (14,96%). Само на територији Полицијске управе за град Београд је у 2021. године расписно 25 ванредних обавештења, а току 2022. године, 21 обавештење.

Прегледом снимака или фотографија, у неким случајевима учиниоци кривичних дела се могу идентификовати на основу регистарских ознака возила. Идентификација лица на овај начин подразумева позивање свих власника или

корисника возила чије регистарске ознаке се могу видети на видео запису или фотографији као и обављање разговора са њима ради утврђивања релевантних чињеница које можда могу довести до идентификације учиниоца кривичног дела. Међутим, отежавајућа околност у већем броју случајева је чињеница да учиниоци кривичних дела на отвореном простору не користе возила или у случајевима да их користе они често прекрију или уклоне регистарске ознаке возила или за извршење кривичног дела користе украдена возила или регистарске таблице.

Применом других полицијских овлашћења, мера и радњи, што укључује и коришћење односно анализу података о оствареном телекомуникационом саобраћају, могуће је у одређеним случајевима идентификовати учиниоца кривичних дела. Међутим, и овде треба имати у виду чињеницу да учиниоци кривичних дела углавном користе „припејд“ СИМ картице за краткотрајну употребу или уопште не користе мобилне телефоне јер су свесни чињенице да се преко њих могу идентификовати.

Чињеница је и да учиниоци кривичних дела све чешће за међусобну комуникацију користе нове технологије, посебне апликације или специјализоване криптоване телефоне[4], како би онемогућили или знатно отежали идентификацију од стране полицијских службеника, те је неопходно да и полиција у свом раду користи модерне технологије и да, ако вероватно не може да буде испред, онда је нужно да у погледу употребе модерних технологија буде на бар приближно истом нивоу са криминалним структурама.

Стратешки циљ Владе Републике Србије и Министарства јесте изградња савремене, ефикасне, функционалне и високо професионализоване полиције која доприноси безбедности Републике Србије, ужива поверење свих њених грађана и представља поузданог партнера у међународној полицијској сарадњи.

Задаци Министарства су превасходно усмерени на смањење стопе криминала, ефикасније, ефективније и економичније обављање полицијских послова, законито и морално поступање полицијских службеника, поштовање људских права и повећање осећаја сигурности грађана Републике Србије.

Стратешком проценом јавне безбедности Министарства унутрашњих послова (2022-2025)[5]. дефинисани су приоритети рада Министарства где је, поред супротстављања организованом криминалу и корупцији као највећим безбедносним претњама и ризицима, један од кључних приоритета истакнуто супротстављање „уличном криминалу“ односно спречавање кривичних дела која се врше на јавном простору.

Током 2021. године само на територији града Београда извршено је укупно 7.457 кривичних дела на јавном простору (*улични криминал*). У истом временском периоду расветљено је 2.606 кривичнх дела (34.94%).

[4] криптовани мобилни телефон „Anonimus“, чија цена се креће око 2.000 евра за период коришћења од шест месеци

[5] http://www.mup.gov.rs/wps/wcm/connect/98632591-2b0d-4cba-9cd1-e7ff993705a6/Strateska+procena+javne+bezbednosti+MUP.pdf?MOD=AJPERES&CVID=nYH6yro

Имајући у виду све наведено, неопходно ја да полиција има могућност да обрадом биометријских података о личности брже и једноставније идентификације учиниоце кривичних дела. Свако задирање у основна права и слободе лица које би оваква обрада података могла да изазове, било би сразмерно и пропорционално интересу националне, односно јавне безбедности, имајући у виду да је пре свега усмерено на спречавање, истрагу и откривања кривичних дела, гоњење учинилаца кривичних дела укључујући заштиту права и слобода других.

Евентуално задирање у право на приватан живот, односно слободу удруживања, окупљања, мишљења и изражавања, права на миран протест, слободу кретања, слободе мисли, савести, уверења и вероисповести, забране дискриминације, обрадом биометријских података о личности као посебне врсте података које би се издвојиле из видео записа или фотографија, сразмерно је циљу заштите интереса јавне и националне безбедности, спречавања нереда (јавни ред и мир) или криминала као и заштити права и слобода других и у складу је са чл. 8 ст. 2. Европске конвенције о људским правима.

Имајући у виду да је законски оквир основни/кључни предуслов за обраду биометријских података о личности, и да други закони који се примењују у Републици Србији не уређују обраду биометријских података у сврху „идентификације лица“, од стране Министарства покренута је процедура за доношење новог закона о унутрашњим пословима којим би се поред осталог уредила и обрада биометријских података као посебно овалашћење полиције. Након консултација са заменицима тужиоца Вишег јавног тужилаштва у Београду и судијама за претходни поступак Вишег суда у Београду, закључено је да је неопходно успоставити правни оквир за примену овлашћења полиције да у складу са одредбама закона којим се уређује кривични поступак изврши претраживање видео записа и фотографија ради издвајања биометријских карактеристика лика и њиховог поређења са подацима који се у посебне сврхе обрађују у складу са законом. С тим у вези, треба размотрити и неопходност измене Законика о кривичном поступку у погледу овлашћења полиције.

Министарство од децембра 2021. године води друштвени дијалог са представницима цивилног друштва у који је, у одређеној мери, укључен и Повереник за информације од јавног значаја и заштиту података о личности. Током овог дијалога у одређеној мери размотрен је *Предлог Уредбе Европског парламента и Савета о утврђивању једнообразних правила за вештачку интелигенцијју и изменама одређених прописа Уније,* којим су поред осталог дефинисани и различити системи вештачке интелигенције са опцијом биометријске иденетификације: 1) систем за биометријску категоризацију, 1) систем за даљинску биометријску идентификацију, 3) систем за даљинску биометријску идентификацију у стварном времену (уживо) и 4) систем за накнадну биометријску идентификацију на даљину.

