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

D2.3 Privacy impact of next-generation biometric border control

Author: Franck Dumortier (UNAMUR)

Deliverable nature:	Report
Dissemination level: (Confidentiality)	PU
Version:	1.1
Date:	31/08/2018
Keywords:	Privacy, purpose limitation, data protection, sensitive data, explicit consent ,data security, data protection impact assessment

Executive summary

This document is Deliverable D2.3 of Task T2.4, WP2 – Privacy of the PROTECT project. The aim of D2.3 is to analyse whether the PROTECT project entails a potential substantial interference into individuals' rights to privacy and to data protection, as protected under articles 7 & 8 of the Charter of Fundamental Rights, and if so to manage the identified risks to these rights of data subject by proceeding to an impact assessment. As a reminder, the PROTECT project implies the collection and storage of emerging biometric data of a huge number of "bona fide" travellers (in addition to the biometric data already collected and stored in the travel documents and the IT databases which were described in D2.2 – Legal framework of biometric border control).

In D2.2, it was assumed that the purpose of the PROTECT system was to "facilitate" public border control authorities to speed up their public interest missions of border control management by enrolling emerging biometrics in travel documents (or smartphone apps acting as travel documents) in addition to passport information (including traditional biometric modalities: facial image and fingerprints). However, the main conclusion of D2.2 was that the abovementioned scenario should certainly be considered as beyond the scope of current EU legislation. One of the main reasons for D2.2's conclusion is that consent of travellers cannot legally be considered as a legitimate basis of lawfulness under the GDPR to allow public border control authorities to speed up their public interest missions by enrolling additional biometrics in travel documents (which currently may not be replaced by a smartphone app). This finding of illegality of D3.1 scenarios in "real-world conditions" does not oppose the goals of the demonstration phase of the PROTECT project. Trials conducted exclusively for research purposes could demonstrate the feasibility of combining passport information (including traditional biometrics) and additional contactless biometrics of volunteers, with their explicit consent, with the aim of matching their identities against fictional (emulated) "watchlists" specifically developed for these scientific trials. The data protection safeguards of such trials (such as consent forms and security requirements) will be described in a future version of D2.1 – "Data management Plan".

The purpose of this Deliverable "D2.3 - Privacy impact of next-generation biometric border control" is to analyse whether, as an alternative to D3.1 scenarios, emerging biometric modalities could be processed in a "passport companion", such as a smartphone for "comfort and convenience purposes" of travellers, on the basis of a contract with the PROTECT's data controller and travellers' explicit consent. The idea is to analyse − from a privacy and data protection point of view − the possibility and the conditions in real-world conditions to enrol emerging biometrics in a smartphone app for travellers willing to join a "PROTECT programme" allowing them to be given priority in waiting areas for "traditional" security and border checks and/or allowing them to benefit from additional conveniences such as access to VIP parking zones or waiting lounges. In order to carry out this analysis, this Deliverable performs a Data Protection Impact Assessment (DPIA) which is required by Article 35 of the GDPR. A DPIA is a process designed to describe the processing, assess its necessity and proportionality, and help manage risks to the rights and freedoms of natural persons resulting from the processing of personal data, by assessing the risks and determining the measures to address them. In this Deliverable, the methodology which was chosen to conduct this DPIA is based on the one which was developed by the French Data Protection Authority (CNIL) in February 2018.

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**	M24	**Actual**	M24

Authors (names and affiliations)	**Franck Dumortier (UNAMUR)**

Reviewers (names and affiliations)	**Krzysztof Romanowski (ITTI)**

Version Log			
Issue Date	**Rev. No.**	**Author**	**Change**
17/08/2018	V1.0	Franck Dumortier	
29/08/2018	V1.1	Catherine Moss	Minor editing changes.

Table of Contents

List of figures

List of tables

Abbreviations

BCA	Biometric Capture Area
CFR	Charter of Fundamental Rights
DPIA	Data Protection Impact Assessment
ECHR	European Convention of Human Rights
ECtHR	European Court of Human Rights
ECJ	European Court of Justice
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
SBC	Schengen Border Code
SIS	Schengen Information System
TCN	Third-Country National
TCNVE	Third-Country National Visa exempted
TCNVH	Third-Country National Visa holder
WP29	Article 29 Working Party
PROTECT	Pervasive and UseR Focused BiomeTrics BordEr ProjeCT

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.

Biometric Capture Area (BCA): a short corridor with biometric sensors that capture biometric modalities on the move.

