EUROPEAN DATA
PROTECTION SUPERVISOR

Opinion of the European Data Protection Supervisor on a research project funded by the European Union under the Seventh Framework Programme (FP7) for Research and Technology Development - Turbine (TrUsted Revocable Biometric IdeNtitiEs)

THE EUROPEAN DATA PROTECTION SUPERVISOR,

Having regard to the Treaty on the Functioning of the European Union, and in particular its Article 16,

Having regard to the Charter of Fundamental Rights of the European Union, and in particular its Article 7 and 8,

Having regard to Regulation (EC) No 45/2001 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data, in particular Article 41,

Giving effect to his policy paper entitled "The EDPS and EU Research and Technological Development" which relates to the ongoing Seventh Framework Programme as well as future Framework Programmes for Research and Technological Development;

HAS ADOPTED THE FOLLOWING OPINION:

1. Introduction

1.1 General

1. For the first time, the EDPS adopts an opinion giving effect to his 2008 policy paper entitled "The EDPS and EU Research and Technological Development" describing the possible roles the institution could play for research and development (RTD) projects in the context of the Seventh Framework Programme for Research and Technological development (FP7) launched by the Commission at the end of 2006[1].

2. In 2008, after having analysed the elements of the EU project “TrUsted Revocable Biometric IdeNtitiEs” (Turbine) which aims at conducting research in the field of revocable biometrics, the EDPS decided to reply favourably to the consortium’s request to produce an opinion on the EU project[2]. The EDPS considered that the

[1] http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/Publications/Papers/PolicyP/08-04-28_PP_RTD_EN.pdf.

[2] See European Data Protection Supervisor, Annual Report 2008, p. 70.

conditions he set in his policy paper in order to accept the request for an opinion were met by the Turbine consortium. The EDPS welcomed the strong relevance of the project to ‘data protection issues’ and considered it would fit with the priorities identified in his Annual Report.

1.2 The instrument of an Opinion on EU Research and Technological Development

3. This policy paper presents the selection criteria for the projects that qualify for EDPS action and the ways in which the EDPS could contribute to these projects. One of EDPS' contributions to EU RTD is that of an opinion in relation to individual RTD projects.

4. According to the EDPS policy paper, "a consortium of a project can request an opinion from the EDPS. Although the EDPS will not contribute to a proposal for a project, the proposal can envisage to ask for an EDPS opinion during the life cycle of the project in the case it is awarded. In this case, the EDPS has to be informed and has to give his agreement for introducing a reference to a future EDPS opinion before the submission of the answer to the call for proposals. The consortium will have to clarify in the submitted documents relating to its proposal that the EDPS opinion will be given in his role as an independent authority". The independence of the EDPS in such exercises is clearly underlined in the paper, as well as in the communications with the project stakeholders contacting him.

1.3 Aim and scope of the opinion

5. The overall objective of the EDPS contribution is to promote and reinforce the application of the principle of ‘*privacy by design*’ within European RTD projects and to therefore facilitate the implementation of the EU data protection regulatory framework. The opinion does not only deal with the technical developments envisaged by the research project as such, but also with the research methodology and procedures implemented by the project.

6. The aim of the EDPS' opinion is not to supplement the role of reviewers of the project, nor the relevant national data protection authorities, but to provide an expert view on the data protection aspects of a given project. As a consequence, the EDPS does not analyse all the deliverables but requested access to the documents of the project which he found most relevant from a data protection perspective.

7. The consortium of the project provided the EDPS with all relevant documents on the data protection aspects of the research conducted in the Turbine project. The EDPS also held several discussions with some representatives of the consortium in order to obtain further clarification, and where required, further documents. Finally, the EDPS received comments of the consortium on a draft of this opinion.

