Assessment of the Impact of Personal Data Processing Using Biometric Data Processing Software in the Video Surveillance System of the Ministry of Interior [of the Republic of Serbia] on the Protection of Personal Data

1. Description of Data Processing

In accordance with the legal powers of the police, police officers undertake the necessary measures in order to determine the identity of an individual.

Based on the data from a video recording retrieved from the video surveillance system of the Ministry of Interior, the identification of an individual, in accordance with the existing Law on Police, without processing biometric data, can be carried out: [a] through recognition during the recording by an authorized police officer or [b] through recognition in subsequent examination of the recorded material by an authorized police officer, or by another person who is, in accordance with the law, allowed to view the video.

Pursuant to the Draft Law on Internal Affairs, the measures taken in order to identify an individual may include the processing of biometric data using facial recognition software in the video surveillance system.

The legal basis for the processing of biometric data is the law and not the consent of an individual, and biometric data is processed on the basis of the law regulating data processing in the field of internal affairs.

The locations and time of use of cameras connected to facial recognition software are determined in order to protect the interests of public and national security, to prevent disorder (public order and peace) or crime, as well as to protect the rights and liberties of others (Art. 8, paragraph 2 of the European Convention on Human Rights)[1] based on a profile of a security problem[2] or on a profile of a person of security interest[3] or on an assessment of events of security interest using the police-intelligence model.

Processing of biometric data is performed by detecting an individual during the recording, while simultaneously creating a photo/image of a face from a video recording and extracting biometric data from such a photo in the form of a biometric pattern/digital code.

The purpose of processing biometric personal data is the prevention, investigation and discovery of criminal offences, the prosecution of perpetrators of criminal offences, as well as the prevention and protection against threats to public and national security. The Draft Law on Internal Affairs gives the possibility to an authorized police officer to use facial recognition software in the video surveillance system during identity checks, in order to:

- find the perpetrator of a criminal offense for which prosecution is undertaken ex officio;
- find the individual who is reasonably suspected of preparing the commission of the crime of terrorism and related crimes;
- find the wanted person.

---

[1] ARTICLE 8 **Right to respect for private and family life**: 1. Everyone has the right to respect for his private and family life, his home and his correspondence. 2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

[2] A set of data and information collected in order to review, clarify and better understand existing and new forms of crime, in order to initiate or support police activity towards them. - Source: MOI (2016): Manual: “Police-Intelligence Model”, available at: www.mup.gov.rs.

[3] A set of data and information about persons of security interest, criminal groups, victims and witnesses of criminal acts, which initiates or supports operational-police activity towards them. - Source: MOI (2016): Manual: “Police-intelligence model”, available at: http://www.mup.gov.rs/wps/wcm/connect/23a0498f-e93a-4fd3-a507-6ebc568cd10e/Prirucnik+POM+sajt+7.10.2016.pdf?MOD=AJPERES&CVID=mC0sR8O [in Serbian]

The justification of the processing purpose is based on the need to achieve the goals of processing specified by the law, bearing in mind that the Ministry of Interior is the competent authority legally authorized to process biometric personal data for the purpose of unique identification of an individual, and that processing biometric data as a special category data can also be used for the purpose of protecting the vital interests of the data subject or another natural person.

In accordance with the principle of minimization, personal data is collected through the use of facial recognition software, in accordance with the legal powers of the police, and only personal data that are appropriate and essential for determining the identity only of those individuals in relation to the specific purpose of processing are further processed and are not processed for other purposes.

In order to uniquely identify only certain individuals, biometric data collected using face recognition software can be compared with biometric data from existing records, collected for some other purposes (e.g. with biometric data contained in the records of forensically registered individuals).

In accordance with the Law on Personal Data Protection provisions, the Ministry of Interior of the Republic of Serbia is the controller of the data processed within the video surveillance system, that is by using facial recognition software. The Ministry processes data independently, by engaging its own resources.

The recipient of data processed by the Ministry can only be another competent authority, in the sense of Art. 4, item 26 of the Law on Personal Data Protection. The data can also be transferred to the recipient (a competent authority) in another country or to an international organization, in accordance with the law.

Regarding the use of facial recognition software, the Ministry informs the individuals covered by the video surveillance connected to the facial recognition software, through the media and other means of public information (public information media, internet presentations and alike).

PERSONAL DATA BEING PROCESSED

With the use of video surveillance, the following data on natural persons are processed: video recording of the event in which an individual participates, time and place of video recording and

GPS location of the camera, license plates and other vehicle markings, by using individual cameras from the video surveillance system that are connected to facial recognition software the image of a natural person (photo of the face) with separated biometric data in the form of a *pattern/digital code* is also processed.

PROCESSING OPERATIONS

The processing of biometric data in the video surveillance system includes the following processing operations: collection, classification, archiving, access, search, extraction, copying, transmission, comparison, restriction, storage and deletion, or destruction in another way.

Data from video recordings, i.e. video recordings are automatically generated and sorted by the time the video was created and the location of the recording/GPS location of the camera.

The collection of biometric data is performed by detecting an individual during recording, creating a photo of an individual/image of the face from a video recording and extracting biometric data from such a photo in the form of a pattern/digital code.

Detected faces, i.e. photos of individual/images of the face extracted from video recordings, as well as biometric data extracted in the form of a pattern/digital code are automatically generated and sorted by the time of the detection of an individual/creation of the photo or pattern/digital code and by the place of the detection of an individual/GPS location of the camera.

Video records from the cameras are stored on hard storage devices (hard drives, memory cards) of the central data storage system (data center) and are stored according to the circular recording system, i.e. the system automatically cyclically deletes the oldest data when the memory space is full, but not before expiration of 30 days from the day of the recording.

Photographs of detected individuals, with separated biometric data in the form of a pattern/digital code, are stored on the hard storage device of the same central data storage system (data center), but separately from the videos, and are stored for a maximum of 72 hours from the moment the photograph was created.

Access to the data from the video in real time (live stream) is enabled to an authorized police officer[4] through direct observation, in the user center.

[4] For the purposes of this assessment, an authorized police officer is a police officer who is assigned to a workplace whose description includes operating a video surveillance system.

Access to the stored video data in the user center is performed by searching and extracting the selected video on the “workstation” for its playback.

The search of stored videos is performed according to search criteria such as: location or name of the camera/camera site, date and time of the video recording, and the search is also possible based on other criteria using special analytical tools.

Searching and viewing of stored data from video recordings is possible only for authorized police officers in the user center with a special permit or approval. Searching and viewing are limited to the purpose and goals of data collection, and their further processing is carried out in accordance with the powers of police officers (prosecution order or court order, subject of operational processing, etc.).

Access to photographs/images of faces of detected individuals at the time of detection is only possible for authorized police officers in the user center with a special permit or approval.

Searching stored photos and extracting them for viewing at the workstation is performed according to search criteria such as: location or name of camera/camera location, date and time of photo creation.

