

Komenari na Nacrt Procene uticaja radnji obrade podataka o ličnosti
upotrebom softvera za obradu biometrijskih podataka u sistemu video
nadzora Ministarstva unutrašnjih poslova na zaštitu podataka o ličnosti

Beograd, 03.06.2022.

Poštovani,

Obraćamo vam se u vezi sa dokumentom "Nacrt Procene uticaja radnji obrade podataka o ličnosti upotrebom softvera za obradu biometrijskih podataka u sistemu video nadzora Ministarstva unutrašnjih poslova na zaštitu podataka o ličnosti" (u daljem tekstu: Procena uticaja) koji nam je dostavljen 04.05.2022. godine i o kome se diskutovalo na zajedničkom sastanku MUP-a, organizacija civilnog društva i ostalih zainteresovanih strana 13.05.2022. godine.

Želimo pre svega da naglasimo da se SHARE Fondacija i dalje **protivi svakom korišćenju biometrijskog nadzora u javnim prostorima**, bez obzira da li je reč o domaćem ili međunarodnom kontekstu. Taj naš principijelan stav je između ostalog iskazan kroz naš rad i članstvo u [EDRi](#), najznačajnijoj mreži za digitalna prava Evrope, pokretu [Reclaim your face](#), koji okuplja gotovo stotinu organizacija iz celog sveta koje se zalažu za zabranu masovnog biometrijskog nadzora, kao i u lokalnoj inicijativi [#hiljadekamera](#), zajednici pojedinaca i organizacija koje se zalažu za odgovorno korišćenje tehnologije za nadzor.

Primena ovakve tehnologije imala bi **nesagledive posledice po demokratsko društvo, prava i slobode građana**, zbog čega je [Visoki komesarijat za ljudska prava Ujedinjenih nacija](#) preporučio da se uvede **moratorijum** na korišćenje tehnologije za biometrijski nadzor u javnim prostorima.¹ Takođe, [Evropski poverenik za zaštitu podataka \(EDPS\)](#) i [Evropski odbor za zaštitu podataka \(EDPB\)](#) pozvali su na **opštu zabranu** korišćenja naprednih tehnologija za automatsku obradu biometrijskih podataka u javnim prostorima.² Uz to treba napomenuti da je u [nizu gradova u SAD](#) već **zabranjena upotreba** biometrijskog nadzora u javnim prostorima.

Ipak, smatramo da je neophodno otvoriti **transparentnu debatu** o mogućnostima upotrebe ove tehnologije, odnosno koristima, rizicima i posledicama koje ona inherentno nosi sa sobom. Svesni smo da je MUP uložio značajne resurse u izradu Procene uticaja i seriju otvorenih razgovora sa zainteresovanim organizacijama

¹ Urgent action needed over artificial intelligence risks to human rights, 15.09.2021.
<https://news.un.org/en/story/2021/09/1099972>

² EDPB & EDPS call for ban on use of AI for automated recognition of human features in publicly accessible spaces, and some other uses of AI that can lead to unfair discrimination, 21.06.2021.
https://edps.europa.eu/press-publications/press-news/press-releases/2021/edpb-edps-call-ban-use-ai-automated-recognition_en

civilnog društva. Stoga verujemo da je izrada **sveobuhvatne, precizne i informativne Procene uticaja**, kao preduslova za dalje razmatranje ovog pitanja, u opštem interesu društva. U skladu s tim, predstavljamo svoje komentare i zapažanja na dostavljeni dokument.

- **Procena neophodnosti i srazmernosti**

Osnovni preduslovi za upotrebu biometrijskog nadzora u našem pravnom okviru jesu **neophodnost** (član 13 ZZPL, član 5 Konvencije 108+ i član 8 Evropske konvencije o ljudskim pravima) i **srazmernost** (član 14, stav 3, ZZPL i član 5, stav 1, Konvencije 108+) takve obrade podataka. Zahtevi neophodnosti i proporcionalnosti će biti ključni za donošenje odluke da li bi ovakva obrada podataka bila dozvoljena u našem društvu, te smatramo da je njihovo **dokazivanje i demonstracija osnovni preduslov** u okviru izrade Procene uticaja. Stoga, iako procena neophodnosti i srazmernosti nije navedena kao formalni element Procene uticaja obrade koju vrše nadležni organi u posebne svrhe, ona svakako predstavlja indirektni zahtev i temelj na osnovu kog se procenjuju sva ostala pitanja obrađena u Proceni uticaja.