1.4 Turbine

8. Turbine (TrUsted Revocable Biometric IdeNtitiEs) is a research project funded by the European Union under the Seventh Framework Programme (FP7) for Research and Technology Development (http://www.turbine-project.eu). According to the Turbine partners, the overall objectives of Turbine are:

   - to develop an innovative, privacy enhancing technology solution for electronic identity (eID) authentication through fingerprints biometrics, and

- to demonstrate the performance and security of this solution for use in commercial eID management applications as well as its benefit for the citizen in terms of enhanced privacy protection and user trust in electronic identity management through the use of fingerprints.

9. The project aims at elaborating a privacy-friendly biometric method based on fingerprints. The main focus of Turbine has been on the development of a so-called Pseudo Identity protocol (PI protocol) deploying protected (biometric) templates. More particular, in the Pseudo Identity protocol, biometric data is transformed allowing for diversification and unlinkability of biometric identities. More specifically, the method is based on the replacement of the biometric fingerprint with an 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.

10. 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 PI protocol also allows storing biometric data locally, for example, on a token, although other architectures remain possible.

11. As important features of the project, the Turbine technology is aimed to protect the biometric template by cryptographic transformation of the fingerprint information into a **non-invertible key** that allows matching by bit-to-bit comparison. The transformed biometric data is considered irreversible to the biometric samples and original templates. Moreover, to enhance user trust, this key will also be **revocable**, i.e. a new independent key can be generated to re-issue biometric identities.

12. The EDPS views these two elements (the expected non-invertibility (irreversibility) of the key and the revocability of the key) of this technology as the two pillars of the Turbine project. These aspects present the most interest to the EDPS from a data protection perspective and will be discussed further below, after an analysis of the biometric data which are processed in the context of the Turbine project.

2. Legal Analysis

2.1 Biometric data

13. The EDPS has repeatedly underlined that the introduction and processing of biometric data needs to be supported by particularly consistent and strong safeguards. Biometric data, due to their specific nature, present special risks in their implementation which have to be mitigated. These specific characteristics attached to biometric data also explain the interest of the EDPS in the Turbine project and the goals it aims to achieve.

14. The EDPS notes that the legal aspects relating to the use of biometrics have been taken very seriously by the project partners.

15. Indeed, the legal concerns and requirements in relation to the processing of biometric data have been considered since the start of the project. These legal concerns are formulated in various documents, in particular in the Working document on biometrics of the Article 29 Data Protection Working Party[3], as well as in opinions, including those of the EDPS relating to large scale biometric deployment in the EU.[4]

16. The EDPS received a detailed document with legal requirements, intertwined with functional and technical requirements, which was prepared during the first months of the project and was submitted to the project's Advisory Board for further input and discussion[5]. The EDPS believes this shows the commitment of the project partners to implement privacy by design in the lifecycle of the project at an early stage.

2.1.1 Processing of Biometric data

17. Biometric data are the main data processed in the Turbine project. Therefore, it is essential to determine their status.

18. According to Article 29 Working Party[6], biometric data may be defined as “biological properties, physiological characteristics, living traits or repeatable actions where those features and/or actions are both unique to that individual and measurable, even if the patterns used in practice to technically measure them involve a certain degree of probability. Typical examples of such biometric data are provided by fingerprints, retinal patterns, facial structure, voices, but also hand geometry, vein patterns or even some deeply ingrained skill or other behavioural characteristic (such as handwritten signature, keystrokes, particular way to walk or to speak, etc...)”.

19. As the Article 29 Working Party has pointed out: “A particularity of biometric data is that they can be considered both as *content of the information* about a particular individual (Titius has these fingerprints) as well as an element to establish a link between one piece of information and the individual (this object has been touched by someone with these fingerprints and these fingerprints correspond to Titius; therefore this object has been touched by Titius). As such, they can work as "identifiers". Indeed, because of their unique link to a specific individual, biometric data may be used to *identify* the individual”.

20. In the case of the Turbine project, the proposed biometric system uses a method which “pseudonymises” biometric data (fingerprints), replacing them with encrypted irreversible 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 these biometric identities, the raw biometric data retrieval from them is considered not possible, a biometric identity cannot be considered as content of information characterising a person in the sense mentioned

[3] Article 29 Data Protection Working Party, *Working Document on Biometrics*, WP 80, 1 August 2003.

