PROTECT (Pervasive and UseR Focused BiomeTrics BordEr ProjeCT)

Dumortier, Franck

Publication date:
2018

Document Version
Publisher's PDF, also known as Version of record

Pervasive and UseR Focused BiomeTrics BordEr ProjeCT

(PROTECT)

H2020 – 700259

D2.5 Societal impact report (version 1)

Authors: Franck Dumortier - UNAMUR

Deliverable nature:	R
Dissemination level: (Confidentiality)	Public (PU)
Version:	1.1
Date:	16/02/2018
Keywords:	Privacy, data protection, border control legislation, ethics, CPDP, GDPR

Executive summary

This document is deliverable D2.5 (version 1) – "Societal impact report" of Task T2.5 within WP2 – "Privacy" of the PROTECT project. The aim of D2.5 is to identify and address the ethical and legal implications of the technical solutions being developed in the context of the PROTECT project by summarizing discussions between the project partners and exchanges with the Ethical and Legal Advisory Group (ELAG) as well as with other external experts.

The overall PROTECT research project addresses both public security missions (border control) and societal concerns (fundamental rights and social values). The development of a new framework for border control (from physical to increasingly digital borders) and related new methods for the management and control of population flows at borders (e.g. biometric passport, ABC gates, constitution of large scale IT systems managing visa applications, contactless biometric border control) instantiate the tension between two constitutive obligations linking modern states and its citizens, namely between freedom and security. The main ethical challenge in this matter is to find the proportional balance between the legitimate interests at stake in the exercise of border control missions and the preservation of fundamental rights, such as the rights to privacy and data protection of travellers, including both European and third-country nationals. Such concerns appear at the core of PROTECT proposal.

In order to ensure that ethical and legal aspects are thoroughly investigated and addressed within the PROTECT project, a specific work package – "WP2 Privacy" – is dedicated to explore the privacy issues raised by the PROTECT system, translate those issues into operational requirements usable for the system designers and assess the privacy compliance of the technological constructs. In this WP2:

- Ethical and legal experts at UNAMUR study the legal frameworks, conduct acceptability studies of different biometric solutions and examine ethical and privacy issues related to the PROTECT system;
- An Ethical & Legal Advisory Group (ELAG) consisting of three independent experts with extensive experience in privacy or biometrics and identity management issues independently monitor and review the activities and outputs of the project.

This first version of D2.5 – "Societal impact report" – contains a summary of ethical and legal discussions held during 3 different events:

1. A meeting "on the impact of privacy regulations on system architecture & technical solutions" which was organized on 4th July 2017 at the University of Reading. The objective of this meeting was for UNAMUR to present to the other partners the implications of the General Data Protection Regulation (GDPR) on the processing of biometric data in the context of border control;
2. A first ELAG meeting which took place at University of Reading on July 5th 2017. The objective of that meeting was to discuss the ethical and legal implications of a potential scenario implementing the PROTECT solution taking into account existing and forthcoming EU regulations in the field of border control and data protection;
3. A PROTECT panel at the 11th International conference on computers, privacy and data protection (CPDP2018) organized by UNAMUR and which took place on January 25th in Brussels. This panel was entitled "privacy and data protection issues related to the use of contactless multimodal biometrics at border-crossings" and was the opportunity to share some views with important actors such as the European Data Protection Supervisor (EDPS) and the JHA Counsellor at the Permanent Representation of Finland to the EU.

Please note that this deliverable is a first version of D2.5. A second version D2.5 – Societal impact report is due at M34 and will integrate the next discussions and exchanges on ethical and legal issues with the ELAG and other external experts.

Document Information

Project Number	H2020 - 700259	**Acronym**	PROTECT
Full Title	Pervasive and UseR Focused BiomeTrics BordEr ProjeCT		
Project URL	http://www.projectprotect.eu/		
Document URL			
EU Project Officer	Agnieszka Marciniak		

Date of Delivery	**Contractual**	M18	**Actual**	M18

Authors (names and affiliations)	Franck Dumortier - UNAMUR

Reviewers (names and affiliations)	Franck Dumortier UNAMUR Cathy Moss UREAD Juergen Bonfert VERIDOS

Version Log			
Issue Date	**Rev. No.**	**Author**	**Change**
16/02/18	1.0	Franck Dumortier	1st version
22/02/18	1.1	Cathy Moss	Language review
27/02/18	1.2	Juergen Bonfert	Security review

Table of Contents

List of figures

Abbreviations

CPDP2018	Computer, Privacy and Data Protection Conference 2018
EDPS	European Data Protection Supervisor
EEA	European Economic Area
EES	Entry-exit system
ETIAS	The European Travel Information and Authorisation System
EU	European Union
GDPR	General Data Protection Regulation
IBM	Integrated Border Management
MS	Member State
SBC	Schengen Border Code
SIS	Schengen Information System
TCN	Third-Country National
UNAMUR	University of Namur
VIS	Visa Information System
WP29	Article 29 Working Party

Definitions

Article 29 Working Party: The Article 29 Working Party is composed of representatives from all EU Data Protection Authorities, the EDPS and the European Commission. It was set up under the Directive 95/46/EC. It has advisory status and acts independently.

Automated Border Control system: means a system which allows for an automated border passage, and which is composed of a self-service system and an e-gate.

Biometric data: Article 4(14) of the GDPR defines "biometric data" *as personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data.*

E-gate: means an infrastructure operated by electronic means where the effective crossing of an external border takes place

Ethical and Legal Advisory Group: An Ethical and Legal Advisory Group (ELAG) has been appointed in the PROTECT project. The ELAG consists of three independent experts in and legal issues with extensive experience in privacy or biometrics and identity management issues. The presence of an ethical board of independent experts is meant to exert a sort of permanent call to also consider and care about the ethical and social acceptability of the PROTECT conduct and outputs.

European Travel Information and Authorisation System (ETIAS): The system will apply to visa-exempt third country nationals, as well as those who are exempt from the airport transit visa requirement. They will need to obtain a travel authorisation before their trip, via an online application. The information submitted in each application will be automatically processed against other EU databases to determine whether there are grounds to refuse a travel authorisation. When no hits or elements requiring further analysis are identified, the travel authorisation will be issued automatically within a short time. If there is a hit or an element requiring analysis, the application will be handled manually by the competent authorities.

Facial image: means digital images of the face with sufficient image resolution and quality to be used in automated biometric matching

EURODAC system: The EURODAC system enables the comparison of fingerprints of asylum applicants and illegal immigrants. The Members States of the system are the 28 EU members, Iceland, Norway, Liechtenstein and Switzerland. The objective of EURODAC in the asylum process is to facilitate the application of the Dublin III Regulation. This Regulation provides a mechanism for determining which country is responsible for examining applications for international protection lodged in one of the member states.

European Data Protection Supervisor: The European Data Protection Supervisor (EDPS) is an independent institution of the EU, responsible under Article 41(2) of Regulation 45/2001 'With respect to the processing of personal data… for ensuring that the fundamental rights and freedoms of natural persons, and in particular their right to privacy, are respected by the Community institutions and bodies', and '…for advising Community institutions and bodies and data subjects on all matters concerning the processing of personal data'. Under Article 28(2) of Regulation 45/2001, the Commission is required, 'when adopting a legislative Proposal relating to the protection of individuals' rights and freedoms with regard to the processing of personal data...', to consult the EDPS.

Entry-Exit System: the Entry/Exit System (EES) is a system to register entry and exit data and refusal of entry data of third country nationals crossing the external borders of the Member States of the European Union and determining the conditions for access to the EES for law enforcement purposes.

General Data Protection Regulation (GDPR): On 4 May 2016, the official text of the Regulation has been published in the EU Official Journal in all the official languages. The Regulation will enter into force on 24 May 2016. The objective of this new set of rules is to give citizens back control over of their personal data, and to simplify the regulatory environment for business. The data protection reform is a key enabler of the Digital

Single Market which the Commission has prioritised. The reform will allow European citizens and businesses to fully benefit from the digital economy.

Personal data: Article 4(1) of the GDPR defines "personal data" as *any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person*.

Processing: Article 4(14) of the GDPR defines "processing" as *any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction*.

Schengen Area: The Schengen Area is one of the greatest achievements of the EU. It is an area without internal borders, an area within which citizens, many non-EU nationals, business people and tourists can freely circulate without being subjected to border checks. Since 1985, it has gradually grown and encompasses today almost all EU States and a few associated non-EU countries. While having abolished their internal borders, Schengen States have also tightened controls at their common external border on the basis of Schengen rules to ensure the security of those living or travelling in the Schengen Area.

Schengen Border Code: The Schengen Borders Code governs the crossing of the external border, facilitating access for those who have a legitimate interest to enter into the EU. A special Local Border Traffic Regime has also been established to facilitate entry for non-EU border residents who frequently need to cross the EU external border. A common visa policy further facilitates the entry of legal visitors into the EU.

Sensitive personal data: Article 9(1) of the GDPR defines "sensitive personal" data as *personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.*

Schengen Information System: The Schengen Information System (SIS) is a highly efficient large-scale information system that supports external border control and law enforcement cooperation in the Schengen States. The SIS enables competent authorities, such as police and border guards, to enter and consult alerts on certain categories of wanted or missing persons and objects. An SIS alert not only contains information about a particular person or object but also clear instructions on what to do when the person or object has been found. Specialised national SIRENE Bureaux serve as single points of contact for any supplementary information exchange and coordination of activities related to SIS alerts.

Self-service system: means an automated system which performs all or some of the border checks that are applicable to a person

Template: a biometric template is a digital representation of the unique features that have been extracted from a biometric sample.

Visa Information System (VIS): The Visa Information System (VIS) allows Schengen States to exchange visa data. It consists of a central IT system and of a communication infrastructure that links this central system to national systems. VIS connects consulates in non-EU countries and all external border crossing points of Schengen States. It processes data and decisions relating to applications for short-stay visas to visit, or to transit through, the Schengen Area. The system can perform biometric matching, primarily of fingerprints, for identification and verification purposes.

1 Introduction

The PROTECT concept has been designed to develop a multimodal biometric solution for identity confirmation "on the move" of travellers, with the aim to facilitate the Schengen Area external cross-border movements. The system should, therefore, process various "emerging" biometric modalities which could be processed in a contactless way. For the purposes of multimodal biometric ID verification, project partners proposed to design and develop a biometric corridor, which would incorporate a number of biometric sensors. The initial plan was to include such biometrics as: face recognition, iris recognition, vein pattern recognition, speaker recognition as well as anthropometric recognition. When operational, the beneficiaries of the multimodal biometric system being developed within the PROTECT project should be persons enjoying the Union right of free movement as well as third country nationals.

A critical issue with biometrics arises with the collection of biometric data, which could be construed as being in conflict with fundamental human rights such as the right of liberty and the rights to privacy and data protection. Since greater use of personal data impacts upon human rights, there needs to be an honest and assertive study of what the risks are to privacy and how these risks are mitigated and balanced by improving the travel experience and security of the citizen. Therefore, critical evaluations of the biometric person identification system from a privacy point of view, investigations of social acceptability, and contributions to European legal frameworks are integral parts of the PROTECT project.

In order to ensure that ethical and legal aspects are thoroughly investigated and addressed within the PROTECT project, a specific work package – "WP2 Privacy" – is dedicated to explore the privacy issues raised by the PROTECT system, translate those issues into operational requirements usable for the system designers and assess the privacy compliance of the technological constructs. In this WP2:

- Ethical and legal experts at UNAMUR study the legal frameworks, conduct acceptability studies of different biometric solutions and examine ethical and privacy issues related to the PROTECT system;
- An Ethical & Legal Advisory Group (ELAG), consisting of three independent experts with extensive experience in privacy or biometrics and identity management issues, independently monitor and review the activities and outputs of the project.

1.1 Purpose of the document

This document is deliverable D2.5 (version 1) – "Societal impact report" of Task T2.5 within WP2 – "Privacy" of the PROTECT project. The aim of D2.5 is to identify and address the ethical and legal implications of the technical solutions being developed in the context of the PROTECT project by summarizing discussions between the project partners and exchanges with the Ethical and Legal Advisory Group (ELAG) as well as with other external experts.

1.2 Document scope

The document consists of an introduction and three main sections:

- **Section 2** provides for an overview of the presentation given by UNAMUR at the meeting "on the impact of privacy regulations on system architecture & technical solutions" which was organized on 4th July 2017 at the University of Reading. The purpose of this meeting was to present to the PROTECT partners the implications of the General Data Protection Regulation (GDPR) on the processing of biometric data in the context of border control;
- **Section 3** contains a summary of the discussions held during the first ELAG meeting which took place at the University of Reading on July 5th 2017. The objective of that meeting was to discuss the ethical and legal implications of a potential scenario implementing the PROTECT solution taking into account existing and forthcoming EU regulations in the field of border control and data protection;

- **Section 4** contains a summary of the discussions held at the PROTECT panel at the 11th International conference on computers, privacy and data protection (CPDP2018) organized by UNAMUR and which took place on January 25th in Brussels. This panel was entitled “privacy and data protection issues related to the use of contactless multimodal biometrics at border-crossings” and was the opportunity to share some views with important actors such as the European Data Protection Supervisor (EDPS) and the JHA Counsellor at the Permanent Representation of Finland to the EU.

2 Meeting on the impact of privacy regulations on system architecture & technical solutions

2.1 Introduction

This meeting “on the impact of privacy regulations on system architecture & technical solutions” was organized on 4th July 2017 at the University of Reading in the context of Task 5.6. This task explicitly examines the design and implementation of privacy enhancing technology. In order to complete the first stage of this task, this meeting was organized in order to present to the consortium members the General Data Protection Regulation (GDPR) and impacts on sensors, data processing and system architecture. On 4 May 2016, the official text of the GDPR has been published in the EU Official Journal and shall apply from 25 May 2018.

The points covered by Franck Dumortier (UNAMUR) in this introduction to the GDPR to the consortium members were:

- What aspects are covered by the GDPR?
- How does it relate to national law?
- How does it affect European citizens compared to registered traveller programs?
- How much can be covered by consent forms?
- Which biometric modalities have to be protected?

2.2 Presentation

It was first recalled that the GDPR is a Regulation. A "regulation" is a binding legislative act. It must be applied in its entirety across the EU and even beyond.

Indeed, according to the GDPR, *“1. This Regulation applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not. 2. This Regulation applies to the processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union, where the processing activities are related to: (a) the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union; or (b) the monitoring of their behaviour as far as their behaviour takes place within the Union. 3. This Regulation applies to the processing of personal data by a controller not established in the Union, but in a place where Member State law applies by virtue of public international law.”*

In principle, the objective is complete harmonization but the GDPR leaves scope for divergences between MS in a number of areas including in the field of conditions for processing of biometric data.

The GDPR applies when there is: “processing” of “personal data” wholly or partly by automatic means or (organized manually in a filing system). However, the GDPR does not apply to processing of personal data by a natural person in the course of a purely personal or household activity. This being said, the processing of personal data in the context of border-crossing cannot be considered as a purely personal or household activity: hence the GDPR applies.