Размотрене су и препоруке *Европског одбора за заштиту података о личности, за обраду биометријских података од значаја за обраду путем видео надзора са опцијом препознавања лица* као и бројне примедбе и сугестије цивилног друштва у вези са ризицима и вероватноћом утицаја на права и слободе грађана.

III ПОДАЦИ О ЛИЧНОСТИ КОЈИ СЕ ОБРАЂУЈУ

Употребом видео надзора који Министрство тренутно користи, обрађују се следећи подаци о личности: видео запис лица и догађаја у којем лице учествује, време и место настанка видео записа, локација камере, регистарске и друге ознаке возила.

Намера Министарства је да употребом одговарајућег софтверског решења врши накнадну обраду односно претраживање видео записа или фотографија издвајањем биометријских карактеристика лика, ради њиховог поређења са подацима који се у посебне сврхе обрађују у складу са законом.

IV РАДЊЕ ОБРАДЕ

Обрада података употребом система видео надзора подразумева следеће радње обраде: прикупљање, разврставање, претраживање, издвајање упоређивање, увид, преношење, ограничавање, чување и брисање односно уништавање на други начин.

Видео записи са камера се у складу са законом похрањују на чврсту меморију - хард дискови централног система за складиштење података (*datacentar*) и чувају најмање 30 дана. Намера Министарства је, да се у складу са новим Законом о обради података у области унутрашњих послова, ови подаци на централном систему за складиштење података чувају најмање тридесет дана, а најдуже годину дана, по систему кружног снимања.

Приликом складиштења на централном систему, видео записи се аутоматски генеришу и разврставају по времену настанка видео записа и по месту снимања/локација камере.

Увид у видео запис (податке који се обрађују) у реалном времену у току снимања (*live stream*), омогућен је овлашћеном полицијском службенику[6] непосредним посматрањем, у корисничком центру. Увид у видео запис могуће је извршити претраживањем и издвајањем одабраног видео записа и његовом репродукцијом на радној станици[7].

Претраживање похрањених видео записа ради њиховог издвајања врши се према неком од критеријума као што су: локација односно назив камере/камерног места, датум и време настанка видео записа, али је могуће и према регистарској или другој ознаци возила употребом камера за препознавање регистарских ознака.

---

[6] 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 и обраду видео записа. Ови полицијски службеници су едуковани и одобрена су им разуличита права приступа..Немају сви полицијски службеници исти ниво приступа. Под овлашћеним полицијским службеником се такође подразумева и поступајући полицијски службеник (у конкретном случају задужен за поступање).

[7] Радна станица се за потребе израде овог документа посматра као посебан рачунар који је смештен у издвојену просторију ван корисничког центра и која је обезбеђена посебним мерама физичкок техничке заштите. Улазак и боравак у просторију као и приступ овом рачунару омогућен је само одређени полицијским службеницима са посебним одобрењем.

Претраживање и увид у похрањене видео записе омогућено је само полицијским службеницима са посебном дозволом односно одобрењем и то у корисником центру или на радној станици ван корисничког центра. Ово претраживање и вршење увида ограничено је на сврху и циљеве прикупљања података, а њихова даља обрада врши се у складу са законом односно овлашћењима полицијских службеника.

Видео записи или фотографије се у сврху прописану законом могу пренети копирањем на носач података (цд/двд или екстерни хард диск) ако је то потребно ради вршења увида или других радњи обраде ван корисничког центра. Фотографије издвојене из сегмента видео записа се осим копирања и преношења на други носач података могу копирати/умножавати и штампањем на папиру (ако је то потребно на пример ради креирања ванредног обавештења).

Након умножавања/копирања издвојеног видео записа или фотографија, они се у складу са законом чувају у другим евиденцијама Министарства и даље се обрађују у зависности конкретне сврхе обраде. Копије се, у појединачним случајевима, могу пренети овлашћеним примаоцима као што су други надлежни органи (тужилаштво, суд) или лице на које се подаци односе и то достављањем на носачу података.

У систему видео надзора који Министарство тренутно користи, идентификација лица врши се непосредно од стране полицијског сужбеника и то претраживањем и вршењем увида у похрањене видео записе или издвајањем одређеног сегмента видео записа ради његове репродукције на радној станици ван корисничког центра.

Намеравана радња обраде биометријских података употребом посебног софтверског решења вршила би се у случајевима када непосредним увидом у видео запис од стране полицијског службеника, није могуће идентификовти лице те је неопходно да се претраживањем похрањеног видео записа или фотографија издвоје биометријски подаци (биометријске каракеристике лика) ради њиховог поређења са расположивим биометријским подацима које Министарство у посебне сврхе обрађује у складу са законом. Код овакве обраде биометријских података, потребно је да радна станица на којој се врши обрада видео записа или фотографија, буде повезана са одређеном евиденцијом у којој се налазе биометријски подаци, а које Министарство у посебне сврхе обрађује у складу са законом (“ форензички регистрована лица“).

Обрада биометријских података о личности на овај начин подразумевала би обраду похрањених видео записа која би била ограничена, односно трајала би само током поређења. Обрада података односила би се само на лица из одређеног видео записа, само са одређених камера, а који су сачињени у одређеном временском периоду. Биометријски подаци би се поредили само са подацима одређене групе лица (форензички регистрована лица).

Уколко би софтвер пронашао подударне биометријске податке, на радној станици би се креирао извештај који би требало да садржи податке лица чији су биометријски подаци најприближнији биометријским подацима из обрађеног видео записа са исказаним степеном подударности или би се приказао извештај да нема подударних података. Овакав извештај би се доставио поступајућем полицијском службенику који би даље предузимао друге неопходне активности ради проналаска лица са видео записа или фотографије. Дакле поступајући полицијски службеник

би доносио одлуку о предузимању других радњи, односно примени других полицијских овлашћења у циљу проналаска лица, јер се идентитет лице не може потврдити само на основу софтверског резултата поређења.

