Guidelines for the introduction of biometric measures

The guidelines provide answers to frequently asked questions about biometric measures and their regulation under Personal Data Protection Act.

INFORMATION COMMISSIONER

The purpose of the document:	The purpose of the document: The guidelines provide answers to frequently asked questions of employees and employers regarding the provisions of the Personal Data Protection Act and at the same time harmonize the requirements and practices of the inspection supervision.
Target publics:	Subjects of private and public sector who are considering implementation of biometrics.
Status:	Public
Version:	1.0
Dated:	29. 2. 2008
Author:	Information Commissioner RS
Key words:	Guidelines, biometrics, public sector, private sector, biometric properties, fingerprints, decision, monitoring of working time, access control.

CONTENTS

About Guidelines

The purpose of the Information Commissioner's guidelines is to provide common practical instructions and procedures for data controllers in a clear and appropriate manner. It seeks to address the most common questions from the area of personal data protection that different data controllers are faced with. With the help of such answers and guidelines, companies and data controllers should accordingly be able to comply with the statutory provisions of the Personal Data Protection Act (Official Gazette of the Republic of Slovenia, No. 94/07 – official consolidated text; hereinafter: ZVOP-1-UPB1).

The legal basis for the Information Commissioner (hereinafter: the Commissioner) to issue the guidelines is provided by Article 49 of the ZVOP-1-UPB1 which stipulates that the Commissioner shall give non-binding opinions, explanations and positions regarding personal data protection, and, further to this, publish these on its website or in other suitable formats, as well as prepare and offer instructions and recommendations regarding personal data protection in individual areas.

See also:

- Commissioner's opinions: http://www.ip-rs.si/index.php?id=383
- Commissioner's brochures: http://www.ip-rs.si/index.php?id=388
- The Commissioner's Guidelines are published on the website: http://www.ip-rs.si/index.php?id=491

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 … 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, i.e. the "Big Brother effect". 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. The interpretation needs to follow the provisions of ZVOP-1-UPB1 which stipulate the rights, obligations, principles and actions by means of which unconstitutional, unlawful and unjustified intrusions into individual's privacy and dignity in personal data processing are prevented.

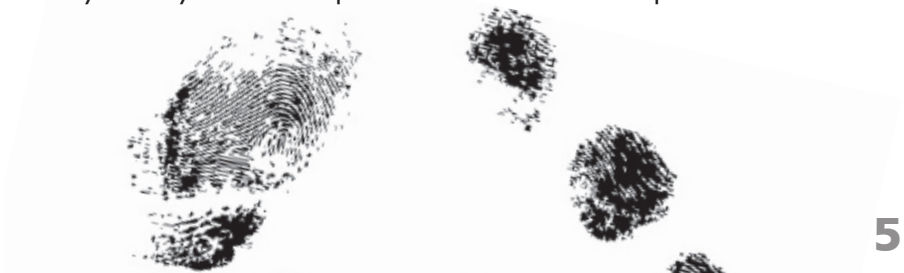
The purpose of these Guidelines is to explain the basic characteristics of biometric measures, to illustrate some of the dilemmas regarding processing of personal data in the context of biometrics, to present the legal framework for implementation of biometrics and to provide answers to frequently asked questions encountered by private and public sector subjects considering the introduction of biometric measures

General information about biometrics

What is biometrics?

The word biometrics stems from the ancient Greek bios (life) and metron (measurement). Simply defined, biometrics or biometrics, as it sometimes referred to, is the science of identifying a person on basis of their physiological or behavioural 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. Personal data also encompasses such physical data as the weight and height of a person; however, these are not biometric characteristics due to the fact that they do not enable the unique differentiation of a person, and thus they prove unsuitable for the identification of an individual. Certain physical, physiological and behavioural 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.

Biometrics is only one of the ways used to establish or verify identity today; other established methods have been in use for a longer period. Such methods are based on those items a person has in their physical or mental possession (e.g. a magnetic card, or a personal password or PIN-code). Biometrics belongs to the third group, and is based on what a person is. This measure is hence a physical or behavioural characteristic, which is idiosyncratic and germane to that individual. From such aspects as practicality and security, such a method of verification has an advantage over items or information in the possession of an individual. Magnetic cards may be lost, borrowed or stolen; personal passwords may be forgotten or revealed to others; biometric characteristics, however, remain the same (at least in principle) forever; they cannot be lost or forgotten, and they are very difficult to replicate or transfer to another person.



