GUIDELINES REGARDING THE INTRODUCTION OF BIOMETRIC DATA

(APENDIX BIOMETRICS IN THE WORK PLACE)

Component 2
Activity 2.1.4 -

Version - September

I. INTRODUCTION

Biometrics is gaining significance in the modern world, however the society is also faced with many important decisions regarding long term attitude towards it. The use of biometrics is by all means increasing; it can be spotted in numerous areas and it has been used for different purposes: defense, state border measures, immigrations, passports, banks and financial institutions, information systems etc. From the aspect of the individual, biometrics has certain practical advantages. As any other technology it can be used in a manner friendly to the individual's privacy, but on the other hand it may invoke serious intrusion into the individual's privacy.

The practical advantages of biometrics are as a rule instantly visible, contrary to some aspects which prove that biometrics is not almighty and perfect which are not visible on first sight. Biometric measures by its nature represent an intrusion into individual's privacy and dignity, hence all the conditions for its use have to be interpreted in the light of privacy and dignity protection.

Purpose/aim of the document

This Guidelines explaining the rules as to when and under what conditions data controllers may introduce biometric personal data, as well as what they are obliged to take into consideration.

The purpose of these Guidelines is to explain the basic characteristics of biometric measures, to illustrate some of the dilemmas regarding processing of personal data in the context of biometrics, and to provide answers to frequently asked questions encountered by private and public sector subjects considering the introduction of biometric measures. They also address introduction to the biometrics in the work place.

With the help of such explanations, answers and guidelines, companies and other data controllers and processors should accordingly be able to comply with the provisions and principles of the Law on the Protection of Personal Data (Official Gazette No.07/05 with amendments published in the Official Gazette under no. 103/08 and under no. 124/10 and no.135/11; hereinafter "the LPDP"), international standards and principles and the EU regulations (Directive 95/46/EC of the European Parliament and of the Council of 24.10.1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data).

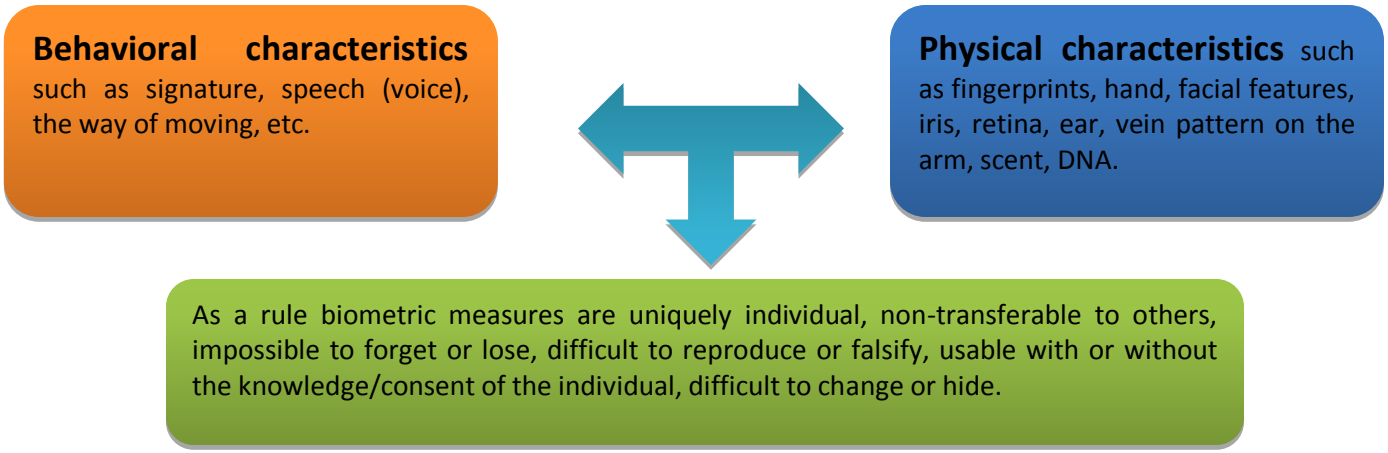
To whom these guidelines are addressed?

These Guidelines are addressed to data controllers, data processors and whatever companies who process biometric personal data. However, also data subjects and broad public find a number of information regarding the fulfillment of their rights given to them by the Law on Personal Data Protection.

What does Biometric personal data actually means?