Important definitions of the GDPR were then recalled:

- Personal data is defined in art. 4 of the GDPR as "any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person". This definition takes into account evolutions of technology and must be interpreted in a very broad way. Indeed, Recital 26 of the GDPR states that: "To determine whether a natural person is identifiable, account should be taken of all the means reasonably likely to be used, such as singling out, either by the controller or by another person to identify the natural person directly or indirectly. To ascertain whether means are reasonably likely to be used to identify the natural person, account should be taken of all objective factors, such as the costs of and the amount of time required for identification, taking into consideration the available technology at the time of the processing and technological developments". Recital 30 also confirm this broad interpretation by stating that: "Natural persons may be associated with online identifiers provided by their devices, applications, tools and protocols, such as internet protocol addresses, cookie identifiers or other identifiers such as radio frequency identification tags. This may leave traces which, in particular when combined with unique identifiers and other information received by the servers, may be used to create profiles of the natural persons and identify them".
- Article 4 (14) of the GDPR defines "biometric data" as "personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data". Opinion 4/2007 (WP136) of the Article 29 Working Party clarifies that "even if the patterns used in practice to technically measure them involve a certain degree of probability", "templates" are considered as being "biometric data".
- "Processing" is defined in art. 4(2) of the GDPR as "any operation or set of operations which is performed upon personal data, whether or not by automatic means such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by means of transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction of personal data". Even anonymization or erasure of personal data must be considered as a "processing".
- "Controller" is defined in art. 4(7) of the GDPR as "the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law". In the frame of the project, we should distinguish contexts of "project demonstrations" (controller = the PROTECT consortium/members) & "real life" (controller = a company or authority determined by Union or MS law).
- "Processor" is defined in art.4(8) of the GDPR: "a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller. Here again, depending on the actual implementation of the system, we should distinguish contexts of "project demonstrations" (processors = the PROTECT members) & "real life" (processor = authority or company determined by the data controller).

Franck Dumortier then discussed the legal basis for processing of biometric data under the GDPR in the border control context. He recalled the principle of Article 9 of the GDPR according to which "processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited". He also reminded Recital 51 of the GDPR according to which

"Such personal data should not be processed, unless processing is allowed in specific cases set out in this Regulation, taking into account that Member States law may lay down specific provisions on data protection in order to adapt the application of the rules of this Regulation for compliance with a legal obligation or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller. In addition to the specific requirements for such processing, the general principles and other rules of this Regulation should apply, in particular as regards the conditions for lawful processing. Derogations from the general prohibition for processing such special categories of personal data should be explicitly provided, *inter alia*, where the data subject gives his or her explicit consent or in respect of specific needs in particular where the processing is carried out in the course of legitimate activities by certain associations or foundations the purpose of which is to permit the exercise of fundamental freedoms".

By consequence, exceptions to the prohibition of processing biometric data in the context of the PROTECT project are only possible when:

- the data subject has given explicit consent to the processing of those personal data for one or more specified purposes, except where Union or Member State law provide that the prohibition may not be lifted by the data subject;
- processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject;
- processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes.

It was also recalled that Member States may maintain or introduce further conditions, including limitations, with regard to the processing of biometric data. This means that even if based on consent, we have to take into account mandatory requirements of Union or Member State law in the context of PROTECT.

The first legal basis which was analysed for processing biometrics in the context of PROTECT was consent of the travellers. Consent" is defined in art. 4(11) of the GDP as "any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her". Additionally, for biometric data, consent must be "explicit". Furthermore, according to the GDPR, conditions for consent are the following:

"1. Where processing is based on consent, the controller shall be able to demonstrate that the data subject has consented to processing of his or her personal data. 2. If the data subject's consent is given in the context of a written declaration which also concerns other matters, the request for consent shall be presented in a manner which is clearly distinguishable from the other matters, in an intelligible and easily accessible form, using clear and plain language. Any part of such a declaration which constitutes an infringement of this Regulation shall not be binding. 3. The data subject shall have the right to withdraw his or her consent at any time. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal. Prior to giving consent, the data subject shall be informed thereof. It shall be as easy to withdraw as to give consent. 4. When assessing whether consent is freely given, utmost account shall be taken of whether, inter alia, the performance of a contract, including the provision of a service, is conditional on consent to the processing of personal data that is not necessary for the performance of that contract".

When applied to biometrics, the Article Working Party 29 considers renewability and revocability of consent as essential by stating that "Biometric systems should be designed in a way that allows to revoke the identity link, either in order to renew it or to permanently delete it e.g. when the consent is revoked". Franck also stressed that Recital 43 expressly states that: "in order to ensure that consent is freely given, consent should not provide a valid legal ground for the processing of personal data in a specific case where there is a clear imbalance between the data subject and the controller, in particular where the controller is a public authority and it is therefore unlikely that consent was freely given in all the circumstances of that specific situation".

This means that consent of travellers could not be used by public border control authorities to speed up their public interest missions.

This being said, consent would still be a possible legal basis for "commercial" purposes. For example, in a 2005 deliberation, the CNIL (French DPA) authorized the use of fingerprints on a fidelity chipcard for frequent travellers of the airport of Nice. The system was designed for convenience purposes (facilitate access to parking zones, additional services, etc): Important criteria were the 1) the voluntary use, and 2) the storage on an object (no centralized database).

The second legal basis which was analysed for the processing of biometric data in the context of border control was Art. 8(d) of Regulation (EU) 2017/2225 (amending the Schengen Borders Code) which allows MS to legislate on voluntary "National Facilitation Programs" (NFPs). It was recalled that the purpose of such NFPs was only to allow pre-vetted and pre-cleared third country nationals (TCNs) to waive them from the requirement to be subject to an interview on their means of subsistence, purpose of travel and point of departure and destination. This means two important things in the context of PROTECT: 1) this legal basis could not be used for EU/EEA/CH travellers; 2) for TCNs it could only be used to "facilitate" the requirements of interview on their means of subsistence, purpose of travel and point of departure and destination as the purpose of NFPs is not to "speed up border control databases checks". Indeed, SIS, VIS and EES will still have to be checked on the basis of "traditional" biometrics (as legally standardized).

Thirdly, it was mentioned that the processing of additional biometric data in the context of the PROTECT project was of course possible because it is "necessary for scientific purposes". That is why consent forms have been prepared in D2.1 for volunteers willing to participate in our demonstrations.

Finally, after having analysed these legal bases for additional biometric processing in the context of border control, Franck Dumortier applied the core data protection principles to biometrics. These principles are enshrined in article 5 of the GDPR which states that personal data shall be:

- processed lawfully, fairly and in a transparent manner;
- collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes ('purpose limitation');
- adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation');
- accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy');
- kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed ('storage limitation');
- processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality').

When applying these principles to the processing of biometric data, it was recalled that the Article 29 Working Party considers that:

- Biometric data may only be used if adequate, relevant and not excessive. It implies a strict assessment of the necessity and proportionality of the processed data and if the intended purpose could be achieved in a less intrusive way. If the benefit is relatively minor, such as an increase in convenience or a slight cost saving, then the loss of privacy is not appropriate.
- Decentralized storage is preferred to centralized databases. It is advisable that biometric systems are based on the reading of biometric data stored as encrypted templates on media that are held exclusively by the relevant data subjects (e.g. smart cards or similar devices). Their biometric features can be compared with the template(s) stored on the card and/or device by means of standard

comparison procedures that are implemented directly on the card and/or device in question, whereby the creation of a database including biometric information should be, in general and if possible, avoided.

- Biometric data should be stored as biometric templates whenever that is possible. Template should be extracted in a way that is specific to that biometric system and not used by other controllers of similar systems in order to make sure that a person can only be identified in those biometric systems that have a legal basis for this operation.
- The definition of the size (the quantity of information) of the template is a crucial issue. On the one hand, the size of the template should be wide enough to manage security (avoiding overlaps between different biometric data, or identity substitutions). On the other hand, the size of the template should not be too large in order to avoid the risks of biometric data reconstruction.
- The generation of the template should be a one-way process, in that it should not be possible to regenerate the raw biometric data from the template.
- To maintain the reliability of a biometric system and prevent identity fraud, the manufacturer has to implement systems aiming to determine if the biometric data is both genuine and still connected to a natural person. In respect of facial recognition, it may be critical to ensure that the face is a real one and not, for example, a picture tied on an impostor's head.
- In order to prevent that biometric information are stored for longer than is necessary for the purposes for which they were collected or subsequently processed, appropriate automated data erasure mechanisms have to be implemented also in case the retention period may be lawfully extended, assuring the timely deletion of personal data that become unnecessary for the operation of the biometric system.
- The biometric system used and the security measures chosen should limit the mentioned risks and make sure that the re-use of the biometric data in question for further purposes is impossible or at least traceable. Mechanisms based on cryptographic technologies, in order to prevent the unauthorised reading, copying, modification or removal of biometric data should be used. When the biometric data are stored on a device that the data subject physically controls, a specific encryption key for the reader devices should be used as an effective safeguard to protect these data from unauthorised access.

3 First Ethical & Legal Advisory Group meeting in Reading

3.1 Introduction

The Ethical & Legal Advisory Group (ELAG) consists of three independent experts in ethical and legal issues with extensive experience in privacy or biometrics and identity management issues. The presence of an ethical board of independent experts is meant to exert a permanent call to also consider and care about the ethical and social acceptability of the PROTECT conduct and outputs. The 3 experts are:

- **Gloria Gonzalez Fuster** (VUB), who is a research professor at VUB, where she investigates legal issues related to fundamental rights, privacy, personal data protection and security, and lectures on fundamental rights protection in European Union (EU) law in the context of the Master of Laws in International and European Law (PILC).
- **Diana Dimitrova** (FIS Karlsruhe), who was a legal researcher for 3.5 years at the law faculty of the University of Leuven (KUL) in Belgium. Her research focuses mainly on privacy and data protection, especially in the Area of Freedom, Security and Justice. She carried out her research in the framework of the FastPass and eVACUATE projects at KUL. In 2012 she completed a five-month traineeship at the Supervision and Enforcement Unit of the European Data Protection Supervisor (EDPS) in Brussels

and holds an LLM in European Law from the University of Leiden, NL. At FIZ Karlsruhe Diana works for the EU project STARR.

- **Monica Vilasau Solana** (UOC) is Lecturer in the Law and Political Science Department at Universitat Oberta de Catalunya and expert in data protection law.

The 3 experts have been invited to participate to a first ELAG meeting that which took place at University of Reading on July 5th 2017. The objective of that meeting was to discuss the following scenario:

1. A registered traveller would be issued a token in the form of a machine-readable smartphone application containing a unique multimodal biometric template, which is swiped on arrival and departure at the border using a self-service system.
2. The self-service system would read the token and the travel document (and residence card/permit/visa, if applicable). The face (and if applicable fingerprints) of the travel document(s) would be compared to the ones stored in EU and national databases, including the SIS (and EES/VIS if applicable).
3. After having walked through the PROTECT Biometric Capture Area, if all checks in the databases are successful, and if he is biometrically authentified, the traveller is able to pass through the automated gate.

This scenario was presented to the three experts by Franck Dumortier and discussed within the ELAG in the presence of Frank Schmalz (VERIDOS) to confront this technical scenario with legal and societal concerns.

Figure 1 - Frank Schmalz answering ELAG's questions

3.2 Discussion

Franck Dumortier started the ELAG session by recalling that PROTECT is a research project which has to enquire on the potential of implementing contactless multimodal biometrics at external border crossing points. This objective was stated by the European Commission, which expressed it as follows in the H2020 call "BES-6-2015: Border crossing points, topic 2: Exploring new modalities in biometric-based border checks": *"Research is needed in order to explore whether it is possible to use other biometric data (potentially already used in another context and in another domain) than fingerprint, iris or facial picture to store in the e-Passport chip, which would guarantee the same or higher level of security, but would be more accurate and could be retrieved in a more efficient manner than in the case of the conventionally used biometric data types. In addition, practical experiences lead to the assumption that for non-critical travellers (EU, bona-fide etc.) a most fluent non-intrusive control process is desired. Therefore, to increase accuracy, in this case the use of contactless techniques (e.g. face, 3D face, iris) and multi-biometric fusion is likely to be preferred over contact-based technologies".*

When keeping this general objective in mind while taking into account current border control and privacy legislation, consortium partners decided to imagine three different types of scenarios for PROTECT's solutions:

1) A model where the PROTECT scenario is fully compliant with existing and forthcoming EU legislation and standards (model 1);

2) A model where the scenario is partly compliant with Schengen border-crossing legislation, but entirely compliant with data protection requirements set by the GDPR as these are human rights requirements (model 2);

3) A model where the scenario is directed entirely towards technical possibility and border control effectiveness, anticipates future business conditions and is less compliant than models 1 and 2 above and requires substantial work to satisfy legal opinion of its future legality (model 3 to be analysed by UNAMUR in D2.3).

Franck Dumortier then explained that during this first ELAG session, it was decided to discuss a potential fully legally compliant ("model 1") scenario taking into account the following 3 types of legal constraints.

First, several constraints derived from current EU rules on ePassports and residence permits should be taken into account:

1) It is important to note that Article 4 of Regulation EC 2252/2004 stipulates that "No information in machine-readable form shall be included in a passport or travel document unless provided for in this Regulation, or its Annex, or unless it is mentioned in the passport or travel document by the issuing Member State in accordance with its national legislation". To be pragmatic, this means that under current EU law, it is very unlikely that inclusion of additional multimodal biometrics features (being not facial image or fingerprints) developed within the PROTECT project could legally be integrated in ePassports. Consent of travellers does not permit to do so. Furthermore, even if an EU Member State would adopt national legislation regulating such integration, it would be easily challenged for privacy and data protection issues.

2) It is important to note that article 4 of Regulation (EC) No 1030/2002 as amended by Regulation (EC) No 380/2008 provides that "No information in machine-readable form shall be included on the resident permit or on the storage medium of the residence permit referred to in Article 4a, unless provided for in this Regulation, or its Annex or unless it is mentioned in the related travel document by the issuing State in accordance with its national legislation. Member States may also store data for e-services such as e-government and e-business as well as additional provisions relating to the residence permit on a chip referred to in point 16 of the Annex. However, all national data must be logically separated from the biometric data referred to in Article 4a". Point 16 of the annex clarifies that "a RF chip shall be used as a storage medium in accordance with Article 4a. Member States may store data on this chip or incorporate in the residence permit a dual interface or a separate contact chip for national use which shall be placed at the back of the card complying with ISO standards and shall in no way interfere with the RF chip". The possibility and conditions

for national legislation to rely on this legal basis in order to integrate additional multimodal biometrics data on a "second" chip of residence permits in the context of the establishment of a voluntary "national facilitation program" (based on consent of TCNs) will be analysed into D2.3 – Privacy impact of next-generation biometric border control.

3) Under current EU law, it also seems very doubtful that mobile devices such as smartphones could legally be used as carriers of biometrics features as means to replace the materials imposed by the annex of Regulation EC 2252/2004 and Regulation EC 1030/2002: smartphones cannot be considered as "Passports or travel documents" in the meaning of article 1 of said Regulations. Nonetheless, for research purposes, this constraint does not oppose to carefully examining the possibility of deriving a "virtual mobile identity" by combining data already present in ePassports or residence permits with additional multimodal biometric features developed within PROTECT and securely loaded onto a mobile device, such as a phone, a wearable, or a token.

A second important set of constraints derive from the fact that, depending on the case, travellers must be checked against SIS II/ VIS/EES on the basis of "traditional" biometrics which are fingerprints and facial image. Therefore, the scenario that was submitted to the ELAG envisages to combine the use of these "traditional" biometrics with the "additional ones" being developed within PROTECT for the purpose of verification of travellers against the above-mentioned IT databases.

A third set of important legal constraints derive from privacy and data protection regulations which general principles are currently mainly enshrined into the GDPR.

Gloria Gonzalez Fuster had the feeling that lots of scenarios were still discussed within the PROTECT consortium and reminded that checking which of the scenarios are possible according to current legislation is of first importance in the context of European research security projects such as PROTECT. She understood that the scenario that we were discussing would be one of the scenarios that fits better the scientific question but had the strange feeling that PROTECT partners still had different views on the objectives to reach.

Frank Schmalz answered that basically in the PROTECT project, partners are of course discussing a lot of scenarios and course checking which of the scenarios are possible according to current legislation. The one that was presented to the ELAG is one possible scenario which fits better our scientific question while being legally compliant. Frank also reminded that multiple objectives are pursued within the PROTECT project:

- one is to have faster biometrics crossing points by improving performance in the control process by using contactless biometrics;
- the other aspect is to use additional biometrics to improve accuracy and speed, and make the process more convenient for the travellers.