This search and viewing of photos of detected individuals/faces is limited to the purpose and goals of biometric data processing and their further processing is carried out in accordance with the powers of police officers (prosecution order or court order, subject of operational processing, etc.). The search of stored separated biometric data in the form of a pattern/digital code is performed using special tools, semi-automated or automated.

A) Semi-automated search (for comparison) of stored biometric data is performed by an authorized police officer, through selecting a specific stored photo/image of a face with extracted biometric data in the form of a pattern/digital code from that photo and querying the facial recognition software that checks their compatibility with biometric data from other records that are linked to facial recognition software for the purposes of that comparison.

These police officers are trained and have rights of access to the video surveillance system. Not all police officers have the same level of access. An authorized police officer also means a police officer who, in a specific case, is in charge of establishing the identity of the perpetrator and other necessary facts related to a criminal act. This police officer receives the order to act from their superior.

This type of biometric data matching is used in cases where it is necessary to identify an unknown perpetrator whose face was detected by one of the cameras connected to the facial recognition software. In such cases, biometric data is compared with data from, for example, the records of forensically registered individuals, where the face recognition software performs a comparison in order to determine whether the biometric data from the photo matches the biometric data from other records. In such cases, the principle of graduality and proportionality, that is the necessity of data processing, is applied as follows: If, for example, the crime of robbery was committed by a male person, the biometric data of the registered male perpetrators of robbery are first extracted from the records of forensically registered individuals in order to find matching biometric data. If the search provides no results, then the biometric data of registered perpetrators of other criminal acts is also extracted. If this search also provides no results, then biometric data from other records are also used.

A semi-automated search of stored biometric data is also possible in situations involving a known perpetrator of a criminal offense or, for example, a wanted person whose biometric data the Ministry already has in its records or has obtained for the purposes of the search. In such cases, at the request of an authorized police officer, the available/acquired biometric data of that individual is linked to facial recognition software which searches the stored data to find biometric data that match the acquired data. This type of biometric data matching check is performed in cases where it is necessary to determine whether one of the cameras connected to the facial recognition software has detected the person the police are looking for.

Also, a photo can be extracted from the stored videos taken by one of the cameras not connected to the facial recognition software, using the appropriate tools, and the facial recognition software will extract biometric data from such a photo in the form of a pattern/digital code, which can be used in already described manner for searching or comparing matches with available biometric data.

B) Automated (simultaneous) comparison of biometric data at the time of detection of an individual and extraction of biometric data is possible only by connecting biometric data that are stored in other records, which the Ministry maintains in accordance with the Law on Records and Data Processing in the Field of Internal Affairs (“Official Journal of the RS”, No. 24/18), with facial recognition software (for example, a database containing information about terrorists/extremists, a database of wanted persons, a database of missing children, a database of persons issued with a ban from attending sports events, a database of persons convicted of

crimes against sexual freedom of minors, etc.). The software performs an automated comparison of biometric data and has the possibility of creating different types of alarms in case of a match. If, during the automated comparison of biometric data, the software finds matching data, the result of the comparison is recorded on the system, displayed to the user on the workstation in the form of a report with the matching result, with the possibility of creating different types of alarms.

The automated comparison of biometric data is limited and can only be applied at certain locations in accordance with the created profile of the security problem and can last only for a certain period of time. This type of data processing is limited only to [the data of] individuals for whom, based on the previously created profile of a person of security interest, the processing is necessary for the purpose of analyzing or predicting their behavior or location of movement. Such processing is in accordance with the principles of legality, legitimacy, necessity and proportionality. For each person individually, the authorized police officer makes a decision on taking other measures and actions and applying police powers with the aim of unique identification. This means that the identity of a person is not determined solely on the basis of automated data processing, i.e. the so-called automatic face recognition is not applied.

The decisions of authorized police officers regarding a person are not applied solely on the basis of automated processing, but in each specific case the role of the police officer is necessary in terms of determining the purpose and method of applying the specific processing action. After the identification of a person, actions can be taken or decisions can be made that produce legal consequences for that person, i.e. affect the person's position.

The extracted videos and photos can be transferred by copying, in accordance with the law, from the workstation to another data carrier (memory cards, CD/DVD, USB flash drives, etc.) for the purpose of viewing and other processing actions outside the user center. In addition to copying to another data carrier, photos can be copied/duplicated by printing on paper.

In individual cases, copied data can be transferred to authorized recipients/other competent authorities (prosecutor's office, court) or to the data subject, by delivering it on a data carrier.

The stored data is automatically permanently deleted in the video surveillance system on the central storage system. Data on the basis of which the identity of the person is not determined is stored for at least 30 days from the date of collection. The period of 30 days prescribed by Art. 47, paragraph 3 of the Law on Records and Data Processing in the Field of Internal Affairs, is

conditioned by the technical limitations of storing data collected in the video surveillance system and is shorter than the deadline set by the Law on Police (Art. 52).

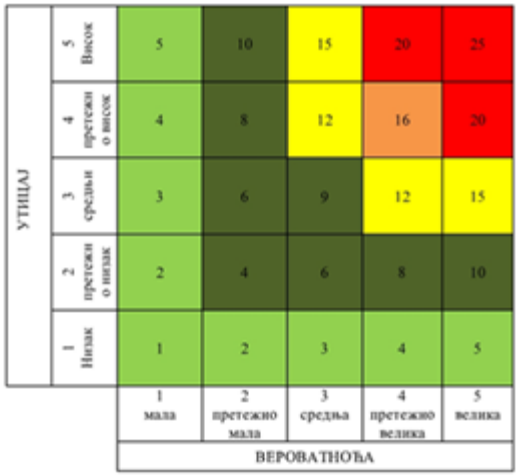
In case of extracting and transferring data for the purpose of viewing outside the user center, the data is stored in accordance with the law.

The data on the basis of which the identity of the person has been determined is transferred to the information carrier and stored for the period prescribed by law, which is necessary to achieve the purpose of the processing.

2. Assessment of Risk to Personal Rights and Liberties

Following the analysis of the data processing actions, the risks to the rights and liberties of persons that may be caused by the use of facial recognition software were identified and assessed. Measures for control and risk reduction were defined, after which the residual risk was assessed. The Ministry, as the personal data controller, will periodically update the risk analysis in accordance with the emergence of threats.

Risk ranking was performed by intersecting impact and probability, and a 5x5 risk matrix was used to measure risk.



The total risk exposure is presented as the product of ranked impact and probability, and the obtained risk exposure results can be presented as following:

1-5 MINOR (no action required)

6-10 PERMISSIBLE (there is no need for additional activities, it is necessary to monitor the situation)

11-15 MODERATE (in the following period it is necessary to plan other measures, monitor certain activities and define the control method)

16-20 SIGNIFICANT (effective mechanisms for the control of risk reduction measures application are needed)

21-25 UNACCEPTABLE (data processing should not be carried out until the risk is reduced)

IDENTIFIED RISKS

Processing of biometric data of an unspecified number of persons - indiscriminate use of facial recognition software

This risk is related to the use of software for collecting and storing biometric data of an unspecified number of persons who happen to be in the recording zone, for the purpose of searching for the matching of their data with the available data of a much smaller number of persons, either at the time of their collection or subsequent search.