Simply defined, **biometrics** is the science of identifying a person on basis of their physiological or behavioral characteristics, which are not shared by any other individual and are therefore unique and constant. Indeed, we are all identifiable by way of such measurable characteristics as fingerprints, papillary lines on a finger, the iris, retina, face, ears, DNA, and even our typical posture and gait. Certain physical, physiological and behavioral data is suitable for the identification of an individual, if such enables a reliable and accurate biometric measure, which may accordingly function as a unique and individual "password" of a person.

The following human characteristics are most frequently used in biometrics:



What does Processing of personal (biometric) data means?

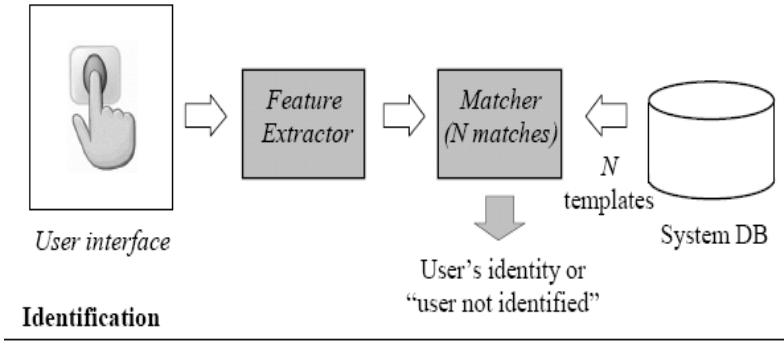
"Personal data processing" shall be every operation or a sum of operations performed on personal data, automatically or otherwise, such as: collection, recording, organizing, storing, adjusting, or altering, withdrawing, consulting, using, revealing through transmitting, publishing or making them otherwise available, aligning, combining, blocking, deleting or destroying;

Biometric data (such as fingerprints, iris, retina, facial features, etc.) provide sources of characteristics that are unique and attributable solely to each and every individual, and as a characteristic by way of which a person is identified or at least identifiable, they undoubtedly represent personal data. Hence, any collection, storage, sharing, sending or destruction of such data shall be deemed to be the processing of personal data, and is consequentially specially regulated by the provisions of the LPDP.

For a better understanding of the processing of biometrics, it is crucial to distinguish between verification and identification. Differentiation between those two fields of application is fundamental because verification and identification applications are used for various tasks in non-comparable areas.

What is biometric identification?

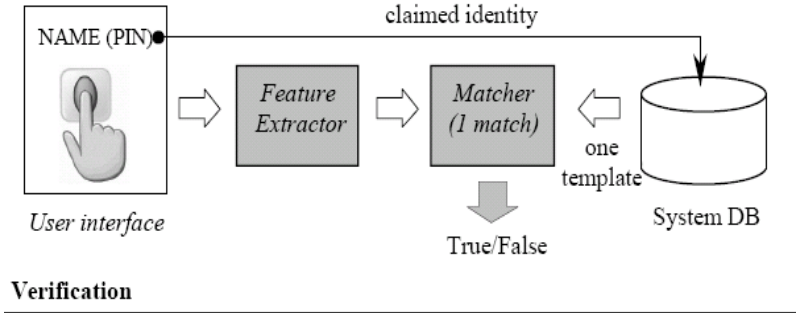
A biometric signature (template) of unknown person is presented to the system. The biometric system compares this template with the templates of known persons whose templates are collected in database. After the comparison process the system answers if template of unknown individual has been found in database. When the search is positive – unknown person is identified. This model is known as "one-to-many".



What is biometric authentication (verification)?

In biometric verification an individual's template is compared with an offered characteristic. For this operation the person must first provide an example of the particular characteristic for verification requirements. This process (called "enrolment") converts it by mathematical methods into a digital form – template - (e.g. finger print image) of the characteristic that can be stored on a computer file or on a smart card memory. The template is used where necessary for comparison against a newly offered set of characteristics for verification.

The system compares two templates – one provided in real time (real feature) the second one as previously inserted into token by which individual proclaims as a part of his/her identity. When the comparison process is identical (highly probable) than the system believe that proclaimed identity is right. This model is known as "one-to-one".



For example

In the verification mode, biometric technologies perform a single comparison of the present data with a template that has been previously stored. An example of this is a fingerprint scanner on an electronic safe. In the identification mode, a biometrics database is used. An individual item of data is then captured, and the system tries to match this piece of data with any of the existing items defined in the database. An example of identification biometrics is a fingerprint database of known criminals.