Which human characteristics are most frequently used in biometrics?

Let us just list the most established ones. These can be divided into physical and behavioural characteristics:

Behavioural characteristics include:

- signature
- speech (voice),
- the way of moving (gait)
- typing.

Physical characteristics include:

- fingerprints,
- hand,
- facial features,
- iris,
- retina,
- ear,
- vein pattern on the arm,
- scent,
- DNA.

Not all biometric characteristics are unique. Retina and DNA are regarded as the most unique; distinction, however, is not absolute. There is, for example, an interesting case pertaining to the use of biometrics in the UK, namely the Crown vs. Raymond Easton, in which it was revealed that two persons can have identical DNA matches (in this particular instance in 6 places), the theoretical possibility of which is 1:37,000,000. So, it seems appropriate to warn that biometrics - from this perspective at least - is not an almighty and error free way of identification, and should not, therefore, be blindly trusted.

How do the biometric measurements work?

There are, for example, several algorithmic methods for capturing fingerprint patterns.

Let us consider fingerprints as the most frequently used biometric measure. The most common methods are based on the detection of a pattern or extraction of minutiae. In the case of algorithms, which are based on minutiae, the fingerprint is composed of rough characteristics such as arches, loops and whorls, together with more detailed characteristics (minutiae) such as bifurcations (splits), deltas ("Y"-form line joins) and ridge endings. A fingerprint has between 30 and 40 such minutiae. The relative position (translated into co-ordinates) and type (bifurcation, delta or ending) and direction (orientation) of each characteristic is recorded. The sum of characteristics of minutiae provides the base for a fingerprint. If the characteristics are accurately captured, then the possibility that two fingerprints exhibit the exact same characteristics is very low.

You can see the animated display of this measure in action:
http://news.bbc.co.uk/2/shared/spl/hi/guides/456900/456993/html/default.stm.

Why is the use of biometrics increasing?

There is increasing demand for automated, accurate and - at the same time - rapid verification and/or confirmation of the identity of individuals. Biometric measures are:

- uniquely individual,
- non-transferable to others,
- impossible to forget or lose,
- difficult to reproduce or falsify,
- usable with or without the knowledge/consent of the individual,
- difficult to change or hide

As a consequence of these characteristics and advantages, biometric measures are being increasingly employed in automated protocols for deciding upon the rights and obligations of an individual.

How is biometrics regulated in Slovenia?

This area is legislated by way of the Personal Data Protection Act RS (ZVOP-1); a special chapter (namely Articles 78 to 81) makes reference to biometric measures as a special area of personal data processing:

General provision – *Article 78*

The properties of an individual shall be determined or compared through the processing of biometric characteristics so as to identify him or confirm his identity (hereinafter: biometric measures) under the conditions provided by this Act.

Biometric measures in the public sector – *Article 79*

(1) Biometric measures in the public sector may only be provided for by statute if it is necessarily required for the security of people or property, or to protect secret data and business secrets, and this purpose cannot be achieved by milder means.

(2) Irrespective of the previous paragraph, biometric measures may be provided by statute where they involve compliance with obligations arising from binding international treaties or for identification of individuals crossing state borders.

Biometric measures in the private sector – *Article 80*

(1) The private sector may implement biometric measures only if they are necessarily required for the performance of its mandated activities, for the security of people or property, or to protect secret data or business secrets. Biometric

measures may only be used on employees if they were informed in writing thereof in advance.

(2) If the implementation of specific biometric measures in the private sector is not regulated by statute, a data controller intending to implement biometric measures shall prior to introducing the measures be obliged to supply the National Supervisory Body with a description of the intended measures and the reasons for the introduction thereof.