Извештај о резултату поређења би требало да садржи и следеће податке о личности: број и датум наредбе и назив суда, број извештаја, име и презиме полицијског службеника и назив организационе јединице у којој он ради, јединствену ознаку радне станице на којој је вршена обрада видео записа или фотографије, датум и време обраде, јединствену ознаку видео записа или фотографије који су обрађени, фотографију, име и презиме, деловодни број и назив евиденције у којој су евидентирана лица чије биометријске карактеристике лика су подударне са биометријским карактеристикама лика издвојених из обрађеног видео записа или фотографије.

Издвојени биометријски подаци из обрађеног видео записа или фотографије се након поређења не би чували, а резултат поређења би се креирао на радној станици. У случају потребе за поновним поређењем биометријских података цео поступак би требало поновити.

Системски журнал треба да бележи датум и време издвајања и обраде видео записа, ознаку видео записа, информације о кориснику радне станице и приступ подацима свих лица из евиденције чији су подаци најприближнији биометријским подацима лица из обрађеног видео записа.

V ПРОЦЕНА РИЗИКА ПО ПРАВА И СЛОБОДЕ ЛИЦА

Разматрајући различите системе вештачке интелигенције које препознаје *Предлог Уредбе Европског парламента и Савета о утврђивању једнообразних правила за вештачку интелигенцијју и изменама одређених прописа Уније,* Министарство налази да би употреба софтвера за „накнадну биометријску идентификацију“, била најприхватљивија, пре свега имајући у виду надлежности и овлашћења за обраду података о личности и сврхе обраде података о личности од стране Министарства с једне стране, односно потенцијалне ризике које таква обрада може имати на зајемчена права и слободе лица као и очување демократског карактера друштва, с друге стране.

Законитост употребе софтвера, уз чију помоћ би се могла вршити „накнадна идентификација“ од стране Министарства, може се посматрати кроз неколико кумулативних елемената:

(а) природа случаја који оправдава употребу софтвера, а нарочито тежина кривичног дела, вероватноћа и обим штете и последица које би настале некоришћењем система;
(б) последице његове употребе на права и слободе свих лица чији подаци би се обрађивали а посебно тежина, вероватноћа и обим тих последица.
(в) остваривање уско дефинисаних законитих циљева (проналазак лица за које постоје основи сумње да је учинило кривично дело за које се гони по службеној дужности), мора бити у складу с неопходним и сразмерним заштитним мерама и условима коришћења, нарочито када је реч о временским и просторним ограничењима за коришћење.

У оквиру овако дефинисаних услова Министарство налази да је за сваку појединачну употребу софтвера неопходно претходно одобрење-наредба надлежног суда односно судије за претходни поступак, а које се издаје на образложен предлог надлежног тужиоца, као и да је у конкретном случају употреба софтвера нужна и сразмерна за постизање прописаних легитимних циљева.

Након анализе описаних радњи обраде података, непходности, сразмерности односно оправданости евентуалне употребе оваквог софтвера, идентификовани су и оцењени ризици по права и слободе лица, до којих може довести обрада биометријских података о личности. Дефинисане су мере за контролу и смањење ризика након чега је оцењен резидуални ризик, а 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.

Степен угрожености/ озбиљност последица	Висок	5	10	15	20	25
	Претежно висок	4	8	12	16	20
	Средњи	3	6	9	12	15
	Претежно низак	2	4	6	8	10
	Низак	1	2	3	4	5
Процена ризика		Мала	Претежно мала	средња	Претежно велика	велика
		Вероватноћа остваривања претње				

1-3…..**НЕЗНАТНА** (не захтева се никаква активност)
4-6…. **ДОПУСТИВА** (нема потребе за додатним активностима, потребно је пратити ситуацију)
7-11…**УМЕРЕНА** (потребно је у наређеном периоду планирати и друге мере, пратити поједине активности и дефинисати начин контроле)
12-15 **ЗНАТНА** (потребни су ефикасни механизми контроле примене мера за смањења ризика)
16-25. **НЕДОПУСТИВА** (обраду података не би требало вршити док се ризик не умањи)

ПРЕПОЗНАТИ РИЗИЦИ:

1. **<u>Обрада података неодређеног броја лица</u>**

Овај ризик код употребе система видео везује се за прикупљање и чување података неодређеног броја лица односно свих лица која се затекну у зони снимања, а чији подаци се могу обрађивати накнадном обрадом видео записа.

Такође, оваквом обрадом података није могуће направити неопходну разлику између појединих врста лица (чл. 9. Закона о заштити података о личности)

односно систем видео надзора прикупља податке сваког лица које се затекне у зони снимања.

Овакав начин обраде 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.

Приликом вршења надзора на јавном простору уз могућност накнадне идентификације, код лица се ствара осећај да су подвргнути константном надзору, а да притом нису ни сигурни да ли је стварно тако, односно да ли ће и када односно у којим све околностима бити идентификовани од стране полиције. 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 видео надзора 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 система немогуће је на јавном простору „заштити“ посебно осетљиве групе лица као што су на пример деца. Оваква неселективна употреба система за надзор на јавном простору где сва лица која се затекну на одређеном простору могу бити предмет обраде односно накнадне идентификације, поред поменутих права угрожава и право на претпоставку невиности.

Степен угрожености/озбиљност последица:висок (5)
Вероватноћа остваривања претње:средњи (4)
Изложеност ризику повреда права и слободе је: недопустива (20)

Умањење овог ризика могуће је пре свега применом законских ограничења и ефикасном контролом, управљањем ризиком, применом организационих и техничких мера заштите.