Biometric data processing is now often used in automated authentication/verification and identification procedures, in particular for the control of entry to both physical and virtual areas (i.e. access to particular electronic systems or services).

Taking into consideration the rapid technical evolution and the increased concern for security, many biometrics systems work by combining different biometric modalities of the user with other identification or authentication technologies. Some systems for instance cumulate face recognition and voice registration.

The collection of biometric samples, the so-called biometric data (e.g. image of the fingerprint, picture of the iris or of the retina, recording of the voice), is carried out during a phase called "enrolment" by using a sensor specific to each type of biometrics. The biometric system extracts from the biometric data user-specific features to build a biometric "template". The template is a structured reduction of a biometric image: the recorded biometric measurement of an individual. It is the template, presented in a digitalized form, which will be stored and not the biometric element itself. In addition, biometric data may be processed as raw data (an image) depending on the functioning of the biometric system that is used who he is, by proceeding with a comparison of the two templates. This also applies to other biometric systems, such as those based on keystroke analysis or distance facial recognition, on account of the specific features of the technology involved. The problematic aspect is, on one hand, that this data collection and processing may be performed without the knowledge of the data subject and on the other hand that regardless of their current reliability, these biometric technologies lend themselves to blanket utilisation on account of their "low-level intrusiveness". Therefore, it seems necessary to lay down specific safeguards in respect of them."[1]

There are some concerns surrounding the area of biometrics technologies and the large-scale storage of biometric data. For example the data might later be used for purposes that an individual has not agreed to, or even that the information could potentially be stolen. Another issue that is sometimes raised is the concern that biometric data stores could be misused to discriminate against certain sectors of the population.

According to the above said it is very important to respect the principles for processing of biometric data for the purpose of lawful and fair processing of personal data according to the provisions laid down in the LPDP.

II. GENERAL PRINCIPLES FOR FAIR PROCESSING

Biometric personal data according to the provisions of the LPDP are considered as special categories of personal data, therefore special requirements for fair processing are set up in the LPDP. Data controllers can process biometric data only if that kind of processing data is determined specifically in a special law. In other cases, in general, processing of biometric personal data is prohibited but as an exemption they can be processed *on the basis of an explicit*

[1] Working document on biometrics 12168/02/EN WP 80 – ARTICLE 29 – Data Protection Working Party

consent of the personal data subject given for processing such data, unless a law envisages that the prohibition for processing such data may not be withdrawn by a written consent of the personal data subject. But even if the data controller wants to process biometric data on the basis of the consent of the data subject the data controller must also obtain approval from the DPDP prior to the processing of the biometric data. (See article 29 of the LPDP)

Principle of purpose and proportionality

The respect of this principle implies firstly a clear determination of the purpose for which the biometric data are collected and processed. Furthermore, an evaluation of the respect for proportionality and the respect for legitimacy is necessary, taking into account the risks for the protection of fundamental rights and freedoms of individuals and notably whether or not the intended purpose could be achieved in a less intrusive way. Therefore controllers and processors must firstly determine the legal basis for processing biometric data. If there is no such legal basis for processing biometric data than this processing is forbidden. Although consent of the data subject for processing biometric data is a legal basis it must be taken in consideration, as said as above, that the data controllers and processors still need prior approval of the DPDP processing personal data and establishing Personal Biometric Data Collection.

For example for access control purposes (authentication/verification), biometric systems related to physical characteristics which do not leave traces (e.g. shape of the hand but not fingerprints) or biometrics systems related to physical characteristics which leave traces but do not rely on the memorisation of the data in the possession of someone other than the individual concerned (in other words, the data is not memorised in the control access device or in a central data base) create less risks for the protection for fundamental rights and freedoms of individuals. This kind of systems in some cases depending of the purpose may be considered as appropriate processing of biometric data.

Right of the data subject to be informed on personal data processing

Where biometric data is being processed, the data subject should be informed of the purposes of processing, the identity of the controller, the categories of data concerned and the recipients or categories of recipients of the data that are stored. Other information should be provided to the data subject, where this is necessary to guarantee fair processing of personal data.

The personal data subject may anytime request from the controller to inform him/her on the scope of personal data or categories of processed personal data related to him/her, on the purpose(s) of processing personal data, means of processing (see articles 10, 11, 12 of LPDP).