(3) The National Supervisory Body shall, on receipt of information from the previous paragraph, be obliged within two months to decide whether the intended introduction of biometric measures complies with this Act, and in particular with the conditions from the first sentence of the first paragraph of this Article. The deadline may be extended by a maximum of one month if the introduction of such measures would affect more than 20 employees in a private sector organisation, or if the representative trade union at said organisation requests its participation in the administrative procedure.

(4) The data controller may implement biometric measures upon receipt of a decision from the previous paragraph whereby the implementation of biometric measures is permitted.

(5) Further to the third paragraph of this Article, there shall be no appeal against a decision of the National Supervisory Body, an administrative dispute, however, may be initiated.

Biometric measures in connection with public sector employees – *Article 81*

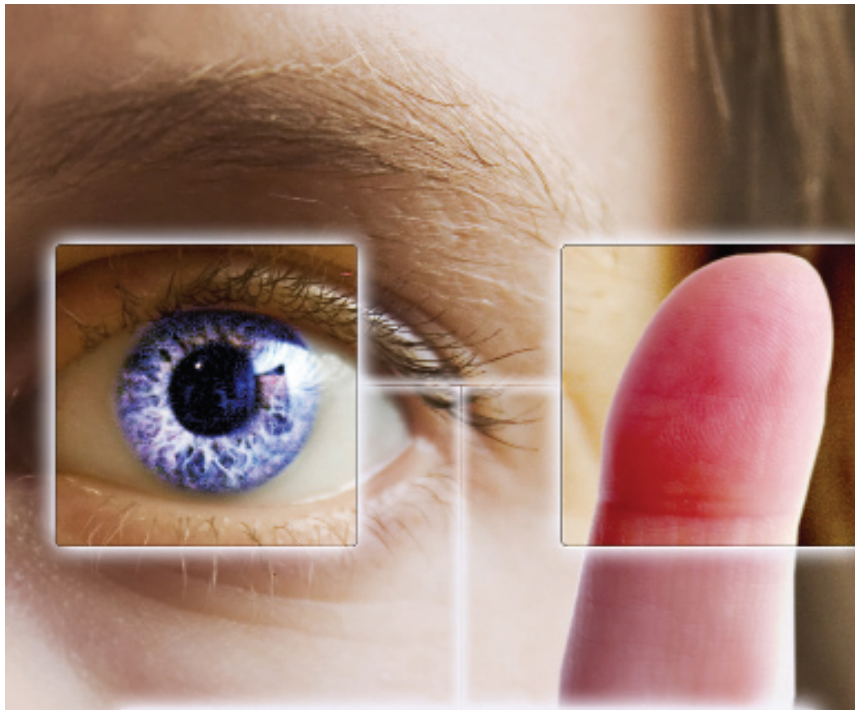
Irrespective of the provision of Article 79 of this Act, biometric measures may be implemented in the public sector in connection with entry into a building or parts of a building, and recording the presence of employees at work; such shall be implemented with the mutatis mutandis application of the second, third and fourth paragraphs of Article 80 of this Act.

Slovenian law hence only permits the use of biometrics in the following cases:

- in the **PUBLIC SECTOR**: when so provided by statute (e.g. Passports of Citizens of the Republic of Slovenia Act), and exceptionally on the basis of special legal provisions, or for entry to a building or sensitive areas of a building and the recording of employees at work.
- in the **PRIVATE SECTOR**: only when such is strictly necessary, e.g.:
  - in the carrying out of a mandated activity,
  - for the protection of people or property,
  - for the protection of sensitive data, or
  - for the maintenance of business secrecy.

Private sector operators may only carry out biometric measures among their own employees if said employees have been previously informed thereof; informing the employee, however, is not in and of itself a sufficient precondition for the introduction of biometric measures, but merely a necessary prerequisite.

If the execution of biometric measures is not provided by law, then the institution or company which wants to introduce biometric measures must acquire a positive decision (approval) from the Information Commissioner.



Why is the field of biometrics regulated by the Personal Data Protection Act (ZVOP-1)?

Fingerprints - as with the iris, retina, facial features etc. - provide sources of biometric data which represent characteristics that are unique and attributable solely to each and every individual; as such, 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 regulated by the provisions of Slovene law regulating personal data protection, namely ZVOP-1.