With this type of data processing, it is not possible to make the necessary distinction between certain types of persons (Article 9 of the Law on Personal Data Protection), i.e. the facial recognition software collects the data of every person who happens to be in the recording area, and in the case of “recognition” that person is treated as a “potential suspect”.

The processing of the data of every “passer-by” seriously affects the reasonable expectations of persons to be anonymous in the public space, which is a prerequisite for many aspects of the democratic process, such as, for example: the free decision to associate with others, attend gatherings and meet people from other social and cultural backgrounds, participate in political protest and alike.

The use of facial recognition software when conducting surveillance in public space creates the feeling in persons that they are under constant surveillance, without even being sure if this is really the case. This feeling can affect the behavior of individuals, which further affects the character of society. An additional aspect of this feeling among individuals is the deterrence from meeting or seeing in public with certain persons (relatives, friends) who are assumed to have had or may have a “problem” with the police. When using facial recognition software in public spaces, it is impossible to limit its application in such a way as to ensure confidential contact with certain persons (such as contact with journalists, lawyers, clergy, doctors, etc.). Also, it is impossible to “protect” particularly sensitive groups of people, such as children, from using this software in a public space. The indiscriminate use of facial recognition technology, where all persons found in a certain area can be subject to processing, in addition to the aforementioned, threatens the right to the presumption of innocence.

The level of impact of violations of the rights and liberties of persons is: mostly high (4)

The level of probability of violations of the rights and liberties of persons is: high (5)

Exposure to the risk of violations of rights and liberties is: unacceptable (20)

Risk control is performed using organizational and technical measures.

The use of facial recognition software must be based on the created profile of the security problem, i.e. the profile of a person of security interest, and the locations and time of use of the cameras connected to the facial recognition software must be determined based on the assessment of security-interesting events using the police-intelligence model, namely: for the purpose of finding the perpetrator of a criminal offense for which the prosecution is undertaken ex officio; finding a person who is reasonably suspected of preparing the commission of the crime of terrorism and related crimes; finding the wanted person.

Photos of detected persons, with extracted biometric data in the form of a pattern/digital code, can be stored on a hard device of the central data storage system (data center) and stored for a maximum of 72 hours from the moment the photo was created. Access to these photos can only be provided to authorized police officers in the user center with a special permit or approval. The search of stored photos and their extraction must be limited to the purpose and goals of processing biometric data and their further processing can only be carried out in accordance with the police officers' authorization (prosecution order or court order, subject of operational processing, etc.). Only an authorized police officer, for the purpose of unique identification, makes a decision on taking other measures and actions and applying police powers, and only for each person individually. The identity of a person will not be determined solely on the basis of automated data processing, that is, the so-called automatic facial recognition will already in each specific case be a necessary role of a police officer in terms of determining the purpose and method of applying a specific processing action.

The police officers' course of action when using software for facial recognition must be based on the organizational structure in the system of assigned roles in terms of performing individual processing actions and deciding on the need for individual identification of a person, which would enable identification only of those persons without whose data processing the purpose of processing cannot be achieved.

The users of this system are police officers who have to have education in legal conditions and the way of exercising police powers, measures and actions, in the established standards of

police work and in the legal regime for the protection of personal data when using this system. Each police officer is assigned with credentials to access the system, which are revoked upon changing jobs or termination of employment, i.e. the access levels are updated. Every access to the system is automatically recorded (system log). Data is stored on the central storage system for a maximum of 72 hours, after which it is automatically deleted.

By applying organizational and technical measures, the residual risk is reduced, but the exposure to risk is considerable, which is further reduced by effective control mechanisms for the application of all protection measures and timely reporting.

The level of impact of violations of the rights and liberties of persons is: mostly high (4)

The level of probability of violations of the rights and liberties of persons is: predominantly high (4)

Exposure to the risk of violations of rights and liberties is: considerable (16)

Risk of insufficient transparency

The risk of insufficient transparency is related to the way of exercising the right to be informed of persons whose data is processed using facial recognition software, that is to insufficient information of persons about whether and in which situations they have been or are still subject to surveillance.

The use of this kind of technology in the public space creates a feeling among people that they are subject to constant surveillance, while not being sure if this is really the case, as a result of which they may have a feeling of insecurity, i.e. uncertainty about the exercise of human rights and liberties, not only the rights guaranteed by the regulations on personal data protection.

The absence or lack of information about the use of facial recognition software further deepens the feeling of insecurity, i.e. discomfort.

The level of impact of violations of the rights and liberties of persons is: medium (3)

The level of probability of violations of the rights and liberties of persons is: medium (3)

Exposure to the risk of violations of rights and liberties is: permissible (9)

Risk control is carried out by applying the intended organizational and technical measures.

Through the transparent use of video surveillance, the subjective feeling of a threat to the right to privacy is reduced, thereby raising citizens' awareness of the level of risk to this right of theirs.

In accordance with the Rulebook on the method of recording in a public place and the method of communicating the intention of such recording (“Official Journal of the RS”, No. 111/20) on the use of software for facial recognition, the Ministry will pass the information to the media and other means of public information (media, internet presentations etc.) to notify the public and thus all persons who may be covered by video surveillance connected to facial recognition software.

The location of the cameras (sports stadiums, border crossings and other places with a high frequency of people) where facial recognition software will be functional, which is performed by simultaneous-automated comparison of biometric data at the moment of detection of a person, must be clearly marked so that all persons who come across at that location are enabled to become familiar with the fact that upon arriving at a certain location, they will actually be under surveillance which includes the processing of their biometric data.

In addition to being informed, individuals must also be enabled to exercise their rights in connection with personal data processing (right to access, copy, deletion or other rights in accordance with the law). The information must also contain notice on how to exercise rights with the data controller (e.g. by submitting a request to the Ministry of Interior for the territorially competent police department, by the location of the cameras).

With the implementation of risk reduction measures, the likelihood of a violation of a person's rights and liberties is also reduced, but there has to be an awareness that despite all the measures taken, there will always be people who will not be informed or who will not understand clearly enough the information provided to them, so that the residual risk, that is the exposure to risk is reduced but remains permissible and can be controlled by effective action according to the requests of citizens for the exercise of rights in connection with the processing of personal data.

The level of impact of violations of the rights and liberties of persons is: medium (3)

The level of probability of violations of the rights and liberties of persons is: mostly low (2)

Exposure to the risk of violations of rights and liberties is: permissible (6)

Profiling of individuals

The risk to individual rights and liberties is related to the possibility of profiling a person. Facial recognition software, as a form of automated data processing, can be used to assess a certain personality trait, especially for the purpose of analyzing or predicting behavior, locations, movements or personal preferences (based on real or assumed affiliation to an association, i.e. religious community, political or other opinion, sexual orientation or other real or assumed personal characteristic). It is the controller's obligation to inform the data subject about the possibility of profiling and to provide additional information that may be necessary to ensure fair and transparent processing.