Наиме, на основу Закона о полицији Министарство врши надзор и снимање јавног места, ради обављања полицијских послова, коришћењем опреме за видео акустичке снимке и фотографисање и врши обраду података о личности у складу са Законом о евиденцијама и обради података у области унутрашњих послова. Правилником о начину снимања на јавном месту и начину саопштавања намере о том снимању („Сл. гласник РС“, број 111/20) предвиђено је да ће Министарство путем медија, других средстава јавног обавештавања (средство јавног информисања, интернет презентације и сл.) обавестити јавност, а самим тим и сва лица која могу бити обухваћена видео надзором.

Министарство је на основу израђеног профила безбедносног проблема односно на основу процене безбедносно интересантних догађаја, применом полицијско-обавештајног модела определило локације камера за снимање на јавном месту, а обрада биометријских података вршила би се накнадном обрадом видео записа и фотографија и то само када је таква обрада неопходна у циљу проналаска лица за које постоје основи сумње да је учинило кривично дело за које се гони по

службеној дужности, само уколико применом других полицијских овлашћења није извршена идентификација лица и то на основу наредбе судије за претходни поступак, а на предлог надлежног тужиоца.

Обрада биометријских података о личности на овај начин подразумевала би обраду похрањених видео записа која би била ограничена односно трајала би само током поређења. Обрада података односила би се само на одређене лица из одређеног видео записа, само са одређених камера, у одређеном временском периоду, а биометријски подаци би се поредили само са подацима одређених лица које ово Министарство обрађује у посебне сврхе.

Обрада биометријских података врши се само у току поређења, дакле без задржавања (чувања) биометријских података, а резултат подударности биометријских података усмеравао би полицијске службенике на друге активности односно примену других мера и радњи у циљу проналаска лица и провере односно утврђивање његовог идентитета. Дакле ни једно лице се не идентификује аутоматски, односно не примењује се тзв.аутоматско препознавање лица, већ је у сваком конкретном случају неопходна улога полицијског службеника.

Обраду биометријских података из похрањеног видео записа и њихово упоређивање врши само овлашћени полицијски службеник по посебној дозволи односно одобрењу. Поступање свих полицијских службеника код обраде биометријских података 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 конкретну сврху обраде података.

Корисници података су само полицијски службеници који морају бити едуковани о законским условима и начину примене полицијских овлашћења, о утврђеним стандардима полицијског рада и о правном режиму заштите података о личности. Сви додељени налози за приступ систему се при промени послова или престанка радног односа укидају, односно нивои приступа се ажурирају. Дакле, постоје ограничења у погледу лица чији подаци се обрађују као и свхе обраде, ограничења чувања и преноса. Такође успостављен је и механизам контроле обраде података и примењених мера заштите. Сваки приступ систему се аутоматски бележи (системски журнал).

Применом организационих и техничких мера и ефикасним механизмима контроле обраде података, може се ефикасно управљати ризиком те се резидуални ризик односно изложеност ризику повреде права и слободе може ефикасно контролисати и умањити.

Степен угрожености/озбиљност последица:висок(5)
Вероватноћа остваривања претње:претежно мала(2)
Изложеност ризику повреда права и слободе је: умерена (10)

2. **<u>Ризик недовољне транспаретности</u>**

Ризик недовољне транспарентности се везује за начин остваривања права на информисаност лица чији се подаци обрађују, односно за недовољну

информисаност лица о томе да ли су се и у којим све ситуацијама обрађивали или се и даље обрађују њихови подаци о личности и да ли ће и каквом све обрадом и којих података бити идентификовани.

Употребом система видео надзора на јавном простору, а посебно код увођења у употребу видео надзора у покрету односно употребом видео надзора који је постављен на полицијским возилима или употребом камера које полицијски службеници могу да носе на униформи, код лица се ствара осећај да су подвргнути константном надзору, а да при том нису сигурни да ли је стварно тако и да ли ће и када, односно у којим све околностима и на којим локацијама бити снимњени или идентификовани, 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.

Овакав осећај се додатно продубљује због чињенице да полиција на јавном месту не поставља обавештење о употреби система видео надзора нити јавно саопштава намеру снимања у случају када примењују посебне доказне радње односно тајно праћење и снимање као ни у случају спровођења теста интегритета,

Изостанак или недовољна информисаност лица о обради податка додатно продубљује осећај несигурности, односно нелагодности.

Степен угрожености/озбиљност последица: средњи (3)
Вероватноћа остваривања претње: средња (3)
Изложеност ризику повреда права и слободе је: умерена (9)

Контрола ризика врши се применом 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, Министарство ће путем медија, других средстава јавног обавештавања (средство јавног информисања, интернет презентације и сл.) обавестити јавност, а самим тим и сва лица која могу бити обухваћена видео надзором.

Локације камера на јавном месту морају бити јасно обележене као и полицијска возила која су опремљена видео надзором 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. Списак локација камера се објављује на интернет сајту министарства[8]. Код употребе камера које полицијски службеници носе на униформама неопходно је да полицијски службеници увек обавесте лица да ће снимати своје, односно поступање лица према којем примењују полицијска овлашћења.

Лицима се поред оваквог општег информисања мора омогућити и конкретно остваривање права у вези са обрадом података о личности (право на увид, копију,

[8] http://www.mup.gov.rs/wps/wcm/connect/b152c15f-16eb-47b3-b9a4-c7f32c2cc1ba/%D0%A0%D0%B5%D0%B4.pdf?MOD=AJPERES&CVID=oqjaLo7

брисање или друга права, у скаду са законом). Информисање без обзрира на начин мора да садржи и обавештавање о начину остваривања права код руковаоца (нпр. подношењем захтева Министарству, територијално надлежној полицијској управи, по месту односно локацији камера, локацији снимања и сл.).