[4] Such as EDPS Opinion of 19 October 2005 on three Proposals regarding the Second Generation Schengen Information System (SIS II) and EDPS Opinion of 23 March 2005 on the Proposal for a Regulation of the European Parliament and of the Council concerning the Visa Information System (VIS) and the exchange of data between Member States on short stay-visas.

[5] See Turbine, deliverable D.1.1.1.

[6] Opinion Nº 4/2007 on the concept of personal data, WP 136, p. 8.

above. Therefore, the use of a biometric identity, instead of the raw biometric fingerprint, enhances the protection of the latter, since it is considered impossible, in technical terms, to extract the fingerprint information directly from the biometric identity as proposed by Turbine. However, due to the fact that the exclusive connection of the biometric identity with a specific person still exists (as only the capture of 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) 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.[7]

21. As repeatedly mentioned in opinions dealing with biometric data, the EDPS also considers that the processing of some biometric data other than the simple storage of photographs alone presents specific risks to the rights and freedoms of data subjects, which subjects such processing operations to prior checking (on the basis of Article 27 (1) of Regulation 45/2001. This view is mainly based on the matching process which presents specific risks and on the nature of biometric data due to some inherent characteristics of this type of data. For example, biometric data changes irrevocably the relation between body and identity, because they make the characteristics of the human body 'machine-readable' and subject to further use. In addition to the highly specific nature of the data, other risks like the possibilities of inter-linkage and the state of play of technical tools may produce unexpected and/or undesirable results for the data subjects. Such processing of biometric data will therefore require specific measures which are analysed below.

2.1.2 Turbine's Features

22. In day to day life, individual's identity and personal data can be compromised. Therefore, it is important to protect them. The same applies to biometric data. However, given that individuals have a limited number of irises and fingers, identity theft of such data compromises corresponding biometric references and renders them as unusable for future use. Indeed, biometric data are closely connected to individuals and by their intangibility, they would be very vulnerable if they were compromised. It is therefore important to ensure the quality of the data processed and their security.

23. The Turbine project promotes two specific features of the biometric data processed and transformed into a biometric key.

Irreversibility of the key

24. In the Turbine project, the fingerprint carrying the identity and access to the personal information of an individual is transformed into a bit-string key which is considered

[7] See reasoning in the Decision of the Hellenic Data Protection Authority N°31/2010.

not invertible[8], i.e. the bit-string is conceived as disconnected from the original fingerprint. This should allow an individual to have several identities or pseudo-identities to which can be associated different personal information: health, financial, legal, etc. Therefore, the use of non invertible key in order to produce renewable templates seems to make the acquisition (from this key) of original biometric reference data impossible.

25. This impossibility of reversibility should better protect the biometric reference data which will no longer be compromised as it is inherently linked with the individual. This feature of irreversibility is welcomed from a data protection and security point of view, in the respect of the data protection principles expressed in Regulation 45/2001. For instance, Article 4.1.b of the said Regulation states that personal data must be collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes. By making the biometric representations irreversible, the system shall prevent the use of biometric data for any other purpose than the one originally intended. It also ensures that the biometric data themselves are not kept for longer than necessary, as they are replaced by the bit-string key.

26. Article 4.1.c also states that personal data must be adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed. Given that the bit string of data replaces the biometric reference data, it implies that only necessary personal data are processed. This system avoids further processing of additional data, which is contained in the biometric reference.

27. From a security point of view (as developed under articles 21 and 22 of Regulation 45/2001), the irreversibility of the key means that there is a greater security attached to the original biometric data as they will not be connected to the key. This security aspect is further strengthened by the aspect of revocability of the key.

Revocability of the key

28. The Turbine project described a procedure whereby the pseudo-identities can be revoked. With such a solution, the data subject shall have alternative means for authentication for the services when the pseudo-identities need to be revoked.

29. The position of the Turbine project is that the risk of compromised biometric references can be mitigated for certain types of attacks by providing methods to allow renewable templates. If various different templates can be extracted from the same biometric reference data, the template can be renewed if it is itself subject to identity theft and hence the compromised template can be revoked.