It is prohibited to make a decision solely on the basis of automated processing carried out by the Ministry as a competent authority for special purposes, including profiling, if such a decision can produce harmful legal consequences for the person to whom the data refer or significantly affect the position of that person, unless making that decision is based on the law and if that law prescribes appropriate measures to protect the rights and liberties of the person to whom the data refer, and at least the right to ensure the participation of a natural person under the controller's supervision in making the decision. Profiling that leads to discrimination of natural persons based on special categories of personal data is prohibited.

The risk to the rights and liberties of individuals is illegal profiling, which would entail making a decision based on automated processing without applying appropriate measures to protect individual rights and liberties, i.e. any form of discrimination based on special category data and which does not aim to analyze or predict behavior, location, the movement of the perpetrator of a criminal offense for which prosecution is undertaken ex officio, finding a person who is reasonably suspected of preparing the commission of a criminal offense of terrorism and related criminal offenses, finding a wanted person.

The level of impact of violations of the rights and liberties of persons is: high (5)

The level of probability of violations of the rights and liberties of persons is: high (5)

Exposure to the risk of violations of rights and liberties is: unacceptable (25)

Risk control is carried out by applying the intended organizational and technical measures.

Data processing carried out by competent authorities for special purposes, which reveals racial or ethnic origin, political opinion, religious or philosophical belief or trade union membership, as well as processing of genetic data, biometric data for the purpose of unique identification of a natural person, data on health status or data about the sexual life or sexual orientation of a natural person is allowed only if it is necessary, with the application of appropriate measures to protect the rights of the person to whom the data refer, in cases where the competent authority is authorized by law to process special categories of personal data; when the processing of special category data is carried out in order to protect the vital interests of the data subject or of another natural person, or when the processing refers to special category data that the person to whom they refer has obviously made available to the public.

Making any decision that produces legal consequences, i.e. that affects the position of the person to whom the data refers must be based on the law and appropriate measures must be taken to protect the rights and liberties of the person, at least the right to ensure the participation of a natural person (an authorized police officer) in making a decision.

For each person individually the authorized police officer is obliged to make a decision on taking measures and actions or applying police powers in order to uniquely identify that person. Therefore, the identity of a person is not determined solely on the basis of automated data processing, but in each specific case the involvement of a police officer is necessary in determining the purpose and method of applying a specific processing action. Only after such identification of a person, actions can be taken or decisions made that produce legal consequences for that person, i.e. that affect the person's position.

The police officers' course of action is based on the organizational structure in the system of assigned roles in terms of performing individual processing actions and deciding on the goal of analyzing the tendencies, behavior and movement of persons, which reduces the possibility of illegal profiling.

Such permitted profiling must be carried out with the application of adequate organizational data protection measures such as the management of user accounts, software generation of search queries, dual access to the system and limited storage of biometric data patterns.

Data processing can only be carried out with the application of appropriate technical data protection measures such as: equipment access control, data carrier control, data storage control, user control, data access control, transfer control, transport control, system recovery, ensuring system integrity, management of user accounts, system log, physical and technical protection of facilities and equipment, protection against damage and theft of resources that make up the video surveillance system.

This system can be used only by qualified and educated police officers. Police officers must be educated about the legal conditions for profiling as well as the way of applying police powers, measures and actions, about the established standards of police work and about the legal regime for the protection of personal data. An additional measure to protect against the risks that arise when police officers change jobs or terminate their employment is termination of accounts for accessing the system, i.e. access levels must be updated. The mechanism for determining disciplinary responsibility is both a preventive and a reactive data protection measure that needs to be applied.

With the implementation of the said risk reduction measures, the residual risk is reduced, but it is still significant, and in order to control it, effective risk exposure control mechanisms are necessary.

The level of impact of violations of the rights and liberties of persons is: mostly high (4)

The level of probability of violations of the rights and liberties of persons is: mostly high (4)

Exposure to the risk of violations of rights and liberties is: considerable (16)

Biometric data in the records for comparison are not accurate

By selecting a particular stored photo with extracted biometric data in the form of a pattern/digital code from that photo and querying the facial recognition software by an authorized police officer, a match is checked with the biometric data from other records that are connected to the facial recognition software for the purpose of that comparison. Also, the automated (simultaneous) comparison of biometric data at the moment of detection of a person and extraction of biometric data will be performed by connecting facial recognition software with

biometric data stored in other records, which the Ministry maintains in accordance with the law (records of forensically registered persons).

The risk to individual rights and liberties that may arise from the use of facial recognition software is related to the processing of inaccurate biometric data contained in the records used for comparison. The processing of such inaccurate data would lead to false identification, i.e. identification of the “wrong” person. Such processing could result in unfounded identification of a person, i.e. unfounded treatment of that person by police officers because incorrect biometric data from other records are associated with them, which would violate one’s right to privacy and dignity.

The level of probability of a violation of individual rights and liberties is determined by the processing of inaccurate data, which can threaten the right to privacy and dignity of the person whose data is being processed. The possibility that the biometric data stored in the Ministry's records are incorrect cannot be ignored, primarily because biometric data were previously collected and processed using different technologies. There are also possibilities that, for example, a photo of one person is linked to the data of another person because a mistake was made during the manual entry of data into the records (when transferring data from records that were previously kept in paper form).

The level of impact of violations of the rights and liberties of persons is: mostly low (2)

The level of probability of violations of the rights and liberties of persons is: low (1)

Exposure to the risk of violations of rights and liberties is: slight (2)

Risk control is carried out by applying the intended organizational and technical measures.

The application of police powers, measures and actions involving the use of facial recognition software must be carried out professionally and in accordance with the established standards of police work, which means that in the case of obvious inaccuracy of the data, the police officer must carry out additional checks before making a decision on further treatment of the person the software has recognized. By implementing continuous education and control-instructive activities, an effective data management mechanism will be enabled, which includes the way of keeping records and an oversight into the actions of police officers.

The police officers' course of action when keeping records must be based on the organizational structure in the system of assigned roles with regard to the performance of individual processing actions, which reduces the possibility of error, i.e. inaccurate or not-up-to-date record keeping, which implies entering, updating, changing or correcting the data contained in those records.

An efficient data management mechanism is also ensured by applying certain technical protection measures such as: equipment access control, data carrier control, data storage control, user control, data access control, transfer control, transport control, system recovery, ensuring system integrity, user account management, system log.

Even in the case of the possible occurrence of this risk, it must be kept in mind that a "human" is the link that represents the greatest threat for inaccurate or not-up-to-date record keeping when it comes to manual data entry. However, we cannot ignore the fact that human error or negligent work is not always the reason for incorrectly entered data in the records, because there is a possibility that, for example, the data that was submitted to the ministry by another controller for entry into the records is not correct or that the data was changed during transmission. By applying effective control mechanisms, a high level of data accuracy can be ensured, and the residual risk can be successfully controlled, i.e. remain at an insignificant level.