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, или да ће полицијски службеници пропустити да их о томе обавесте, те је резидуални ризик, односно изложеност ризику смањена до нивоа допустивог и може се контролисати ефикасним поступањем по захтевима грађана за остваривање права у вези са обрадом података о личности као и едукацијом односно контролом рада полицијских службеника.

Степен угрожености/озбиљност последица: средњи (3)
Вероватноћа остваривања претње:претежно мала (2)
Изложеност ризику повреда права и слободе је: допустива (6)

3. <u>Профилисање лица</u>

Ризик по права и слободе лица везује се за могућност профилисања лица што подразумева да се сваки облик аутоматизоване обраде података, може користити да би се оценило одређено својство личности, посебно у циљу анализе или предвиђања понашања, локација, кретања или личних склоности (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 и пружи му додатне информације како 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 утичу 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 употребом видео надзора и обрадом видео записа и фотографија представљао би 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 које нема за циљ анализу или предвиђање понашања, локације, кретање лица за које се постоји основи сумње да је учинило кривино дело за које се гоњење предузима по службеној дужности.

Степен угрожености/озбиљност последица:претежно висок (4)
Вероватноћа остваривања претње:претежно висока (4)
Изложеност ризику повреда права и слободе је: недопустива (16)

Контрола ризика врши се употребом предвиђених организационих и техничких мера.

Уз примену одговарајућих мера заштите права, слобода и легитимних интереса лица на које се подаци односе допуштено је доношење одлуке на основу аутоматизоване обраде коју врше надлежни органи у посебне сврхе, која укључује и профилисање али таква обрада, односно профилисање мора бити засновано на закону. Забрањено је профилисање које доводи до дискриминације физичких лица, а лице на које се подаци односе има право да поднесе приговор на обраду података.

Доношење било какве одлуке која производи правне последице, односно која утиче на положај лица на које се подаци односе, мора бити засновано на закону, обрада података се мора вршити на основу наредбе судије за претходни поступак која се издаје на предлог надлежног тужиоца и при свакој обради података 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 на основу резултата аутоматизоване обраде, доносе одлуку о предузимању мера и радњи или примене полицијских овлашћења у циљу идентификације тог лица. Дакле, у сваком конкретном случају неопходна је улога полицијског службеника код одређивања сврхе и начина примене конкретне радње обраде. Само на основу обраде података које је извршена уз учешће човека-полицијског службеника, могу се предузети одређене радње или донети одлуке које производе правне последице по то лице, односно које утичу на положај лица.

Поступање полицијских службеника код обраде видео записа и фотографија, односно обраде биометријских података о личности у виду профилисања, засновано је на организационој структури у систему подељених улога и то у погледу вршења појединачних радњи обраде и одлучивања о неопходности 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.
Обрада биометријских података може се вршити само уз примену одговарајућих техничких мера заштите података као што су: контрола приступа опреми, контрола носача података, контрола чувања односно брисања 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.

Полицијски службеници који врше обраду података морају бити едуковани о законским условима за евентуално 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 полицијских

службеника је укидање налога за приступ систему и ажурирање одобрених нивоа приступа. Механизам утврђивања дисциплинске одговорности је истовремено превентивна и реактивна мера заштите података која се мора примењивати.

Уз примену наведених мера за умањење ризика као и чињенице да су радње аутоматизоване обраде података сведене на минимум и да се врше на основу наредбе суда и то накнадном обрадом похрањених видео записа, резидуални ризик је знатно умањен али изложеност ризику и даље постоји, те да би се адекватно управљало овим ризиком, неопходни су ефикасни механизми контроле.

Степен угрожености/озбиљност последица:висок (5)
Вероватноћа остваривања претње: претежно мала (2)
Изложеност ризику повреда права и слободе је: умерена (10)

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

Упоређивањем биометријских података из похрањеног видео записа или фотографије са биометријским подацима које Министарство у складу са законом у посебне сврхе обрађује у својим евиденцијама, проверава се подударност, односно траже се биометријски подаци са највећим степеном подударности.

Ризик по слободе и права лица везује се за обраду биометријских података садржаних у евиденцијама Министарства, а који нису тачни. Обрада таквих нетачних података довела би до погрешног усмеравања полицијских службеника на предузимање одређених мера и радњи односно примену полицијских овлашћења према погрешном лицу. Оваква обрада би за последицу могла имати неосновано идентификовање лица односно неосновано поступање полицијских службеника према „погрешном“ лицу јер се за њега везују нетачни биометријски подаци из евиденција Министарства, 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. Могућност 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 на пример 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).

Степен угрожености/озбиљност последица: претежно низак (2)
Вероватноћа остваривања претње:мала (1)
Изложеност ризику повреда права и слободе је: незнатна (2)

Контрола ризика врши се предузимањем организационих и техничких мера заштите података о личности.

Примена полицијских овлашћења мера и радњи повезаних са обрадом биометријских података мора се вршити професионално и у складу са утврђеним стандардима полицијског рада, што подразумева да полицијски службеник у

случају очигледне нетачности података мора извршити додатне провере пре доношења одлуке о даљем поступању. Спровођењем континуиране едукације и контролно-инструктивне делатности омогућиће се и ефикасан механизам управљања подацима који подразумева уређен начин прикупљања података и вођења евиденција као 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 проверу уноса, ажурирања, измена или исправљање података садржаних у евиденцијама.

Применом одређених техничких мера заштите података као што су: контрола приступа опреми, контрола носача података, контрола уноса, чувања података, контрола корисника, контрола приступа подацима, контрола преноса, контрола транспорта, опоравак система, обезбеђивање интегритета система, управљање корисничким налозима, системски журнал, обезбеђује се ефикасан механизам управљања подацима.

Код изложености овом ризику мора се имати у виду да 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 за нетачно унете податке у евиденције, јер постоји могућност да на пример 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.