Naš stav je da informacije sadržane u Proceni uticaja **ne dokazuju** da je obrada velikih količina biometrijskih podataka **neophodna** za obavljanje konkretnih namena, niti da je **proporcionalna** i **srazmerna** rizicima po prava i slobode građana. Za adekvatno razmatranje ovih uslova, predlažemo **minimalnu listu pitanja** na koje je potrebno pružiti odgovore kako bi se dokazala neophodnost i proporcionalnost, a na osnovu prihvaćenih evropskih standarda (kao što je, između ostalog, navedeno u smernicama za procenu neophodnosti supervizora zaštite podataka u EU,³ te na strani 5 obrasca za procenu uticaja koji je izradila kancelarija britanske poverenice za zaštitu podataka⁴ ili na stranama 6 i 7 sličnog obrasca britanskog komesara za nadzorne kamere⁵).

- *Koje su svrhe koje treba ostvariti i problemi koji treba rešiti (ukoliko ih je više, definisati svaki ponaosob)?*
- *Kako nameravana obrada ostvaruje konkretnu svrhu i rešava određeni problem?*
- *Kako se meri da li nameravana obrada ostvaruje konkretnu svrhu i rešava određeni problem?*
- *Da li postoji drugi razuman način, odnosno manje intruzivna mera da se konkretna svrha ostvari i konkretan problem reši?*

³ Necessity Toolkit, 11.04.2017. https://edps.europa.eu/data-protection/our-work/publications/papers/necessity-toolkit_en

⁴ Sample DPIA template, <https://ico.org.uk/media/for-organisations/documents/2553993/dpia-template.docx>

⁵ Data protection impact assessments, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/886883/SC_ICO_DPIA_Template_V4_.docx

- *Da li postojeće mere i procedure mogu ostvariti konkretnu svrhu i rešiti određeni problem?*
- *Kako će se sprečiti da se prikupljeni podaci ne koriste u druge svrhe?*

- **Sudska odluka kao preduslov za biometrijski nadzor**

Biometrijski nadzor u javnom prostoru predstavlja izuzetno intruzivnu meru, koja sa sobom nosi brojne rizike po osnovne slobode i prava građana. Stoga smatramo da svako dalje razmatranje upotrebe tehnologije za prepoznavanje lica mora za polaznu osnovu da uzme **prethodnu odluku suda kao preduslov za svako konkretno korišćenje ove tehnologije**. Ovo je posebno važno s obzirom na to da Procena uticaja predviđa korišćenje biometrijskog nadzora u izuzetno restriktivnim situacijama, te da metod i svrha predviđene obrade podataka u značajnoj meri podsećaju na **posebne dokazne radnje** predviđene Zakonom o krivičnom postupku, a naročito na **tajno praćenje i snimanje** (članovi 171-173 ZKP) i **računarsko pretraživanje podataka** (članovi 178-180 ZKP) za koje je takođe potrebna **sudska odluka**.

- **Rizici po prava i slobode građana**

Osim rizika po pravo na privatnost i pravo na zaštitu podataka o ličnosti, u Proceni uticaja nisu posebno obrađeni rizici po ostala ljudska prava i slobode koji bi bili ugroženi upotrebom biometrijskog nadzora u javnim prostorima. U tom smislu, posebnu pažnju u okviru Procene uticaja potrebno je posvetiti rizicima koji posredno ili neposredno izazivaju „**efekat zebnje**“ (eng. **chilling effect**). Naime, upotreba široko rasprostranjene i intruzivne tehnologije nadzora u javnim prostorima kod građana stvara osećaj da su podvrgnuti konstantnom nadzoru, a da nisu ni sigurni da li je tako. Osećaj bitno sužene lične slobode drastično menja ponašanje i negativno utiče na ličnost pojedinca, utičući time konačno i na karakter društva.⁶

Zbog snažnog efekta zebnje izazvanog masovnom obradom biometrijskih podataka, direktno je ugrožen **niz ljudskih prava i sloboda**, među kojima su pre svega: sloboda misli, savesti i veroispovesti (član 9 Evropske konvencije o ljudskim pravima), sloboda izražavanja (član 10), sloboda okupljanja i udruživanja (član 11), pravo na zaštitu od diskriminacije (član 14). Više detalja o neposrednim rizicima po ostala ljudska prava izloženo je u izveštaju Visokog komesara UN za ljudska prava (strane 6 i 13)⁷ kao i u

⁶ Understanding Chilling Effects, Minnesota Law Review, 07.06.2021

https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3855619

⁷ A/HRC/48/31: The right to privacy in the digital age - Report of the United Nations High Commissioner for Human Rights, 15.09.2021. <https://www.ohchr.org/en/documents/thematic-reports/ahrc4831-right-privacy-digital-age-report-united-nations-high>

zajedničkom mišljenju EDPB-EDPS o predlogu regulisanja veštačke inteligencije (strana 11⁸).