The level of impact of violations of the rights and liberties of persons is: mostly low (2)

The level of probability of violations of the rights and liberties of persons is: low (1)

Exposure to the risk of violations of rights and liberties is: insignificant (2)

Recording of individuals in private space

A risk to individual rights and liberties exists in situations where a part of the private space is recorded by cameras connected to facial recognition software.

By recording, storing and other actions of processing data on the activity of a person located in a private space, the right to privacy of a person can be threatened.

There is a justifiably expectation that the activities a person undertakes in private space are protected from the view of other people.

The transparent use of video surveillance reduces the subjective feeling of the right to privacy being threatened, thereby raising citizens' awareness of the level of risk to this right of theirs.

The use of the said cameras aims to record public space, and there is a possibility to record private or business space in those places where there are no physical obstacles, which could threaten the right to privacy.

If the said camera is very far from a private or business space, or if it is at an inappropriate angle in relation to a private space, or if such space is obscured by trees, curtains, blinds, fences, etc., the quality of the collected data is poor, and the possibility of infringing the right is negligible.

The level of impact of violations of the rights and liberties of persons is: mostly low (2)

The level of probability of violations of the rights and liberties of persons is: predominantly low (2)

Exposure to the risk of violations of rights and liberties is: insignificant (4)

Risk control is carried out by applying the intended organizational and technical measures.

With the periodic review of the cameras' fields of view, as well as the implementation of control-instructive activity, an oversight into the way of handling cameras and the actions of police officers is possible. The users of the system/cameras are police officers that have to be trained and educated for legal requirements and methods of use of the video surveillance system, i.e. face recognition software. The police officers' course of action when handling cameras is based on an organizational structure in a system of assigned roles.

With the application of technical protection measures such as: equipment access control, data carrier control, data storage control, user control, data access control, transfer control, transport control, ensuring system integrity, user account management, system journal, an efficient data management mechanism is ensured.

The use of facial recognition software in the system of video surveillance of public space in urban areas is an additional challenge for the Ministry as controller. Because the public space that is subject to video surveillance also includes a large number of residential, business and other buildings where people sojourn, and it is impossible to conduct video surveillance in such

a way that these buildings, that is, the people within them are not also surveilled. The design of the video surveillance system must be coordinated with the existing or planned infrastructure, but it should be kept in mind that it is almost impossible for the video surveillance not to include certain objects that are not subject to surveillance. By using appropriate filters, video surveillance can be used in a way that does not threaten the privacy of someone's home or business premises, that is, in a way that does not cause discomfort among citizens due to the fear that they are the subject of surveillance while staying in that space. By applying adequate protection measures and control mechanisms for their application, it is possible to ensure that the level of residual risk is low to negligible.

The level of impact of violations of the rights and liberties of persons is: mostly low (2)

The level of probability of violations of the rights and liberties of persons is: low (1)

Exposure to the risk of violations of rights and liberties is: slight (2)

Software error

The existence of this risk is related to the fact that the recognition of biometric characteristics cannot be seen as a 100% accurate technology, but that it is based on “adjusting the level of sensitivity” in relation to “false negatives” and “false positives”. False results (negative or positive) carry significant risks for the individual (a person can be wrongly recognized/identified as a perpetrator of a criminal offense and vice versa that the facial recognition system does not recognize the perpetrator of a criminal offense at all or the perpetrator of a criminal offense is provided with an alibi due to a software error).

The probability of error must be considered in relation to the circumstances of the use of the software. Namely, using face recognition software in places visited by a large number of people (airports, stadiums, railway stations, etc.) even a small percentage of software errors leads to wrong identification of a large number of individuals. For example, a software error whose efficiency is estimated at 99%, nevertheless includes an error of 1%, which in relation to 100,000 people whose data will be processed by the software during one day at the airport is as many as 1,000 incorrectly identified people.

Unlike these so-called “controlled environments”, where the percentage of error is small, the percentage of the software error certainly increases when it is used in a public space (for example, The Republic Square in Belgrade), where due to various circumstances (lighting, weather, camera distance, using different means to avoid video surveillance such as sunglasses, hats, scarves or masks over the face) there is also an increase of the risk of error.

The accuracy-reliability of facial recognition software is determined based on the manufacturer's data, but there must also be an independent assessment with periodic review of the level of accuracy.

The level of impact of a software error on violations of the right to privacy and dignity of a person is determined by the application of police powers, measures and actions that threaten the rights of that person. The level of probability of infringing the individual rights and liberties is determined in a way that an authorized police officer, for the purpose of identifying a person whose data is processed using facial recognition software, always additionally checks the result of comparing biometric data and makes a decision on taking other measures and actions towards that person. The absence of the necessary verification of the results of the comparison of biometric data increases the risk of violation of the individual rights to privacy and dignity.

The level of impact of violations of the rights and liberties of persons is: mostly high (4)

The level of probability of violations of the rights and liberties of persons is: medium (3)

Exposure to the risk of violations of rights and liberties is: moderate (12)

Risk control is carried out by applying the intended organizational and technical measures. The police officers’ course of action when using video surveillance is based on the organizational structure in the system of assigned roles in terms of performing the necessary checks of the results of comparing biometric data, which reduces the possibility of taking other measures and actions against the person, without performing the necessary checks. The application of police powers, measures and actions, using the video surveillance system, are carried out professionally and in accordance with the established standards of police work. Measures are taken for protection against risks that arise when changing jobs or terminating employment. Employees of the Ministry are educated about the legal regime of personal data protection. Establishing disciplinary liability is a preventive and reactive measure that greatly reduces this

risk. Independent evaluation and periodic review of the level of software accuracy is necessary to assess its reliability.

The necessary prerequisites for the use of software, i.e. reliable processing of personal data are provided by applying technical and organizational measures such as: user control, data access control, storage control, transfer control, transport control, system recovery, ensuring the integrity of software and operating systems, system log, protection against malicious software, ensuring the correct and safe functioning of the system, saving data on events that may be of importance for the security of the system, ensuring that the auditing activities within the system have as little impact on its functioning as possible and ensuring the continuity of work in extraordinary circumstances.

The fact must also be taken into account that despite the fast development of software, the development of artificial intelligence and the application of the intended protection measures, the residual risk cannot be reduced and it will remain at a moderate level.

The level of impact of violations of the rights and liberties of persons is: mostly high (4)

The level of probability of violations of the rights and liberties of persons is: medium (3)

Exposure to the risk of violations of rights and liberties is: moderate (12)

Risk of unauthorized access to data

The existence of this risk is related to the access/possibility of accessing data by unauthorized persons.

Different levels of access are granted to police officers in relation to the organizational structure in the system of assigned roles, and with regard to the performance of individual processing actions. The level of impact on violations of the right to privacy and human dignity is determined by the use of software by authorized persons/authorized police officers, where the level of impact of the violation of rights increases if there is any possibility that unauthorized persons access the software, i.e. the data processed by its application.

