Athens, 4-6-2010

Ref. No.: G/OUT/335-2/04-06-2010

DECISION 31/2010

The Hellenic Data Protection Authority (HDPA), consisting of the President Mr. C. Yeraris, the members Mr. L. Kotsalis, Mr. A. Papaneofytou, Mr. A. Prassos, Mr. A. Metaxas and Mr. A. Roupakiotis and the alternate member Mrs G. Pantziou, substituting the regular member Mr A. Pombortsis, who could not be present due to an impediment, although he was formally invited, convened on 27/5/2010, following an invitation by the President in order to examine the case that is reported herein below. The rapporteurs Ms A. Bourka and Mr K. Moulinos, IT auditors, and Ms E. Hatziliasi, legal expert, as well as the secretary Ms G. Palaiologou, employee of the Administration and Economics Department, were also present without the right to vote.

The HDPA took under consideration the following:

The company 3D General Aviation Applications (hereinafter called "the Controller"), who is engaged in the field of aviation applications and airport security, submitted to the HDPA the notification with ref. no. GN/IN/335/12.3.2010, asking permission for the installation of a pilot biometric access control system in critical infrastructures of the International Airport "Macedonia" in the city of Thessaloniki. The above installation will be performed within the framework of the research project TURBINE ("Trusted Revocable Biometric Identities"), which is carried out by the Controller in cooperation with other European partners and is financed by the European Union.

According to the notification, the TURBINE project aims at elaborating a privacy-friendly biometric method based on fingerprints. More specifically, the method is based on the replacement of the biometric fingerprint with a unique and irrevocable encrypted derivative of the fingerprint, referred to as "biometric identity", using

special hash functions based on cryptographic algorithms. By using different cryptographic algorithms, the production of a respective number of biometric identities for the same fingerprint is made possible. Each biometric identity is connected exclusively with the person whose fingerprint was taken, following the application of a specific algorithm. Using the above method during the operation of a biometric system (e.g. to control access of persons to installations) the identification of persons is accomplished via their biometric identities, in a way that there is no need to retain their raw biometric fingerprints.

The installation of the above mentioned biometric system at the "Macedonia" airport aims at its pilot trial under real case scenarios in order to check possible errors or problems that may arise during its operation. More specifically, the system will operate for one (1) month in specific areas of "Macedonia" airport which are located: a) in the central office of the Controller within the airport headquarters, b) in the special building run by the Controller within the parking area of civil aviation aircrafts, c) in the CARGO building of the airline company OLYMPIC AIR within the airport, and d) in the building of ELGA (Greek Agricultural Insurance Organization) in the airport where there is a special aviation application of monitoring and controlling a hail suppression project. All of the aforementioned installations are deemed critical and their access is allowed to authorized personnel only. The trial will be carried out with the use of personal data of persons working in the above areas and more specifically employees of the Controller, as well as employees of OLYMPIC AIR and ELGA for the CARGO building and the hail suppression application building respectively. The said employees will participate as volunteers following relevant instructions and upon having given their explicit and informed consent (a copy of the information and consent form has been submitted by the Controller to the HDPA together with the notification). The biometric system shall operate exclusively on a trial basis and shall not replace the existing access control systems which are already in use in the airport.

The trial operation shall be structured as follows: during the registration of the volunteers in the biometric system, their fingerprints (one or more) will be taken, from which their biometric identities (one or more for each fingerprint) will be

produced. Multiple biometric identities are required when access rights for the same person in distinct airport installations are graded. The biometric identities shall then be stored in smart cards or in a central database, together with some other data of the volunteers required for their identification, i.e. full name, job description and photograph. These data are already processed by the Controller for the issuance of identification badges worn by those who have access to the specific areas. Following the registration phase, the entrance of the volunteers in the areas where the pilot system will be operating shall be controlled (using either smart cards or the central database) on the basis of biometric identities and the rest of the collected personal data. Part of the processing shall be carried out by processors (partners of the TURBINE project) and specifically the companies Sagem-Orga (Germany), which is involved in the production and personalization of smart cards, and Cryptolog (France), which develops the cryptographic algorithms used. The Controller has submitted to the HDPA, together with the notification, the contracts concluded with the above companies, which include a term concerning the security and protection of personal data. The biometric system data shall be kept until the completion of the project and its final approval by the European Commission (June 2011).