Takođe, masovna i neselektivna upotreba tehnologije prepoznavanja lica, gde je predmet obrade celo građanstvo, posebno ugrožava pravo na pretpostavku nevinosti (član 6 Evropske konvencije o ljudskim pravima).

Svi ovi rizici su iscrpno obrazloženi u [Smericama 5/2022 o upotrebi tehnologije prepoznavanja lica u posebne svrhe](#), na strani 44 (naslov: **Scenario 5**).⁹ Prikazani scenario opisuje situaciju u kojoj policija koristi biometrijski nadzor radi identifikacije osobe od interesa, na konkretnom javnom prostoru, u realnom vremenu. U konkretnom slučaju, zaključak Evropskog odbora za zaštitu podataka (EDPB) je da ovakva obrada predstavlja **neproporcionalno zadiranje u ljudska prava** iz sledećih razloga:

- Primena tehnologije prepoznavanja lica na način predviđen u ovom scenariju značila bi da je broj lica čiji su najosetljiviji podaci predmet obrade izuzetno visok, jer su **pogođeni svi koji prolaze odgovarajućom javnom površinom**;
- u pitanju je obrada koja bi vodila **masovnoj i neselektivnoj obradi podataka već od trenutka prikupljanja biometrijskih podataka**, preko njihove neprestane pretrage u cilju podudaranja podataka iz drugih baza, do njihovog čuvanja u predviđenom roku, što predstavlja obradu sa izuzetno visokim nivoom intruzivnosti i rizika po prava i slobode lica u javnom prostoru (primera radi, situacija u kojoj bi se isto uradilo uzimanjem otisaka prstiju građana, bila bi očigledno nesrazmerna);
- praćenje svakog prolaznika u javnom prostoru ozbiljno utiče na **razumna očekivanja građana da budu anonimni u javnim prostorima**, što je preduslov za mnoge aspekte demokratskog procesa, kao što je odluka o udruživanju sa drugima, posećivanju skupova i upoznavanju ljudi svih društvenih i kulturnih sredina, učestvovanju u političkom protestu i slično;
- dodatni aspekt efekta zebnje je i **odvrćanje od susreta i viđanja u javnosti sa određenim licima** (rođacima, prijateljima) za koje se pretpostavlja da su imali ili mogu imati problem sa policijom;
- **daljinska biometrijska identifikacija gotovo je nemoguća bez masovnog, neselektivnog nadzora i ne postoje pouzdani načini njenog ograničenja**, jer se ona suštinski razlikuje od video nadzora kao takvog; samo korišćenje video snimaka bez biometrijske identifikacije već predstavlja intruzivnu obradu, ali je

⁸ Joint Opinion 5/2021 on the proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act), 18.06.2021.

https://edpb.europa.eu/system/files/2021-06/edpb-edps_joint_opinion_ai_regulation_en.pdf

⁹ Guidelines 05/2022 on the use of facial recognition technology in the area of law enforcement, Adopted on 12 May 2022 https://edpb.europa.eu/system/files/2022-05/edpb-guidelines_202205_frtlawenforcement_en_1.pdf

istovremeno ograničena; u trenutku kada se primeni tehnologija prepoznavanja lica, široko rasprostranjeni sistem video nadzora doživljava promenu kvaliteta ka mnogostruko uvećanoj intruzivnosti;