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

Personal data is any data that refers to an identified or identifiable person, irrespective of the form in which it is expressed. A person is identifiable if they can be recognized directly or indirectly, especially with reference to an identification number or one or more factors which are characteristic of the person's physical, physiological, spiritual or similar such identity, whereby the manner of identification shall be obtainable in a reasonable way, not just for the operator but also for any other person. 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.

On the basis of the above, it can be stated that biometric data, although stored electronically, is forever personal data, because it refers to an identified or at least identifiable individual.

Are biometric characteristics always regarded as sensitive personal data?

No. Although biometric characteristics shall only be regarded as sensitive personal data if an individual could be identified by the use of the characteristics, further to which the law especially lists data on race, ethnic or national origin as well as health condition, as sensitive personal data.

Biometrics and health issues

Various studies reveal that some people are afraid that a number of biometric measures could be harmful to their health. In relation to this mention is made of the use of infra-red light when screening the retina, or infection problems in relation to fingerprint scans. There are not many such cases in practice. Much more significant is latent data on the health condition of an individual which may be »hidden« within biometric data. Namely, biometric data can reveal much more than a person may wish to reveal about themselves, or consented to when the collection was carried out. A DNA sample, for example, used to establish the identity of an individual, may also reveal genetic defects and predispositions towards illnesses. Iridologists - scientists who study the characteristics of irises - claim that medical conditions can also be revealed from an iris. A similar situation also exists in relation to voice identification, which may also be used to reveal the emotional state of a person. All these issues are problematic from the perspective of personal data protection.

We can also envisage a case in which a company introduces access control by means of the voice recognition of its individual employees. For the purpose of entry to premises, biometric data (the voice) is in such an instance used for checking or establishing identity. It may be supposed that the company could subsequently start using the biometric data thus collected to ascertain the emotional state of individual employees, or even tracking them by ascertaining their physical location at any point in time. In any such instance the company would be using data for purposes which are not in compliance with the purposes for which consent was given, and accordingly would be in breach the basic principle laid down in Article 16 of ZVOP-1. Said Article maintains that personal data may only be further processed in a manner solely concordant with the purposes for which it was expressly collected.

A certain medical condition can also represent a hindrance in the application of biometrics. Such is the case with persons who do not possess certain biometric characteristics (e.g. with anridia (no iris), or 'dry' fingerprints, or prints without any characteristics) or who have suffered facial injuries, in which case a face recognition device would be unable to identify the person.

Frequently Asked Questions

This chapter provides answers to frequently asked questions encountered by private sector companies and organizations considering the introduction of biometric measures.

What must an employer who wishes to introduce biometric measures have to take into consideration?

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 secrets (in accordance with the provisions of ZVOP-1). 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 fulfil the employer's needs or obligations.

Before any application is made to the Information Commissioner 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. Is the biometric data going to be stored centrally, or dispersed - e.g. on a card provided to each employee? Furthermore, is the system going to be based on identification or authentication? 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.

Ireland's Personal Data Commissioner - the supervisory authority for personal data protection in Eire - has published a series of questions on its website (www.dataprotection.ie) which any employer would be obliged to provide compelling answers to before biometric measures could be implemented:

1. *Do I have a time management and/or access control system in place?*
2. *Why do I feel I need to replace it?*

3. *What problems are there with the system?*
4. *Are these problems a result of poor administration of the system or an inherent design problem?*
5. *Have I examined a number of types of system that are available?*
6. *Will the non-biometric systems perform the required tasks adequately?*
7. *Do I need a biometric system?*
8. *If so, what kind do I need?*
9. *Do I need a system that identifies employees as opposed to a verification system?*
10. *Do I need a central database?*
11. *If so, what is wrong with a system that does not use a central database?*
12. *What is the biometric system required to achieve for me?*
13. *Is it for time management purposes and/or for access control purposes?*
14. *How accurate shall the data be?*
15. *What procedures are used to ensure accuracy of data?*
16. *Will the data require updating?*
17. *How will the information on it be secured?*
18. *Who shall have access to the data or to logs?*
19. *Why, when and how shall such access be permitted?*
20. *What constitutes an abuse of the system by an employee?*
21. *What procedures shall I put in place to deal with abuse?*
22. *Does the system used employ additional identifiers (e.g. PIN number, smart card) along with the biometric?*
23. *If so, would these additional identifiers be sufficient on their own, rather than requiring operation in conjunction with a biometric?*
24. *How shall I inform employees about the system?*
25. *What information about the system need I provide to employees?*

In the end a solution which might not need resort to questions pertaining to personal data protection is certainly welcome in order to preserve a little humanity in the workplace. An employer should also take into consideration a necessary respect for employee's rights: an employee is not merely a worker but primarily a human being whose rights must be respected in the workplace.