30. A biometric characteristic cannot be revised. Indeed, individuals only have certain fingers and eyes and these biometric data cannot be "renewed". Therefore the danger is that a biometric data which is compromised would be compromised forever. On the basis of these dangers, a revocable template of those biometric data presents various advantages.

[8] In the project, irreversibility refers to the difficulty to derive more information from the protected reference than a verification outcome (other information could for example be the original biometric data or medical information).

31. By using a revocable key, the biometric representation of a fingerprint from which the original biometric cannot be recovered (irreversibility) can be cancelled and reissued.

32. By revoking a compromised template, the system ensures that no further use of the template can be made which would be incompatible with the original purpose (Article 4.1.b of Regulation 45/2001), as the system would no longer recognise this template as a valid.

33. Moreover, the revocability of the template ensures that the accuracy of the data is preserved (Article 4.1.d of Regulation 45/2001). If the data is no longer accurate (compromised, etc), the possibility to revoke and renew the template based on biometric data allows the data to be kept up to date.

2.1.3 Best Practices for research on biometric data

34. According to the information received from the Turbine consortium, legal aspects of Identity Management (Idm) and legal aspects of the use of biometric data were analysed and a set of ten 'Best Practices' for the use of biometric data in identity management schemes were researched and developed[9]. This deliverable on proposed 'Best Practices' was also sent to the EDPS. It is based on opinions of the Data Protection Authorities (DPAs), the EDPS and the Article 29 Data Protection Working Party on one hand, and the new techniques researched, tested and implemented in Turbine on the other. The proposed guidelines were also submitted and discussed with the Advisory Board of the consortium. The EDPS believes these documents show the commitment of the project's consortium to base its research on a sound legal basis.

The best practices identified by the Turbine project are the following:

- Biometric data shall in principle only be used for verification
- User control over biometric data by default
- Multiple identities and pseudonimity
- Revocability of biometric identities and re-issuance
- Credential and/or identity check
- Deletion of the samples and of the original templates
- The use of privacy-enhancing technologies
- Transparency and additional information for the data subjects
- Specification of fall back procedures and of the procedure to appeal a comparison decision
- On the organisation (especially enrolment phase), the security and the certification of biometric IdM system.

35. In October the EDPS proposed that a list of common basic requirements should be drawn up, taking into account the specific characteristics of biometric data. It should be possible to apply the list to any system of any kind which uses biometrics. The common requirements are:

[9] See Turbine Deliverable 1.4.3. ('Turbine Best Practices').

-Targeted impact assessment: **t**his requirement is becoming more relevant in the light of the recent developments as regards policies on Privacy Impact Assessment, outlined by both the Article 29 and the EDPS.

- Emphasis on the enrolment process: enrolment is a critical step in the overall process of biometric identification. All measures must be taken to ensure that the enrolment phase allows for the majority of individuals to enrol. Moreover, the enrolment should also take into account the level of False Rejection Rate or False Acceptance Rate. Furthermore, fallback procedures to cover the impossibility of enrolment should be readily available.

- Fallback procedure: readily available fallback procedures shall be implemented in order to respect the dignity of persons who could have been wrongly identified and to avoid transferring onto them the burden of the system imperfections.

- Highlight the level of accuracy: in relation to the fallback procedures, the level of accuracy of the system and especially its false acceptance and rejection rates have to be defined according to the precision of the system and monitored constantly in relation to the population using the system. The investment which needs to be made in the fallback procedures will be defined by the level of those rates.

36. The EDPS agrees that developing the best practices listed above will help to implement appropriate measures for any biometric Identity Management System conducted in compliance with the EU regulatory framework. Such a check list could indeed allow development of more privacy friendly systems, if they are taken into account from the start of projects. Following discussions with the project partners, the EDPS understands that the project, although not mentioning *stricto sensu* the level of accuracy among its list of best practices, has taken into account this aspect in the research, by setting precise accuracy goals at the beginning of the project. Furthermore, through the research, this level of accuracy has been tested, verified and even improved as to allow that for the use of a biometric system in an operational environment, such precise levels of accuracy will be adopted.