- daljinska biometrijska identifikacija u osnovi menja politički i društveni vrednosni sistem, budući da **svakog građanina tretira kao potencijalnog osumnjičenog** (pogotovo u slučaju „pozitivnog rezultata“ pretrage);
- upotreba tehnologije sa mogućnostima jedinstvene identifikacije osobe, te konstantnog praćenja njenog kretanja i analize mesta na kojima boravi, nužno otkriva **najosetljivije informacije o toj osobi** (što može uključiti njenu seksualnu orijentaciju, versku pripadnost, zdravstvene probleme), a što su sve podaci koji ne moraju biti primarni predmet interesovanja, ali se zbog prirode ove tehnologije njihovo saznavanje ne može ograničiti; istovremeno, ovim je ugrožen čitav niz prava, kao što su pravo na slobodu misli, savesti i veroispovesti ili pravo na zaštitu od diskriminacije;
- nemoguće je zaštititi **posebno osetljive grupe** poput dece; takođe su merama nadzora pogođena lica koja imaju profesionalnu, a često i zakonsku, obavezu zaštite poverljivosti (kao što su novinari, advokati, sveštenstvo, lekari); rizici se odnose na nasumična javna mesta koja mogu biti predmet nadzora, a pogotovo na javne prostore koji su neophodni za pristup institucijama ili profesionalcima u navedenom smislu;
- postoje izazovi u domenu **transparentnosti korišćenja predmetne tehnologije**, pri čemu se postavlja pitanje načina ostvarivanja prava građana na informisanost, počevši od toga da li su i u kojim situacijama bili ili jesu predmet nadzora, do toga kako da ostvaruju sva druga prava garantovana propisima o zaštiti podataka o ličnosti i drugim primenjivim propisima.

● Procena rizika

U Proceni uticaja, delimično je urađena procena rizika na prava i slobode građana. Pored toga što nisu obuhvaćene izuzetno značajne pretnje (odjeljak Rizici po prava i slobode građana), **supstancijalan problem jeste sama matrica upotrebljena za prikazivanje uticaja ovih rizika**. Naime, pored nejasne metodologije kojom su utvrđivani nivoi uticaja i verovatnoće materijalizacije rizika, nomenklatura za nivoje prikazanih rizika ne korespondira sa standardima koji se u praksi koriste.

Konkretnije, ukupna izloženost riziku definisana je u Proceni uticaja u četiri nivoa: nizak, umereni, srednji i visoki nivo. Nijedan nivo izloženosti rizika ne predstavlja neprihvatljiv nivo, a samo „visok“ nivo povlači preduzimanje dodatnih mera i aktivnosti u cilju minimizacije rizika.

Smatramo da je ovakva **postavka procene rizika preterano liberalna i dopušta neodgovorno preuzimanje rizika**, bez definisanja adekvatnih mera njihove

minimizacije. Posebno stoga što u skali od 4 nivoa ne može postojati „srednja“ vrednost. Potrebno je ili **uvesti uvesti skalu od 5 nivoa** (npr. nizak, pretežno nizak, srednji, pretežno visok i visok) ili **zadržati skalu od 4 nivoa, ali sa novom nomenklaturom** (npr. nizak, pretežno nizak, pretežno visok i visok). U svakom od ovih slučajeva smatramo da nivo vrednosti „pretežno visok“ zahteva preduzimanje dodatnih mera i aktivnosti za minimizaciju, pri čemu je nužno odrediti i rizike čija je visina neprihvatljiva.

- **Mere za umanjeње rizika**

Mere i mehanizmi zaštite koji su navedeni u Proceni uticaja nisu dovoljno konkretni, odnosno pojmovi koji se navode mogu podrazumevati različite stvari u tehničkom i organizacionom smislu. Takođe, postoje mere u samom dokumentu koje se planiraju, koje nisu navedene u ovom delu (npr. čuvanje šablona samo 72 sata), a koje konkretno umanjuju određene rizike.

U skladu sa mogućim rizicima, smatramo da je neophodno konkretnije utvrditi odgovarajuće tehničke i organizacione mere za svaki pojedinačni rizik.

Takođe, predlažemo da se u opštem delu dokumenta, tehničke i organizacione mere bliže definišu na sledeći način:

Naziv mere	Vrsta mere	Objašnjenje
Kontrola pristupa opremi Kontrola korisnika Kontrola pristupa podacima Sistemski žurnal	Tehnička	Prilikom svakog pristupa snimljenom materijalu, neophodno je beležiti digitalni zapis o tom pristupu koji bi trebalo da sadrži najmanje sledeće informacije: ime i prezime policijskog službenika, broj značke policijskog službenika, ID uređaja sa koga je pristupljeno, podatke o trajanju sesije, kao i podatke o aktivnostima (resurs kom je pristupljeno, operacije koje su vršene, pretrage koje su rađene itd). Digitalni zapisi o pristupu (logovi) se zauvek čuvaju u sistemskom žurnalu (logbook).
Obavezna dvostruka potvrda identiteta (2FA)	Tehnička	Prilikom pristupanja informacionom sistemu, za sve dodeljene korisničke naloge mora biti podešena dodatna autentifikacija prilikom pristupa snimljenim materijalima, koja bi se ostvarivala putem službene legitimacije ili lične karte.
Kontrola nosača	Tehnička	Uređaji i nosači informacija (CD, DVD, eksterni