Numerous studies reveal that any exaggerated implementation of surveillance of employees is not only detrimental for the employees but also for the performance of the company. A study entitled Reasonableness in the Context of Workplace Privacy, undertaken in Ontario, Canada, which was presented at the 2001 Toronto Infonex Conference, revealed that there is a close correlation between employee surveillance and stress; a consequence of this is increased expenses for the company due to absenteeism as well as employees prematurely leaving the company. Such experiences confirm that it is more beneficial for management to invest into the development of suitable interpersonal relationships in the workplace and - with that - bolstering trust and enhancing loyalty in the mutual creation of an inspiring working environment, than it is in any omnipresent technological surveillance of employees. In other words: technical solutions do not provide solutions to social problems. Surveillance destroys both trust and any positive atmosphere in a company, it also promotes disturbance and dissatisfaction. Further to such philosophy, there is an abundance of European and North American judicial precedent governing the realm of abuse of surveillance systems in the workplace (Aljaž Marn, Dnevnik nove ekonomije).

Can biometrics be implemented in a company in order to record the working time of employees?

Pursuant to the provisions of Article 80 of ZVOP-1, biometric measures can only be implemented if they are necessarily required for the performance of mandated activities, for the security of people or property, or to protect confidential data and business secrets. By way of such a provision the legislator pursued the principle of proportionality (Article 3 of the ZVOP-1) and enshrined said principle with regard to the processing of special kinds of personal data - i.e. biometric data - and accordingly, when undertaking the implementation of biometric measures, limited the possibility of exaggerated or unjustifiable impingement upon the privacy and dignity of the individual.

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.

If a company wants to implement biometric measures (which are necessarily required for the secure performance of its mandatory activities, for the security of people or property, or to protect confidential data and business secrets) 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. The latter reason is often stated only in a general manner, and insufficient proof is provided in relation to the absolute need for biometrics 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 implementa-

tion of biometrics without a suitable substantiation, supported by proof, does not meet the legal prerequisites.

The website of the Information Commissioner provides links to decisions handed down by foreign personal data protection authorities with regard to implementation of biometric measures within the workplace.

Can biometric measures be implemented in relation to persons who are not employed by the company?

The legislation is very clear as regards this. Biometric measures utilized by operators in the private sector can only be applied in relation to employees of that company (see: first paragraph of Article 80 of ZVOP-1). Because the aforementioned Article provides a basis only for employees, and the legislation pertaining to personal data protection is subject to the principle that anything which is not explicitly sanctioned by the law shall be prohibited, the application of biometric measures in relation to other persons is not allowed.

Employees are deemed to be persons who have concluded a contract of employment with the controller (company), i.e. individuals who are in a direct contractual relationship with that company. Subcontractors, persons who work temporarily through the students employment service, or on the basis of other agreements, shall not be regarded as employees.

Are the Information Commissioner's decisions - issued in relation to procedures on the implementation of biometric measures - publicly accessible?

The Information Commissioner's website publishes decisions on the implementation of biometric measures (search using the keywords *biometrija, biometrics*).

Why is biometrics in the private sector subject to examination by the Information Commissioner? Is this not another bureaucratic obstacle to the free operation of the private sector?

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 behavioural 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 behavioural characteristics. If we for a moment leave aside those questions that pertain to the basic human right of integrity and dignity of the person, any 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.