Степен угрожености/озбиљност последица: претежно низак (2)
Вероватноћа остваривања претње: мала (1)
Изложеност ризику повреда права и слободе је: незнатна (2)

5. Снимање лица у приватном простору

Ризик по права и слободе лица постоји у ситуацијама када се снимање на јавном простору врши камерама које снимају 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. Овај ризик се знатно увећава очекивним увођењем у употребу камера које полицијски службеници носе на униформи.

Лице оправдано очекује да су активности које предузима у приватном простору заштићене од погледа других људи и да их нико без њихове дозволе односно сагласности неће снимати док бораве у приватном простору.
Транспарентном употребом видео надзора, и обавештавањем о снимању умањује се субјективни осећај угрожености права на приватност лица, чиме се подиже свест грађана о висини ризика по ово њихово право.

Употреба система видео надзора има за циљ снимање јавног простора, али постоји могућност да се сними и приватни или пословни простор на оним местима на којим

не постоје физичке препреке или ако полицијски службеник који носи камеру на униформи уђе у приватни или пословни простор и укључи камеру, чиме се угрожава право на приватност.

Уколико је 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 претежно мала. Могућност повреде права снимањем од стране полицијског службеника камером коју носи на униформи се може умањити само уколико полицијски службеник увек проверава да ли је камера коју носи на униформи укључена или не.

Степен угрожености/озбиљност последица:висок (5)
Вероватноћа остваривања претње: претежно мала (2)
Изложеност ризику повреда права и слободе је: умерена (10)

Контрола ризика врши се спровођењем организационих и техничких мера.

Уз периодично преиспитивање видног поља камера, као и спровођењем контролно-инструктивне делатности и едукацијом полицијских службеника омогућен је увид у начин руковања камерама и поступања полицијских службеника. Корисници система су полицијски службеници који морају бити оспособљени и едуковани за руковање камерама као и о законским условима и начину употребе система видео надзора без обзира на врсту уређаја и опреме која се користи за снимање. Поступање полицијских службеника приликом руковања камерама засновано је на организационој структури у систему подељених улога.

Обрада снимљеног материјала вршила би се на основу судске наредбе и подразумевала би обраду похрањених видео записа која би била ограничена односно трајала би само током поређења. Обрада података односила би се само на лица из одређеног видео записа, само са одређених камера а који су сачињени у одређеном временском периоду а биометријски подаци би се поредили само са подацима одређених лица које ово министарство обрађује у посебне сврхе.

Такође, уз примену техничких мера заштите као што су: контрола приступа опреми, контрола носача података, контрола снимања, чувања података, контрола корисника, контрола приступа подацима, контрола преноса, контрола транспорта, обезбеђивање интегритета система, управљање корисничким налозима, системски журнал обезбеђује се ефикасан механизам управљања подацима.

Јавни простор који се снима употребом видео надзора 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 обухвата и одређене објекте који нису предмет надзора. Употребом одговарајућих филтера, видео надзор се може користити на начин да се не угрожава приватност нечијег дома или пословног простора, односно на начин да не изазива нелагодност код грађана због бојазни да су предмет надзора док бораве у том простору. Применом адекватних мера заштите и механизама

контроле њихове примене, може се обезбедити да ниво резидуалног ризика буде допустив.

Степен угрожености/озбиљност последица:висок (5)
Вероватноћа остваривања претње: мала (1)
Изложеност ризику повреда права и слободе је: допустива (5)

6. Грешка софтвера

Постојање ризика везује се за чињеницу да се обрада биометријских карактеристика (претраживање, упоређивање) 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 означено као извршилац кривичног дела или обрнуто, да софтвер за обраду биометријских видео записа уопште не детектује лик извршиоца кривичног дела или се извршиоцу кривичног дела услед грешке софтвера обезбеђује алиби).

Вероватноћа грешке мора се посматрати у односу на квалитет видео записа или фотографија које се обрађују ради обраде биометријских података. За разлику од условно речено „контролисаних окружења“ или окружења која су у потпуности покривена видео надзором, где се обезбеђује висок квалитет видео записа и где вероватноћа грешке мала али свакако да проценат грешке расте када се користи видео запис са камера где је квалитет видео записа лошији услед различитих околности (осветљење, временске прилике, удаљеност камере, коришћење различитих средстава за избегавање видео надзора попут наочара за сунце, капе, шала или маске преко лица) повећава се и ризик од грешке.

Тачност и поузданост обраде биометријских података одређује се на основу податка произвођача али мора постојати и независно оцењивање уз периодично преиспитивање нивоа тачности.

Ни једна одлука која на било који начин може да утиче на права лица се не сме доносити само на основу аутоматизоване обраде односно на основу резултата рада софтвера односно резултата упоређивања података. Ниво утицаја грешке софтвера на повреде права на приватност и достојанство лица код обраде биометријских података о личности 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 на основу обраде биометријских података увек додатно проверава резултат њиховог упоређивања и доноси одлуку о предузимању других мера и радњи према лицу. Изостанак потребне провере резултата упоређивања биометријских података повећава се и ризик повреде права на приватност и достојанство лица.

Степен угрожености/озбиљност последица:средњи(3)
Вероватноћа остваривања претње: средња (3)
Изложеност ризику повреда права и слободе је: умерена (9)

Контрола ризика врши се спровођењем предвиђених организационих и техничких мера. Поступање полицијских службеника приликом обраде видео записа

засновано је на организационој структури у систему подељених улога у погледу вршења неопходних провера резултата упоређивања биометријских података, чиме је умањена могућност предузимања било каквих мера и радњи према лицу, без вршења неопходне провере. Обрада видео записа или фотографија и упоређивање биометријских података врши 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 обраде, контрола чувања, контрола брисања, 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 поуздану обраду података о личности.

Мора се имати у виду и чињеница 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.