The level of probability of violation of the right to privacy and dignity of a person is determined in relation to the possibility of access to data by unauthorized persons, through unauthorized access to equipment or data carriers. The very fact that such a possibility exists causes an additional feeling of insecurity among citizens, and it must be completely eliminated or at least reduced to the smallest possible extent by applying protective measures.

The level of impact of violations of the rights and liberties of persons is: mostly high (4)

The level of probability of violations of the rights and liberties of persons is: mostly low (2)

Exposure to the risk of violations of rights and liberties is: admissible (8)

Risk control is carried out by applying the intended organizational and technical measures.

Devices and equipment for automatic data processing and information carriers (CD, DVD, external hard drives, etc.) on which data are recorded within the system must be secured, kept in special rooms that can be locked, secured by an access control system, video surveillance, with measures to protect against fire, flooding, electric shock and other incidents, encrypted. Information carriers must not be taken out of the premises except for clearly defined needs, such as making backup copies or recovering the system from backup copies. In the event of an incident, the integrity of the data within the system and the restoration of the system's functionality must be ensured, which is achieved by regularly making backup copies of data (daily, monthly, annual level) that can be accessed only by authorized employees (system administrators) and only in the event of an incident when it is necessary to perform system recovery. A reliable data management system is provided by applying technical and organizational measures such as data carrier control, data storage control, user control, data access control, transmission control, transport control, system recovery, ensuring the integrity of software and operating systems, system log, protection against malicious software, ensuring correct and safe functioning of the system, saving data of events that may be of importance for the security of the system, ensuring that system auditing activities have as little impact on its functioning as possible and ensuring the continuity of work in emergency circumstances, as well as saving biometric data patterns within 72 hours. In addition to the said measures, the risk can be controlled by revoking or updating access rights in cases of changing jobs or terminating employment, as well as by continuous education of employees regarding reporting and responding in case of incidents.

It is almost impossible to completely eliminate the risk of unauthorized access to data, but the residual risk can be significantly reduced by effective application of security measures.

The level of impact of violations of the rights and liberties of persons is: mostly high (4)

The level of probability of violations of the rights and liberties of persons is: low (1)

Exposure to the risk of violations of rights and liberties is: insignificant (4)

Risk of abuse by authorized persons

The existence of this risk refers to the possibility of data abuse by authorized persons/police officers who have been assigned with access to the data. Abuses are possible at the time of data collection or during their further processing (an authorized police officer may perform identification of a person without a proper basis, i.e. use the software for the recognition of a person for purposes for which it is not intended, where this risk is usually motivated by personal reasons).

An authorized police officer may inspect the stored data without a legal basis, or may extract, copy and transfer the stored data to an unauthorized person for further use, which may also include unauthorized disclosure of data. Also, this risk is related to the possibility that the authorized police officer fails to additionally check the result of the matching of the compared data obtained by using the software, as a result of which a wrong decision on taking other measures and actions against the person may be made, and thereby endanger individual rights.

The level of impact of violations of the rights and liberties of persons is: mostly high (4)

The level of probability of violations of the rights and liberties of persons is: medium (3)

Exposure to the risk of violations of rights and liberties is: moderate (12)

Risk control is carried out by applying the intended organizational and technical measures.

In order to properly use facial recognition software and process data collected by the video surveillance system, it is necessary to ensure that every time the recorded material is accessed, a digital record of that access is logged, which should contain at least the following information:

first and last name of the police officer, official identification card number or the master citizen number of the police officer, ID of the device from which access was performed, data on the duration of each session, as well as data on activities. Digital records of access are permanently stored in the system log.

When accessing the information system, additional (two-factor) authentication must be set for all assigned user accounts when accessing recorded materials, which would be achieved for example through official identification cards.

It is recommended that when accessing the system, no devices with the ability to record audio or video, such as mobile phones, cameras, voice recorders and the like, be brought into the premises, as well as to limit the ability to transfer data to data carriers (USB or CD).

By defining the privileges and roles for each police officer with the authority to access recorded material, it is necessary to determine the appropriate level of access in accordance with the workplace, i.e. position within the organizational unit. For example, only certain officers (system administrators) have administrative access to the information system, which enables more advanced options such as creating and deleting accounts for other officers. Only certain police officers can be assigned a role that allows them to view footage, without the ability to download, edit or delete material, while other police officers have the ability to download data. Each download of data is recorded with the number of copies made, reasons for exclusion, etc. It is necessary to ensure that the appropriate access request is software-defined, so that during each access it is recorded on the basis of which request is acted upon.

After termination of employment or transfer to another position within the Ministry, user accounts for access to the system whose authorization has expired must be deactivated and archived, i.e. access to the system from those accounts must be disabled as soon as possible.

With the application of effective measures to reduce the risk, one must take into account the fact that a “human” always appears as the weakest link, and the possibility of abuse always exists, which always entails certain consequences for the data subject, but with the effective application of residual measures the risk can be reduced to the level of tolerable.

The level of impact of violations of the rights and liberties of persons is: mostly high (4)

The level of probability of violations of the rights and liberties of persons is: mostly low (2)

Exposure to the risk of violation of rights and liberties is: admissible (8)

Risk of loss, destruction or alteration of data or lack of supervision

The existence of this risk is related to the loss, destruction and alteration of data by authorized or unauthorized persons. The existence of this risk is also related to the absence of adequate supervision and notification and response in case of incidents that may lead to loss, modification or destruction of data. The occurrence of risks is possible both at the time of data collection and during their further processing. An authorized police officer may modify or destroy data without legal grounds (by abusing authority or authorized level of access). Irresponsible handling of data leads to data loss (e.g. during transfer, transport of data carriers, inadequate data storage also leads to data loss).

The level of impact of violations of the rights and liberties of persons is: predominantly high (4)

The level of probability of violations of the rights and liberties of persons is: mostly low (2)

Exposure to the risk of violation of rights and liberties is: admissible (8)

Risk control is carried out by applying the intended organizational and technical measures.

To establish an efficient data management mechanism, following measures are necessary: data carrier control, data storage control, data access control, transfer control, transport control, system log, protection against malicious software, ensuring the correct and safe functioning of the system, saving data on events that may be of importance to the security of the system.

In each instance of accessing data, it is necessary to record a digital record of that access (system log). When accessing the information system, additional/two-factor authentication must be set for all assigned user accounts, and privileges and roles must be defined for each police officer.

Processing of data by using the video surveillance system must be done professionally and in accordance with the established standards of police work, but it is impossible to eliminate the

risk when it is taken into account that the authorized person-police officer is still only a “human” who, as has been stated many times, is the weakest link and it is impossible to reach the consciousness of every individual, but with the effective application of preventive and reactive measures, the residual risk can be reduced.

Effective application of the said measures can reduce the residual risk to the level of insignificant.