Apart from the foregoing data, the Controller has asked to retain also the raw biometric data (fingerprints) taken during the trials for a period of three (3) months. These data shall be stored in a special database which shall not be connected with the biometric system. The processing is optional, i.e. it is not deemed indispensable for the realization of the pilot project in “Macedonia” airport. On the contrary, the database shall be used for the quality control and the statistical processing of the total results of the TURBINE project, in connection with relevant data kept by the rest of the partners, with the general aim of improving the cryptographic algorithms currently in use. This task shall be performed by a processor and specifically the GUC University (Norway), partner in the TURBINE project. The Controller has submitted to the HDPA, together with the notification, the contract concluded with the aforesaid partner, in which there is a term referred to the security and protection of personal data.

The HDPA, after having examined the foregoing information, listened to the rapporteurs and discussed the facts thoroughly,

DELIBERATED ACCORDING TO THE LAW

1. Article 2 of Law 2472/1997 stipulates that “personal data” is “any information relating to the data subject”. “Data subject” is “any natural person to whom such data refer and whose identity is known or may be found, i.e. his/her identity may be determined directly or indirectly, in particular by reference to an identity card number or to one or more factors specific to his/her physical, physiological, mental, economic, cultural, political or social identity”. As the E.U. Article 29 Working Party has pointed out, biometric data constitute personal data since they may be considered both as *content of information* characterizing specific biological traits, physiological characteristics and/or personal features unique to an individual (e.g. “A has X fingerprints”), as well *as a way to connect* this piece of information to a specific individual (e.g. “the object Y bears the X fingerprints which belong to A, consequently A has touched object Y”). Thus, biometric data, due to their exclusive connection with a specific person, may operate as a means of *identification* of this person.

2. In the case of the TURBINE project, the proposed biometric system uses a method which “pseudonymizes” biometric data (fingerprints), replacing them with encrypted irrevocable derivatives (biometric identities) arising through one-way cryptography techniques with the application of hash functions. Taking into account that, due to the technical means of producing biometric identities, the extraction of raw biometric data from them is not possible, a biometric identity cannot be considered as content of information characterizing a person in the sense mentioned above. Therefore, the use of a biometric identity, instead of the raw biometric fingerprint, enhances the protection of the latter, since it is impossible, in technical terms, to extract the fingerprint information directly from the biometric identity. However, due to the fact that the exclusive connection of the biometric identity with a specific person still exists (as only the fingerprint of the same person could lead each time to the production of the same biometric identity with the use of the same cryptographic algorithm), the biometric identity may lead to the identification of that

person, in the same way that the raw biometric element does. In other words, although the biometric identity could not independently lead to disclosure of information relating to a person, it may nevertheless lead to the identification of this person within the framework of the biometric system operation (e.g. during access control) and in combination with other personal data kept in the system for the same person (e.g. full name). In this sense, the biometric identity, as it is produced and used by the TURBINE project, also constitutes personal data.

3. According to article 4 par. 1 item a of law 2472/1997, personal data, in order to be lawfully processed, must be collected fairly and lawfully for specific, explicit and legitimate purposes and should be fairly and lawfully processed in view of these purposes. In the framework of the TURBINE project, there are two cases of personal data processing: a) processing via the pilot biometric system (based on the use of biometric identities), b) processing of raw biometric data in an independent database. In both cases, the aim of the processing is scientific research with special focus on the encryption of biometric data, which falls under the wider research field of developing Privacy Enhancing Technologies (PET). Processing in view of the foregoing purpose is carried out pursuant to paragraph 1 of article 5 of Law 2472/1997 with the consent of the data subjects.

4. According to article 4 par. 1 item b of Law 2472/1997, personal data must be adequate, relevant and not excessive in relation to the purposes for which they are processed. This provision sets out, as a criterion for the lawfulness of each processing, the principle of proportionality, according to which it must be examined each time whether the processing of specific personal data is essential for the purpose aimed at and that this purpose cannot be met by less onerous means. As for the two cases of processing carried out within the framework of the TURBINE project, the following apply:

i) In the case of the pilot biometric system, the principle of proportionality is met, taking into consideration the nature of the purpose that is scientific research, as well as the fact that the retention of data is limited to biometric identities (instead of raw biometric data), from which information about the data subject cannot be disclosed.