Information to data subject must be provided in an intelligible form, using a clear and plain language, in particular for any processing addressed specifically to minors. When a card is issued, the card holder should be properly informed about how to use his/her card and what to do in case of fraud or unauthorised disclosure.

Whenever personal data is being processed by a biometric system, the data subject should be alerted (eg. sound signal), unless he/she already has this information.

III. The Directorate for personal data protection

In the broadest sense, the Directorate for Personal Data Protection is responsible for proper implementation of the Law on Personal Data Protection. This means that the Directorate cares for personal data protection of the citizens and protects their rights.

This role is carried out by the Directorate through:

- resolving citizen's complaints for violation of their data protection rights throughout inspection;
- conducting inspection ex officio to check whether the data protection principles are implemented properly.

However, it should be noted that Directorate has not only repressive role – does not solely solve problems when they occur. Rather, the role of the Directorate is to acquaint citizens closer to their rights.

How to submit a request for obtaining approval for processing biometric personal data?

As said previously, if the data controller is planning to process biometric data on the basis of the consent of the data subject, it has to obtain approval from the DPDP before starting the processing. There is no special Form in which the Request should be submitted but the LPDP determines the data/information that should be contained in the request. It is obligatory or the data controller to state the following data in order to obtain approval from the DPDP for processing personal data:

Data information that needed to be insert in the request for approval for processing personal data	Explanation
1. The title of the personal data collection	**Simple the data controller only states the name/title of the collection** Ex. Personal data collection of biometric data for…….
2. Title i.e the personal name of the controller and his/her head office, i.e. address, as well as the name and the address of his/her representative, if any	
3. Purpose or purposes of the processing	**The purpose for processing is very important so the controller must determine the purpose and explain the justification of the purpose** Ex. Entering or gaining access to a bank safe, entering in premises that contain highly sensitive and expensive equipment or premises which are sensitive regarding the overall security and etc.
4. Legal basis for the establishment of a personal data collection	**The controller states that the legal basis for processing of biometric data is the consent of the data subject** **IMPORTANT: If the legal basis for processing personal data is established in a law than there is no need for a request for approval for processing personal data**
5. Category or categories of the personal data subjects and personal data i.e categories of personal data referring to him/her or them	**The categories of biometric data that are subject of the processing must be stated** Ex. fingerprints, hand, facial features, iris, retina, ear, vein pattern on the arm, scent, DNA and etc.
6. The users or the categories of users to whom the personal data may be given for use	**If the data controller planes to transfer the biometric data to someone else or to a data processor he must state the Title i.e. name and address of the user** **IMPORTANT: In order for the biometric data to be given to users there must be legal basis set up in law. In this case the data controller stipulates the legal basis**
7. Time period for keeping the personal data	**The biometric data can be kept only for the time period which is need to meet the purposes for which the data**

	have been collected for further processing
8. Transfer of personal data to other states	The controller must stipulate if the biometric data is transferred to other state but must take in consideration the provisions of the LPDP regarding transfer of personal data
9. General description that shall enable primary assessment of the properness of the undertaken technical and organizational measures for personal data protection and their processing	Because the biometric data is considered as sensitive category of personal data the controller must provide full detail explanation of the undertaken technical and organizational security measures. IMPORTANT: The technical and organizational measures must be harmonized with the security measures stated in the Rulebook for technical and organizational measures for obtaining secrecy and protection of the processing of personal data

FAQ - Frequently Asked Questions

Are templates used in contemporary biometric systems also regarded as personal data?

Personal data, (according to point 1, paragraph one of the Article 2 of the LPDP Personal data) shall be any information pertaining to an identified or identifiable natural person, the identifiable entity being an entity whose identity can be determined, directly or indirectly, on the basis of one or more characteristics, specific for his/her physical, mental, economic, cultural or social identity any data that refers to an identified or identifiable person, irrespective of the form in which it is expressed.

By its very nature, biometric data is data which refers to an identified or at least identifiable person, e.g., fingerprints belong solely to a certain nameable individual. The question is: does this also refer to biometric data stored in a reduced, digitalized form - a template? A report issued by the Council of Europe noted that the dilemma as to whether biometric data is forever personal data, or only when certain conditions are fulfilled, is irrelevant. Namely, if biometric data is collected with the purpose of subsequent automatic processing¸ then there is always a possibility that such data can be attributed to an identified or identifiable person, which, accordingly, corresponds to the definition of personal data.