Степен угрожености/озбиљност последица:средњи(3)
Вероватноћа остваривања претње: средња (3)
Изложеност ризику повреда права и слободе је: умерена (9)

7. <u>Ризик од приступања подацима од стране неовлашћених лица</u>

Постојање овог ризика везује се за приступ односно 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 система видео надзора и софтвера за обраду биометријских података од стране овлашћених лица/овлашћених полицијских службеника, где ниво утицаја повреде права расте уколико постоји било каква могућност за приступ неовлашћених лица.

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.

Степен угрожености/озбиљност последица:средњи(3)
Вероватноћа остваривања претње: претежно мала (2)
Изложеност ризику повреда права и слободе је: допустива (6)

Контрола ризика врши се спровођењем организационих и техничких мера.

Уређаји и опрема за обраду података и носачи информација (ЦД, ДВД, екстерни хард дискови) на које су подаци похрањени, копирани или пренети, морају бити обезбеђени, чувани у посебним просторијама које се закључавају, обезбеђене системом контроле приступа, видео-надзором, уз примену 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 мора 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 забрана копирања, умножавања и преноса података без похрањивања обезбеђује поуздан систем управљања подацима. Поред наведених мера, ризик се може контролисати укидањем или ажурирањем права приступа при промени послова или престанка радног односа, као и континуираном едукацијом 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.

Степен угрожености/озбиљност последица:средњи(3)
Вероватноћа остваривања претње: мала (1)
Изложеност ризику повреда права и слободе је: незнатна (3)

8. Ризик од злоупотреба које могу извршити овлашћена лица.

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 ивршити обраду података без правог основа, без претходно издате наредбе судије за претходни поступак, односно користити уређаје и опрему у сврхе за које нису намењени где је најчешће овај ризик мотивисан разлозима личне природе).

Овлашћени полицијски службеник може снимати, 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. Овлашћени полицијски службеник може без судске наредбе извршити обраду биометријских података или профилисање. Такође, овај ризик се везује и за могућност да овлашћени полицијски службеник пропусти да додатно провери резултат подударности упоређивања биометријских података услед чега може донети погрешну одлуку о предузимању других мера и радњи према лицу и на тај начин угрозити његова права.

Степен угрожености/озбиљност последица:средњи(3)
Вероватноћа остваривања претње: претежно мала (2)
Изложеност ризику повреда права и слободе је: допустива (6)

Контрола ризика врши се спровођењем организационих и техничких мера.

Ради правилне и законите обраде биометријских података 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, јединствену ознаку уређаја са кога је приступљено, податке о трајању сваке сесије, као и податке о активностима. Дигитални записи о приступу се чувају у системском журналу. Приликом употребе софтвера за обраду биометријских података обрађује се одређени похрањени видео запис или фотографија лица који је означен јединственом ознаком забележеног видео записа или фотографије временом и местом настанка видео записа или фотографије, локацијом камере, а резултат обраде, односно поређења, се у форми извештаја креира на радној станици за обраду видео записа или фотографија. Извештај о резултату поређења поред осталих података садржи и: број и датум наредбе и назив суда, број извештаја, име и презиме полицијског службеника, назив организационе јединице у којој ради полицијски службеник, јединствену ознаку радне станице на којој је вршена обрада видео записа или фотографије, датум и време обраде, а приступ и све активности предузете на радној станици за обраду видео записа или фотографија чува се у системском журналу. Системски журнал бележи и приступ подацима свих лица из евиденције чији су подаци најприближнији биометријским подацима лица из обрађеног видео записа. На основу овако упостављене евиденције увек је могуће недвосмислено утврдити који полицијски службеник је вршио обраду података и на којој радној станици као и какав је био резултат обраде. Ова евиденција се може ставити на увид Поверенику за инфорамције од јавног значаја и заштиту података о личности ради вршења послова из његове надлежности.

Приликом приступања 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). Такође предвиђена је забрана односно

немогућност чувања/похрањивања, копирања, умножавања или преноса биометријских података.

Дефинисањем привилегија 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 и њихову даљу обраду. 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 ризика мора се имати у виду чињеница да се „човек“ увек појављује као најслабија карика те да могућност злоупотребе увек постоји и она увек за собом повлачи и одређене последице за лице на које се подаци односе али се ефикасном применом мера резидуални ризик може контролисати.

Степен угрожености/озбиљност последица:средњи(3)
Вероватноћа остваривања претње: претежно мала (2))
Изложеност ризику повреда права и слободе је: допустива (6)

9. <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 приступа). Неодговорно поступање са подацима доводи до губитка података (нпр. приликом преноса, транспорта носача податка, неадекватно чување података такође доводи до губитка података).

Степен угрожености/озбиљност последица:средњи(3)
Вероватноћа остваривања претње: претежно мала (2)
Изложеност ризику повреда права и слободе је: допустива (6)

Контрола ризика врши се спровођењем 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 се може умањити да постане незнатан.

Степен угрожености/озбиљност последица:средњи(3)
Вероватноћа остваривања претње: мала (1)
Изложеност ризику повреда права и слободе је: незнатна (3)

10. Недопуштено објављивање података

Постојање овог ризика односи се на могућности злоупотребе од стране овлашћених лица/полицијских службеника којима је одобрен приступ подацима. Злоупотребе су могуће у тренутку прикупљања података или током њихове даље обраде где је овај ризик најчешће мотивисан разлозима личне природе. Не искључује се могућност и да овлашћени полицијски службеник може вршити увид у похрањене податке, издвојити, обрадити, копирати и пренети податке неовлашћеном лицу самоиницијативно или на основу налога надређеног. Мора се имати у виду да се овај ризик посматра само у односу на недопуштено објављивање података 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 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.

Степен угрожености/озбиљност последица:висок(5)
Вероватноћа остваривања претње: средња (3)
Изложеност ризику повреда права и слободе је: знатна (15)

Контрола ризика врши се спровођењем организационих и техничких мера.

