OFFICE OF THE PERSONAL DATA PROTECTION INSPECTOR

Recommendations on Processing of Biometric Data

Present document is elaborated on the basis of the analysis Law of Georgia on Personal Data Protection, European data protection standards and international practice. The document is recommendatory in its nature and is intended to be used by public and private sector data controllers.

Recommendation aims to interpret obligations of data controllers and other issues related to processing of biometric data.

I. Introduction

Increasing amount of biometric data processing provides the necessity of relevant regulations and establishment of effective evaluation methods. In practice biometric data is processed for issuing passports, protecting confidential information, border control, migration management, IT security and other purposes. Processing biometric data has a lot of practical advantages, but at the same time due to the unique and permanent nature of such data, it is important that the data controller considers and analyzes principles and requirements of internal and international legislation for such processing in details.

Collection and processing of biometric data for different purposes, on different legal grounds raises questions on the necessity of biometric systems. Legitimacy, adequacy and proportionality of biometric data processing are issues regulated by Law of Georgia on Personal Data Protection. Law exhaustively prescribes legal grounds, aims and principles for processing biometric data, security measures, rights of data subject and obligation to provide information to the Personal Data Protection Inspector.

II. What is Biometric Data?

According to the Article 2 (c) of Law of Georgia on Personal Data Protection **biometric data means any physical, mental or behavioral feature which is unique and constant for each natural person and which can be used to identify this person (fingerprints, foot prints, iris, retina (retinal image), facial features).**

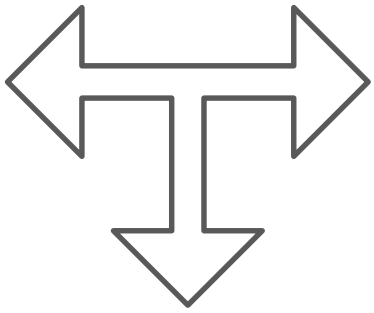
It should also be mentioned that according to the Law of Georgia on Personal Data Protection, **biometric data constitutes special category of data, when it allows identifying individual by features related to for example, racial or ethnic origin, state of health, conviction and etc.**

Hence, for processing such data, existence of at least one of the legal grounds envisaged by Article 6 of the Law is mandatory – for example, written consent of the data subject.

In international practice, individual's physical and behavioral features are most commonly used during biometric data processing.

Behavioral features

Handwriting, voice, walking style and etc.



Physical features

Fingerprint, facial features, retina, iris and etc.

Biometric features are constant, unique and non-transformable; it is difficult to produce, forge or to change them.

III. Processing of biometric data

According to Article 2 of the Law of Georgia on Personal Data Protection, data processing is any operation performed upon personal data, in particular, collection, recording, photographing, audio recording, video recording, organization, storage, alteration, restoration, usage, disclosure, dissemination, grouping, combination, locking, deletion, destruction and etc. Data might be processed by automated (by using computer program), as well as by non-automated (keeping a journal, manual recoding of data) and semi-automated means.

Existence of a legal ground, clearly defined legitimate purpose and compliance with data processing principles are obligatory for legitimacy of biometric data processing.

- **Legitimate purpose and legal grounds for biometric data processing**

Due to the specificity of biometrics, legislation provides separate regulation for their processing and strictly defines purposes for processing of such data.

Public institutions are allowed to process biometric data for the purposes of one's security and protection of property; besides processing of biometrics is allowed for the protection of the confidential information. Achieving these purposes should be impossible by other means or should be related to disproportionate efforts. For example: Using fingerprints to control the fact of entrance and exit to and from the building by public servants is unambiguously non-adequate and non-proportionate measure to achieve the goal. Therefore, processing of personal data for the purpose of controlling employees is illegal. But entrance to the particular part of the building,

where confidential data is stored, using the fingerprint, is legitimate and is considered as proportionate to the aim pursued.

> Pursuant to Article 9 of the Law of Georgia on Personal Data Protection, processing of biometrics for the purpose of issuing an identity document under procedures established by Law, or for identifying person crossing the state border, is legitimate.

Private organizations and individuals may only process biometric data if it is necessary to perform their activities, to ensure human safety and protection of property, as well as to prevent disclosure of confidential information, if achieving these goals is impossible by other means or requires unjustifiably great efforts. For example: Biometric data may be processed by banks in order to ensure protection of repository in branches, instead of allocating separate staff responsible for ensuring security of repositories. Allocation of additional staff might be considered as disproportional effort for the bank.