Although system manufacturers may claim that abuse is practically impossible, history reminds that no code is unbreakable, and that which is unforeseen is greater than that which is known. So why would biometric systems be an exception? Manufacturers claim that their systems store templates, i.e. reduced, digitalized forms of biometric characteristics in such a manner that the reconstruction of original data is no longer possible. They also claim that the system captures unique data - on, for example, fingerprints - processes it and transforms it into a template on the basis of which the identity of the person to which it belongs can no longer be established. This claim is supposedly substantiated on the precept that the system uses a unique algorithm, thus preventing any reconstruction of the original biometric characteristics. Any such statement is questionable from the perspective of information security from at least from two aspects.

The first relates to the question as to whether the reconstruction of biometric characteristics is possible from the template, and in relation to this what is the possibility that the algorithm may be deciphered thus releasing any 'encoded' biometric data. If we find the parallels in cryptographic algorithms, then we see that the safest algorithms are those which are exposed to public examination, and are available to anyone who tries to break them with all available means. For any algorithm or method of encryption, we can only deem it to be safe on the basis of the opinion of the available experts who test it using extant technology, without resort to exceptional means or time, hence in reality it is difficult to assess how safe and unbreakable they actually are. Personal data protection cannot be predicated on the secrecy of algorithms or the inaccessibility of technology. Security mechanisms anticipate the ignorance of hackers, which, given today's rapid level of development, is quite self-deluding. You can find more information as to the possibilities of reconstructing original biometric data in Manfred Bromba's article, obtainable from: http://www.bromba.com/knowhow/temppriv.htm

The second aspect is connected with the question as to whether prevention of the reconstruction of original biometric data is really a key factor in upholding and maintaining the privacy of the individual, and this is presented in more detail in the answer to the last question in the Guidelines ("If the image of a fingerprint is not stored, but only a coded pattern - a digital template - of the print, which does not enable its reconstruction, is this also regarded as processing personal data?"). National supervisory authorities for personal data protection all too frequently encounter cases in which personal data is initially collected for one purpose but is later used for entirely different purposes. And when that happens, the individuals concerned have to continuously put tremendous amounts of effort into preserving their privacy. It cannot be claimed that the collection of biometric data is in any way immune to the above phenomenon.

Biometrics has another significant limitation, which arises from its very nature. Namely, biometric characteristics are not keys, since they do not have the basic characteristics of keys. As opposed to passwords or digital confirmations, biometric characteristics are not hidden, they cannot be altered, destroyed or declared invalid (the fingerprint is a graphic example of this). Keys, on the other hand, can be hidden, we can acquire new ones, we can destroy old ones, alter or disable them; however, we cannot cancel a fingerprint and issue a new one. Moreover, one of the basic principles of security is that we do not use the same key for everything, and that - on the basis of the notion that its best not to keep all our eggs in the same basket - we use different keys for the car, the house, the office, the garage etc. The risk of theft or abuse of any such universal key would be too high. Imagine that some day we will »unlock« everything using a single biometric characteristic - a fingerprint say - then we are in the same situation as if we had just one single key for everything; the difference being that we cannot "change the lock" , let alone all the locks.

This problem can be clarified in another way. Biometrics, in its essence, is not a so-called challenge and response system. To put it simply: the answer to the question: »What is the print of your right index finger?« is always the same. Conversely, the system of challenge and response forever asks different questions and is capable of ascertaining the answer (think of the generators of single-use passwords of the type used in on-line banking).

Biometrics nevertheless has its advantages; we must, however, be aware of and acknowledge its limitations. The questions of personal data security when using biometrics are explicitly addressed in this presentation.

If we examine biometrics merely from the aspect of the protection of privacy, then we can say that biometrics, like other technology, is neither a threat nor a protector, intrinsically it is neither benign nor malignant. The implementation of the technology - its use or abuse - remains decisive. Biometrics can be used to enhance privacy, if, of course, is carried out in compliance with basic tenets and rules governing personal data protection (and such principles as proportionality, transparency, strict application and appropriate protection). Indeed, Article 20 of EU Directive 95/46/EU provides that permission by the national supervisory authority for personal data protection should be required prior to the implementation of certain measures. On the basis of this European Directive, Slovenia's legislator decided to introduce statutory examination and assessment of proposed biometric measures, prior to any introduction into the workplace.