Whatever shall apply for biometric characteristics as such, shall also apply to the digital recording of those same characteristics, regardless of the fact as to the nature of the derivative or how many times such a recording has latterly been altered. Although the quantity of detail may diminish in the process of transformation it potentially remains a unique connection with a person: the form, format, manner of recording or other alteration is not a substantial factor.

Based on the above, it can be said that biometric data, although stored in a reduced digitalized form, shall continue to be regarded as personal data because it exclusively pertains to a certain - or identifiable - individual.

Why is the field of biometrics regulated in Law on the Protection of Personal Data (LPDP)?

Biometric data (such as fingerprints, iris, retina, facial features, etc.) provide sources of characteristics that are unique and attributable solely to each and every individual, and as a characteristic by way of which a person is identified or at least identifiable, they undoubtedly represent personal data. Hence, any collection, storage, sharing, sending or destruction of such data shall be deemed to be the processing of personal data, and shall be consequentially specially regulated by the provisions of the LPDP.

Why is biometrics subject to approval?

We need to be aware that biometrics is not just a method of ascertaining or verifying identity, but a technology that uses the human body - or indeed our innate physical or behavioral characteristics - as its instrument. There is a strong tendency by producers and distributors of biometric systems towards trivialization of the collection of data on human physical and behavioral characteristics. Non-critical or uncontrolled use of biometrics can have real and serious consequences for the individual. Our privacy can be seriously jeopardized as a consequence of the unnecessary and unauthorized collection, use, inappropriate storage, integration, or transmission of our personal data.

The Directorate is accordingly obliged to carry out a thorough examination of projected biometric measures and assess whether their introduction is in compliance with principles and rules governing personal data protection. When assessing an individual technology, besides the purpose pursued by the controller, the Directorate also has to consider the technological characteristics of the intended biometric measures, especially and implicitly the level of risk of a given biometric technology, such as the possibility of linkage, and the opportunity for control over one's own personal data.

APPENDIX - Introducing biometric in the workplace

This Appendix follows to the document Guidelines regarding the introduction of biometric measures and it focuses on processing of biometric data in workplace. This guidance is intended to encourage employers to fully consider if biometric system complies with data protection principles set up by the Law on Personal Data Protection (LPDP).

A real and justifiable reason must underlie any requirement for biometric examination or verification of identity, while it must also be substantiated that the purpose for which the controller is exercising control cannot be satisfactorily achieved using another (non biometric) means of identification or verification that would not impinge upon the privacy or dignity of the individual. The employer has to establish why the introduction of biometric measures is necessary, namely what is the purpose and goal of such implementation. Stated purposes and intentions should be serious, well-founded and supported by proof (evidence); moreover, an assessment must be made as to whether the implementation of biometric measures is a necessary requisite for operational reasons, for the security of people or property, or the protection of confidential data or business. Before implementing any biometric measures, the employer is obliged to consider the possibility as to whether there is any other suitable non-biometric method for ascertaining or verifying identity that can satisfactorily fulfill the employer's needs or obligations.

Before any application is made to the Directorate for a decision approving the implementation of biometric measures, it is necessary to decide as to what sort of system is necessary, as well as how it is to be implemented. The more the system interferes with the privacy of an individual (including those questions surrounding the possibility of abuse), the more serious and well founded the reason for the implementation of such biometric measures must be. The argumentation must also embrace technical aspects.

If a company wants to implement biometric measures and succeeds in proving that biometric measures are not only necessary but prerequisite, and that the essential objective cannot be reached in any other less intrusive or detrimental way from the perspective of human privacy and dignity, then the use of predetermined and prescribed biometric measures may be permitted in the workplace. Practice, however, reveals that controllers tend to implement biometric measures in the workplace merely because it is more practical than a swipe-card system, and they merely want to prevent abuse which occurs as a result of the borrowing/lending of cards between employees. Employer has to proof an absolute need for biometrics measures in the workplace for essential operational reasons, for the security of people or property, or to protect

confidential data and business secrets. The mere listing of reasons for the implementation of biometrics without a suitable substantiation, supported by proof, does not meet the legal prerequisites.

1. Biometrics systems

Biometric system operates with automatic processing of personal data for identification or authentication/verification of individuals (data subjects).

