INTRODUCTION OF BIOMETRIC DATA PROCESSING SYSTEM IN THE STATE BORDER GUARD

Inta Siliniece[1], Jolanta Gaigalniece –Zelenova[2]
[1]State Border Guard College, Latvia, e-mail: inta.siliniece@rs.gov.lv
[2]State Border Guard College, Latvia, e-mail: jolanta.gaigalniece@rs.gov.lv

Abstract: *Biometric data authentication systems are used widely nowadays. Biometric technologies are based on person's biometric data, compared with data of a specific person. In 2017, a new functionality was introduced at the State Border Guard on the technological platform of the Biometric Data Processing System for data input on foreigners detained under the Immigration Law. The fingerprint information system of asylum seekers was modernised. New workstations were installed in several State Border Guard units.*

Keywords: *State Border Guard, biometric, data processing system, asylum, workstations.*

The aim of the paper is to study the implementation of the Biometric Data Processing System at the State Border Guard, to analyse the shortcomings and problems in the implementation of the system and the possibilities of the system's development and improvement.

Biometric data authentication systems are widely used nowadays. Biometric technologies are based on person's biometric data by comparing data of a particular person.

The word *biometrics* originates from the Greek *bios* – life, and *metron* – measure. Using such systems, it is possible to identify a person based on data acquired at birth (DNA, fingerprints, iris of an eye), over time or changes according to age (handwriting, voice, gait). Biometrics is a set of methods used for the processing of biological data, while biometric data is a set of physiological characteristics and indications that are personally identifiable to a person. Biometric data are as following:

1) fingerprints;
2) hand geometry, palm prints;
3) facial biometrics;
4) ear and voice geometry;
5) iris of an eye, the retina;
6) vein structure;
7) DNS;
8) signature of a person (10).

In order to identify a particular person, biometrics uses not what a person owns, but the inherent and unrepeatable characteristics of a person. Thus, this person identification method is the most reliable, and it practically eliminates the possibility of using a false identity. As a result,

biometrics is increasingly used in a wide range of everyday life. Biometric identification is used by the Public Administration (passports, identification cards, driving licenses), public order and security (identification and verification of persons, access rights), health care, finances (payment and credit cards), trade (loyalty cards), education (student cards), etc.

The so-called 3A principle (Authentication, Authorization and Administration) is being respected when developing biometric authentication systems and protecting information from unauthorized access.

The issue of security is topical in the European Union and in Latvia with the increase in the threat of terrorism in the world. One of the security measures is the inclusion of biometric data (facial digital image, fingerprints, etc.) in identity documents, travel documents, visas and residence permits, and the use of further processing of these data.

The Council of Europe defines the term "data" as "any fact, information or concept for processing in a computer system in an appropriate form" in the Convention on Cybercrime on November 23, 2001. Regardless of the form and place where the information is stored, it must always be protected adequately. Security of information is characterized by its confidentiality: information should be available only to those, who are authorized to receive it. The unlawful use of data may pose a threat to national security, public order and negatively affect the economy of a country, and may cause moral or material damage to a natural person.

As a result of the rapid development of information technology, a large amount of information to be processed relates directly to individuals. This information is called personal data, and it is used in various state and municipal institutions, including the State Border Guard. When processing personal data, the human rights to private life or privacy are being compromised. They are guaranteed in the UN Universal Declaration of Human Rights of 1948 (Article 12), the International Covenant on Civil and Political Rights of 1966 (Article 17), the European Convention for the Protection of Human Rights and Fundamental Freedoms of 1950 (Article 8), and Article 96 of the Constitution of the Republic of Latvia - "Everyone has the right to inviolability of private life, housing and correspondence".

In Latvia, many international documents have been adopted in the field of biometric data protection, national laws and regulations have been adopted, as well as the legislation has been improved in order to respect both the rights and freedoms of an individual and the interests of the state and public security.

The Regulation (EU) 2016/679 of the European Parliament and the Council (April 27, 2016) on the protection of natural persons with regard to the processing of personal data and on the free movement of such data

repeals Directive 95/46/EC (General Data Protection Regulation) that contains precisely defined rules of personal data protection. In accordance with this Directive, each piece of information that identifies a natural person should be protected. Further processing of data without the permission of an identified person is permitted only in certain cases provided for in regulatory acts.

The Member States use Article 1 of this Regulation to protect the fundamental rights and freedoms of natural persons and, in particular, their right to respect for private life, regarding the processing of personal data.