Existence of legal ground for data processing is obligatory to ensure legitimacy of biometric data processing. If biometric data does not constitute a special category of personal data, legal grounds specified in Article 5 of the Law of Georgia on Personal Data Protection are applicable. If biometric data constitutes a sensitive category of personal information it should be processed only if one of the legal grounds envisaged by Article 6 (2) is in place.

! Data controller shall define legal grounds for biometric data processing; otherwise the process will be considered illegal.

- **Principles of biometric data processing**

During personal data processing, data controller shall respect principle of fairness and lawfulness, rights and freedoms guaranteed by the Constitution of Georgia, including rights to respect human dignity, private and family life and right for free development of an individual.

Principles of personal data processing are set out in Article 4 of the Law of Georgia on Personal Data Protection, which are obligatory for public and private organizations and individuals as well.

Following principles of data processing shall be taken into account:

- **Principle of fairness and lawfulness**

  Data should be processed fairly and lawfully, without any prejudice to human dignity of a data subject. For example: publishing biometric photo by a photo studio, placing a photo to the internet or to the social network for the hilarious purposes will be considered as abusing human dignity and essential violation of the principle of fairness and lawfulness.

- **Principle of legitimate purpose**

  Data may be processed only for specific, clearly defined and legitimate purposes. Processing of data for purposes that are incompatible with the original purpose shall be inadmissible. For any further data processing separate legitimate purpose shall exist. For example: photographing the customer by the photo studio for the purposes of its activity is a separate purpose, but using a photo for marketing purposes (in practice there are occasions when photos of customers are used for marketing purposes by photo studios) is considered as incompatible with the original purpose of the processing.

- **Adequacy and proportionality**

  Data shall be processed only to the extent necessary to achieve the respective legitimate purpose. The data must be adequate and proportionate to the purpose for which it is processed. For example: Using fingerprints by organizations to control attendance of the employees at the workplace is inadequate and disproportionate, this aim might be easily achieved without processing of biometric data.

- Data must be valid, accurate, and kept up to date, if necessary. Data collected without legal grounds and irrelevant to the processing purpose must be blocked, deleted or destroyed.

- Data might be kept only for the period necessary to achieve the purpose of data processing; after the purpose of data processing is achieved, information should be blocked, deleted or destroyed, or stored in a form excluding identification of an individual. For example: If an employee left his/her job, employer is obliged to erase his/her biometric data which was processed during period of employment, otherwise processing of biometric data will be considered as disproportionate and inadequate.

! It is important for public agencies and private organizations to evaluate necessity of storage of biometrics and define specific period for it.

IV. Methods of processing biometric data

Technological development leads to establishment of different methods of biometric data processing; these methods might be used separately or in a combined manner. For example, some systems use methods of identification of voice and face at the same time. Along with the technological progress, the risk of using one's biometric data without his/her consent is rising.

In the modern world, two main methods of biometric data processing are utilized: verification and identification. There is essential difference between them. Biometric data is mainly processed

through these two methods, to control access in a physical as well as in a virtual space (access to particular system or space).

Identification means checking biometric authenticity with information kept in the database and is known as one-to-many method that enables to determine whether or not biometric data (fingerprint, voice, signature and etc.) belongs to the particular person. Therefore, system compares biometric data with all examples stored in the database. Existence of a database in itself constitutes comparably low level of security, as there is risk of illegal usage of data.

Verification means checking authenticity of biometric data without a database. Namely, system compares biometric placed on an identifier (for example, work ID card, manufactured for particular person who involves biometrics of this person) with the information with biometrics of the particular person in the database. The method is known as on-to-one method. It is considered that verification method is more secure, as database on which the system is based does not provide opportunity for illegal access. All data in such a system are encrypted and activated only when data subject uses abovementioned biometric identifier. To process data by this method is more costly, but it ensures higher level of security; on the other hand it requires special software support. When verification system is used, devise containing biometrics (work card, ID card and etc.) is possessed by the data subject, which reduces risk of unauthorized access.

V. Data Security and obligations of data controllers

Data controller shall acknowledge importance of biometric data and ensure its security. It is recommended to assess needs in advance and decide afterwards which method of processing of biometric data is necessary and which security measures are appropriate. Organization shall assess three components to ensure security – environment, aim and effectiveness. Data controller is obliged to take all necessary measures, which will be adequate to the risks related to data processing. Person involved in data processing is obliged not to exceed limits of his/her authority and to ensure data confidentiality, even after termination of his/her term of office.