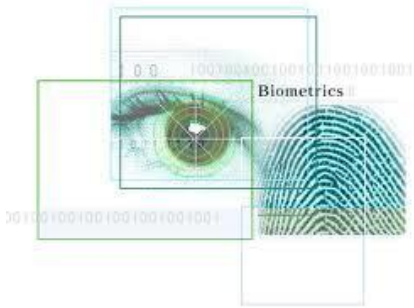
Biometric data may be created from physical, physiological or behavioural characteristics of a person (as example a fingerprint, an iris, a retina, outline of a hand, a face, voice pattern, DNA, body odour, handwriting, keystroke analysis, etc.). A digitalized template is produced by special software. Then, the template is compared with one submitted by employee to the reader in real time.

In many biometric systems applied in a workplace is used encrypted partial data (consisting from original image, however cannot be used to reconstruct the complete original image of biometric data).

There are two basic types of biometric systems

- identification system: the system confirms the identity of an individual (for such a system is necessary create acentral database with personal data. Central database stores the templates on a central system which is then searched each time am employee presents at a reader. System is also called 1 to many).

- authentication/verification system: the system confirms that a biometric derived from a person in real time is identical with the template previously stored on a card (the system compare two biometrics; it is also called 1 to one).



2. Data protection principles concerning biometrics on the work place

Proportionality

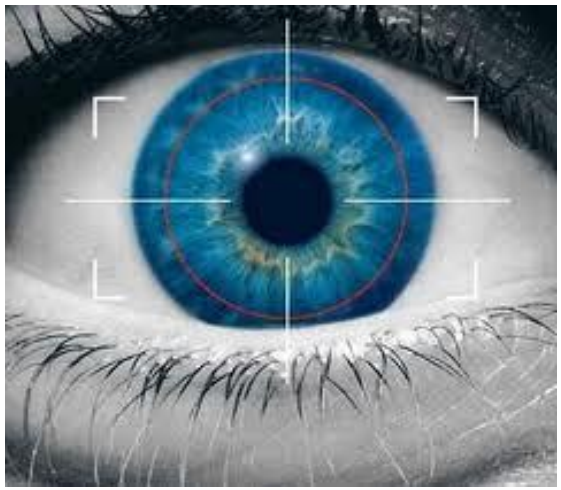
Article 5 of the Law on Personal Data Protection (LPDP) states that *"Personal data shall be: appropriate, relevant and not too extensive in relation to the purposes for collecting and processing"*

The important and almost key word in this sentence is **"excessive"** . When considering the implementation of biometric system the first question is – what is the need for it? Does exists less intrusive

alternatives system which gives the same effect and results? Does employer aware that employees have fundamental rights which are protected by the Constitution, Human Rights Convention a Law on Personal Data Protection? Employer must conduct as assessment of the need for biometric system and evaluate the different types of alternative introduction of particular biometric system.

Another important criteria which shall be taken into consideration – circumstances (environment), purpose, efficiency and reliability.

Circumstances – the employer shall evaluate the nature of workplace (does the workplace really require high level of security?). Is it necessary process sensitive data (biometric)?



Purpose – the employer shall answer the question "Can the intended purpose be achieved in a less intrusive way?"

Efficiency – an employer shall answer the question – "Am I ready to provide all administration steps which are necessary for deployment of the system?

Fair obtaining information and processing

The Article 5 of the LPDP stipulates *"Personal data shall be processed fairly and pursuant to law".*

In order to meet compliance with this provision of Article 5, at least one of the provisions of Article 6 of the LPDP must be met:

- Employee consent

- When the performance is necessary for executing the agreement where the employee is contracting party or upon the employee's request prior to his/her accepting of the agreement

- For compliance with a legal obligation to which the employer is subject

- Where the processing is necessary for protection of the life or fundamental rights of employees

- Where the processing is necessary for the purposes of public interest or an official authorization of the employer

- Where the processing is necessary for purposes of legitimate interest pursued by the employer or by a third party to whom the data are disclosed, unless the processing prejudice to the fundamental rights and freedoms or legitimate rights of employees.

It must be added that the consent of employee is not generally a satisfactory legitimised in an employment context if it is not freely given. Only when an employer offers a processing of biometric data as an option, then consent may be seen to be freely given (i.e. the employer has a choice).

Fair obtaining of sensitive data

It must be reminded that in accordance the provision of Article 2 of the LPDP a biometric data shall be regarded as "a special personal data" (i.e. as a sensitive data).