Gloria asked how and when concretely the information of the passport (and the traditional biometrics contained therein) would be "mixed" with the additional ones being developed within the PROTECT project.

Frank Schmalz answered that in a certain way we would have to link the additional biometrics to the person and one manner to do that is by issuing a token. One possibility would be to use information that is stored inside the passport and this would be signed together with the additional biometric templates and then stored on a smartphone. So later, we could read the information from the phone, decrypt it, and use this identifier to link the information to the identity the person. Indeed, during the verification biometric matching itself, it would not make sense to identify a person without knowing which person we are identifying.

Gloria asked if passport information would be stored inside the smartphone in this scenario. Frank Schmalz answered that basically this information could, for example, be a hash of the information that is stored within the passport. It is then not passport information that is stored on the phone but a link to the passport. This would be a suitable solution in Frank Schmalz's opinion.

Diana Dimitrova then asked if during the biometric matching phase against the EU IT databases, the consortium was planning to use both the passport and the smartphone of travellers or only the smartphone

which would contain the passport's information. By asking this question, Diana recalled that the information stored on the passports was officially needed to carry out all of the background checks.

Frank Schmalz answered Diana by saying that in the normative scenario ("model 1") we are discussing, we would need both the passport (for background checks based on traditional biometrics) and the phone to carry additional biometrics. The reason therefore is that under the current legal situation we cannot install the additional biometrics in the passport because this document is very strictly regulated. So we need to use another data carrier for additional biometrics which could be a smartphone. But later on, if doing so, when checking information in the smartphone, we will need to make the connection between the person and the information in the smartphone. The reason therefore is that additional biometrics is useless if you just recognize someone you don't know who he is. So, storing a hash of passport information in the smartphone to make the link between both carriers would be a possibility.

Monica Vilasau Solana asked Frank Schmalz some additional information about the linking process that was happening in the smartphone. Frank explained that during the enrolment phase of the additional biometrics being developed within PROTECT, we will have to make the link to the person. In the passport, which is a booklet, alphanumerical data is stored but also facial image and fingerprints. On the other hand, we have PROTECT's additional biometrics. What we could do is extract the biometric templates from the passport, encrypt them and calculate some hash of it to obtain a unique identifier of the information contained within the passport's chip. This identifier could only be retrieved when the passport is read out. So, this is not an official document number, but a new unique token specific to the passport. Franck Dumortier added that in such a scenario it would be impossible to reconstruct the information which is stored in the passport with the hash but only to use this hash for a linking purpose between both data carriers.

Frank Schmalz continued by explaining that this hash and the templates of the additional biometrics would then be stored together on the traveller's smartphone. A digital signature would also be needed to make a strong connection between both kinds of information when these are retrieved. When arriving to the kiosk, the traveller presents his passport, the information can be extracted, the hash can be calculated and the smartphone is transferring its data as well. It is then possible to make the link again between the information stored in both data carriers.

Monica Vilasau Solana asked for additional information about when exactly the passport hash would be calculated. Frank Schmalz answered that this would happen during the enrolment phase. Franck Dumortier added that the data controller of such a system would probably be a company or authority, that the traveller would have to sign a consent form to use the "facilitation" service and that after this, additional biometrics would be enrolled together with a hash of the passport being calculated at that precise moment. All this information would be packed together in an encrypted form and stored in the traveller's smartphone. Monica then asked if this identification hash (or token) would still be unique for each enrolling traveller. Frank confirmed that this hash would be unique to each traveller. Monica asked if this unique identification number would be stored only in the smartphone. Frank again answered positively. Diana asked whether it would be possible to identify the exact passport of a traveller just by reading the hash. Frank answered that the hash function is a one-way process and that the link could only be retrieved when the passport is read. This also makes sense because usually you get a new passport at least every 10 years because your biometrics change. This is also true for additional biometrics: these also change with time. So, it makes sense that if you need a new travel document, you also would need to enrol the additional PROTECT's biometrics.

Gloria Gonzalez Fuster asked Frank some additional information about the process that would happen when the traveller is passing through the corridor. Frank answered that the main objective of PROTECT in this scenario was to make the connection with a passport but not to verify the authenticity of a passport (which can be done by the actual border control system). Gloria asked if in the corridor (or e-gate), the biometric match for passport authentication would be a parallel process with the additional biometric matching for identity confirmation, or whether the same token would be attributed to the two processes. Diana clarified this question by asking exactly which checks are performed when the traveller was passing through the corridor. Is it 1) to verify that the biometrics of the person walking through the corridor corresponds to the ones in the passport or 2) to verify that the biometrics stored on the smartphone correspond to the ones of

the person or 3) both? Frank Schmalz answered that both were performed but clarified that the first check was started at the kiosk and that sensors in the corridor would perform the second checks. In the corridor we would have different sensors like a face camera and iris recognition, and both kinds of biometrics could be checked against the ones stored in the smartphone.

Diana Dimitrova questioned the purpose of enrolling/check additional biometrics if the goal is to gain speed during the border control process. Frank answered that the main technical challenge of the PROTECT project was to demonstrate enough quality of biometrics when processing them “on the move”. If a traveller stands still and looks into a camera, you get far better matching results than if the traveller is moving. So, if you add additional biometrics you can be more confident that the person is the one to be identified when walking. Gloria commented that if the purpose of the system is to do checks on travellers while they move to win a couple of seconds but they still have to go to a place and cue for enrolling additional biometrics, there is no real overall speed increase. Frank answered that this really depends on how often a traveller is crossing the borders in comparison with the time taken for the enrolment phase. Gloria acknowledged that for a small minority of travellers this would make some sense.

Gloria asked if the token which is assigned to a traveller at the kiosk would be stored for a little time when he’s travelling through the corridor, and if so, for how long. Frank answered that once the verification had been done, it would be destroyed. This automatic erasure feature has been implemented in the PROTECT architecture concept. Gloria was happy to hear that no data was retained.

Frank Schmalz continued to explain that, after the background checks processes in databases (depending on the case: SIS/VIS/EES) have been started when the passport is read at the kiosk, when a traveller is passing through the Biometric Capture Area, sensors such as face recognition or iris recognition cameras could continue to identify him thanks to the additional biometrics stored in the phone.

Frank Schmalz stressed again that the purpose of the PROTECT project is not to change the strictly regulated background checks processes in EU border databases but to try to improve the quality of the matching by developing additional biometrics on-the-move to increase the speed with which people can walk to the gate while background checks are being performed. In this scenario, some speed can be gained by reducing the bottleneck at e-gates (which process information slowly with people standing still) by starting the background checks at the kiosks and being able to subsequently track travellers while they are walking to the gates, using the additional biometrics stored in their phones. While the travellers are walking through the corridor, border guards can then get information about which people have to be checked more thoroughly and which not.

In this scenario, a traveller has both a biometric passport and an app on his smartphone (with the hash and the additional biometrics fused), and the system verifies that 1) the owner of the passport is lawful (thus verifying that the face of the owner matches the facial image in the passport) and 2) whether the additional biometrics such as iris, anthropometrics of the traveller match the templates stored in the smartphone. In view of this, Diana Dimitrova asked what would happen if the biometric verification against the passport was successful but not the one against the templates stored into the smartphone. What would the border guard do in this case? Frank answered that if we have a positive match against the face on-the-move in the Biometric Capture Area, we wouldn’t need to look at the other biometrics. He explained that in the biometric field, you never have a 1 or 0 decision but a decision based on 1) image quality and 2) matching quality. The goal is only to make a statement on the likeliness that someone is the same person: it's not a 100% match objective. According to Frank, the situation described by Diana already happens in the current E-gate situation. For example, a traveller with a beard could not always be successfully identified at E-gates and border guards would already need to perform additional checks manually to identify the person. In our proposed scenario, Frank said that the quality of biometric facial recognition “on-the-move” is lower as you cannot get as good images than when travellers are standing still. So the goal of additional biometrics is also give some confidence that if the score of one biometric matching is low but other are high, you can make the statement that, given the combination of the results, it's very unlikely that someone is able to forge two, three or four biometric features at the same time. In this case, the border guard could take the decision to let the traveller pass through.

Diana Dimitrova still raised the question of the legal ground that could allow a border guard to take a negative decision or to perform more thorough checks on the basis of additional biometrics if the facial matching against the passport did not raise any suspicion. According to her, this scenario would create a new identity check which falls outside the law. Gloria commented that according to her, the purpose of these additional biometrics would be to assist border guards in their decisions in case of doubt, which is what they already do manually in the current situation without the help of such technology. Frank added that if the face match is perfect and accepted because it's beyond the threshold, the system will consider the traveller as being trustworthy and there would be no reason for border guards to consider the additional biometric features.

Diana did not agree with that explanation. She asked what would happen if a traveller passes the facial 1 to 1 check against his passport but fails the second one which is on the move and based on different biometrics to the passport ones. Could a border guard stop the traveller who passed all checks required by law only by a decision taken on the basis of additional biometrics? Frank answered that, indeed, there is no legal ground for such a decision by a border guard. Frank added that the scenario looked it the other way around and was focussing on the case where there is dubitable face matching and additional biometrics would be used to assist the border guards to deal with those doubts. In this case, there is a legal ground for border guards to perform additional checks. Gloria commented that in this "on-the-move" scenario, the face image matching would be of lower quality and that hence additional biometrics would often have to be checked by border guards to deal with doubts. For this reason, Gloria did not see the absolute necessity (in regard to travellers' right to privacy) to design a border control system on-the-move since it would *de facto* generate more intrusive checks and process more personal data. Frank recalled that the potential of implementing on-the-move border crossing points was the objective pursued by PROTECT answering the European Commission H2020 call "BES-6-2015: Border crossing points, topic 2: Exploring new modalities in biometric-based border checks", which is described as follows:

"Research is needed in order to explore whether it is possible to use other biometric data (potentially already used in another context and in another domain) than fingerprint, iris or facial picture to store in the e-Passport chip, which would guarantee the same or higher level of security, but would be more accurate and could be retrieved in a more efficient manner than in the case of the conventionally used biometric data types. In addition, practical experiences lead to the assumption that for non-critical travellers (EU, bona-fide etc.) a most fluent non-intrusive control process is desired. Therefore, to increase accuracy, in this case the use of contactless techniques (e.g. face, 3D face, iris) and multi-biometric fusion is likely to be preferred over contact-based technologies".

Monica Vilasau asked why the PROTECT consortium was not considering only processing the iris of passengers since it is a more reliable feature than the facial image. Frank answered that indeed iris is better than face but that we cannot get rid of face for legal reasons we discussed before. Monica Vilasau referred to the principle of data minimization, which requires that processing of personal data is limited to what is necessary for purposes for which they are collected. Frank answered that in the current legal environment, background checks must be based on face and cannot be realized on the basis of iris. Frank Schmalz also reminded that we were not talking in this ELAG meeting about the most performant scenario, but about one that was imagined to cope with the current legal constraints.

The last question that was discussed with the ELAG was whether consent of travellers could be a legal ground to process additional biometric data to speed up the travellers' experience. Concretely, in this scenario, consent would be asked of the traveller by asking him to press a button in his app and a dialogue box would appear. This would comply with the explicit and informed consent requirements from the GDPR. From the legal perspective, the ELAG members recalled that the GDPR requires consent to be freely given and that Recital 43 of the GDPR explicitly states that: "in order to ensure that consent is freely given, consent should not provide a valid legal ground for the processing of personal data in a specific case where there is a clear imbalance between the data subject and the controller, in particular where the controller is a public authority and it is therefore unlikely that consent was freely given in all the circumstances of that specific situation". ELAG members agreed that it would be doubtful that consent of travellers could legally be used by public border control authorities to speed up their public interest missions.

4 PROTECT panel at the 2018 International conference on computers, privacy and data protection

4.1 Introduction

The University of Namur (UNAMUR) organized a panel on behalf of the PROTECT project at the 11th International conference on computers, privacy and data protection (CPDP2018). This conference offered 85 panel sessions with 420 international speakers from academia, public and private sectors and civil society. CPDP2018 received 1110 registrations in total. The conference was attended by over 1000 attendees from 55 countries and over 70% of the attendees coming from outside Belgium.

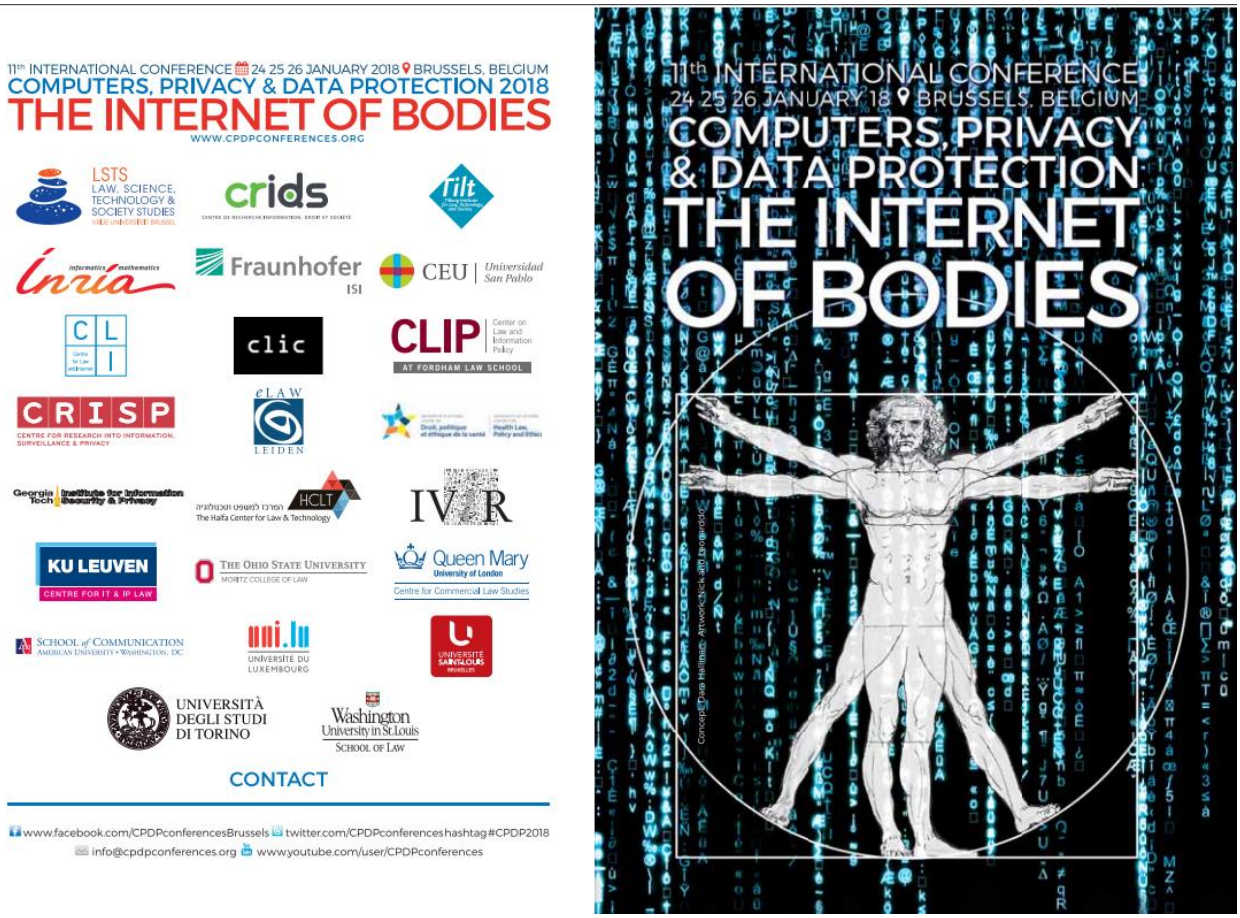


Figure 2 - Presentation of the CPDP2018

The programme of this conference is available for download at this address: http://www.cpdpconferences.org/assets/CPDP2018_PROGRAM_FINAL.pdf

The panel organized by UNAMUR at CPDP 2018 took place on January 25th at 16.00 and was entitled **"Privacy and data protection issues related to the use of contactless multimodal biometrics at border-crossings"**. The topic of this panel was as follows:

"In order to facilitate security and fluency of Schengen Area external cross-border movements, projects propose to develop multimodal biometric solutions for contactless identity confirmation of travellers. For the purposes of multimodal biometric ID verification, project partners proposed to design and develop a biometric corridor, which would incorporate a number of biometric sensors. The initial plan is to include such biometrics as: face recognition, iris recognition, vein pattern recognition, speaker recognition as well as

anthropometric recognition. When operational, the beneficiaries of the multimodal biometric system being developed should be persons enjoying the Union right of free movement as well as third country nationals. This session will bring together academic experts in the field of data protection at border-crossings and policy representatives to discuss the privacy implications of contactless multimodal biometrics at the external borders".