37. However, the EDPS notes that the list of best practices developed by the Turbine project does not seem to insist specifically on the setting of the precise level of accuracy expected from a biometric system. The EDPS considers this to be of great importance. Therefore, such a level of accuracy should be established early in the system and reviewed on a regular basis. It should therefore not only be applied but it should also be an integral part of the best practices.

2.1.4 The use of proprietary and publicly available biometric databases

38. In order to test and evaluate the algorithms developed by the project, the Turbine partners conducted performance tests. For testing and evaluation purposes, the Turbine partners decided at the start of the project (in the Description of Work) to run the tests on proprietary database and publicly available biometric fingerprint databases.

Proprietary databases

39. As regards the proprietary databases, the EDPS understands that some of the project partners made use of their own proprietary databases[10] as well as a Norwegian proprietary database.

40. The project consortium demonstrated that they ensured that these proprietary biometric databases were in compliance with the national data protection legislations of the countries where these activities take place and where these partners are established.

41. For instance, the following conditions were established for the running of the Norwegian database:

    - Volunteers were informed orally and in writing of the fact that biometric samples ('raw data') were collected for storage in a database for use for research purposes.
    - If the volunteers agreed, they *consented in writing*, providing fingerprint images for teaching, research and testing purposes. The written consent forms are kept by the Norwegian University (partner of the project), which is the controller.
    - The data subjects were also given the right to object at all times.
    - The DPA in Norway was informed regarding data collection ('Meldeskjema') in January 2008 before the start of the project and their regulations followed.
    - Organisational and technical security measures were taken to secure and protect the biometric data. For instance, the data are stored in computers with username/password, and they are located in rooms with locks. In addition, the computers are not connected to the Internet or any other network.
    - The data of this database are kept by Gjøvik University College (GUC) only and access is restricted to authorised researchers of GUC with a need to use the data. The tests were conducted in Norway.
    - The data is not transmitted to any third parties or project partners.

42. In the light of the different measures implemented in the context of proprietary databases, the EDPS is satisfied that Turbine partners have implemented data protection requirements in the light of the national legislation on data protection in force in the Member States where they used the aforementioned databases.

Publicly available databases

43. The tests made by some of the partners were also based on publicly available databases of biometrics. It was described that one of them developed in Italy was used by different project partners.

44. The EDPS analysed the use for solely testing and research purposes of *publicly available biometric databases* obtained from a third party.

[10] It was further stated that they are general research databases owned by the respective companies and kept in respectively France and Sweden. In Sweden, the data representative of the company, whose name is communicated to the Swedish DPA, ensures and overviews the lawful and correct processing of the biometric data. In France, discussions took place with the CNIL in relation with the conditions for the use of biometric databases for research purposes with a view to obtain authorization for all these proprietary databases in accordance with French law. A decision was adopted by the CNIL in July 2010 ("Délibération 2010-336").

45. As explained above, the EDPS considers that the presence of some biometric data, other than photographs alone, and the use of a matching process presents specific risks to the rights and freedoms of data subjects.

46. Therefore, based on the above mentioned reasoning, the biometrics data should be considered as personal data, as they may be used to identify individuals and related national legislation shall be applied. For some national data protection authorities as for the EDPS[11], such databases of biometrics are subject to a notification procedure.

47. For instance, it seems to the EDPS that in Italy, various processing of biometric data must be notified to the Italian Data Protection Authority (*Garante*). In addition, the processing and collection of biometric data in view of building a biometric database is a processing operation likely to present specific risks to the right and freedoms of data subjects by virtue of their nature (biometric data). In the case of the project, it would therefore seem necessary to verify whether the biometric data provided to the consortium have been collected in compliance with the national regulatory framework and that the relevant Data Protection Authority has issued an opinion/authorisation on the legality of the database.