<p>podataka</p> <p>Kontrola čuvanja podataka</p> <p>Fizička i tehnička zaštita objekata i opreme</p> <p>Zaštita od oštećenja i krađe sredstava koja čine sistem video nadzora</p>		<p>hard diskovi itd) na koje su podaci u okviru sistema snimljeni moraju biti enkriptovani, čuvani u posebnim prostorijama koje se zaključavaju i koje su obezbeđene zaštitom od požara, poplave, strujnog udara i drugih incidenata, kao i video-nadzorom. Za pristup nosačima informacija neophodan je isti nivo pristupa kao za pristupanje informacionom sistemu. Nosači informacija se ne smeju iznositi iz prostorija osim za jasno definisane potrebe, kao što je recimo oporavak sistema iz rezervnih kopija. Prilikom pristupa sistemu u prostorije se ne smeju unositi bilo kakvi uređaji sa mogućnošću snimanja audio ili video zapisa, kao što su mobilni telefoni, kamere, diktafoni itd.</p>
<p>Oporavak sistema</p> <p>Obezbeđivanje integriteta sistema</p>	Tehnička	<p>U slučaju incidenta moraju se obezbediti integritet podataka u okviru sistema i obnova funkcionalnosti sistema, što se postiže redovnom izradom rezervnih kopija podataka (dnevni, mesečni, godišnji nivo) kojima mogu pristupati samo ovlašćeni zaposleni (sistem administratori) i samo u slučaju incidenta kada je neophodno izvršiti oporavak sistema. Rezervne kopije podataka moraju biti zaštićene savremenim enkripcionim standardima (npr. AES 256-bit).</p>
<p>Upravljanje korisničkim nalogima</p>	Organizaciona	<p>Definisanje privilegija i rola: za svakog policijskog službenika sa ovlašćenjem da pristupa snimljenom materijalu neophodno je propisati odgovarajući nivo pristupa u skladu sa radnim mestom, tj. pozicijom u okviru organizacione jedinice. Na primer, samo određeni službenici (sistem administratori) bi trebalo da imaju administratorski pristup informacionom sistemu, koji omogućava naprednije opcije poput kreiranja i brisanja naloga za druge službenike, dok ostali mogu dobiti ulogu koja im omogućava da samo pregledaju snimke, odnosno naloge bez mogućnosti preuzimanja, izmene ili brisanja materijala. Nadređenim službenicima se mora obezbediti mogućnost da na korisničkom nalogu kreiraju naloge za pretragu.</p>
Softversko	Organizaciona	Nadređeni službenik bi u skladu sa sudskim

generisanje naloga za pretragu		nalogom trebalo da softverski definiše odgovarajući pristupni zahtev, kako bi prilikom svakog pristupa bilo jasno na osnovu kog zahteva nadređenog se postupa.
Dvostruki pristup sistemu	Organizaciona	Sistemu u kome se obrađuju podaci radi pretrage moraju da pristupe najmanje dva autentifikovana službenika u isto vreme koji moraju biti u istoj prostoriji određenoj za tu namenu. Ista dva službenika ne mogu raditi zajedno pretrage više od jednom sedmično.
Mere zaštite od rizika koji nastaju pri promeni poslova ili prestanka radnog odnosa	Organizaciona	Nakon prestanka radnog odnosa ili premeštaja na drugo radno mesto u okviru MUP, korisnički nalozi za pristup sistemu kojima je isteklo ovlašćenje moraju biti deaktivirani i arhivirani, tj. mora biti onemogućen pristup sistemu sa tih naloga u najkraćem mogućem roku.
Ograničeno čuvanje šablona biometrijskih podataka	Organizaciona	Šabloni biometrijskih podataka nastalih upotrebom sistema ne smeju se čuvati duže od 72 sata od trenutka izdvajanja šablona, odnosno nakon tog roka se moraju obrisati.

- **Baze za ukrštanje podataka**

U Proceni uticaja se na više mesta navodi da se u cilju jedinstvene identifikacije biometrijski podaci prikupljeni upotrebom softvera mogu upoređivati sa biometrijskim podacima iz „postojećih“ evidencija. Smatramo da načela propisana ZZPL-om – a naročito načelo zakonitosti, poštenja i transparentnosti, načelo ograničenosti u odnosu na svrhu obrade, te načelo minimizacije – zahtevaju da se **konkretno definišu evidencije koje bi se koristile u cilju jedinstvene identifikacije lica.**

Srdačno,
SHARE Fondacija