The Regulation states the following:

- *personal data* is any information relating to an identified or identifiable natural person ("data subject"); an identifiable person is one, who can be identified directly or indirectly by indicating the registration number or one or more factors of that person's physical, physiological, mental, economic, cultural or social identity;
- *processing of personal data* (*processing*) is any action or set of operations performed with personal data with or without automated means, such as collecting, registering, organizing, storing, applying or modifying, correcting, consulting, using, disclosing, transmitting, distribution or otherwise making available, grouping or joining, closing, deleting or destroying access;
- *the controller* is a natural or legal person, a public authority, an agency or any other entity that determines, individually or jointly with others, the purposes and means of personal data processing (6).

The Member States have a duty to protect the fundamental rights and freedoms of natural persons, and, in particular, their right to the protection of personal data. They also have to ensure that the exchange of personal data between competent authorities in the Union, when such exchanges are required by Union or the laws of the Member States, is not restricted or prohibited for reasons connected with the protection of natural persons with regard to the processing of personal data (7). There are strict requirements for the processing and storage of personal data and the procedures by which this information is transmitted to other organizations, institutions or foreign countries with reliable and adequate protection.

There is the Law on the Biometric Data Processing System in Latvia that aims to ensure the development of a unified biometric data processing system in order to determine the identity of natural persons, as well as to prevent the use of a false identity. The Biometric Data Processing System is a state information system, the manager and holder of which is the Information Centre of the Ministry of Interior. The conceptual issues related to biometric data are viewed by the Ministry of Interior which is

responsible for the Concept on the use of biometric data of natural persons in Latvia.

Biometric data processing systems collect, process and store biometric data of natural persons - a digital image of face, images of finger (palm) prints/footprints. In addition, basic biographical data of a person (name, surname, personal identity number, date of birth, gender, nationality and its type), as well as separate attribute data, such as the date of receipt of biometric data, the acquiring institution, the grounds for obtaining, are included.

One of the most important tasks of the State Border Guard in the field of control of the state border guard and immigration is the compliance with the rules on entry, residence, departure and transit of foreigners in the territory of the Republic of Latvia as well as to carry out activities provided for in the Asylum Law within the framework of its competence (9).

Since 2009, the State Border Guard units have started using of the Automated Fingerprint Identification System (hereinafter AFIS), in which the fingerprints obtained from border inspection posts and immigration departments are inspected, added and stored. The system improved and accelerated the identification of offenders and data verification, thus improving the effectiveness of the fight against State border violations and ensuring compliance with the requirements of the Schengen Agreement.

In 2017, a new functionality was introduced on the Biometric Data Processing System's technological platform within the framework of the project No IC/PMIF/2016/4 "Integration of Automatic Fingerprint Identification System of the State Border Guard with Biometric Data Processing System (hereinafter BDPS) maintained by the Information Centre" by the Asylum, Migration and Integration Fund. It was developed for entering data on foreigners detained under the Immigration Law, Sections 51 and 60. A new Automated Fingerprint Identification System was created; the work of the previous Automated Fingerprint Identification System was stopped and all data was transferred to the new system. The Asylum Seekers Fingerprint Information System (hereinafter - *Eurodac*) was modernized as well as new workstations were installed in several State Border Guard units.

Data of the Automated Fingerprint Identification System are available to the State Border Guard for conducting inspections related to the control of compliance with the rules of entry, residence, departure and transit of a person. In addition, when carrying out processing of personal data, the State Border Guard officials ensure that all data is collected only for specific purposes and processed legally, accurately and not disproportionately. The State Border Guard ensures that all biometric data acquired is not stored

for longer than is necessary to achieve a specific purpose and is stored in a safe way, preventing the access of third party.

The Order No 1474 "On the use of AFIS and *Eurodac* systems" "Temporary Provisions on the Use of the Automated Fingerprint Identification System (AFIS) and the Asylum Seekers Fingerprint Information System (*Eurodac*) in the State Border Guard Units" entered into force on October 3, 2017. The Provisions determine the procedures by which officials of the State Border Guard Units carry out processing of personal data in the Automated Fingerprint Identification System and the Asylum Seeker Fingerprint Information System.

In the data entry procedure, the AFIS introduces data on foreigners detained in accordance with Article 51 or Article 60 of the Immigration Law. Depending on the reason for the detention of a foreigner, data may be entered into different categories depending on the nature of the violation, place, and other conditions.

During the data input procedure in the *Eurodac* system, data is entered in accordance with the *Eurodac* Regulations on asylum seekers.