48. From the exchange of information between the EDPS and the project consortium, a distinction has been made by the project between the country in which the publicly available database has been set up by a data controller and the countries in which the data from the database have been used by the project partners.

49. The project consortium stated that it conducted the verification of the legality of the processing operations in the countries where this database was further used by the Turbine partners by submitting its processing operations to the National Data Protection Authorities. However, it has not been possible for the EDPS to establish clearly whether such verification has been conducted by the consortium with regards to the publicly available database based in Italy. In such a case, the consortium should request from the provider of the data, the insurance that the data were collected in respect of the national data protection legislation implementing the data protection directive. Therefore, the EDPS is not in a position to assess whether the consortium has received sufficient guarantees that this database is legally compliant with the national law of the country in which the controller is established.

2.2. Secure access control protocol

50. According to the information provided, the secure access control protocol proposed in Turbine aims at extending the properties of match-on-card, which provide both high accuracy and strong privacy guarantees, to a solution that supports identification procedure.

51. One question which must be dealt with is to know whether the local storage of the biometric data in a secured hardware (i.e. terminal) without the need for a token, and its processing meets the security requirements, and the privacy and data protection requirements for the use of biometric data. This should require a contextual analysis of the situation itself and be based on an analysis by the respective national data protection authority.

[11] The EDPS requires from the European institutions and bodies notification for prior-checking of such biometric databases.

52. In principle, the EDPS favours the use of "one to one" search mode whereby the identification unit would compare the biometric data of the individual with a unique template (associated to the identity). Such a search mode system provides more accurate results.

53. The EDPS usually favour systems that store the biometric templates in chips rather than in central databases unless it is required according to specific conditions. Storage in chips is obviously more privacy friendly insofar as the template is stored on a medium (e.g. badge with chip) which is in the possession of the respective data subject. Thus, the data subject him/herself has direct control and responsibility for his/her template. No one else has access nor is in possession of his/her template. An additional problem with the storage in central databases is that it triggers the risk of so-called "phishing expeditions", facilitating access to the database for purposes different from those for which the database had been conceived. A decentralised system solves this risk without compromising the security level in most cases.

54. Indeed, the EDPS considers that security measures should not only be implemented against external threats but also against actions stemming from users themselves especially in the case of decentralised system. Turbine partners underlined that the security analysis undertaken by the project includes insider attackers, including registered users. Furthermore, the project solutions were designed to be further embedded into a system architecture with all the classical, technical and organisational security measures, including measures against attacks from inside users. The EDPS welcomes such an approach in order to preserve the integrity of the data.

2.3 Demonstrators

55. The EDPS analysed the way the Turbine project implemented the research in real life scenarios. As mentioned in the documents provided, two demonstrators have been developed; one in Thessaloniki airport (Greece) involving two scenarios, and another in a mock up pharmacist in Germany.

56. The two demonstrators aim to demonstrate the technology developed in Turbine. The EDPS is pleased to note that, from the start of the development of the demonstrators, the Turbine partners have established contacts with the relevant national Data Protection Authorities and submitted the relevant documents. The EDPS also facilitated contacts with the relevant DPAs, as part of his possible actions in respect of his policy paper.

2.3.1 Greek demonstrator:

57. The Greek demonstrator relates to the installation of a pilot biometric access control system in critical infrastructures of the International Airport “Macedonia” of Thessaloniki. The installation performed within the framework of Turbine was carried out by the data controller (a general aviation applications company) in cooperation with other European partners and is financed by the European Union. The documents provided to the EDPS described the procedures and measures implemented in the demonstrator.

58. Turbine also described in detail to the EDPS the conditions under which the access control adopting Turbine technology was implemented at Thessaloniki airport.

Mainly, the access control is only installed for controlling access to places demanding special security measures. It also involves only a limited number of volunteers.