In order to ensure biometric data security, data controller shall objectively define existing environment, aim and decide which method will be effective for processing of biometrics accordingly. Data controller shall assess:

- **environment**

It is important for a data controller to assess environment in which biometric data will be processed. Main question in this respect is - **whether or not it is necessary to process biometric data?**

- **Aim**

It is important to analyze the aim for which biometric data shall be processed. In accordance with the Law of Georgia on Personal Data Protection, biometric data might be processed for the

purposes of security, protection of property and confidential information, as well as for carrying out activities, but these goals shall be achieved through methods which enable less interference into private life and in the right to personal data protection. Main question which should be answered is - **whether it is possible to achieve goals with other means and not by biometric data processing?**

- **Effectiveness**

Processing of biometric data obliges organizations to ensure effective methods of data security. According to Article 17 of the Law of Georgia on Personal Data Protection, data controller is obliged to take such organizational and technical measures which will ensure protection of data against accidental or unlawful destruction, alteration, disclosure, collection or any other form of unlawful use, and accidental or unlawful loss. Besides data controller is obliged to ensure registration of all operations performed in relation to electronic data. Main question that shall be answered by the data controller is - **whether organization is ready to ensure appropriate organizational and technical safeguards for data protection?**

! According to Article 10 of the Law of Georgia on Personal Data Protection, data controller is obliged to provide to the Personal Data Protection Inspector the same information which is provided to the data subject, namely, purpose of biometric data processing and measures taken to ensure data security.

VI. Data subject's rights

According to the Law of Georgia on Personal Data Protection, data subject has the right to receive information. Data subject has the right to request from the data controller information processed about her/him. Namely, data controller is obliged to provide to the data subject following information:

- What kind of biometric data is processed;
- Purpose of biometric data processing;
- Legal ground for biometric data processing;
- Source of biometric data;
- Whether or not biometric data is transmitted to the third party, legal ground for transmission and its purpose.

Data subject has the right to request from the data controller to correct, update, edit, erase or destroy personal data. Data controller is obliged to take appropriate measures within 15 days from the receiving of request and notify data subject on its decision.

One of the legal grounds for data processing is the data subject's consent. According to the Law of Georgia on Personal Data Protection consent is defined as a voluntary consent of a data subject, after receipt of the respective information, on his/her personal data processing for specific

purposes expressed orally, through telecommunication or other appropriate means, which enables clearly establishing the will of the data subject. According to Article 6 of the same law, for processing sensitive categories of personal data, written consent is obligatory. In case of a dispute with respect to the existence of a data subject's consent to process data, a data controller shall carry the burden of proof.

A data subject shall have the right to, at any time and without explanation, withdraw his/her consent and to request termination of data processing or destroying of data. Data controller shall be obliged to terminate the data processing and/or destroy the processed data according to the request of a data subject within five days after the application is submitted, unless there are other grounds to process data.

According to the Law of Georgia on Personal Data Protection, data subject has the right to appeal. In case of a violation of his/her rights related to the data protection, data subject can apply to the Personal Data Protection Inspector or to the Court. If a data controller is a public institution, data subject may also submit a complaint to the same or higher administrative body. A data subject shall have the right to require from a body considering the case to block data until a decision is made. A data subject shall have the right to appeal the decision of a higher administrative body or the Personal Data Protection Inspector to the Court.

Frequently asked questions regarding biometric data processing

Which biometric data is processed most commonly in the world?

- Fingerprints, voice, retina, facial features, handwriting and "hand geometry" are most commonly processed biometrics in practice. Testing of other variations of biometric data is in process by scientists;

Whether it is possible to alter biometric data?

- Alteration or disguising of biometric data is achieved through huge efforts (occasions of distortion or alteration of fingerprints through surgery methods were revealed). Behavioral features might be also altered (manner of walking or talking, and etc.);

Can a system distinguish twins' biometric data?

- Despite the fact that twins are similar at the first sight, their physical and behavioral features are easily distinguishable by biometric systems.

How biometric systems deal with security issues?

- Biometric system is a part of the whole security. Security problems cannot be solved using only biometric system.

What is the specificity of biometric systems?

- Operation of biometric systems is based on four stages: data collection, extraction, comparison, decision. At the collection stage system through sensor identifies data and modifies it to digital format. Extraction stage transforms digital data to compact set-up. At the comparison stage system measures and compares the given sample with other examples in the database. On the basis of the comparison stage, system makes decision whether provided example is in compliance with others and gives or denies access to the physical or virtual system.