Prior to entering data into the particular system, a person's identification has to be carried out with the aim of obtaining information about the previous registrations (if there were any). The BDPS user's obligation is to provide the following information to a person before entering data into the system:

- name, surname and position of the user who carries out the data processing;
- the reason and justification for the data processing, delivering a person upon signature the informational sheet in the case of the AFIS data check and input, or a common leaflet developed by the European Commission with relevant information in the case of entering data in the *Eurodac* system, depending on the reason for the data input;
- on the right of a person to access the data entered and the right to propose the editing of the entered data if the data is entered incorrectly or the deletion of the entered data if data is entered unlawfully.

Data in the Biometric Data Processing System can be obtained in the following ways:

- in paper form - a natural person about himself/herself and his/her children under the age of 18 or his/her authorized representative, as well as a legal representative for a person under his/her custody or guardianship;
- using the online data transmission - the State Police, the Office of Citizenship and Migration Affairs, the State security authorities and the public prosecutor's office if the data of the system is necessary for

the fulfilment of the functions prescribed by regulatory enactments regulating the activities of the institution concerned.

The person's identification in the Biometric Data Processing System of the State Border Guard is carried out using a frontal face picture or fingerprints of a person.

The most effective method for the person identification is the comparison of the fingerprint images. Fingerprints are one of the most convenient and useful biometric parameters in different access systems. The uniqueness and originality of fingerprints is determined by the fact that their formation is influenced by genetics and environmental conditions of development. At the same time, changes in fingerprints are immaterial over time, as even after severe physical damage, the skin returns to its previous appearance.

Processing of data in the Biometric Data Processing System is provided by:

- data entry workstation "*LivesScan*" with the application "CAPS" - for data entry into systems with "live" four-finger scanners and photo equipment supplied with the workstation;
- data entry workstation "*Cardscan*" with application "CAPS" - for data entry in the systems with flatbed scanners for obtaining the fingerprints from dactyloscopic cards for data entry into systems and photo equipment supplied by the workstation.

Qualitative photo equipment is used to obtain a face photo in the State Border Guard, nevertheless, in order to obtain an image of appropriate quality, lighting and background play an important role. Therefore, the placement of workstations in well-designed premises is essential for the qualitative acquisition of a face image.

Conclusions and suggestions

1. The inclusion of biometric data (facial digital image and fingerprints) in identity documents, travel documents, visas and residence permits as well as the further use and processing of these data is a topical issue with the increase in the threat of terrorism.
2. Nowadays, none of the state administration institutions, including the State Border Guard, can function properly without the help of biometric data processing systems.
3. The legal framework of the Republic of Latvia is wide. It resolves a number of cooperation and procedural issues that are of great importance in the use of the Biometric Data Processing System.

4. To improve the technical equipment and placement of the Biometric Data Processing Systems in premises with the necessary lighting, ensuring the quality of obtaining and processing of biometric data.
5. In the regulatory enactments, to define precisely whether and which biometric data is considered as sensitive data and to which processing more strict protection and control requirements are attributed to.

References

1. Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems.
2. The Universal Declaration of Human Rights.
3. Contact group "Return Directive" (2008/115/EC) March 18, 2016
4. Convention for the protection of human rights and fundamental freedoms – Journal of Latvia -1997. – Nr143/144.
5. Regulation (EU) No 603/2013 of the European Parliament and of the council of 26 June, 2013.
6. Regulation (EU) 2016/679 of the European Parliament and of the council of 27 April, 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).
7. Directive (EU) 2016/680 of the European Parliament and of the council of 27 April, 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA.
8. The Constitution of the Republic of Latvia of February 15, 1922.
9. Border Guard Law of December 16, 1997. - Journal of Latvia - 1997. – 329/330.
10. Jain, A.K., Flun, P., Ross, A. (2008). Handbook of Biometric, Springer Science+Bussiness Media, LLC, 4. p.
11. Biometric Data Processing System Law of May 21, 2009. – Journal of Latvia - 2009. – Nr.90 (4076).
12. Personal Data Protection Law of April 20, 2000.- Journal of Latvia -2000. - Nr.123/124.
13. Law on State Information Systems of June 5, 2002. - Journal of Latvia – 2002. – Nr.76.
14. Immigration Law of October 31, 2002. - Journal of Latvia – 2002. - Nr.169 (2744).
15. Asylum Law of December 17, 2015. - Journal of Latvia – 2015. – Nr.2 (5574).
16. Biometric Data Processing System (BDAS) programmes and database improvements. CAPS Identity Manager application. Us_ic-sl/72-IC/PMIF/2016/42016-CAPS-IDM-LR. 19.06.2017 version 9.0.