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.*

Biometric template: Key features can be extracted from the raw form of biometric data (e.g. facial measurements from an image) and stored for later processing rather than the raw data itself. This forms the biometric template of the data. 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.

Biometric enrolment: Encompasses all the processes that are carried out within a biometric system in order to extract biometric data from a biometric source and link this data to an individual. The quantity and the quality of data required during enrolment should be sufficient to allow for his/her accurate identification, authentication, categorization or verification without recording excessive data. The amount of data extracted from a biometric source during the enrolment phase has to be adequate for the purpose of the processing and the level of performance of the biometric system.

Biometric storage: The data obtained during enrolment can be stored locally in the operations centre where the enrolment took place (e.g. in a reader) for later use, or on a device carried by the individual (e.g. on a smart card) or could be sent and stored in a centralized database accessible by one or more biometric systems.

Biometric matching: The comparison of a reference template against a verification template extracted from acquired sensor data (e.g. image to image match).

Biometric identification: The identification of an individual by a biometric system is typically the process of comparing biometric data of an individual (acquired at the time of the identification) to a number of biometric templates stored in a database (i.e. a one-to-many matching process).

Biometric verification/authentication: The verification of an individual by a biometric system is typically the process of comparing the biometric data of an individual (acquired at the time of the verification) to a single biometric template stored in a device (i.e. a one-to-one matching process).

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

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 prioritized. The reform will allow European citizens and businesses to fully benefit from the digital economy.

Multi-modal biometrics: They can be defined as the combination of different biometric technologies to enhance the accuracy or performance of the system (it is also called multilevel biometrics). Biometric systems use two or more biometric traits / modalities from the same individual in the matching process. These systems can work in different ways, either collecting different biometrics with different sensors or by collecting multiple units of the same biometric.

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 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.

Source of biometric data: The source of biometric data can vary widely and includes physical, physiological, behavioural or psychological elements of an individual. According to the Article 29 Working Party: "the

sources of biometric data (e.g. human tissue samples) cannot be considered as biometric data themselves but can be used for the collection of biometric data (through the extraction of information from them)".

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

As a reminder, the aim of D2.2 was to explore the current and proposed European legal framework regulating both biometric border control and personal data protection in order to identify the legal constraints which should be taken into account by the scenarios being defined in D3.1. In D2.2, it was assumed that the purpose of the PROTECT system was to "facilitate" public border control authorities to speed up their public interest missions of border control management by enrolling emerging biometrics in travel documents (or smartphone apps acting as travel documents) in addition of passport information (including traditional biometric modalities – facial image and fingerprints). By consequence, D2.2 was dedicated to analyse the hereunder main legal questions and resulted in the following findings:

1) Under current EU law, is there a possibility for electronic machine-readable documents to support an enhanced set of contactless biometrics? In other words, could emerging biometrics (other than facial image and fingerprints) be included in travel documents under current EU law?

   Answer: Under current EU Regulation, 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 (or residence permits) without a national legislation of a Member State allowing it. Furthermore, even if a national law would allow such integration of additional biometrics, it would certainly be challenged in Court for privacy reasons related to proportionality and data minimization.

2) Under current EU law, could a smartphone be considered as a travel document to support traditional biometrics (fingerprints and facial image) as well as an enhanced set of contactless biometrics?

   Answer: Under current EU law, it seems very doubtful that mobile devices such as smartphones could legally be used to replace travel documents as a result of strict rules regulating the materials of travel documents. In other words, smartphones cannot be considered as "travel documents" under current EU law and therefore cannot support traditional biometrics (fingerprints and facial image) as well as an enhanced set of contactless biometrics for the purpose of border control management.

3) Under current EU law, could consent of a traveller be the legal basis to enrol additional biometrics in a travel document for "government use of their personal data"?

   Answer: Recital 43 of the GDPR 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 it seems that consent of travellers cannot be considered as a legitimate basis of lawfulness in PROTECT scenarios to allow public border control authorities to speed up their public interest missions by enrolling additional biometrics in travel documents.

4) Under current EU law, which constraints related to the entry/exit external border checks for both persons enjoying the EU right to free movement and TCNs should be taken into account by the PROTECT scenarios?

   Answer: Both for persons enjoying the EU right to free movement and for TCNs, the travel document must be presented for verification at each entry/exit of the Schengen area. For this reason, it is very doubtful that the passport scenario at land border crossing points described in D3.1 which envisages to transmit passport data via a mobile application could be considered as legal under current EU border control regulation since that that travel documents must be presented at each entry/exit of the Schengen area.