The level of impact of violations of the rights and liberties of persons is: mostly high (4)

The level of probability of violations of the rights and liberties of persons is: low (1)

Exposure to the risk of violations of rights and liberties is: insignificant (1)

Illicit publication of data

The existence of this risk refers to the possibility of abuse by authorized persons/police officers who have been assigned with access to the data. Abuses are possible at the time of data collection or during their further processing (an authorized police officer can identify a person without a valid basis and transfer the data to an unauthorized recipient, or by subsequent processing of the stored data copy and transfer it to an unauthorized recipient, where this risk is most often motivated by personal reasons). There is also a possibility that an authorized police officer can inspect the stored data and extract, copy and transfer it to an unauthorized person on their own initiative or on the basis of a superior's order without a legal basis.

It must be kept in mind that the risk refers only to the illicit publication of data, and in this sense it is necessary to make a clear distinction from the publication that is permitted.

Illicit publication of data collected by the video surveillance system, through the media, social networks or using other means of communication will threaten the rights and liberties of the person whose data is being processed.

The right to private life is violated when an insight into the activities of a person covered by video surveillance is provided to the public, i.e. published in the media, on social networking platforms or disseminated through other means of communication.

Publishing information related to a person's private life will jeopardize the reputation, honor, dignity, personal and moral integrity of the person whose data is processed by video surveillance.

Illicit publication of data collected by video surveillance, through the media, social networks or using other means of communication will violate the rights and liberties of the person whose data is being processed.

The number of recorded cases of illicit publication of data by employees of the ministry is small.

The level of impact of violations of the rights and liberties of persons is: predominantly high (4)

The level of probability of violations of the rights and liberties of persons is: predominantly high (4)

Exposure to the risk of violation of rights and liberties is: considerable (16)

Risk control is carried out by applying the intended organizational and technical measures.

In order to properly use facial recognition software and process data collected by the video surveillance system, it is necessary to ensure that every time the recorded material is accessed, a digital record of that access is recorded, which should contain at least the following information: first and last name of the police officer, official identification card number or the master citizen number of the police officer, ID of the device from which it was accessed, data on the duration of each session, as well as data on activities. Digital records of access are permanently stored in the system log.

When accessing the information system, additional (two-factor) authentication must be set for all assigned user accounts when accessing recorded materials, which would be achieved for example through official identification.

It is recommended that when accessing the system, no devices with the ability to record audio or video, such as mobile phones, cameras, voice recorders and the like, be brought into the premises, as well as to limit the ability to transfer data to data carriers (USB or CD).

By defining the privileges and roles for each police officer with the authority to access recorded material, it is necessary to determine the appropriate level of access in accordance with the

workplace, i.e. position within the organizational unit. For example, only certain officers (system administrators) have administrative access to the information system, which enables more advanced options such as creating and deleting accounts for other officers. Only certain police officers can be assigned a role that allows them to view footage, without the ability to download, edit or delete material, while other police officers have the ability to download data. Every download of data must be recorded, indicating the number of copies made, the reasons for exclusion, etc. It is necessary to ensure that the appropriate access request is defined in software, so that during each access it is recorded on the basis of which request is acted upon. After termination of employment or transfer to another position within the Ministry, user accounts for accessing the system must be deactivated and archived, i.e. access to the system from those accounts must be disabled as soon as possible.

An efficient and reliable data management mechanism is provided by security measures such as equipment access control, data carrier control, data retention control, user control, data access control, transfer control, transport control, system recovery, system integrity assurance, user account management, system log, malware protection, physical and technical protection of facilities and equipment, protection against damage and theft of assets that make up the video surveillance system.

The police officers' course of action during the use of video surveillance is based on the organizational structure in the system of assigned roles regarding the performance of individual processing actions, which reduces the possibility of unauthorized publication of data and enables the determination of individual responsibility of police officers.

Along with the application of effective measures to reduce risks, one must keep in mind the fact that even here the "human" is the weakest link, and the possibility of abuse in the form of unauthorized publication of data always exists, which as such almost always entails certain consequences for the data subject. The application of police powers, measures and actions, using the video surveillance system, are carried out professionally and in accordance with the established standards of police work, and the determination of disciplinary responsibility and initiation for the determination of criminal responsibility by the competent authority are also necessary elements of an effective data management mechanism by which the residual risk can be reduced to a certain level but will remain moderate.

The level of impact of violations of the rights and liberties of persons is: predominantly high (4)

The level of probability of violations of the rights and liberties of persons is: predominantly high (3)

Exposure to the risk of violation of rights and liberties is: moderate (12)

3. Description of Protection Measures and Mechanisms in Relation to Risk to Individual Rights And Liberties - Data security protection measures and mechanisms for protecting individual rights

Data security is ensured by the application of provisions on permitted data processing, provisions related to the rights of individuals, as well as by the application of technical, organizational and personnel measures in accordance with the law.

The described risks to the individual rights and liberties are effectively removed, that is, reduced to the smallest possible extent by the application of general organizational, personnel and technical data protection measures, i.e. mechanisms to protect the rights and liberties of individuals in connection with the processing of personal data. These measures and mechanisms are prescribed by the Law on Protection of Personal Data and other regulations, such as the Law on Information Security, the Law on Police, the Law on Records and Data Processing in the Field of Internal Affairs, and the by-laws adopted by the Ministry.

Data security protection measures and individual rights protection mechanisms are applied in a specific way in the video surveillance system. Some of these measures and mechanisms are applied in relation to several different risks and in the same or different way, while other measures and mechanisms are applied only in relation to an individually determined risk.

The application of technical measures for protection of data and equipment in the video surveillance system, and related organizational protection measures, is regulated by the Law on Records and Data Processing in the Field of Internal Affairs, the Instruction on information security measures in the information and communication system of the Ministry of Interior, the Instruction on conditions of construction, use and maintenance of the video surveillance system in the Ministry of Interior, and the Instruction on how to keep records in the field of video-acoustic recording.

The construction of the video surveillance system is carried out based on the grounded proposal of the Police Directorate, and based on the decision of the minister, or the person authorized by the minister to make this decision. In order to make a decision on the construction of a video surveillance system or a part of this system, an analysis of the need to install cameras at certain camera locations is performed, according to the described criteria. In doing so, in the context of assessing the level of certainty of risk occurrence, special attention is paid to achieving the purpose of video surveillance, that is to say that by placing cameras in adequate positions, recording of private space is impossible to the greatest extent.

The video surveillance system is an integral part of the information and communication system (ICT), which is managed by the Ministry. This system is effectively protected, among other things, by appropriate technical measures of information security that are applied according to the data and equipment used.

TECHNICAL PROTECTION MEASURES

Technical measures such as equipment access control, user control, data access control, system log, mean that in each instance of access to recorded material, it is necessary to log a digital record of that access, which should contain at least the following information: first and last name of the police officer, official identification card or police officer badges number, the officer's master citizen number, ID of the device from which access was made, session duration data, as well as activity data (all operations performed, queries made, etc.). Digital access records (logs) must be permanently stored in the system log.

Mandatory two-factor authentication (2FA) means that when accessing the information system, additional authentication must be set for all assigned user accounts when accessing recorded

materials, which is achieved through the official identification of the police officer-user of the system.

