

Comments on the Draft Impact Assessment of personal data processing activities by using biometric data processing software within the video surveillance system of the Ministry of Interior on personal data protection

Belgrade, 8 December 2022

Dear Sir/Madam,

We are hereby writing to you on the subject of the amended working document titled *"Draft Impact Assessment of personal data processing activities by using biometric data processing software within the video surveillance system of the Ministry of Interior on personal data protection"* (hereinafter: Impact Assessment), which was sent to us on 21 November 2022 and was discussed on the meeting of the Ministry of Interior (Mol), civil society and other interested parties on 30 November 2022.

First, we would like to reiterate that SHARE Foundation is still **against any use of biometric surveillance in public spaces**, both in the domestic and international context. Our principal standpoint has been reinforced through our work and membership in [EDRi](#), the most important digital rights network in Europe, the [Reclaim your face](#) movement which gathers almost a hundred organisations from across the world advocating for the ban of mass biometric surveillance, as well as the local [#hiljadekamera](#) ("Thousands of Cameras") initiative, a community of individuals and organisations demanding responsible use of surveillance technology.

The application of this technology would have **devastating consequences for democratic society and citizens' rights and freedoms**, because of which the [UN Human Rights Commissioner](#) recommended introducing a **moratorium** on the use of biometric surveillance technology in public spaces.¹ Also, the [European Data Protection Supervisor \(EDPS\)](#) and the [European Data Protection Board \(EDPB\)](#) called for a **general ban** on the use of advanced technologies for automated biometric personal data processing in public spaces.² It should also be noted that a [series of cities in the United States](#) **have already banned** the use of biometric surveillance in public spaces. Also, during the process of drafting the AI Act, [177 Members of the](#)

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

[European Parliament](#) asked for the ban on mass biometric surveillance in public spaces.³

Nevertheless, we still believe that it is necessary to open a **transparent debate** about the possibilities of using this technology, i.e. the benefits, risks and consequences that it inherently carries with it. We are aware that the Ministry has invested significant resources in the preparation of the Impact Assessment and a series of open discussions with interested civil society organisations, and that certain comments we sent you on 3 June 2022 were implemented in the new version of the Impact Assessment. We believe that the preparation of a **comprehensive, precise and informative Impact Assessment** is a prerequisite for further consideration of this issue, in the general interest of society. Accordingly, we are submitting comments on the latest version of the Impact Assessment.

- **Necessity and proportionality assessment**

The basic prerequisites for the use of biometric surveillance in our legal framework are **necessity** (Article 13 of the Law on Personal Data Protection (LPDP), Article 5 of the Convention 108+ and Article 8 of the European Convention on Human Rights) and **proportionality** (Article 14, paragraph 3 of the LPDP and Article 5, paragraph 1 of the Convention 108+) of such data processing. The requirements of necessity and proportionality will be key to making a decision as to whether this kind of data processing would be allowed in our society, and we believe that **their proof and demonstration is a basic prerequisite** in the preparation of the Impact Assessment. Therefore, although the assessment of necessity and proportionality is not listed as a formal element of the Impact Assessment of processing carried out by competent authorities for special purposes, it certainly represents an indirect requirement and the basis on which all other issues addressed in the Impact Assessment are assessed.

Our position is that the information contained in the Impact Assessment **does not prove** that the processing of large amounts of biometric data is **necessary** for the performance of specific purposes, nor that it is **proportionate** to the risks to the rights and freedoms of citizens. For adequate consideration of these conditions, we propose a **minimum list of questions** to which answers must be provided in order to prove necessity and proportionality, based on accepted European standards (as it is inter alia stated in the EU Data Protection Supervisor Necessity Toolkit,⁴ on page 5 of

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/>

⁴ Necessity Toolkit, 11.04.2017.
https://edps.europa.eu/data-protection/our-work/publications/papers/necessity-toolkit_en

the template published by the UK Information Commissioner's Office⁵ or on pages 6 and 7 of a similar template provided by the UK Surveillance Camera Commissioner⁶).