The questions that were discussed included:

- How to improve the border control process with new biometric modalities and increase convenience and speed? Practical aspects.
- Legal constraints deriving from legislation regulating EU travel documents, Schengen IT systems and legislation regulating privacy and data protection?
- Contactless biometrics in the context of the legislative initiatives related to Smart Borders and "interoperability" of large-scale IT databases?

The integrality of this panel discussion is available on Youtube at the following address: https://www.youtube.com/watch?v=maAROMvCCSQ

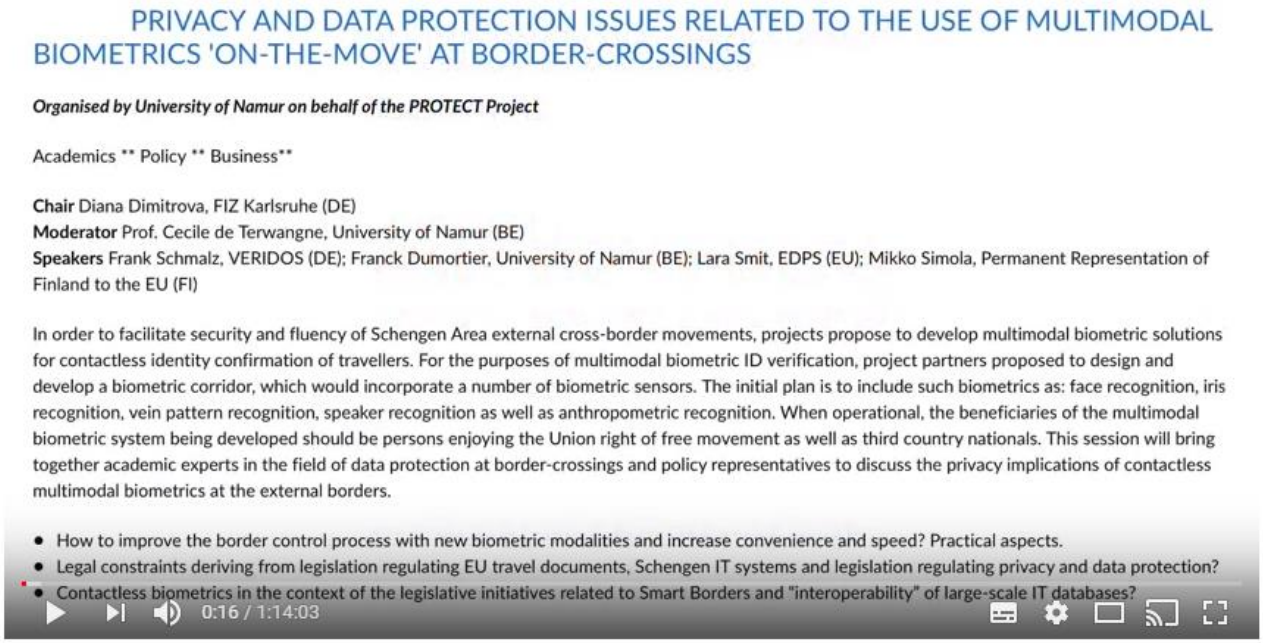


Figure 3 - PROTECT panel at the CPDP2018 on Youtube

4.2 Panelists

Chair: **Diana Dimitrova** is a researcher at FIZ Karlsruhe. Previously she worked as a legal researcher for 3.5 years at the law faculty of the University of Leuven (KUL) in Belgium. Her research focuses mainly on privacy and data protection, especially in the Area of Freedom, Security and Justice. She carried out her research in the framework of the FastPass and eVACUATE projects at KUL. In 2012 she completed a five-month traineeship at the Supervision and Enforcement Unit of the European Data Protection Supervisor (EDPS) in Brussels and holds an LLM in European Law from the University of Leiden, NL.

Moderator: Prof. Cecile de Terwangne has a MD in Law (University of Louvain), a PhD in Law (University of Namur) and a LLM in European and International Law (European Universitary Institute of Florence). She is professor at the Law Faculty of the University of Namur (Belgium). She teaches courses in Computer and

Human Rights, and Data Protection. She is director of the post-graduate Program in Law and Management of Information and Communication Technologies at the University of Namur. She is head of the Freedoms in the Information Society Unit of the Research Centre in ICT, law and Society (CRIDS – University of Namur). She has taken part to numerous European and national researches in the fields of data protection, privacy and ICT, freedom of information, e.Governement, etc. She is director of the « Revue du droit des technologies de l'information » (R.D.T.I.). She has also written numerous articles published in national and international scientific journals.

Speakers:

- **Frank Schmalz** is Director Innovations & Business Development at Veridos.

- **Mikko Simola** is JHA Counsellor at the Permanent Representation of Finland to the EU.

- **Franck Dumortier** is senior researcher at the Information Technology, Law and Society Research Centre (CRIDS) at the University of Namur since 2005. He also was assistant teacher in "Sources and Principles of law" between 2008 and 2013. His research particularly focuses on cybersecurity and cybercrime law and their links with the fundamental human rights to privacy and to data protection. He published numerous articles in national and international journals and participated to several European projects – such as the B-CCENTRE (the Belgian Cybercrime Centre of Excellence for Training and Education) - in his research fields. He is lecturer of legal aspects of IT security in the Master in Cybersecurity and teaches cybercrime and cybersecurity law in several educational programs.

- **Lara Smit** is legal officer in the policy and consultation unit of the European Data Protection Supervisor (EDPS). She mainly focuses on large-scale IT systems for border control, migration and police cooperation.

4.3 Discussion

Professor Cecile de Terwangne opened the panel by recalling that the event was linked to the PROTECT project and presented the speakers, highlighting that these had very complimentary profiles: two researchers in the field of data protection (Diana Dimitrova and Franck Dumortier), a speaker representing industry (Frank Schmalz), a specialist in border control (Mikko Simola) and a representative of the European Data Protection Supervisor (Lara Smit).

Figure 4 - Audience at the PROTECT panel

The floor was first given to **Diana Dimitrova** who is data protection researcher at FIZ Karlsruhe and carried out research in the framework of the FastPass project. In her introduction, Diana gave a brief overview of the existing large-scale IT databases at EU level in the context of border control. She started by presenting the SISII database, recalling that it contains numerous alerts – one category of alerts concerning return decisions against third country nationals (TCNs) who are not allowed to enter the Schengen Area if they are subjects of an entry ban. Another category of alerts in SISII concerns law enforcement cooperation and consists of alerts on missing people, suspects, victims of crime as well as information about stolen objects such as identity documents, banknotes and vehicles. The biometrics stored in SISII are currently facial image and fingerprints but the SISII is currently being revised, and there are proposals to also include DNA and palm prints in it. Another information system is the visa information system (VIS) which contains data on TCNs who apply for a short stay visa to enter the Schengen area. VIS contains an alphanumeric date or biographical data such as a name, passport number, nationality, as well as fingerprints and facial images. EURODAC is a third existing database containing currently only the fingerprints of asylum seekers. The purpose of this database is to make sure that that an asylum seeker hasn't already applied for asylum in another Member State. If they have, they should be returned to that Member State to apply for asylum. There is a plan to expand the EURODAC to also include alphanumeric data or biographical data and to lower the age of the of the people who should be fingerprinted from 14 to 6 years of age. SISII, VIS and EURODAC are the existing EU large-scale databases in the border control context but three more are in the pipeline. One of them is the entry exit system (EES), which just got its legal basis and is starting to be built. It will apply to all TCNs who enter the European Union or Schengen area for a short visit to ensure that they do not overstay the 90 day limit. In the EES, people will also have to provide fingerprints and facial images next to the alphanumeric data and it will apply to all TCNs on a short stay visit no matter whether they need to have a visa there or not. There is also

the proposal on the European criminal records for third country nationals (ECRIS TCN-system) so that there is a common database for TCNs who are convicted in a Member State. This database will also contain fingerprints and facial images and it's more a tool for judicial cooperation. Last but not least, there is a proposal called ETIAS (The European Travel Information and Authorisation System), which would seek to collect only biographical data without biometric data for all those TCNs who don't need a visa to enter the Schengen area. Since the ETIAS system does not contain biometrics it does not directly relate to the panel's discussion topic, but is worth mentioning as part of the interoperability concept. After presenting the background of existing and possibly future IT large scale databases in the context of EU external border control, Diana Dimitrova gave the floor to Franck Dumortier.

Franck Dumortier is senior researcher at the Information Technology, Law and Society Research Centre (CRIDS) at the University of Namur and lecturer in cybersecurity law. His research particularly focuses on security and cybercrime law and their links with the fundamental human rights to privacy and to data protection. He is the legal and privacy adviser in the context of the PROTECT project. Franck spoke about the legal constraints that are raised in the PROTECT project. First, he recalled that the earth is a globe on which free movement of people is the most natural thing; on the contrary, borders are human legal constructions which constitute interferences with fundamental rights such as free movement and privacy. The right to privacy is mainly regulated by article 8 of the European Convention on Human Rights (ECHR). According to article 8, §2 ECHR, interferences with that right must be provided by law and proportionate for the aim that is pursued. The concept of the PROTECT project is to develop a multimodal biometric solution for identity confirmation on the move of travellers with the aim to enhance border security as well as facilitate cross-border movement. The first question raised by Franck is what is meant by "facilitating cross-border movement". According to him, that purpose is not very clear because lots of things can be "facilitated" in the context of cross-border movement. Specifying more clearly the purpose of PROTECT is important in the context of data protection in order to apply the purpose limitation principle, which is one of the core principles of personal data protection regulation. Franck continued by explaining that to pursue that non-specific purpose, the PROTECT project proposes to process various emerging biometric modalities which would be fused such 3d face, periocular, finger veins, voice and anthropometrics.

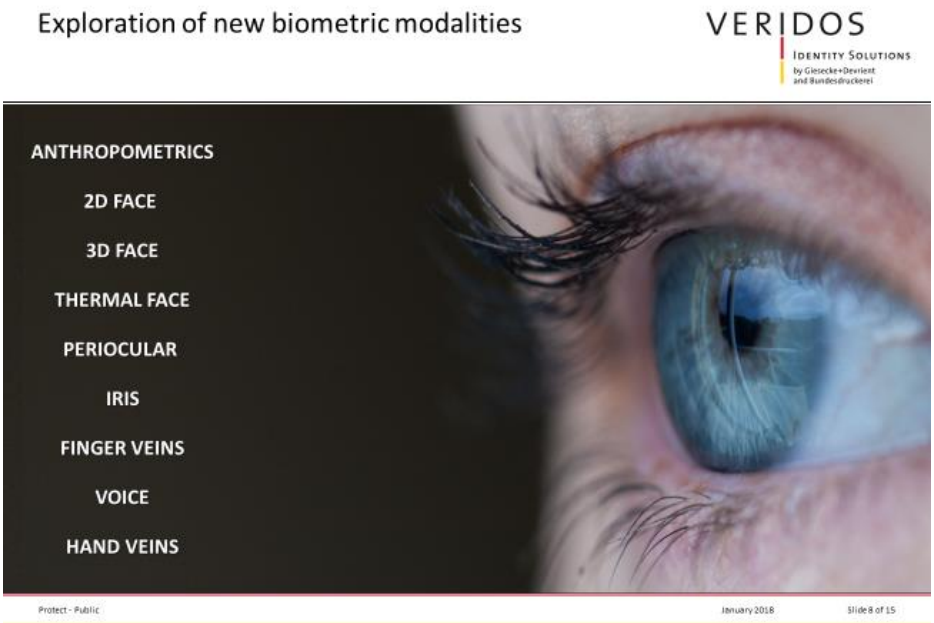


Figure 5 - Additional biometrics developed in PROTECT

An important question related to the development of such additional biometric modalities is how to combine these new modalities with the statement of the European Council of Thessaloniki in 2003 which affirmed that a coherent approach is needed in the European Union on biometric identifiers or biometric data for

documents for TCNs, European citizens passports and information systems. As Diana recalled, current IT databases (SISII, VIS and EES) contain facial images and fingerprints. This is also the case in passports and resident permits. By consequence, travellers are checked on the basis of these "traditional" biometrics when crossing external borders.

Travel document/ IT system	Biometrics included
EU passport	Fingerprints and facial image
Residence permit	Fingerprints and facial image
Schengen visa	Not in the sticker itself but inclusion of biometrics in the VIS during the visa application
VIS	Fingerprints, facial image
SIS II (immigration control)	Fingerprints and facial image (according to SIS II proposals on borders and return)
EES	Fingerprints and facial image (for TCNVEs)

Figure 6 - Biometrics in current travel documents and existing EU databases

Taking this into account, from a pragmatic point of view, the main question in PROTECT is how to implement new biometric modalities, taking into account the fact that EU cross-border databases will still have to be checked on the basis of facial images and fingerprints. A second question is which basis of lawfulness could legitimate the processing of these additional biometrics. Article 4(14) of the GDPR defines "biometric data" as "personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data". In its Opinion 4/2007 (WP136), the Article 29 Working Party specified that biometric data are "biological properties, behavioural aspects, 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." By consequence, biometric data (raw and templates) are considered as "sensitive data" under the GDPR. As stated by article 9(1) of the GDPR, the principle is that "processing biometric data for the purpose of uniquely identifying a natural person […] shall be prohibited". Exceptions to that principle are listed in article 9(2) of the GDPR: processing of biometric data for border-crossing purposes is possible only if:

- the data subject has given explicit consent to the processing of those personal data for one or more specified purposes, except where Union or Member State law provide that the prohibition may not be lifted by the data subject;

- processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.

Taking this legal reality into account, an important question is hence to determine the adequate basis of lawfulness for the use of new contactless biometric modalities which are being developed in the PROTECT project.

Could consent be used as an adequate basis of lawfulness for the use of these new biometric modalities? According to article 4(11) of the GDPR "Consent means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her". Furthermore, according to article 7(3), "the data subject shall have the right to withdraw his or her consent at any time". Additionally, for biometric data, consent must be "explicit". Concerning renewability and revocability, in its opinion 3/2012, the Article 29 Working Party stated that "as the source of biometric data cannot be changed, biometric systems whose purpose is to establish an identity link must be designed in a way that the enrolment process and the processing of biometric data allows that multiple and independent biometric templates can be extracted from the same source in order to be able to replace them in the case of a data breach or a technological evolution. Biometric systems should be designed in a way that allows to revoke the identity link, either in order to renew it or to permanently delete it e.g. when the consent is revoked". More importantly, Franck asked whether free choice of data subjects for border control convenience is possible. This is very doubtful when looking at recital 43 of the GDPR, which states that "in order to ensure that consent is freely given, consent should not provide a valid legal ground for the processing of personal data in a specific case where there is a clear imbalance between the data subject and the controller, in particular where the controller is a public authority and it is therefore unlikely that consent was freely given in all the circumstances of that specific situation". This means that the use of additional biometrics on the basis of consent for "facilitating" public authorities' mission in the field of border control is at least very controversial, if not illegal. However, the basis of consent is still possible for "commercial" purposes which are not strictly linked to public authorities' missions. For example, in a 2005 deliberation, the CNIL (French DPA) authorized the use of fingerprints on a fidelity chipcard for frequent travellers of the airport of Nice. The system was designed for convenience purposes (facilitate access to parking zones, additional services, etc). In this context, important conditions imposed by CNIL were 1) the voluntary use, and 2) the storage on an object (no centralized database).

