

IDENTIFICATION SYSTEMS CONTROL AND THE PROTECTION OF PERSONALLITY

Bc. Ivan PAHUT, Ing. Ján KOLESÁR, PhD.

Technical University of Košice

Faculty of Aeronautic, Department of air traffic management

Rampová7, 041 21 Košice, Slovak Republic

*Corresponding author: inpht1@gmail.com, kolesar.jan@tuke.sk

Summary: The work deals with the protection of personal data and the protection of individuals at the airport, but also in the process of handling at the airport. They also include individuals that these data handling as we call them, and the like. The work described also discusses the modern identification systems, which help in identifying the persons under examination at the airport, but also for visitors to the airport. They also work highlights the advantages and disadvantages of each system and what are at present opportunities for the use of such systems at airports.

Keywords: Detection, personal protection, personal data, biometrics, biometric detection system

1. INTRODUCTION

Nowadays electronisation and mobilization of the population is important to protect sensitive personal information and it is also important the protection of personality. Personal data should be protected especially because they can not be used by others for illegal purposes, in order to abuse people and so on.

Personal data are entrance doors to the privacy of each and every person. Personal data are applied daily in various social relationships, but it is difficult to define exactly what is considered personal information.

2. PERSONAL DATA AND PROTECTION OF PERSONAL IDENTIFIABLE INFORMATION

Personal data may be defined as information relating to an identified or identifiable person, where such a person is one who can be identified directly or indirectly, mainly based on universal usable identifier or based on one or more features or symbols. These symbols together are making physical, physiological, psychological, mental, economic, cultural and social identity. It is really hard to find the precise definition of term „personal data“ due to complexity of this issue. However, the term of personal data consists of several basic elements. These elements are acting together as identifiers and belong to particular individual and his identity. If we are talking about area of fundamental human rights and freedom, which belong exclusively to every person, the personal data are reported to a privacy law. But on the other hand, if we are mentioning the data defining a legal person / entity or natural person, and these data are going to be processed in the information system of the operator, there are not personal data and therefore it is not possible to be within field of the law.

So personal data are the only data which are relating to the particular individual only. We could say, that personal data can be any data relating to a specific person and that is why the law is not defining the exact amount of information which could be regarded as personal data. Data of groups or individuals processed from video surveillance and sound recording systems are also considered as personal data, because they can themselves provide some information also. The criteria for term

personal data can be fulfilled if we have a freely distributable text in writing or electronically, which contains personal information about individual or group of people. Thus to define if we are talking about personal data or not, we need to consider this on specific situation, based on data, which are available at this time, and which data could be attributed to a natural person.

3. BIOMETRIC DATA PROCESSING

Trend in biometric data processing associated with the use of biometric technologies is very progressive and increasingly promoted in various spheres of life of human beings. The biometric data is used also in scientific research or in applied forensic science. These are valuable elements of different systems that provide clarity, and uniqueness of the individual, strengthen authentication methods, or allow controlled entries into a designated area. However, biometric data given their nature and diversity, have a features, which are very sensitive for every person and also with regard to the fact that they cannot be changed for example like an entry password.

Biometric data is a personal data of every individual indicating his biological or physiological feature or characteristic, by which is clearly unmistakably determinable. On behalf of biometric data we are mainly talking about fingerprints, palmprint or analysis of deoxyribonucleic acid.

The definition of term biometrics due to personal data protection is based on three fundamental and correlated elements (data indicating biological or physiological feature/characteristic belonging exclusively to individuals), two specific characteristics (uniqueness and non-interchangeability) and listing of biometric identifiers such as (fingerprints, palmprint, retina, biometric signature, gait etc).

In other words, the biometric data are biological characteristics, physiological features or repeatable activities, for which these properties and / or activities are specific to particular individual. There are able to measure, even if the methods used for their technical measurements are working with a certain degree of probability. Their value is based on specific universal biometric sample (every individual owns the specific feature/attribute). That sample implies its uniqueness (natural separation from others), stability (an element that remains throughout life) and measurability (feature can be compared with others and quantified). Processing of biometric data can be done only in that condition, when operator requests a special registration (except when biometric data would be processed under the separate legislation. After successful registration and approval, the operator shall be entitled to process biometric data. Under the Law, approval of special registration and permit for processing of biometric data is without prejudice to other operator's obligations.

The regulation mentioned above shall be applied from the beginning of the process. It includes obtaining of raw biometric data, to completion and finally destruction of all personal data processed in the information system, which was legally built for purpose of biometric data processing. The processing of raw biometric data with mathematical algorithm, that is stored in biometrical template, is not an impact to the legal information system of personal data for biometric purposes in the overall process. Therefore in terms of law, the personal data filling system for biometric purposes is considered as a whole and taking into account all aspects of mutual relations.

4. PERSONAL DATA PROTECTION IN CIVIL AVIATION

Personal data protection in civil aviation is very essential, we are not only talking about protection during the check in process or passport control, but during the security check at the airport, where personal data protection could not be compromised. Mostly during the hand searching and

cabin baggage screening. Hand searching of passengers is done by the employees of airport security, that control must be done before reaching clear zone according to European Union regulation no.185 of 2010. If the metal detector goes off during the security check of travellers, security member is allowed to start hand searching of affected passenger, until his confidence.