Technical protection measures such as control of data carriers, control of data storage, physical and technical protection of objects and equipment, protection against damage and theft of assets that constitute the video surveillance system, mean that devices and information carriers (CD, DVD, external hard drives, etc.) used for recording the data within the system must be encrypted, stored in special rooms that can be locked and secured from fire, flood, electric shock and other incidents, as well as by video surveillance. Access to information carriers requires the same level of access as to the information system. Information carriers must not be removed from the premises except for clearly defined purposes, such as making copies or restoring the system from backup copies. When accessing the system, no devices with the ability to record audio or video, such as mobile phones, cameras, voice recorders, etc., may be brought into the premises.

System recovery and ensuring system integrity means that in the event of an incident, the integrity of data within the system and the restoration of system functionality must be ensured, which is achieved by making regular backup copies of data (daily, monthly, annual level) that can only be accessed by authorized employees (system administrators) and only in case of an incident when it is necessary to restore the system. Data backups must be protected by modern encryption standards

Software improvement means regular software updates to improve system performance and the application of artificial intelligence (machine learning).

ORGANIZATIONAL PROTECTION MEASURES

Managing user accounts means defining privileges and roles for each police officer with the authority to access recorded material and it is necessary to determine/prescribe the appropriate level of access in accordance with the workplace, i.e. position within the organizational unit. For example, only certain officers (system administrators) should have administrative access to the information system, which allows more advanced options such as creating and deleting accounts for other officers, while others can be assigned a role that allows them to only view

recordings, i.e. accounts without the ability to download, modify or delete material. Supervising officers must be enabled to generate or to create user accounts for search.

The software generation of an account for search implies a software-defined access request, so that during each access it is visible/clear on the basis of which/whose request/order is being processed.

Measures to protect against risks that arise when changing jobs or terminating employment imply that after termination of employment or transfer to another position within the MIA, user accounts for accessing the system whose authorization has expired must be deactivated and archived, i.e. access to the system from those accounts must be disabled as soon as possible.

The measures of limited storage of biometric data patterns include a software solution that biometric data patterns generated by the use of the system are stored for 72 hours from the moment the pattern is extracted, i.e. after that period they are deleted.

The system of assigned roles in the processing of personal data implies that one police officer cannot independently, without the participation of other authorized officials, undertake data processing actions that would lead to the identification of a person, which greatly reduces the possibility of abuse and the likelihood of risk. Data collection is performed by a person assigned within one organizational unit, and further processing and use of data is performed by other officers deployed in several different organizational units. The system of assigned roles as an organizational measure shown in the table implies that the video surveillance system should be created so that it can be functional only in the system of assigned roles. This means that in the collection and further processing of data in the video surveillance system in the context of assessing the level of certainty of a risk occurrence, it is simply not possible organizationally, technically and legally to imagine a situation in which, outside the system of assigned roles, a decision is made to undertake processing actions aimed at identifying a person.

The application of this organizational measure effectively prevents any individual attempt to abuse police powers, because one authorized person can never on one’s own, without the participation of other authorized persons, undertake all the processing actions indicated by the risks described in the previous chapter. In this way, the probability of a risk occurrence is minimized to the greatest extent.

The system of assigning roles in the video surveillance system is based on the Rulebook on internal organization and systematization of workplaces in the Ministry. This act regulates the competence of individual organizational units of the Ministry, as well as the description of jobs and tasks for each individual workplace, which also includes the prescription of general and special conditions for assignment to a workplace.

Employees deployed in certain workplaces in the video surveillance system, with the authority to collect and further process data, have the status of authorized officials. In the performance of their duties and tasks in the video surveillance system, they are deployed in organizational units of the Ministry.

In each of the organizational units of the Ministry, each authorized person is assigned a predetermined level of decision-making, that is, the authorization to undertake certain processing actions. Thus, individual authorized persons also have the role of controlling the execution of duties and tasks in the video surveillance system.

In the video surveillance system operated by the Ministry, each processing action is performed by a person who is authorized to undertake that action. Moreover, none of the persons engaged in the video surveillance system has the authority to undertake all processing actions. Thus, for example, only a person who is assigned within an organizational unit has the authority to collect data, while other officials who are assigned to several different organizational units have the authority to use data, on the basis of which it is possible to identify the data subject, as well as to decide on the necessity of identifying that person.

The control of legality, that is, the regularity of the exercise of authority, is directly carried out by the authorized persons who manage individual organizational units in the video surveillance system, the Internal Control Sector, as well as organizational units responsible for control of the legality of work. Such control, among other things, is provided by recording each processing operation, that is, by technically enabling the determination of facts related to the use of cameras and other equipment in the video surveillance system in each specific case (system log).

The application of technical protection measures in the video surveillance system is also based on a system of assigned roles according to the competences of different organizational units.

Informing citizens implies that, in addition to information, individuals must also be enabled to exercise their rights in connection with the processing of personal data (right to access, copy, delete or other rights in accordance with the law). The information must also contain notice on the controller's methods of exercising the rights (e.g. by submitting a request to the Ministry of Interior for the territorially competent police department, by the location of the cameras).

Discipline and conscientiousness of police officers

The legal and professional conduct of police officers in the application of video surveillance is ensured by the application of proactive and reactive protection measures that raise the level of awareness of the necessity of protecting data security and respecting the rights and liberties of individuals, which to the greatest extent reduces the likelihood of the occurrence of risks. Preventive measures include security checks of candidates for employment and employees of the Ministry, continuous education of authorized police officers in connection with the application of the provisions of the Law and other regulations related to the protection of personal data. Education tasks are carried out in accordance with the Regulation on professional training and development in the Ministry of Interior, based on the Professional Development Program of Police Officers of the Ministry of Interior and the Directive on the way of performing work related to the protection of personal data in the Ministry of Interior. Reactive measures are applied in case of violation of data security or personal rights. The first group of these measures refers to a breach of data security, regardless of whether in the specific case the security breach was responded to by another protection mechanism. The application of measures from this group is prescribed by the Law and the Instruction on the manner of record keeping and notification of personal data breaches in the Ministry of Interior. The second group of these measures are disciplinary measures and they are prescribed by the Law on Police. The third group of measures prescribed by the law and the Criminal Code is applied by the Ministry of Interior, the prosecution and the court. The fourth group consists of measures applied by the Commissioner for Information of Public Importance and Personal Data Protection, in accordance with the law.

Mechanisms for the protection of individual rights

Any person whose data is processed by the Ministry may apply to the Ministry for the exercise or protection of rights, in accordance with the Law. The mechanism of control of actions according to the requests of the person whose data is processed is entrusted to the Data

Protection Officer of the Ministry, and the forms of control are regulated by the Directive on the way of performing tasks related to the protection of personal data.

In accordance with Art. 54, paragraph 3 of the law, the opinion of the Data Protection Officer of the Ministry was obtained, which is attached to this document.

In Belgrade, on _____ 2022