Given that consent is not the most adequate basis of lawfulness for the use of additional biometrics in a public context, another option is to use is Union and or Member State law. Article 8(d) of Regulation (EU) 2017/2225 of 30 November 2017 amending the Schengen Border Code (SBC) allows Member States to establish "voluntary" National Facilitation Programs (NFPs). As stated by this Regulation, the purpose of NFPs would be to waive pre-vetted and pre-cleared TCNs from the requirement to be interviewed on their means of subsistence, purpose of travel and point of departure and destination. By consequence, the issues with this basis of lawfulness are twofold: first, according to the SBC amendment, NFPs would be possible only for TCNs but not for EU/EEA/CH travellers; secondly, the purpose of such NFPs would be only to "facilitate" TCNs' requirements for interview on their means of subsistence, purpose of travel and point of departure and destination…but not to "speed up border control databases checks". So even for TCNs, SIS, VIS and EES will still have to be checked and "traditional" biometrics (as legally standardized) would still be required.

By consequence, taking into account the SBC amendment, the purpose of using additional biometrics being developed within the PROTECT project could legally only be used by TCNs under potential NFPs national laws for the abovementioned purposes. Additionally, such national laws should be proportionate and comply with data protection principles enshrined in article 5 of the GDPR: purpose limitation, data minimization, accuracy, storage limitation, integrity and confidentiality.

Concerning proportionality, in its opinion 3/2012, the Article 29 Working Party stated that "The use of biometrics raises the issue of proportionality of each category of processed data in the light of the purpose for which the data are processed. As biometric data may only be used if adequate, relevant and not excessive, it implies a strict assessment of the necessity and proportionality of the processed data and if the intended purpose could be achieved in a less intrusive way. 1) In analysing the proportionality of a proposed biometric system a prior consideration is whether the system is necessary to meet the identified need, i.e. is essential for satisfying that need rather than being the most convenient or cost effective. 2) A second factor to take into consideration is whether the system is likely to be effective in meeting that need by having regard to the specific characteristics of the biometric technology planned to be used. 3) A third aspect to consider is whether the resulting loss of privacy is proportional to any anticipated benefit. If the benefit is relatively minor, such as an increase in convenience or a slight cost saving, then the loss of privacy is not appropriate. 4) The fourth aspect in assessing the adequacy of a biometric system is to consider whether a less privacy intrusive means could achieve the desired end". Moreover, the Article 29 Working Party emphasizes that "whenever it is permitted to process biometric data, it is preferred to avoid the centralised storage of the personal biometric information". Especially for verification, the Working Party considers it advisable that "biometric systems are based on the reading of biometric data stored as encrypted templates on media that are held exclusively by the relevant data subjects (e.g. smart cards or similar devices). Their biometric features can be compared with the template(s) stored on the card and/or device by means of standard comparison procedures that are implemented directly on the card and/or device in question, whereby the creation of a database including biometric information should be, in general and if possible, avoided. Indeed, if the card and/or device is lost or mislaid, there are currently limited risks that the biometric information they contain may be misused. To reduce the risk of identity theft, limited identification data related to the data subject should be stored in such devices". Applying the principle of data minimization to biometrics, the Article 29 Working Party considers that "biometric data should be stored as biometric templates whenever that is possible. Template should be extracted in a way that is specific to that biometric system and not used by other controllers of similar systems in order to make sure that a person can only be identified in those biometric systems that have a legal basis for this operation". The goal of this statement is obviously to avoid illegitimate interoperability. Additionally, the Article 29 Working Party emphasizes that "The definition of the size (the quantity of information) of the template is a crucial issue. On the one hand, the size of the template should be wide enough to manage security (avoiding overlaps between different biometric data, or identity substitutions), on the other hand, the size of the template should not be too large so as to avoid the risks of biometric data reconstruction. The generation of the template should be a one-way process, in that it should not be possible to regenerate the raw biometric data from the template". The accuracy principle should also be applied to biometrics: the Article 29 Working Party recommends anti-spoofing mechanisms by stating that "to maintain the reliability of a biometric system and prevent identity fraud, the manufacturer has to implement systems aiming to determine if the biometric data is both genuine and still connected to a natural person. In respect of facial recognition, it may be critical to ensure that the face is a real one and not, for example, a picture tied on an impostor's head". Concerning the storage limitation principle, automated data erasure mechanisms are recommended: "in order to prevent that biometric information are stored for longer than is necessary for the purposes for which they were collected or subsequently processed, appropriate automated data erasure mechanisms have to be implemented also in case the retention period may be lawfully extended, assuring the timely deletion of personal data that become unnecessary for the operation of the biometric system. When using integrated storage on the reader, manufacturers may also implement storage of the biometric templates on volatile memory that guarantees that the data will be erased when the reader is unplugged. Therefore, no biometric database remains when the reader is sold or uninstalled. Anti-pulling switches may also be used to automatically erase the data if someone tries to steal the reader". Finally, the Article 29 Working Party applies the data security principle to biometrics by writing that "the biometric system used and the security measures chosen should limit the mentioned risks and make sure that the re-use of the biometric data in question for further purposes is impossible or at least traceable. Mechanisms based on cryptographic technologies, in order to prevent the unauthorised reading, copying, modification or removal of biometric data should be used (…) When the biometric data are stored on a device

that the data subject physically controls, a specific encryption key for the reader devices should be used as an effective safeguard to protect these data from unauthorised access".

The floor was then given to **Frank Schmalz,** who is Director Innovations and Business Development at Veridos GmbH. Frank started his presentation by recalling that the H2020 call by the European Union to make this PROTECT research project is obviously the consequence of statistics on the progress of air traffic and travellers: in the next 20 years, there will be a doubling of air traffic travellers and we have of course the issue how to handle these travellers at the borders.

Figure 7 - Air traffic increase in the next 20 years

Two options are possible. The first is to install more E-gates but this basically means that we will need more space at the airports, where space is very limited and the perspective of 20 years will probably not change this issue. The second option is basically to speed up the process at the borders but therefore new approaches are needed since the E-gates are processing travellers too slowly. Frank then reminded the main aims of the BES-6 call "Secure societies – Protecting freedom and security of Europe and its citizens":1) Exploration of new biometric modalities at borders, 2) a most fluent non-intrusive control process is desired and 3) the ethical, societal and data protection aspects should be embraced. Frank continued by presenting the PROTECT consortium members explaining that not only Universities are involved but also end users, for example the Polish border guard and the UK Home Office, and Veridos as industry partner.

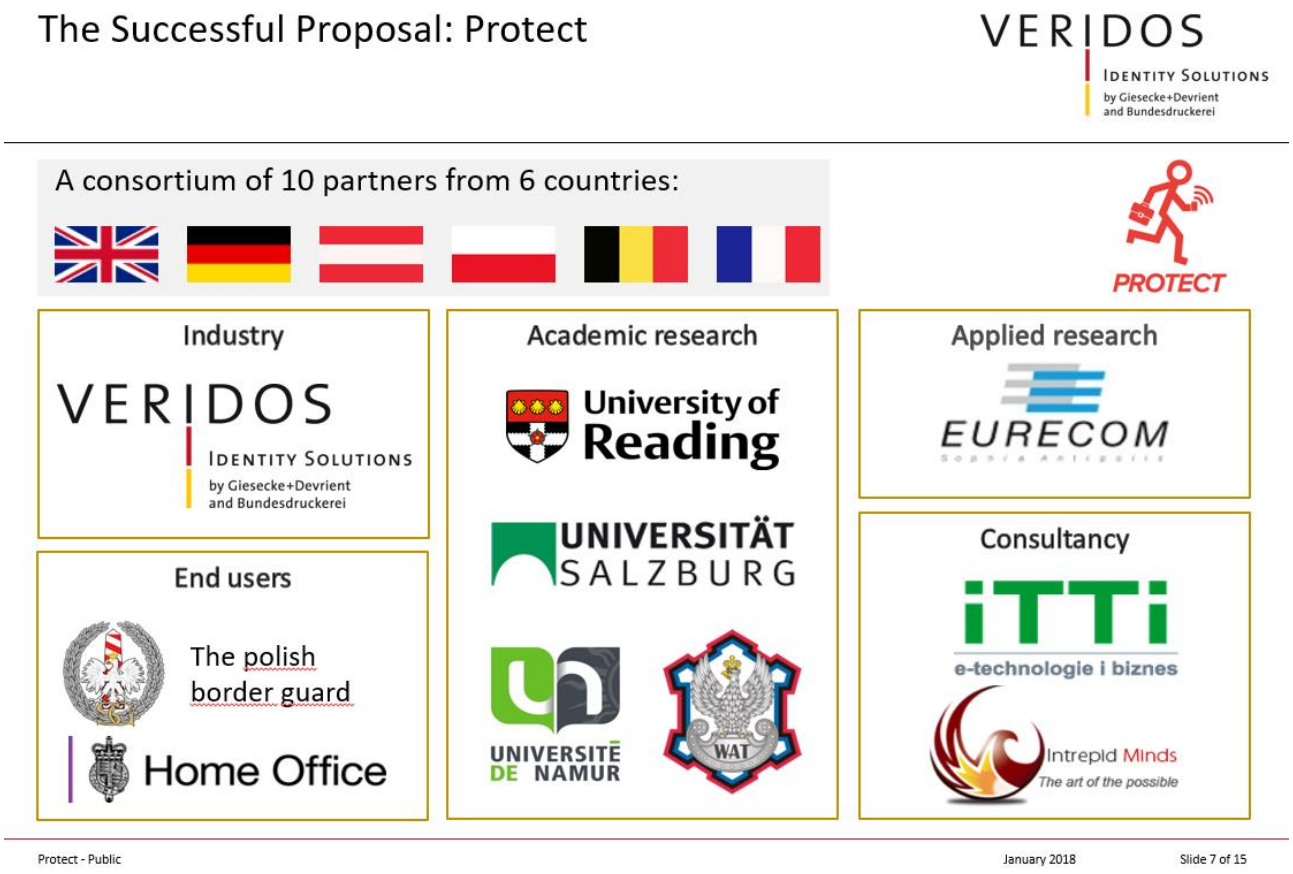


Figure 8 - Presentation of the PROTECT's consortium

The final goal of the PROTECT project is building a demonstrator that should show how the new modalities developed by PROTECT academic partners could work. One central research question within PROTECT is template protection. One major issue with template protection is that it reduces accuracy, while the law imposes to take care of accuracy and anti-spoofing at the same time. A way to achieve such a goal is to combine several biometric features to have better accuracy - even though we have template protection - and also to have better anti-spoofing capabilities. So this would be the advantage to use multiple biometrics in the area we are looking at in PROTECT. Within the PROTECT project, we are looking at two scenarios: a) air & sea border where individuals are on the move and b) land border where individuals are in or on vehicles.

Figure 9 - Border contexts taken into account within PROTECT

When focusing on the first scenario, for travellers walking over the border, the current technical system that is used for automated order control is E-gates. If you're looking at speeds, we can see that reading out the document takes about five to six seconds and the next step that is taking a lot of time is the gate mechanics which takes about 10 seconds. If everything goes well, the total processing time is 15 to 18 seconds for E-gates. So coming to the question on how can we can gain speed, if you are looking at the reading of the document, we have a lot of issues stemming from the fact that people have to put the document on the reader. Ideally, it takes five to six seconds to read out the document, but if travellers make mistakes – and this happens often – then it's taking even longer: so this is an interesting point to ameliorate. When looking at additional biometrics, enrollment could be required once per document lifetime. Kiosks could be located at foreign airports where travellers would enroll additional biometrics such as anthropometrics, 2D face, 3D face, thermal face, periocular, iris, finger veins, voice and hand veins. Those data would be stored on the smartphones of the travellers, because we cannot put them on the passport since the content of travel documents is being strictly regulated. We could store those additional biometric data in a database but we don't want to do that because this is also something that is not desirable from the legal point of view from what we have seen so far from European decisions of the European Parliament. Using smartphones as data carriers bypass these problems, and offers additional benefits: travellers carry them on their person all the time, and data transmission methods with smartphones are very easy to handle and so the handling problems we have currently with the passport reading are avoided.

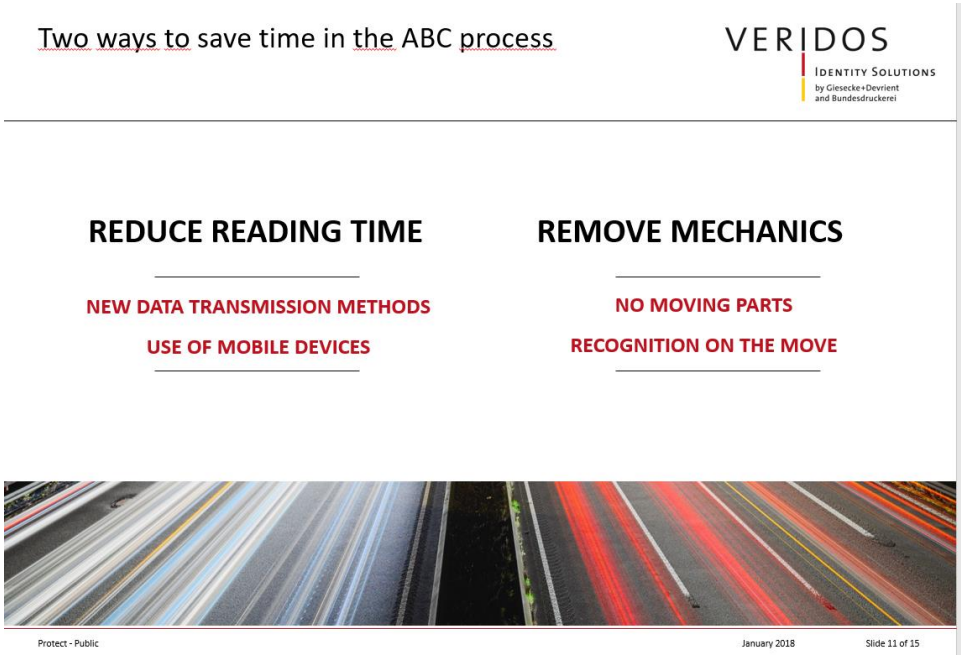


Figure 10 - Two ways to save time in the ABC process

Frank then illustrated the proposed verification process being proposed by the PROTECT consortium. A traveller would approach the border with a smartphone and then walk into a corridor where he is on the move. The biometrics are verified before the data is transferred to the system from the smartphones: so a user presses a button, the data is transferred to the system then the verification takes place and then afterwards the data can be erased from the system again. So, this is a very similar process to that currently used with the E-gates.