The biometric identities are used solely for the data subjects' identification in combination with other relevant personal data (full name, job details, photograph) which are already known to the Controller. It should be noted that even under real use case scenarios (i.e. when the purpose ceases to be research), the above processing might be deemed lawful according to article 4 par.1 item b and article 5 par. 2 item e of Law 2472/1997 in cases where advanced security measures for access control in critical infrastructures should be applied (see DPA's Directive 115/2001 for the protection of personal data in the work field and Decisions 9/2003, 52/2008, 56/2009). As far as the storage of biometric identities is concerned, it is worth pointing out that, under real case scenarios, the best way to store them would be locally in smart cards (and not in a central database); this enables data subjects to have greater control over their personal data. Under the pilot trial case, though, it cannot be deemed that data processing in a central database is not acceptable, since it constitutes an essential requirement for the realization of the research (comparison of method effectiveness both with the use of cards and central storage), provided that the Controller takes all necessary technical and organizational measures for the security of the data, according to article 10 of Law 2472/1997. Finally, with regard to the data retention period, it is fixed to one (1) year, the minimum according to the requirements of the European Commission that must be able to check the results after the completion of the project by June 2011 at the latest.

ii) On the contrary, in the case of the raw biometric data, the processing contravenes the principle of proportionality since: a) the necessity of the retention of this data for a period of three (3) months is not properly justified by the Controller, in the context of the operation of the specific pilot project, b) the data are stored in a central database, which may probably be interconnected with the partners' systems, thus creating concerns with regard to the security of the personal data involved. Particularly, as for the latter, it should be pointed out that the exact way of carrying out the statistical analysis of the raw biometric data (including the measures which must be taken for their protection) within the framework of the project is neither known to the Controller nor is it described precisely in the contract concluded with the processor.

5. As for the volunteers' consent, which constitutes the legal base of the processing, pursuant to article 5 par. 1 of Law 2472/1997, the following is in force: according to article 2 of Law 2472/1997 the data subject's consent is considered to be "any freely given, explicit and specific indication of will, whereby the data subject expressly and fully cognizant signifies his/her informed agreement to personal data relating to him/her being processed". In the framework of the TURBINE project consent is free, since the data subjects voluntarily participate in the pilot trials, and at the same time they are given alternative ways for accessing the airport installations (the pilot system shall not substitute current procedures). Furthermore, the consent is explicit and express as it is given via filling in a special form. By this form, volunteers are also informed about the processing of their personal data, the identity of the Controller, the purpose of the processing, as well as the way in which data subjects may exercise their rights of access and objection according to Law 2472/1997 (articles 12 and 13). It is noted that the information note should additionally mention explicitly the categories of personal data under processing, the precise areas in the "Macedonia" airport where the pilot project will be operating, as well as the processors involved and their particular duties. Moreover, the note should explicitly mention that there are no other recipients of the personal data except for the authorized employees of the Controller and the processors (according to the relevant contracts of project assignment).

ON THOSE GROUNDS

The Hellenic Data Protection Authority decided by majority that the installation of the aforementioned biometric system exclusively for scientific research purposes does not contravene the provisions of Law 2472/1997, insofar as the following terms are fulfilled:

1. The Controller is obliged to revise the current information and consent form according to what is mentioned in the present Decision.

2. The Controller is obliged to develop a security policy for the processing of personal data in the framework of the pilot biometric system and to notify correspondingly the HDPA within three (3) months from the issuance of the present Decision.

3. The Controller is obliged to notify the HDPA about the destruction of data retained within the framework of the pilot biometric system after the end of the one (1) year period which is required for the accomplishment of the processing purpose. The notification should take place within fifteen (15) days after the destruction of the data. The Controller should submit the data destruction protocol to the HDPA.

4. The retention of raw biometric data, resulting from the trials, in a central database, is forbidden.

5. Any expansion of operations or other technical change or change of procedures relating to the application and operation of the biometric system, without the HDPA's prior notification and approval, is forbidden.

The President	The Secretary
Christos Yeraris	Georgia Palaiologou