- *What are the purposes to be achieved and the problems to be solved (if there are more of them, define each separately)?*
- *How does the intended processing achieve a specific purpose and solve a specific problem?*
- *How is it measured whether the intended processing achieves a specific purpose and solves a specific problem?*
- *Is there another reasonable way, i.e. a less intrusive measure to achieve a specific purpose and solve a specific problem?*
- *Can existing measures and procedures achieve a specific purpose and solve a specific problem?*
- *How will it be prevented that the collected data is not being used for other purposes?*

- **Court decision as a prerequisite for biometric surveillance**

Biometric surveillance in public space is an extremely intrusive measure, which carries with it numerous risks for the basic freedoms and rights of citizens. Therefore, we believe that any further consideration of the use of facial recognition technology must take as a starting point the **previous decision of the court as a prerequisite for any specific use of this technology**. This is particularly important given that the Impact Assessment envisages the use of biometric surveillance in extremely restrictive situations, and that the method and purpose of the envisaged data processing are to a significant extent reminiscent of the **special evidentiary actions** provided for by the Criminal Procedure Code (CPC), and in particular **secret monitoring and recording** (Articles 171-173 of the CPC) and **computer data search** (Articles 178-180 of the CPC) which also require a **court decision**.

- **Rights and freedoms risk assessment**

We believe that the proposed matrix does not realistically reflect the impact of risks on human rights and freedoms. Threats that can cause major consequences even if the probability of their realisation is very small must be taken extremely seriously and the threatened values must be protected in full and should not be classified as insignificant risks. Therefore, we propose **a new matrix** and a new definition of risk acceptability:

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/SCC_ICO_DPIA_Template_V4_.docx

Threat degree / Severity of consequences	High	5	10	15	20	25
	Mostly High	4	8	12	16	20
	Medium	3	6	9	12	15
	Mostly Low	2	4	6	8	10
	Low	1	2	3	4	5
RISK ASSESSMENT		Low	Mostly Low	Medium	Mostly High	High
		Probability of threat realisation				

Legend

1-3 INSIGNIFICANT (no activity required)

4-6 ACCEPTABLE (no need for additional activities, it is necessary to monitor the situation)

7-11 MODERATE (in the following period, it is necessary to plan measures, monitor certain activities and define the method of control)

12-15 CONSIDERABLE (effective mechanisms for controlling the application of risk reduction measures are needed)

16-25 UNACCEPTABLE (data processing should not be performed)

The matrix proposed in this way treats all risk levels equally. This is clearly seen by comparing it with the matrix proposed in the Impact Assessment:

Assessed risk level	Number of fields (Impact Assessment)	Number of fields (our proposal)
Insignificant	10	5
Moderate	7	7
Acceptable	4	5
Considerable	1	4
Unacceptable	3	4

Finally, despite the low criteria for risk assessment, **Indiscriminate use of facial recognition software** and **Profiling** were assessed as **unacceptable** risks in the, and subsequently reduced to significant risks through the application of technical and

organisational measures. We believe that these risks have been correctly assessed, and we emphasise that unacceptable risks are not managed and especially that they cannot be reduced by applying technical and organisational measures.

- **Protection measures and mechanisms in relation to the risk to the rights and freedoms of persons**

In the new working version of the Impact Assessment, a large number of SHARE Foundation's comments and proposals regarding technical and organisational protection measures have been accepted. Unfortunately, the mentioned measures are general and no specific and appropriate impact in terms of risk management has been shown. For example, only security checks of candidates for employment in the Ministry and continuous education of authorised police officers are not sufficient preventive organisational measures, bearing in mind the complexity of the system, the possibility of abuse and the risks involved with processing biometric data of a large number of citizens.

The system in the Impact Assessment is set up in a way that leaves a lot of room for data leaks, as it foresees a number of ways to export data from the system to external media, such as memory cards, CDs, DVDs, USB flash drives, external hard drives and other media for data transmission, where the Ministry of Interior loses any possibility of controlling the copying of data from these media and their leaking, sharing with unauthorised persons and publication. We have already witnessed similar situations, such as the leak of the video of a car crash in front of the building of the Government of the Republic of Serbia. The public does not know whether the responsible perpetrators concerning these cases have been found and adequately prosecuted.

- **Cross-referencing databases**

The Impact Assessment states in several places that for the purpose of unique identification, biometric data collected using software can be compared with biometric data from "existing" records. We believe that the principles prescribed by the Law on Personal Data Protection - and in particular the principle of legality, honesty and transparency, the principle of limitation in relation to the purpose of processing, and the principle of minimisation - require that the **records that would be used for the purpose of unique identification of a person be specifically defined.**

Sincerely,
SHARE Foundation