The Information Commissioner is accordingly obliged to carry out a thorough examination of projected biometric measures and assess whether their introduction is in compliance with those principles and rules governing personal data protection. When assessing an individual technology, besides the purpose pursued by the controller, the Commissioner 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 its apparent overtness / covertness, its containment (centralized or decentralized storage), the leaving of traces, the possibility of linkage, and the opportunity for control over one's own personal data.

Is it also necessary to obtain permission for the implementation of - for example - biometric locks in a private house, or on a computer or mobile telephone?

Since the processing of personal data for domestic purposes does not represent a risk from the perspective of the privacy of an individual, the legislator has foreseen in Article 7 of the ZVOP-1 an exception that ensures the provisions of this Act shall not apply to the processing of personal data by private individuals exclusively for personal use, family life or for other domestic needs. Biometric locks on household doors, computers or other devices used for private purposes may encompass personal data processing for which ZVOP-1 shall not apply. Consequently it is not necessary to obtain permission from the Information Commissioner in order to implement such measures.

Further to this, the aforementioned devices store biometric data in such way that it is not evident to which person they belong, and/or are stored in such a manner that no collection of personal data is established in the process. Consequently, ZVOP-1 does not apply and no permission is needed from the Information Commissioner.

If we have the signed statements of employees agreeing to the implementation of biometrics, do we still need to obtain permission from the Information Commissioner?

The second paragraph of Article 80 of the ZVOP-1 provides that if the implementation of specific biometric measures in the private sector is not regulated by statute, a data controller intending to implement biometric measures shall, prior to any introduction, be obliged to supply the National Supervisory Body with a description of those same measures as well as the reasons for the introduction thereof. The fourth paragraph of the same Article further provides that the data controller may implement biometric measures upon receipt of a favourable decision from the National Supervisory Body whereby the implementation of biometric measures shall be permitted. It is also set forth that biometric measures may only be used in relation to employees, if those same employees were informed in writing thereof in advance. Thus it arises from the aforementioned that the consent of employees is not sufficient in itself for the legal implementation of biometric measures in the private sector workplace. Although such is indeed necessary, it is insufficient. The implementation of biometric measures is only sanctioned if law provides for such, and a decision by the National Supervisory Body - the Information Commissioner - endorses their implementation.

To whom should any request for permission for the implementation of biometric measures be addressed? Is there a template or a form that should be used, and are there any costs involved?

You can find a sample of the application form for a request for the introduction of biometric measures at the Information Commissioner's website:

http://www.ip-rs.si/fileadmin/user_upload/doc/obrazci/PRIJAVA_BIOMETRIJSKIH_UKREPOV.doc

The use of this form is not compulsory but it can help when writing any application for permission to introduce biometric measures. Applications should be sent to the Information Commissioner RS, Vošnjakova 1, PO Box 78, 1000 Ljubljana, Slovenia. Administrative stamp duty needs to be paid in accordance with tariff numbers 1 and 3 of the Administrative Fees Act (Official Gazette of the RS, No. 42/2007, consolidated version 3). This admin fee, which currently (as of January 2009) stands at 17.73 euros, is payable into account No. 01100-1000315637 (reference 11 or 18 12157-7111002).

What shall the application include, are there any recommendations as regards filing?

With a view as to the requirements of the ZVOP-1 it is of crucial importance to substantiate that the implementation of biometric measures is essential for the fulfilment of one or more exhaustively listed objectives: the performance of mandatory activities, the protection of people and property, the protection of confidential data or business secrets. If possible, enclose documentation by way of which it can be proven that - within the premises for which it is planned to implement biometric control - secret or highly sensitive data is located and processed (for example permissions to access classified Ministry of the Interior data). Reading the decisions already handed down by the Information Commissioner - which are published on the website - will also be of use.

