

Komentari 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, 08.12.2022.

Poštovani,

Obraćamo vam se u vezi sa dopunjenim radnim tekstom “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 21.11.2022. godine i o kome se diskutovalo na zajedničkom sastanku MUP-a, organizacija civilnog društva i ostalih zainteresovanih strana 30.11.2022. godine.

Želimo pre svega da ponovimo 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. Takođe, u procesu izrade Zakona o veštačkoj inteligenciji (AI Act), [177 poslanika u Evropskom parlamentu](#) tražilo je **zabranu masovnog biometrijskog nadzora** nad javnim prostorima.³

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

³ European Parliament calls loud and clear for a ban on biometric mass surveillance in AI Act, 14.09.2022.
<https://edri.org/our-work/european-parliament-calls-loud-and-clear-for-a-ban-on-biometric-mass-surveillance-in-ai-act/>

Ipak, i dalje 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 civilnog društva, te da su određeni komentari koje smo vam uputili 03.06.2022. godine implementirani u novu verziju Procene uticaja. Verujemo da je izrada **sveobuhvatne, precizne i informativne Procene uticaja** preduslov za dalje razmatranje ovog pitanja, u opštem interesu društva. U skladu s tim, dostavljamo komentare na poslednju verziju Procene uticaja.

- **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,⁴ te na strani 5 obrasca za procenu uticaja koji je izradila kancelarija britanske poverenice za zaštitu podataka⁵ ili na stranama 6 i 7 sličnog obrasca britanskog komesara za nadzorne kamere⁶).

- *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?*

⁴ Necessity Toolkit, 11.04.2017.

https://edps.europa.eu/data-protection/our-work/publications/papers/necessity-toolkit_en

⁵ Sample DPIA template, <https://ico.org.uk/media/for-organisations/documents/2553993/dpia-template.docx>

⁶ Data protection impact assessments,

https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/886883/CC_ICO_DPIA_Template_V4_.docx

- *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?*
- *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**.

- **Procena rizika po prava i slobode lica**

Smatramo da predložena matrica ne oslikava realno uticaj rizika na ljudska prava i slobode. Ugrožavanja koja mogu da nanesu velike posledice čak i ako je verovatnoća njihovog ostvarenja veoma mala, moraju se krajnje ozbiljno uzeti u obzir i te ugrožene vrednosti se neizostavno moraju štiti i ne bi ih trebalo svrstati u neznatne rizike. Stoga predlažemo **novu matricu** i novo definisanje prihvatljivosti rizika:

Stepen ugroženosti / ozbiljnost posledica	Visok	5	10	15	20	25
	Pretežno visok	4	8	12	16	20
	Srednji	3	6	9	12	15
	Pretežno nizak	2	4	6	8	10
	Nizak	1	2	3	4	5
PROCENA RIZIKA		Mala	Pretežno mala	Srednja	Pretežno velika	Velika
		Verovatnoća ostvarenja pretnje				

Legenda

1-3 NEZNATNA (ne zahteva se nikakva aktivnost)

4-6 DOPUSTIVA (nema potrebe za dodatnim aktivnostima, potrebno je pratiti situaciju)

7-11 UMERENA (potrebno je u narednom periodu planirati mere, pratiti pojedine aktivnosti i definisati način kontrole)

12-15 ZNATNA (potrebni su efikasni mehanizmi kontrole primene mera za smanjenje rizika)

16-25 NEDOPUSTIVA (obradu podataka ne bi trebalo vršiti)

Ovako predložena matrica ravnomerno tretira sve nivoe rizika. To se jasno vidi poređenjem sa matricom koja je predložena u Proceni uticaja:

Procenjeni nivo rizika	Broj polja (Procena uticaja)	Broj polja (naš predlog)
Neznatni	10	5
Umereni	7	7
Dopustivi	4	5
Znatni	1	4
Nedopustivi	3	4

Konačno, i pored niskih kriterijuma za ocenu rizika, **Neselektivna upotreba softvera za prepoznavanje lica i Profilisanje lica** su u proceni uticaja ocenjeni kao **nedopustivi rizici**, te naknadno primenom tehničkih i organizacionih mera svedeni na znatne rizike. Smatramo da su ovi rizici ispravno procenjeni, te ističemo da se nedopustivim rizicima ne upravlja, a naročito da se oni ne mogu umanjiti primenom tehničkih i organizacionih mera.

- **Mere i mehanizmi zaštite u odnosu na rizik po prava i slobode lica**

U novoj radnoj verziji Procene uticaja prihvaćen je veliki broj komentara i predloga SHARE Fondacije u pogledu tehničkih i organizacionih mera zaštite. Nažalost, navedene mere su opšteg karaktera, te nije prikazan konkretan i odgovarajuć uticaj u smislu upravljanja rizicima. Primera radi, samo bezbednosne provere kandidata za prijem u radni odnos u Ministarstvu i kontinuirana edukacija ovlašćenih policijskih službenika nisu dovoljne preventivne organizacione mere, imajući u vidu kompleksnost sistema, mogućnosti zloupotreba i rizike koje sa sobom nosi obrada biometrijskih podataka velikog broja građana.

Sistem je u Proceni uticaja postavljen na način koji ostavlja veliki prostor za curenje podataka, jer predviđa niz načina za iznošenje podataka iz sistema na eksterne

medije, kao što su memorijske kartice, CD, DVD, USB fleš memorije, eksterni hard diskovi i drugi mediji za prenos podataka, gde MUP gubi svaku mogućnost kontrolisanja kopiranja podataka sa ovih medija i njihovo curenje, deljenje sa neovlašćenim licima i objavljivanje. Već smo bili svedoci sličnih situacija, poput curenja snimka sudara ispred zgrade Vlade Republike Srbije, dok u tim slučajevima javnosti nije poznato da li su odgovorni počionioci pronađeni i adekvatno procesuirani.

- **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