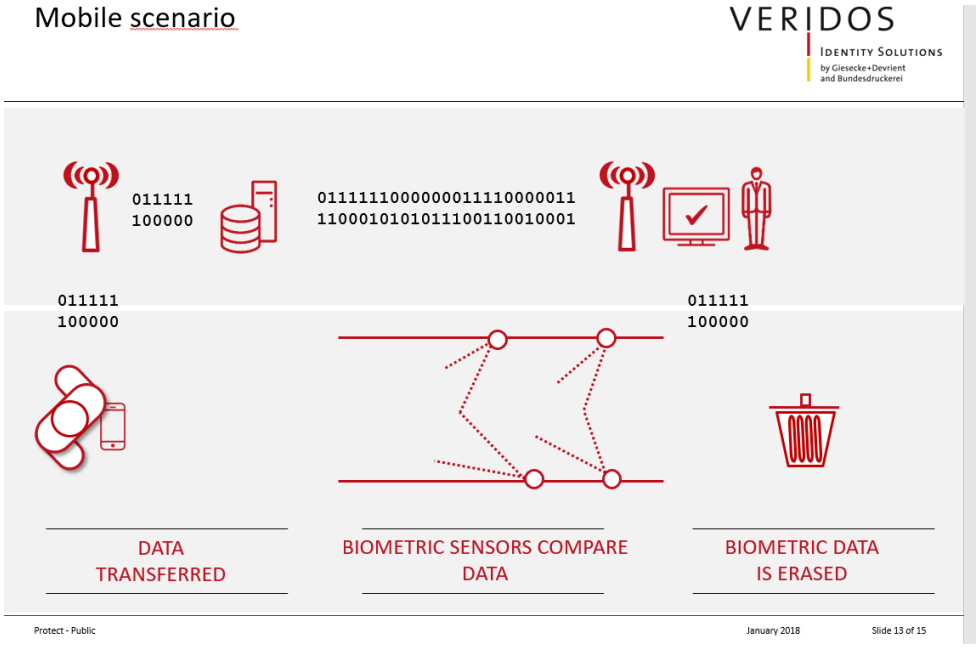


Figure 11 - Mobile scenario description

One issue of course if you are dealing with smartphones is the fact that these are not very secure devices. Some manufacturers take measures to improve security but that's very individual to each model so what we're thinking about is basically putting the data not in plain on the smartphone but in an encrypted manner.

The encryption keys would be in the background system and would be accessed at the moment when the verification takes place. So the encrypted data is transferred to the system, it's decrypted, used and then it's thrown away.

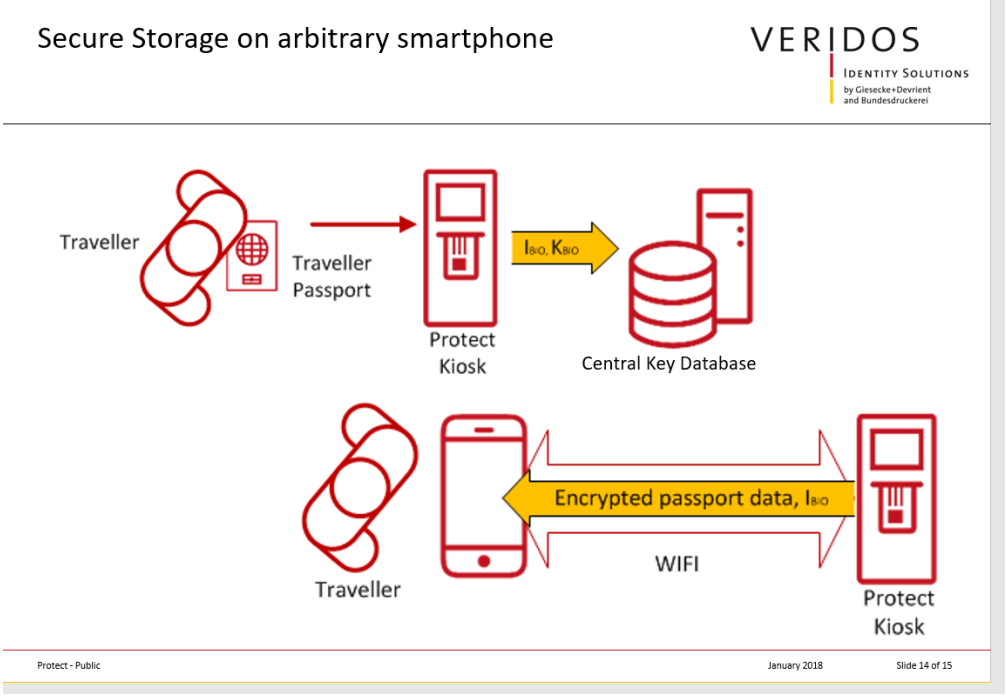


Figure 12 - Secure storage on arbitrary smartphone

Cecile de Terwangne gave the floor to **Mikko Simola,** who is JHA Counsellor at the Permanent Representation of Finland to the EU. Mikko Simola has previously worked as a border security expert responsible for EU coordination and Schengen matters and has practical border control experience for almost twenty years.

Mikko Simola's intervention 1) focused on how to facilitate security and fluency of cross-border traffic when further developing the use of biometrics, 2) mentioned the operational environment from the EU external borders' point of view and then 3) explored aspects which from the speaker's point of view are important to take into account when further developing the use of biometrics in the future. Currently, the scale of estimated border crossings via the border crossing points at the external borders of the EU is just over 700 million annually, and based on some studies it has been estimated that in five years it will be approximately 880 million. The vast majority will definitely travel by airports but we have heard already today that it's important not to forget the almost 300 million other passengers that travel to EU via land borders which is certainly an important aspect from the Finnish point of view. Also important is to take into account people travelling via the sea borders. During the last years in the migration crisis, sometimes when you are following the public debate from the speaker's point of view, the focus is - for obvious reasons perhaps - on the border surveillance which is happening between the border crossing points, not so much on the border crossing points activities which is important certainly taking into account the fact that the main bulk of the border crossings will luckily take place in the future at the border crossing points. So for example, thinking about the main migration crisis from the EU perspective in 2015, the detections of illegal border crossings at the

Figure 13 - Mikko Simola at PROTECT's CPDP2018 panel

border crossing points was something like 1.8 million if we calculate the travelling through the Western Balkans as well and still it's quite a small figure comparing to the 800 million via these border crossing points. Looking at the environment at the external borders, it's important to remember- also in the development projects - that changes are quite rapid and it's difficult to predict different factors from political or economic instability to climate change, but certainly the main challenges for border management are related to the secure and fluent control of the continuously growing passenger flows. This so called double aim of border checks, not only focusing on the security but remembering the fluency is an important point because from the speaker's point of view fluency contributes the to the security from the border guard perspective.

Mikko Simola then gave a few words on the integrated border management (IBM) concept. Nowadays, use of state-of-the-art technology is one of the 11 strategic elements of the IBM integrated border management concept which was for the first time defined on legislative level in 2016 when the regulation on the European border and Coast Guard entered into force. Technical development is one new element because, as we have heard from the previous speakers, it enables many things in the future and it's important that the border management is supported by advanced mobile and interoperable European technical systems because what border guards needs as end-users is fast and seamless access to information they need based on the law in order to perform their tasks taking into account the fluency aspect as well. Therefore, these large-scale IT systems we heard from the first intervention need to be continuously aligned with the strategic objectives. Availability and quality of the information are two important points. Practical measures for ensuring data accuracy is also one thing which need to be focused on: a main challenge is the problem of multiple identities. Biometrics is necessary for combating that problem. The entry exit system (EES) which hopefully will be in place in 2020 for third country nationals is important for enhancing the efficiency of politics. The implementation phase of the EES which is currently ongoing is an important thing: facial image and fingerprints will play a crucial role for identifying TCNs in a reliable way. Mikko Simola then mentioned that sometimes the second part of the double aim of border checks - the fluency - is forgotten in the debates and discussions when the EU regulations are being negotiated. These technologies should allow "bona fide" and business travellers to be identified properly and conveniently in a short period of time and they should not be mixed or with so-called "mala fide" travellers having, for example, the same name and alphanumerical data. According to the speaker, one could even say that the fluency of cross-border traffic is a fundamental right of a person: his right to freedom of movement. Having this perspective in mind, one reason explaining the problem related to incomplete information, difficulties to detect multiple identities and combat identity fraud is that the identity data including biometrics is nowadays stored in separate information systems which are quite fragmented from the end users' point of view. It is still quite difficult to detect multiple identities and to combat identity fraud since it's nowadays possible that people are recorded under different identities in different systems without being detected. So hopefully this problem will be mainly solved and tackled by the latest Commission's proposals related to the interoperability of the EU information systems. From the practitioners' point of view that kind of component which would show the links between multiple identities corresponding to the same biometric identifiers to the authorities which are involved in the border management could provide a powerful tool for detecting and combating identity fraud and improving internal security. This so-called shared biometric matching service would enable searches across different information systems holding biometric data. Mikko Simola then said a few words about pragmatic issues. End users realized that border checks improvement should take into account different conditions and means of transportation when analyzing technical solutions. For example, checking the biometrics in a moving train while ensuring fluency at the same time or outside on a car lane where the passengers are in the car in a temperature of minus 35 degrees certainly create challenges for ensuring the smooth and convenient way of handling the border checks and proceed to biometrical verification. Looking a bit more to the future, Mikko Simola expressed his view that certainly the kind of research activity conducted within the PROTECT project can create important basis for changing and widening the use of biometrics in a proper manner. Solutions which are proposed such as biometric corridors using face recognition or other biometrics on the move and identifying passengers at the airports would certainly benefit travellers and border guards if the verification could be done before the passengers arrive to the border control. Finally, the speaker mentioned four points for further developing biometric solutions. First, it's important to set and develop time limits for biometric data to be pre-checked and transmitted. With this regard the issue of using proper templates is an

important factor because otherwise we will create huge delays in performing border checks at the border crossing points. Secondly, the quality of biometrical data is an important challenge: there can be difficulties in enrolling biometrics with the proper quality, especially in challenging field conditions outside or in moving carriers. Admission of lower quality of biometrics would result in reduced application performance which would cause delays and challenges for the law enforcement authorities. Thirdly, the so-called query capacity of different IT systems we are using now needs to be updated to cope with the increased number of passengers. The fourth point is the most important and perhaps the most practical one. Practical aspects and common-sense need to be remembered. So-called facilitation programs are important to consider when further developing the use of biometrics at the border crossing points from the practitioners' point of view. In addition to the operational environment and conditions of the border crossing points, the interests of "bona fide" travellers like businessmen need to be taken into account in a wise manner. For example, biometrics of so called pre-vetted trusted travellers benefiting from these facilitation programs should not always be verified electronically. This is one important aspect we managed to put into the new entry exit system regulation because in that way we can give border guard practitioners more time to focus on detecting those passengers which should be detected.

The floor was then given to **Lara Smit**, who represented the European Data Protection Supervisor (EDPS). Lara Smit is legal officer in the policy and consultation unit of the EDPS. She mainly focuses on large-scale IT systems for border control, migration and police cooperation.

Lara started by recalling that migration border control and these large-scale IT systems haven't been off the agenda for many years. Actually, a lot has been going on in this area at EU level and a lot is still going on. In her speech, she first wanted to discuss a bit more about the smart borders package and then say a few words about the recent legislative proposals of the Commission on interoperability of large-scale IT systems. Starting with the smart borders package, the speaker recalled that the package was made of two regulations that were proposed by the Commission back in 2016: one establishing the entry exit system (EES) and the other integrating the changes that are needed to use the EES in the Schengen Border Code. The EES will record all entries and exits of TCNs (non-EU citizens) in the Schengen area but also all refusals of entry. By doing so, the idea is to replace the current system of stamping all passports of country nationals and to record these entry entries and exits electronically in a large-scale database. This idea of creating the EES is not new: it dates back to 2008 when it appeared for the first time in a Commission communication and so after almost ten years it has now become law. The regulations were published in the Official Journal in December and entered into force in December. The reason why it took a very long time is because it was a first smart border package was tabled back in 2013 but it got stopped at the time by the European Parliament due to data protection concerns because the EES needed to store very important amounts of personal data (alphanumeric data but also biometric data). In the current EES regulation, the system will rely on the facial image and four fingerprints but the first proposal required the storage of ten fingerprints and the facial image of all TCNs for 181 days. In the current regulation, the collection of biometric data is reduced to four fingerprints and the facial image but the storage period (5 years) has increased compared to the first proposal. The EDPS has been involved in in these debates from the very first start and issued opinions on both the first and the second smart borders packages. Since the entry/exit will imply a significant collection, storage and use of personal data of TCNs, the legislator had among others considerations for fundamental rights to privacy and data protection that are protected under article 7 & 8 of the EU Charter. The data processing envisaged with the building up of this of this new large-scale IT system to be compatible with the Charter had to comply with all the conditions of article 52 including the requirements of necessity and proportionality. The EDPS considered from the start that the processing of personal data implied by the EES were significant and intrusive, especially when taking into account the number of persons that would be affected by the system, the type of information (alphanumeric data and biometric data) that would be processed through the system, but also

Figure 14 - Lara Smit at PROTECT's CPDP2018 panel

the different purposes of the system because aside from the border management and the facilitation purposes there is also a law enforcement access that is created in the in the regulation. Under certain conditions, national competent authorities could have access to the EES data. So in the second entry exit proposal, the EDPS has welcomed the fact that the datasets and the number of biometric data that TCNs have to provide had been reduced. We also raised concerns regarding several aspects of the text such as the longer data retention periods and, finally, we also had concerns about the necessity and proportionality of these accesses by law enforcement authorities. They would have to make a request and this meets a number of conditions but we still had concerns about the necessity and proportionality of such access. The plan is now to have this system ready by 2020. The new agency in charge of large-scale IT system (ELISA) is responsible for building the system and for managing the system once it starts its operation. The question remains how exactly the collection and the matching of these four fingerprints and the facial in image will take place at border crossing points. This is not very clear in the entry exit regulation. For travellers who have a visa, they won't need to have their fingerprints taken a second time since their fingerprints are already available in the visa information system (VIS) so this information will be retrieved from the visa information system (VIS). The second regulation of the small borders package contains a modification of the Schengen Borders Code and it provides some precisions in this regard and it includes provisions on the use of automated border control systems such as self-service systems and E-gates where the passengers would be able to proceed themselves to not all but some of the border checks. It provides definitions for this technology but it leaves it to Member States to decide whether or not and to what extent they will use these technologies. For instance they could use a combination of E-gate and self-service system, one of them or all of them. The text specifies that this technology should always be used under the supervision of border guards in order to be able to detect any fraud. To be able to use this technology, TCNs will need a passport with a chip whose authenticity will have to be checked and on which a facial image will have to be stored to allow identity verification. They should be designed in such a way that they can be used by all travellers except for children under 12 and also in a way that fully respects human dignity in particular in cases involving vulnerable persons. Finally, another precision in the Schengen Borders Code is that a sufficient number of staff members should also be present to assist travellers with the use of this system, which might be very easy for some of us but not for everyone. All these specifications in the Schengen Border Code still leaves much room for maneuver to Member States, so perhaps we'll see the possibility to collect this biometric data on the move but also on the way they will implement data protection safeguards for the use of these technologies which could have a very direct and concrete impact on travellers.

After having talked about the Smart Border package Lara Smit then said also few words on Interoperability. The EDPS still have not issued a position on this proposal that was tabled in December. The EDPS was involved in the work of the high-level expert group on information systems that was launched by the Commission and that was assessing the different possibilities to set up interoperability between the existing and future large-scale IT systems. The EDPS also issued a preliminary statement in annex to their final report and a reflection paper on interoperability but no public position of the EDPS on the final proposal is available yet. In any event, what the Commission is proposing with these two proposals on interoperability is to stop the functioning of existing and future large-scale IT systems in silos, and to make them talk with each other. To do so they propose to build what they call a European search portal that would allow border guards to search the system at once, simultaneously, and have combined results from all of them instead of having to go and check SIS, VIS and EURODAC one by one. So the results will be quicker and they would have combined results, but also a shared biometric matching system that would allow search based on biometrics across several systems - based for now on only the facial image and fingerprints and a common identity repository alphanumeric data of different systems. The EDPS will issue an opinion in the next months on this proposal.

5 Conclusion

A critical issue with the processing of biometrics at border crossings is that it constitutes in an interference with fundamental human rights such as the right of liberty and the rights to privacy and data protection. Since greater use of personal data impacts upon human rights, there needs to be an honest and assertive

study of what the risks are to privacy and how these risks are mitigated. For that reason, the aim of D2.5 is to identify and address the ethical and legal implications of the technical solutions being developed in the context of the PROTECT project by summarizing discussions between the project partners and exchanges with the Ethical and Legal Advisory Group (ELAG) as well as with other external experts.