Article 2(10) stipulates - "*Special categories of personal data" shall be personal data revealing the racial or ethnic origin, the political views, religious or other beliefs, membership in a trade union and data relating to the health condition of the people, including genetic data,* ***biometric data*** *or data referring to the sexual life*".

For processing of biometric data (as a sensitive data), at least one provision of Article 8 of the LPDP must be met:

- The explicit consent of the employee
- The processing is necessary for exercising or performing a specific rights and obligation which is imposed or conferred by Labour Law (in connection to employment)
- The processing is necessary for the protection of fundamental interests of employee or other persons
- The processing is necessary for the purpose of determining or meeting individual legal interest
- The processing is necessary for purposes of acquiring, exercising or defending legal rights of employees.

It must be reminded that the key word with abovementioned provisions is "necessary".

Transparency

The Article 10 of the LPDP requires that data subject must be "informed" on several aspects of processing of data.

In accordance with this article 10 an employer shall provide at least the following information to employees when processing of their personal data:

- The identity of employer (or its authorized representative)

- The purpose of the processing of data

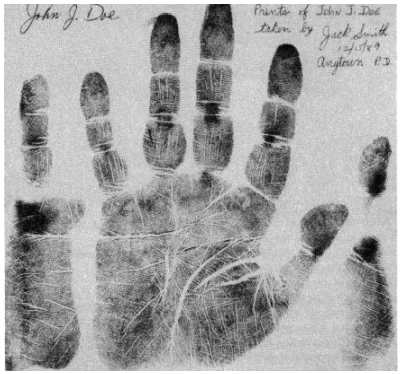
- Any third party to whom the biometric data will be disclosed. (Disclosure of data is the issue if another company administers, maintains or manages the system. Disclosure also covers sending biometric data to a parent company).

The essential requirement is that employees are aware of the purpose for which biometric data is collected and will be processed. This means that an employer must carefully think through any purpose. Transparency is very important in a case where the biometric system does not require the knowledge or active participation of employee (as example facial recognition system may capture and process images of employee without his/her knowledge).

Accuracy

The Article 5 of LPDP stipulates that *"Personal data shall be accurate , complete and, where necessary, updated, whereby all proper measures for deleting and correcting the inaccurate or incomplete data shall be undertaken, considering the purposes for which they have been collected or processed"* .

Any biometric system must accurately identify the persons whose data are processed by the system. If a physical or physiological characteristics of employee is changed this must be reflected to the template. The template shall not be outdated. The procedure of changing template must ensure that data are kept up to date.



Security

The Article 23 of the LPDP requires that "*in order to provide secrecy and protection of the processing of the subject's personal data, the controller and processor have to apply proper technical and organizational measures for protection of accidental or illegal damaging of the personal data, or their accidental loss, change, unauthorized disclosing or approach, especially when the processing includes transmission of data over a network and protection of any kind of illegal forms of processing*".

An employer shall assess and decide upon what constitutes an appropriate security measures. To do so, at least four factors should be taken into account:

- the state of technological development
- the cost of implementation of a technology
- the nature of the data being protected
- the harm and risks that may result from unlawful processing of data.

There are some minimum standard of security for the system of biometric data processing:

- an access to the biometric system shall be restricted to authorised staff only (on a "need-to-know" principle in accordance with internal defined policy);
- password protected computer system;
- technical documents, information of screens , technical manual files shall be hidden from persons who are not authorised to see them;
- regular back-up procedure of computer data; off-site back-up data storage;
- employees are aware of the workplace's security regime and measures and they comply with them;
- all documents, computer printouts, etc. are use under careful disposal regime;
- a persons responsible for security of the system are designated;
- periodical review of security regime, measures and practice is made;
- a work premises are adequate protected when they are unoccupied;
- if the processing of personal data is carried out by a data processor on behalf of employer, a written contract should be in place.

Data retention

Article 5 of the LPDP stipulates that processed personal data may be "*stored in a form which enables identification of the personal data subject, not longer than necessary to meet the purposes for which the data have been collected for further processing".*

In the context of biometric system in a workplace, it is necessary to devise and write a data retention policy, In particular relating to biometric data. This policy shall be adopted in advance the deployment of the system. It must be also ensured that as soon as an employee permanently leaves a workplace, his/her biometric data shall be immediately deleted.