59. In compliance with the national law, a notification of the system was sent to the Greek Data Protection Authority who issued an opinion. The Hellenic DPA decided that the installation of the biometric system used exclusively for scientific research purposes did not contravene the provisions of Hellenic law on Data Protection and granted an authorisation to process for the demonstrator. The Hellenic DPA did however require some terms to be met; the demonstrator took place as notified except that the collection and keeping of original biometric samples (raw) for additional performance testing purposes was not allowed.

60. The EDPS welcomed that a secure and privacy friendly enrolment procedure was developed to the extent that the persons assisting in and realising the enrolment procedure have been informed, trained and supported with the aim of attaining a qualitative and secure capture of the biometric data for further reference purposes.

61. The EDPS also notes that presentations were prepared and training took place during which the importance of data protection in the enrolment phase was stressed. Further training was provided by Turbine partner experts during the actual phase of enrolment. Furthermore, the consent and information forms were provided and discussed with possible volunteers several weeks before the start of the enrolment.

62. Such procedures contribute to the general implementation of data protection principles in the life cycle of the project. By ensuring the provision of correct information to the individuals and the accuracy of the data which are processed in the enrolment phase, the project ensures a high level of data quality.

63. Moreover, when an enrolment of biometrics takes place, the EDPS also analyses the way fallback procedures are implemented. In the Greek demonstrator, the fall back procedure was ensured by the fact that the existing access control measures were not replaced by Turbine solution but were working at the same time, allowing participants to fall back, in case of failure of the Turbine demonstrator, to these existing access controls.

2.3.2 German Demonstrator (GADM)

64. As to the German demonstrator, it was clarified that according to German law[12], the GADM did not need to be registered or notified, provided a Data Protection Official is appointed by the controller, which was the case. Therefore, the Data Protection Official at Sagem-Orga has been duly informed by the controller and keeps the information as set out by the law. For the GADM demonstrator, an information note has been submitted to the Data Protection Official at Sagem-Orga to comply with the registration requirements set out in article 4e of the German Federal Data Protection Act. As required, the Data Protection Official at Sagem-Orga was informed of the elements as required under German legislation, including the name of the controller, the name of the persons responsible for the data processing, the persons authorised to access the data and the purposes. A consent form was prepared for volunteers giving a clear overview of what data will be processed for what

[12] Article 4d (2) Federal Data Protection Act and Article 4f – see also Art. 4 d (3) which refers to consent as basis for non obligatory registration.

purposes during the demonstrator. The volunteers were also duly informed of their rights.

65. In this demonstrator, it was foreseen that the administrators of the enrolment would be equally informed of the need for secure and privacy friendly (transparent) enrolment and trained. It was also underlined that the administrators of the GADM enrolment are experts in biometric data processing and are aware of the need for good qualitative reference data.

2.3.3 Summarizing

66. The EDPS concludes that in the conduct of the two demonstrators, the project consortium implemented the principle of privacy by design in a way that facilitates the assessment conducted by the relevant data protection authorities.

3. Conclusion

67. The EDPS welcomes the project as it demonstrates that implementing "privacy by design" as a key principle in research is an effective mean to ensure "privacy compliant" solutions. "Privacy by design" extends not only to the design and technical solutions of ICT systems, but it comprises the various steps in the set up of the project and its organisational practices. This latter aspect can be achieved by ensuring legal compliance, implementing the required data protection principles, and by implementing procedures and training developed to ensure correct information and training of all the parties involved. Moreover, the demonstrators provide the possibility to test the advantages of the implementation of the principle in real case scenarios.

68. The development of best practices in the context of the use of biometric data should be encouraged in order to ensure future research is based on a sound privacy approach.

69. The implementation of the two features, irreversibility and revocability of biometric identification, contributes significantly to this compliance by providing acceptable privacy compliant solutions.

70. The EDPS recommends taking the following observations into account:

- The development of a list of best practices should also take into account that a precise level of accuracy should be established and reviewed on a regular basis.

- Moreover, although conducting the research under strict legal conditions, the project consortium should require evidences from its providers of biometric data that they fully comply with their national data protection legislation.

Brussels, 1 February 2011

(**signed**)

Giovanni BUTTARELLI
Assistant European Data Protection Supervisor