The meeting “on the impact of privacy regulations on system architecture & technical solutions” (which was organized on 4th July 2017), the first ELAG meeting (which was held on July 5th 2017) and the panel at the 11th International conference on computers, privacy and data protection (which took place on January 25th 2018) were three important opportunities for constructive exchanges about legal, privacy and data protection issues related to the development and use of contactless multimodal biometrics at external border crossings.

Both the regulatory framework governing EU border control databases and the one regulating data protection were recently, or are currently being, modified. Some examples are the GDPR, the EES Regulation, the SBC amendment, the ETIAS proposal and the interoperability initiative. All of these new constraints as well as the general privacy principles should be carefully assessed while developing contactless multimodal biometrics at border crossings in the PROTECT project. The interesting exchanges on these issues with the ELAG and with other experts will, of course, be taken into account.

Please note that this deliverable is a first version of D2.5. A second version D2.5 – Societal impact report is due at M34 and will integrate the next discussions and exchanges on ethical and legal issues with the ELAG and other external experts.

References

[1] Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (GDPR).

[2] Council Regulation (EC) No 2252/2004 of 13 December 2004 on standards for security features and biometrics in passports and travel documents issued by Member States.

[3] Council Regulation (EC) No 1030/2002 of 13 June 2002 laying down a uniform format for residence permits for third-country nationals as amended by Regulation EC No 380/2008.

[4] Regulation (EU) 2017/2226 of the European Parliament and of the Council of 30 November 2017 establishing an Entry/Exit System (EES) to register entry and exit data and refusal of entry data of third-country nationals crossing the external borders of the Member States and determining the conditions for access to the EES for law enforcement purposes, and amending the Convention implementing the Schengen Agreement and Regulations (EC) No 767/2008 and (EU) No 1077/2011.

[5] Regulation (EU) 2017/2225 of the European Parliament and of the Council of 30 November 2017 amending Regulation (EU) 2016/399 as regards the use of the Entry/Exit System.

[6] Article 29 Data Protection Working Party, Opinion No 4/2007 on the concept of personal data, adopted on 20 June 2007 (WP 136).

[7] Article 29 Data Protection Working Party, Opinion 3/2012 on developments in biometric technologies, adopted on 27 April 2012 (WP 193).

Appendix I Presentations given at the CPDP2018 conference

I.1 Franck Dumortier's presentation

CPDP 2018 - Privacy and data protection issues related to the use of contactless multimodal biometrics at border-crossings

Legal contraints

Franck Dumortier – UNAMUR
Franck.dumortier@unamur.be

PROTECT system vs European logic

- The concept of the PROTECT project is to **develop a multimodal biometric solution for identity confirmation "on the move"** of travelers with the aim to enhance border security as well as *facilitate* (?) the cross-border movement.
- The system should, therefore, **process various "emerging" biometric modalities such as 2D face, iris and periocular, hand and finger veins, voice and anthropometrics** of travelers.
- Question: how to combine this with the statement of the European Council of Thessaloniki (2003) : ***"a coherent approach is needed in the European Union on biometric identifiers or biometric data for documents for third country nationals, European Union citizens' passports and information systems"*** ?

2

Travel document/ IT system	Biometrics included
EU passport	Fingerprints and facial image
Residence permit	Fingerprints and facial image
Schengen visa	Not in the sticker itself but inclusion of biometrics in the VIS during the visa application
VIS	Fingerprints, facial image
SIS II (immigration control)	Fingerprints and facial image (according to SIS II proposals on borders and return)
EES	Fingerprints and facial image (for TCNVEs)

GDPR - Biometric data (1)

- GDPR – Art. 4 (14): "biometric data' means **personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics** of a natural person, **which allow or confirm the unique identification of that natural person**, such as facial images or dactyloscopic data".
- Opinion 4/2007 (WP136) of WP29: "biological properties, behavioural aspects, 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**."
- **Biometric data (raw and templates) are considered as "sensitive data".**

4

GDPR - Biometric data (2)

- GDPR, Art. 9(1) - **PRINCIPLE** : " Processing **biometric data for the purpose of uniquely identifying a natural person** [...] **shall be prohibited**"
- GDPR, Art. 9(2) - **EXCEPTIONS**: processing of biometric data for border-crossing purposes is possible only if:
  - (a) the data subject **has given explicit consent** to the processing of those personal data for one or more specified purposes, **except where Union or Member State law provide that the prohibition may not be lifted by the data subject;**
  - (g) processing is **necessary for reasons of substantial public interest, on the basis of Union or Member State law which shall be proportionate to the aim pursued**, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.

5

Which basis of lawfulness?

- Legal basis in Union law for facial image and fingerprints in passports, residence permits, VIS, SIS II and EES
- **Which basis of lawfulness for additional « contactless » biometrics** such as iris and periocular, hand and finger veins, voice and anthropometrics ?

6

Consent ? (1)

- GDPR, Art. 4(11) - "Consent means **any freely given, specific, informed and unambiguous indication** of the data subject's wishes by which he or she, **by a statement or by a clear affirmative action**, signifies agreement to the processing of personal data relating to him or her".

- GDPR, Art. 7(3): The data subject shall have the **right to withdraw his or her consent at any time**.

- **Additionally, for biometric data, consent must be "explicit".**

7

Consent ? (2)

- Opinion 3/2012 of WP29- **Renewability and revocability is essential**

- "As the source of biometric data cannot be changed, biometric systems whose purpose is to establish an identity link must be designed in a way that the enrolment process and the processing of biometric data allows that multiple and independent biometric templates can be extracted from the same source in order to be able to replace them in the case of a data breach or a technological evolution. **Biometric systems should be designed in a way that allows to revoke the identity link, either in order to renew it or to permanently delete it e.g. when the consent is revoked**"

8

Consent ? (3)

- Free choice of data subjects for border control convenience ?
- GDPR, Rec. 43: "In order to ensure that consent is freely given, **consent should not provide a valid legal ground for the processing of personal data in a specific case where there is a clear imbalance between the data subject and the controller, in particular where the controller is a public authority** and it is therefore unlikely that consent was freely given in all the circumstances of that specific situation".
- **However, consent is still possible for "commercial" purposes**. Ex: In a 2005 deliberation, the CNIL (french DPA) authorized the use of fingerprints on a fidelity chipcard for frequent travelers of the airport of Nice. The system was designed for convenience purposes (facilitate access to parking zones, additional services, etc): Important criteria were the 1) the voluntary use, and 2) the storage on an object (no centralized database).

9

Union/Member State law ? (1)

- Regulation (EU) 2017/2225 of 30 November 2017 amending the Schengen Border Code
- Art. 8(d) allows MS to establish **"voluntary" National Facilitation Programmes** (NFPs)
- Purpose of NFPs ? **To allow pre-vetted and pre-cleared TCNs to waive them from the requirement to be subject to an interview on their means of subsistence, purpose of travel and point of departure and destination**

10

Union/Member State law ? (2)

- Art. 8(d) of Regulation (EU) 2017/2225 allows MS to legislate on "voluntary" (?) NFPs…
- Only for TCNs ! **What about EU/EEA/CH travelers ?**
- Only to "facilitate" the requirements of interview on their means of subsistence, purpose of travel and point of departure and destination… **Purpose is not to "speed up border control databases checks"** (purpose limitation)
- **SIS, VIS and EES will still have to be checked… Hence "traditional" biometrics (as legally standardized) are still required**.

11

National NFP laws should be proportionate

- Personal data shall be: (Art. 5 GDPR)
  - processed lawfully, fairly and in a transparent manner
  - collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes **('purpose limitation')**
  - adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed **('data minimisation')**;
  - accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay **('accuracy')**;
  - kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed **('storage limitation')**;
  - processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures **('integrity and confidentiality')**.
- The controller shall be responsible for, and be able to demonstrate compliance these principles **('accountability')**.

12

Proportionality applied to biometrics (1)

- Opinion 3/2012 of WP29

- "The use of biometrics raises the issue of proportionality of each category of processed data in the light of the purpose for which the data are processed. **As biometric data may only be used if adequate, relevant and not excessive, it implies a strict assessment of the necessity and proportionality of the processed data and if the intended purpose could be achieved in a less intrusive way**.
  - 1) In analysing the proportionality of a proposed biometric system **a prior consideration is whether the system is necessary to meet the identified need**, i.e. is essential for satisfying that need rather than being the most convenient or cost effective.
  - 2) **A second factor to take into consideration is whether the system is likely to be effective in meeting that need** by having regard to the specific characteristics of the biometric technology planned to be used .
  - 3) **A third aspect to weigh is whether the resulting loss of privacy is proportional to any anticipated benefit. If the benefit is relatively minor, such as an increase in convenience or a slight cost saving, then the loss of privacy is not appropriate**.
  - 4) The fourth aspect in assessing the adequacy of a biometric system is to **consider whether a less privacy intrusive means could achieve the desired end**"

13

Proportionality applied to biometrics (2)

- Opinion 3/2012 of WP29: *"Whenever it is permitted to process biometric data, **it is preferred to avoid the centralised storage** of the personal biometric information".*

- *"Especially for verification, the Working Party considers **advisable that biometric systems are based on the reading of biometric data stored** as encrypted templates **on media that are held exclusively by the relevant data subjects** (e.g. smart cards or similar devices). **Their biometric features can be compared with the template(s) stored on the card and/or device by means of standard comparison procedures that are implemented directly on the card and/or device in question**, whereby the creation of a database including biometric information should be, in general and if possible, avoided. Indeed, if the card and/or device is lost or mislaid, there are currently limited risks that the biometric information they contain may be misused. To reduce the risk of identity theft, limited identification data related to the data subject should be stored in such devices".*

14

Data minimisation applied to biometrics (1)

- Opinion 3/2012 of WP29
- *"**Biometric data should be stored as biometric templates whenever that is possible**. **Template should be extracted in a way that is specific to that biometric system and not used by other controllers of similar systems** in order to make sure that a person can only be identified in those biometric systems that have a legal basis for this operation".*
- Goal is to avoid illegitimate interoperability.

15

Data minimisation applied to biometrics (2)

- Opinion 3/2012 of WP29 concerning the size of biometric templates
- ***"The definition of the size (the quantity of information) of the template is a crucial issue**. On the one hand, the size of the template should be wide enough to manage security (avoiding overlaps between different biometric data, or identity substitutions), on the other hand, the size of the template should not be too large so as to avoid the risks of biometric data reconstruction.*
- ***The generation of the template should be a one-way process**, in that it should not be possible to regenerate the raw biometric data from the template".*

16

Accuracy applied to biometrics

- Opinion 3/2012 of WP29 recommends anti-spoofing mechanisms

- "To maintain the reliability of a biometric system and prevent identity fraud, **the manufacturer has to implement systems aiming to determine if the biometric data is both genuine and still connected to a natural person**. In respect of facial recognition, it may be critical to ensure that the face is a real one and not, for example, a picture tied on an impostor's head".

17

Storage limitation applied to biometrics

- Opinion 3/2012 of WP29 recommends automated data erasure mechanisms

- *"In order to prevent that biometric information are stored for longer than is necessary for the purposes for which they were collected or subsequently processed,* ***appropriate automated data erasure mechanisms have to be implemented*** *also in case the retention period may be lawfully extended,* ***assuring the timely deletion of personal data that become unnecessary for the operation of the biometric system****. When using integrated storage on the reader, manufacturers may also implement storage of the biometric templates on volatile memory that guarantees that the data will be erased when the reader is unplugged. Therefore no biometric database remains when the reader is sold or uninstalled. Anti-pulling switches may also be used to automatically erase the data if someone tries to steal the reader".*

18

Security applied to biometrics

- Opinion 3/2012 of WP29
- *"The biometric system used and the security measures chosen should limit the mentioned risks and make sure that the re-use of the biometric data in question for further purposes is impossible or at least traceable.* ***Mechanisms based on cryptographic technologies****, in order to prevent the unauthorised reading, copying, modification or removal of biometric data should be used".*
- *"****When the biometric data are stored on a device that the data subject physically controls, a specific encryption key for the reader devices should be used*** *as an effective safeguard to protect these data from unauthorised access".*

19

Thank you!

http://projectprotect.eu

Franck Dumortier
franck.dumortier@unamur.be

I.2 Frank Schmalz's presentation

PROTECT

VERIDOS
IDENTITY SOLUTIONS
by Giesecke+Devrient
and Bundesdruckerei

The PROTECT EU Research & Innovation Project

Enabling faster and more convenient border crossing

Computers, Privacy and Data Protection 2018
January, 25th, 2018

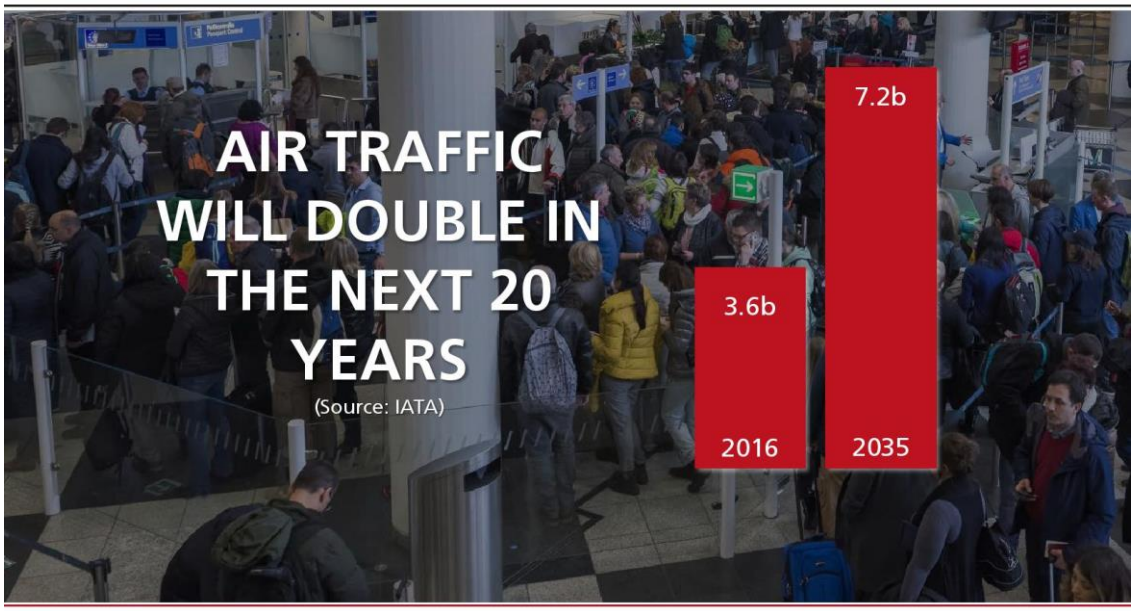
Frank Schmalz

European Commission

This project has received funding from the European Research Council (ERC) under the European Union's Horizon 2020 research and innovation programme (grant agreement n° 700259)

Background

VERIDOS
IDENTITY SOLUTIONS
by Giesecke+Devrient
and Bundesdruckerei



Two ways to address the challenge

VERIDOS IDENTITY SOLUTIONS by Giesecke+Devrient and Bundesdruckerei

MORE SPACE

INCREASING SPACE AT AIRPORTS IS DIFFICULT

Two ways to address the challenge

VERIDOS IDENTITY SOLUTIONS by Giesecke+Devrient and Bundesdruckerei

MORE SPACE

SPEED UP

INCREASING SPEED REQUIRES NEW APPROACHES

The Call BES-6

European Commission | Horizon 2020 European Union funding for Research & Innovation

VERIDOS Identity Solutions by Giesecke+Devrient and Bundesdruckerei

Secure societies –
Protecting freedom and security of Europe and its citizens BES-6