Ради правилне и законите 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 (радне станице), податке о трајању сваке сесије, као и податке о активностима. Дигитални записи о приступу се 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). Такође, предвиђена је забрана односно немогућност копирања, умножавања и преноса података.

Дефинисањем привилегија 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 и даље обраде података. Свако преузимање података се мора евидентирати уз означавање броја израђених копија, разлоге 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 брисања података, контрола корисника, контрола приступа подацима, контрола обраде, 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 ефикасан 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 је 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 поступка за утврђивање кривичне одговорности од стране надлежног органа такође су неопходни елементи ефикасног механизма управљања подацима којим се резидуални ризик може умањити до умереног.

Степен угрожености/озбиљност последица: висок(5)
Вероватноћа остваривања претње: претежно мала (2)
Изложеност ризику повреда права и слободе је: умерена (10)

VI 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 прописа о допуштеној обради података, као и 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. Мере и механизми заштите 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 у систему видео надзора примењују се на специфичан начин. 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.

Обрада биометријских података подразумевала би и успостављање нових евиденција на основу којих се увек може утрдити ко је и када, на којој радној станици вршио обраду података. За успостављање овакве евиденције као и за утврђивање процедура поступања полицијских службеника, механизама контроле и друге неопходне мере заштите податка неопходно је доношење одговарајућих подзаконских односно инструктивних аката од стране Министарства. Доношење ових аката проистиче из одредби Закона о унутрашњим пословима и Закона о обради података у области унутрашњих послова који су тренутно у фази нацрта, а чије доношење је предуслов за обраду биометријских података у сврху идентификације лица од стране Министарства.

Систем видео надзора којим рукује Министарство, чини скуп фиксних и мобилних камера, као и других уређаја и опреме који су намењени за надзор и снимање. 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 врши се анализа потреба постављања камера на појединим камерним местима, а према раније поменутој методологији и 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.

Техничке мере заштите

Контрола приступа опреми, контрола корисника, контрола приступа подацима и 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 (радна станица), 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 чувати у системском журналу.

Обавезна двострука потврда идентитета (2ФА) подразумева да приликом приступања 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 уређај и носачи информација на које су подаци у оквиру система снимљени морају бити 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 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.

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

Организационе мере заштите

Управљање корисничким налозима подразумева дефинисање привилегија за сваког полицијског службеника са овлашћењем да приступа снимљеном 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 имају администраторски приступ систему који омогућава напредније опције, попут креирања и брисања налога за друге службенике, док остали могу 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 или чијег захтева, односно налога се поступа.

Мере заштите од ризика који настају при промени послова или престанка радног односа подразумевају да након престанка радног односа или премештања 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.

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 биометријских података, 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 података врше друга службена лица која су распоређена у другим организационим јединица. Систем подељених улога као организациона мера 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 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.

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 унутрашњих послова. Овим актом уређује се надлежност појединих организационих јединица Министарства, као и опис послова и задатака за 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 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 извршавања послова и задатака.

У систему видео надзора којим рукује Министарство, сваку радњу обраде врши лице које је овлашћено за предузимање те радње. При томе, ни једно од ангажованих лица 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 обраду и коришћење биометријских података као и за одлучивање о неопходности предузимања других мера и радњи које треба да доведу до идентификације једног 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, 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 система у сваком конкретном случају (системски журнал).

Праћење примене закона и других прописа који се односе на заштиту података о личности у оквиру Министарства и контролу примењених мера заштите врши лице за заштиту података о личности у Министарству, у сарадњи са другим полицијским службеницима, које одреди министар.

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

Информисање грађана подразумева да се лицима, 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, територијално надлежној полицијској управи, по месту локације камера, односно месту снимања).

Дисциплинованост и савесност полицијских службеника законито и професионално поступање полицијских службеника 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, на основу Програма стручног усавршавања полицијских службеника Министарства и Директиве о начину обављања послова у вези са заштитом података о личности у Министарству.

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. Друга група ових мера јесу дисциплинске мере и оне су прописане Законом о полицији. Трећу групу мера које су прописане Законом о заштити података о личности и Кривичним закоником примењује Министарство, 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 подразумевају да свако лице чије податке обрађује Министарство, може да се обрати захтевом за остваривање, односно заштиту права у складу са законом. Механизам контроле поступања по захтевима лица чији се подаци обрађују такође се поверава лицу за заштиту података о личности у министарству.

VII МИШЉЕЊЕ ЛИЦА ЗА ЗАШТИТУ ПОДАТАКА О ЛИЧНОСТИ

У складу са чланом 54. и чланом 58. Закона о заштити података о личности, у Министарству је сачињен овај документ, а од стране Лица за заштиту података о личности дата препорука да се документ достави на мишљење Поверенику за информације од јавног значаја и заштиту података о личности као и да се у целини или скраћеном облику јавно објави на интернет страници Министарства или се на други пригодан начин учини доступним јавности.

Такође, дата је препорука је да се овај документ презентује приликом наставка јавне расправе на Нацрт закона о унутрашњим пословима и на Нацрт закона о обради података у области унутрашњих послова.

Имајући у виду да је процена утицаја намераваних радњи обраде биометријских података о личности на заштиту података о личности, извршена у поступку за доношење закона, препорука је да се документ, након спроведене процедуре прибављања мишљења других органа, достави и Влади Републике Србије приликом достављања предлога поменутих Нацрта закона.

На крају, Лице за заштиту података о личности, напомиње да је након доношења закона, а пре почетка обраде биометријских података потребно извршити ажурање ове процене утицаја, имајући у виду да намераване радње обраде биометријских података о личности подразумевају употребу нових технологија евентуално формирање нових збирки података.

У Београду
27.04.2023. године
Број: 07-7-117/23

в.д. СЕКРЕТАРА МИНИСТАРСТВА

Мирослав Панић