Of course, passengers rights of personal data protection shall not be violated during the screening. It follows that if a security member is checking the suspects, and he is not quite sure or he has a suspicion, or can be some danger done from object in passenger possession, he is allowed to do a more detailed body search in a separate room.

However, security personnel is not allowed to perform body cavity search. This operation can be performed only by persons, who are authorized to carry out such examination.

Of course, there may occur a situation, when passenger is marked as a suspect by police dog, or he looks suspicious during the screening, next step will be the detailed hand search. Hand search can be only performed by trained personnel with special permission for this kind of checks.

Unless the passenger must undergo such an examination, the examination must be carried out so as not to disturb personal data rights. It means, that the person, which is undergoing this kind of examination must be separated from other travelers, not in public areas. Affected person must be informed about upcoming examination.

5. SYSTEM OF PERSON IDENTIFICATION AT THE AIRPORTS

Nowadays, at most part of the worlds airports there are very simple systems for personal identification, or even are not in use in general. Identification is being performed by trained security personnel. Disadvantage is, when the security member must use a ID cards for the person identification. The photos on IDs might be outdated or in bad quality.

Unless this occurs, security member should notice some characteristics of person face, which are not changing during the lifetime, for example nose, ears, eyes, facial injuries or other characteristics. The following characters must clearly identify if the specific documents truly belongs to particular person.

The bigger issue may occur during the infant identification. For example, in the Great Britain young child or even infant has held a passport with validation for ten years of issue date. Just for the information, the infant in Slovak republic would get the passport only validated for two years. Because of great changing in baby or child face during the first three of four years of life. That is one of the issues , when the infant or child is entering a Slovak republic. The security officer might not be sure with face identification during the passport control or security checks. In these cases, or in many others the big help for the airport employees would be a system of person identification based on modern technology such as above mentioned biometrics. There are many options, for example systems for fingerprint screening, retina scanning, identification of people by face, PalmSecure technology.

6. THE APPLICATION OF ADVANCED TECHNOLOGIES AT AIRPORTS AND PROTECTION OF PERSONALITY

Of the methods described above each can be used relative to the airport. Of course, through all the world's airports every day of travel a few million people and technology that would be used to identify and verify individuals must be secure, nowadays it is mainly in terms of information security, it must be very fast, and the main condition for such a system It is that technology must be reliable.

Today, the world's airports technology is used the comparison of fingerprints, which is the oldest and also the most reliable. If we wanted to use this technology to speed up the check-in process and it will replace the travel document, it would have to change the legislation, and would need to create an

extremely large global database that would be accessible to the airport, to check-in passengers were able to work with that database and of course it would be ready for such a system and airport-stop systems, which in the real-time database compared with fingerprints. This technology is used worldwide by police forces, is used for passport control and, for example, in the United States, the fingerprint is used for comparison with the data that is in the passport of the passenger.

In terms of handling process at the airport, this technology is almost better than a verification identification technology, as the fingerprint can be copied and misused. The advantage of this verification person is that as long as we have two persons to each other, like we can in the process of tripping fingerprint to distinguish that person specifically include identity documents. Disadvantages of this and other technologies is the fact that if they want to use to identify people need to have a large database of biometric data, which could be compared to a real person.

Another technique that can be used at airports, but rather in terms of security personnel entering certain premises is a technology based sensor records the pulse of people, pressure, heartbeat and the like, and based on these data is able to identify a particular person. The application of this technology it is necessary to use a special concrete personal bracelet, in which integrated sensors to the various above-mentioned data can be recorded. Of course, given the technology it does not consist only of the bracelet can be embedded in watches, jewelry and the like, or can be used special sensors that are affixed directly to the body. Based on the longer-term data acquisition system can recognize, according to the particular behavior of the human body, about what exactly is a person. If we use this technology in data transmission system using RFID readers, such as employees of the airport would not have this bracelet attached to a special reader, which is able to read this data but it would be enough to approach a certain distance by a system based on transmission by radio waves proved which identify the person in question. In the case of the use of such devices it is preferable to use data transfer using active RFID system, because the sensor when the bracelet to send data to a particular person in the reader, which would be completed electronically identify a specific person, and on the basis of identification would allow access to secure areas of the airport.

LITERATURE LIST

- [1]. The Office for Personal Data Protection of the Slovak Republic: Methodological Guideline No.1 / 2013 on the concept of personal data, the website [online]. July 1, 2013. [cit.2015-2-26] to Available on Internet : http://dataprotection.gov.sk/uouu/sites/default/files/metodicke_usmernenie_c._1_2013_k_pojmu_osobne_udaje.pdf.
- [2]. European Commission: Communication to the European Parliament and the Council on the use of security scanners at EU airports, website [online]. June, 15, 2010. [cit.2015-3-24]. Available on the Internet:<http://ec.europa.eu/transparency/regdoc/rep/1/2010/SK/1-2010-311-SK-F1-1.Pdf>.
- [3]. Ministry of Interior of the Slovak Republic: the Schengen Borders Code website [online]. March, 2010. [cit.2015-4-1]. Available at: www.minv.sk/?dokumenty-na-stiahnutie-2&subor=90629.
- [4]. Fujitsu PalmSecure, website [online]. [cit.2015-4-18]. Available on the Internet:<http://www.fujitsu.com/global/solutions/business-technology/security/palmsecure/technology/index.html>.