Exploration of new biometric modalities at borders

A most fluent non-intrusive control process is desired

Embrace the related ethical, societal and data protection aspects

The Successful Proposal: Protect

VERIDOS Identity Solutions by Giesecke+Devrient and Bundesdruckerei

A consortium of 10 partners from 6 countries:

PROTECT

Industry
VERIDOS Identity Solutions by Giesecke+Devrient and Bundesdruckerei

End users
The polish border guard
Home Office

Academic research
University of Reading
UNIVERSITÄT SALZBURG
UNIVERSITÉ DE NAMUR
WAT

Applied research
EURECOM

Consultancy
iTTi e-technologie i biznes
Intrepid Minds The art of the possible

Exploration of new biometric modalities

VERIDOS IDENTITY SOLUTIONS by Giesecke+Devrient and Bundesdruckerei

Protect - Public January 2018 Slide 7 of 15

PROTECT focuses on two border crossing scenarios

VERIDOS IDENTITY SOLUTIONS by Giesecke+Devrient and Bundesdruckerei

Protect - Public January 2018 Slide 8 of 15

How to gain speed…

VERIDOS
IDENTITY SOLUTIONS
by Giesecke+Devrient and Bundesdruckerei

SCENARIO A

AIR & SEA BORDER

INDIVIDUALS
ON THE MOVE

Protect - Public January 2018 Slide 9 of 15

How to gain speed…

VERIDOS
IDENTITY SOLUTIONS
by Giesecke+Devrient and Bundesdruckerei

READING DOCUMENT 5-6S

VERIFYING DOCUMENT

BACKGROUND CHECKS

FACE RECOGNITION

GATE MECHANICS UP TO 10S

Protect - Public January 2018 Slide 10 of 15

Two ways to save time in the ABC process

VERIDOS IDENTITY SOLUTIONS by Giesecke+Devrient and Bundesdruckerei

REDUCE READING TIME

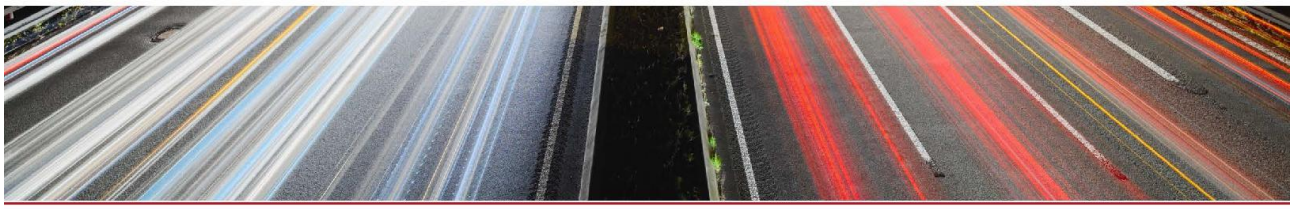
NEW DATA TRANSMISSION METHODS

USE OF MOBILE DEVICES

REMOVE MECHANICS

NO MOVING PARTS

RECOGNITION ON THE MOVE



Protect - Public January 2018 Slide 11 of 15

Enrollment (once)

VERIDOS IDENTITY SOLUTIONS by Giesecke+Devrient and Bundesdruckerei

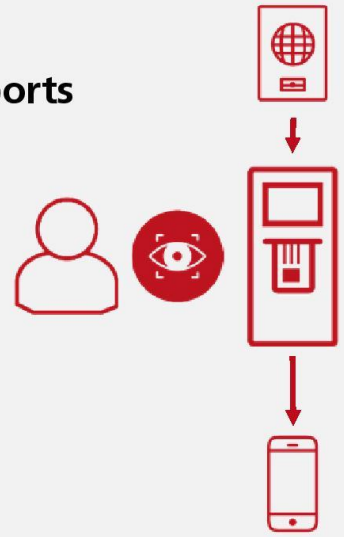
Enrollment could be required once per document lifetime

Kiosk could be located at foreign airports

Traveller enrolls at a special kiosk

Additional biometrics are enrolled

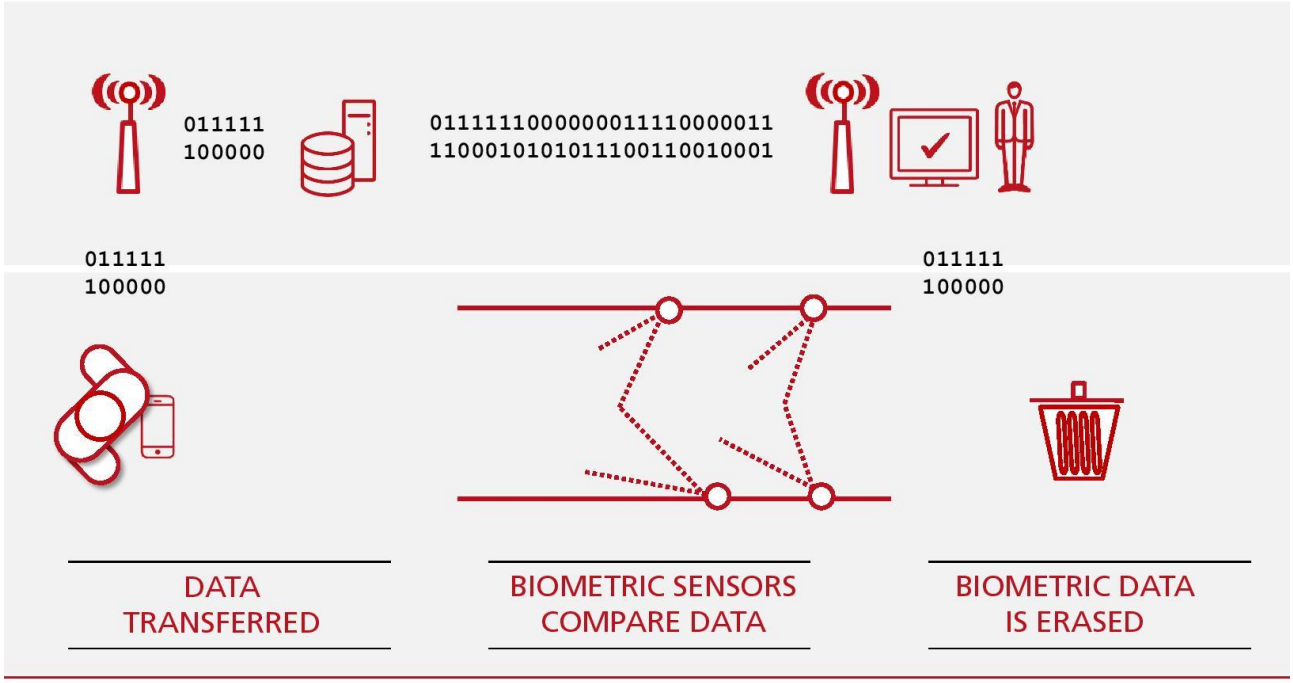
Data is stored on the mobile



Protect - Public January 2018 Slide 12 of 15

Mobile scenario

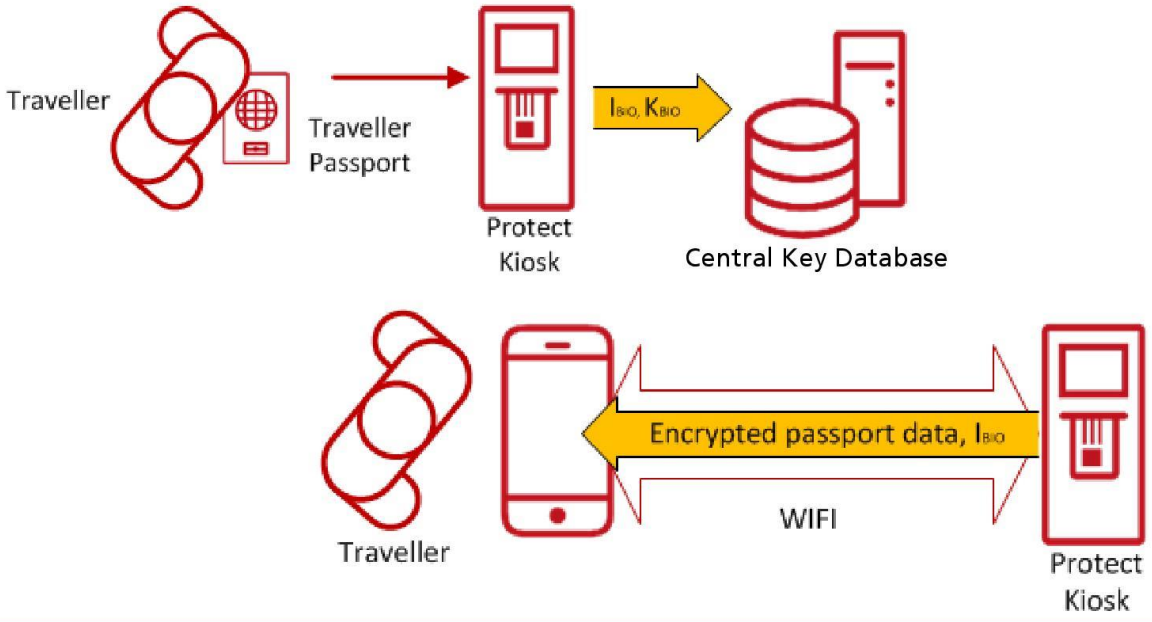
VERIDOS IDENTITY SOLUTIONS by Giesecke+Devrient and Bundesdruckerei



Protect - Public January 2018 Slide 13 of 15

Secure Storage on arbitrary smartphone

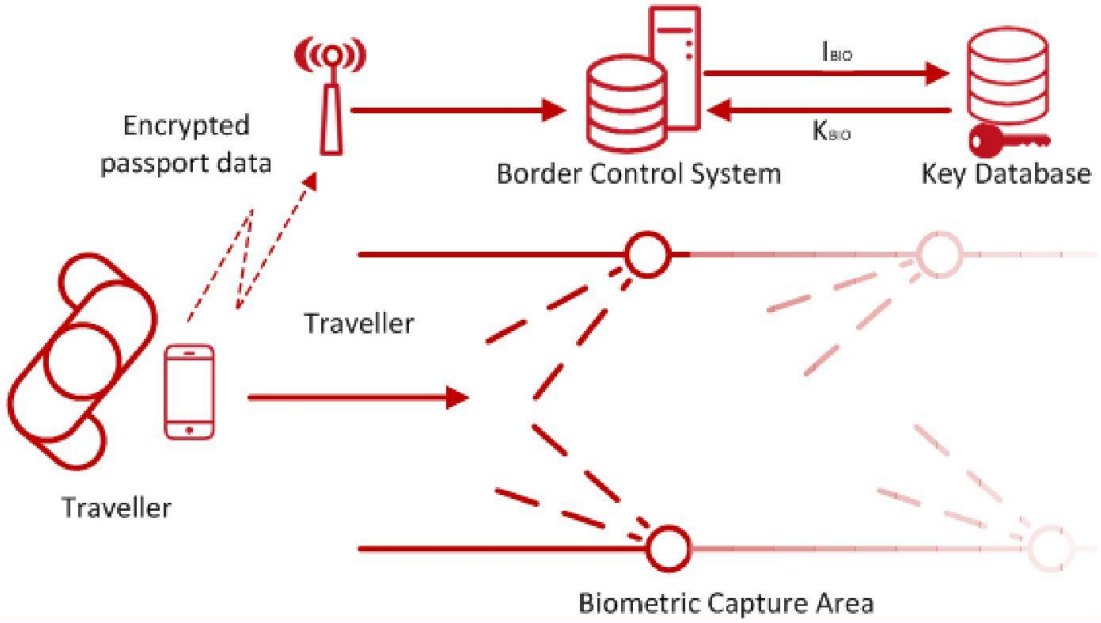
VERIDOS IDENTITY SOLUTIONS by Giesecke+Devrient and Bundesdruckerei



Protect - Public January 2018 Slide 14 of 15

Approaching the border

VERIDOS
IDENTITY SOLUTIONS
by Giesecke+Devrient and Bundesdruckerei



Protect - Public January 2018 Slide 15 of 15

Thank you for your attention!

VERIDOS
IDENTITY SOLUTIONS
by Giesecke+Devrient and Bundesdruckerei

PROTECT

VERIDOS
IDENTITY SOLUTIONS
by Giesecke+Devrient and Bundesdruckerei

Frank Schmalz
Director Innovation
Frank.Schmalz@veridos.com

This project has received funding from the European Research Council (ERC) under the European Union's Horizon 2020 research and innovation programme (grant agreement n° 700259)

European Commission

Pervasive and UseR Focused BiomeTrics BordEr ProjeCT

(PROTECT)

H2020 – 700259

Security Sensitivity Assessment

Publication number:	D2.5
Publication title:	Societal impact report (version 1)
Publication type:	Deliverable
Related WP number:	WP2
Which conference/journal, etc.	
Dissemination level: (Confidentiality)	PU
Version reviewed:	1.1
Date:	27/02/2018

Objective

This form is related to the Security Sensitivity Assessment procedure which will assure that no sensitive information will be included in the publications and deliverables of the PROTECT project.

Security sensitive information means here all information in whatever form or mode of transmission that is classified by Council Decision on the security rules for protecting EU classified information (2011/292/EU) and all relevant national laws and regulations. The information can be already classified, or such that it should be classified.

In practice the following criteria is used:

- Information is already classified
- Information may describe shortcomings of existing safety, security or operating systems
- Information is such, that it might be misused.
- Information that can cause harm to
    - European Union
    - a Member State
    - society
    - industry and companies
    - third country
    - citizen or an individual person of a country.

Document Information

Project Number	H2020 - 700259	**Acronym**	PROTECT
Full Title	Pervasive and UseR Focused BiomeTrics BordEr ProjeCT		
Project URL	http://www.projectprotect.eu/		
Document URL			
EU Project Officer	Agnieszka Marciniak		

Authors (names and affiliations)	Franck Dumortier UNAMUR

Assessment form for the main author

Please fill in the form below:

This is: *pre-assessment* ☐ *final assessment* X

***List the input material used in the publication/deliverable*:**

This first version of D2.5 – "Societal impact report" – contains a summary of ethical and legal discussions held during 3 different events:

1. A meeting "on the impact of privacy regulations on system architecture & technical solutions" which was organized on 4th July 2017 at the University of Reading. The objective of this meeting was for UNAMUR to present to the other partners the implications of the General Data Protection Regulation (GDPR) on the processing of biometric data in the context of border control;
2. A first ELAG meeting which took place at University of Reading on July 5th 2017. The objective of that meeting was to discuss the ethical and legal implications of a potential scenario implementing the PROTECT solution taking into account existing and forthcoming EU regulations in the field of border control and data protection;
3. A PROTECT panel at the 11th International conference on computers, privacy and data protection (CPDP2018) organized by UNAMUR and which took place on January 25th in Brussels. This panel was entitled "privacy and data protection issues related to the use of contactless multimodal biometrics at border-crossings" and was the opportunity to share some views with important actors such as the European Data Protection Supervisor (EDPS) and the JHA Counsellor at the Permanent Representation of Finland to the EU.

***List the results developed and presented in the publication/deliverable*:**

This deliverable contains a summary of the discussions mentioned at the 3 events mentioned above.

The draft publication

X is attached to this statement

☐ can be found in link:

This publication does not include any data or information that could be interpreted as security sensitive.

X True

☐ Not sure

If not sure, please specify what are the material / results that you are not sure if they are security sensitive? Why?

Date: 28/02/2018

Signature of the Responsible Author:

Comments from the SAB member

X The publication can be published as it is.

Comments:

☐ Before publication the following modifications are needed:

-
-

Date	February 27th, 2018
Name: **On behalf of the Security Advisory Board (SAB)**	Jürgen Bonfert
Signature of the member of the SAB