The Information Commissioner draws attention to the fact that - as mentioned above - the introduction of biometric measures is only justifiable if there is a fundamental and well-founded reason for such, and/or that such is necessar-

ily required in order to achieve a mandated objective. Reasons of practicality, or because of the absence of collateral worries (which are, for example, a legitimate concern in relation to abuses of swipe-card systems), or because biometric measures represent a useful alternative solution in the prevention of unauthorized access, or because the technology is modern and attractive, are not in themselves legitimate or well-founded reasons for the implementation of biometrics in the workplace. The introduction of biometric measures merely because they are more practical than systems which are based on, for example, swipe-cards, cannot be defined as necessary or required to achieve a mandated objective, as is defined in the first paragraph of Article 80 of the ZVOP-1.

The Information Commissioner also draws attention to the fact that the application for permission must be addressed to the Information Commissioner by the potential user of the biometrics and not the producer or distributor of the equipment. The decision of the Information Commissioner also cannot be influenced by standard wordings, prepared by vendors or distributors of the equipment; indeed, it is the user of the biometric measures who must especially and specifically explain the purpose behind the introduction of biometric measures, as well as substantiate the degree and urgency of such measures. Written materials, provided by system manufacturers or their agents can be enclosed with the application in order to help explain the technical characteristics and function of specific equipment, but this shall not replace the necessary substantiation of the purpose which is - as mentioned before - the task of the applicant, i.e. the potential user and controller of the biometric device.

Appropriate proof that the employees have been informed of the intended introduction of biometric measures – for example a dated and stamped notification to the employees, or a document bearing the signatures of the employees - must also be enclosed with the application to the Information Commissioner. If representative trade union(s) also exist, then the registered address of said trade union(s), which the Commissioner is bound to inform as to the proposed introduction of biometrics, must also be entered into the application. If, in a specific instance, the trade union issue is not applicable, then this too must be stated in the application.

After all the information has been received – or related in legal language – and the application has been thus completed, the Information Commissioner shall decide within 2 months whether the intended introduction of biometric measures is to be allowed.

If the image of a fingerprint is not stored, but only a coded pattern - a digital template - of the print, which does not enable its reconstruction, is this also regarded as processing personal data?

Manufacturers and suppliers of biometric equipment often state that the privacy of users is ensured, because the restoration of, for example, a fingerprint is not possible from a digital template. Let us suppose for a moment that this is true. Let us also suppose that the restoration of the original data is really impossible. Although that might be true, the privacy of the user is still not secure because the pattern of the fingerprint and the pattern in the digital form are uniform identifications, and hence the latter represents a derivative identity of the individual. Let us imagine a scenario when instead of submitting biometric data the system would operate on the basis of a personal identification number. Although we cannot reconstruct the original fingerprint data because we do not know how it was transformed, the exclusive identification number the individual has been assigned also represents personal data. The question of breaking the algorithm code and reconstruction of the original fingerprint data is irrelevant, regardless as to whether a very simple algorithm or a highly sophisticated mathematical formula is used.

The key questions from the perspective of privacy of the individual pertain to the use, connectivity and security of any identifier that may be employed. A potential hacker would more easily achieve the same intention by acquiring the latent fingerprint (e.g. on a glass), than in investing a great deal of effort, means and time into deciphering an algorithm which would also yield the original data.

That which is valid for biometric characteristics, as such, is also applicable for digitalised records composed on the basis of that same unique characteristic, regardless of the fact how many times has such a recording has been processed or altered. Regardless of the form, manner of recording or other alteration, and even though the amount of detail may diminish in the process of transformation, it forever retains the same unique connection with an individual (see page 36 of At face value: on biometrical identification and privacy; Registratiekamer, September 1999).

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.

CONCLUSIONS

The decision regarding the regulation and admissibility of the introduction of biometric measures is, in compliance with Directive 95/46/EU, left to the separate discretion of the legislator in each member state. Biometrics will inevitably become ever more present in different spheres of our lives. The path chosen by Slovenia might be relatively strict, however, with the currently valid system of prior approval by an independent state authority a so-called privacy impact assessment is carried out prior to the introduction of biometric measures. If biometric measures were to be implemented without any assessment obligation or obtainment of permission, the only available protection of the basic human right to privacy would be post festum inspection control. The Commissioner considers that ex ante assessment is more effective from the aspect of the protection of privacy, especially as regards the question of technology, which is still in the process of development and establishment. In the light of ongoing technological development, the adequacy of the legal framework will need to be reassessed in the longer term.