5) Under current EU law, which constraints should be taken into account by the PROTECT scenarios when making use of technologies such as self-service systems, eGates and automated border control systems?

   Answer: Both for persons enjoying the EU right to free movement and for TCNs, it seems very doubtful that automated border checks could be operated on the basis of "additional biometrics" (other than fingerprints or facial image). Indeed, for persons enjoying the EU right to free movement article 8(2) of the SBC explicitly states that "*where there are doubts as to the authenticity of the travel document or the identity of its holder, at least one of the biometric identifiers integrated into the passports and travel documents issued in accordance with Regulation (EC) No 2252/2004 shall be verified".* As for TCNs, According to article 8b of the SBC, one of the conditions for persons whose border crossing is subject to a registration in the EES to be permitted to use automated border control systems is that *"the travel document contains a facial image recorded in the electronic storage medium (chip) which can be technically accessed by the self-service system so as to verify the identity of the holder of the travel document, by comparing that facial image with his or her live facial image"*. For this reason, and according to the data minimization principle, it seems legally doubtful to use additional biometrics (other than facial image – and in certain cases fingerprints) for the aforementioned purpose.

6) Under current EU law, which checks against databases should be taken into account by the PROTECT scenarios and which legal constraints derive from these in relation to the development of a contactless solution?

   Answer: Under current EU law, checks which should be taken into account at external border crossings are mainly the ones against the SIS, SLTD, VIS, EES, EURODAC (and the proposed ETIAS) databases as well as the API framework. An overview of the legal constraints related to this background is provided in Section 4 of Deliverable 2.2. Currently, one of the main legal constraints to take into account when developing a "full" contactless solution is that the VIS is used to verify the identity of visa holders by comparing his/her fingerprints with the fingerprints stored in the VIS on request of the border guards. The fact that TCNVHs could be required to provide their fingerprint at the entry of the Schengen Area should be taken into account when developing a complete contactless biometric-based cross-border control solution. The use the facial image for biometric matching against the VIS has not yet been implemented. This issue could be resolved once the EES becomes functional and TCNVHs would be able to pre-enrol their facial image into that system.

7) Does the PROTECT scenarios fit in with the EU's own future border control plans, in particular the EC's proposal for a Regulation on establishing a framework for interoperability between EU information systems?

   Answer: The EC's proposed shared biometric matching service confirms the intention of the European Council of Thessaloniki to develop a coherent approach on biometric identifiers or biometric data for documents for third country nationals, European Union citizens' passports and information systems.[1] Fingerprints and facial images are increasingly being promoted by the EU as the biometric features which should be used in both travel documents and in border control management databases to enhance the tasks of border guards. For this reason, the enrolment of additional biometric features (other than fingerprints or facial image) in travel documents for the purpose of "facilitating" border control processes, as described in D3.1, should be considered as being in contradiction with the data minimization principle enshrined in article 5(c) of the GDPR, which reads as follows: "personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed". Therefore, for the purposes of D3.1 scenarios, it is recommended to PROTECT technical partners to only focus on the development of

[1] The Presidency conclusions of the Thessaloniki European Council of 19 and 20 June 2003 are available at http://data.consilium.europa.eu/doc/document/ST-11638-2003-INIT/en/pdf

"emerging" biometric features which could update current facial image standards, for example 2D face, iris, periocular and 3D face.

As a result of the answers to the aforementioned questions, the main conclusion of D2.2 was that the scenarios proposed by D3.1 should certainly be considered as beyond the scope of current legislation. One of the main reasons of this negative conclusion is that consent of travellers cannot be considered legitimate under the GDPR, to allow public border control authorities to speed up their public interest missions by enrolling additional biometrics in travel documents (which currently may not be replaced by a smartphone app).

This conclusion that the purpose of the PROTECT system, as defined by D3.1, should be considered non-compliant with EU norms regulating both travel documents and data protection has fundamental consequences on the work to be performed in this Deliverable "D2.3 - Privacy impact of next-generation biometric border" control. Indeed, Article 5, 1(b) of the GDPR lists the purpose limitation principle among the key data protection principles. It provides that personal data must be "collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes". Specification of purpose is thus an essential first step in applying data protection laws and designing data protection safeguards for any processing operation. Indeed, specification of the purpose is a pre-requisite for applying other data quality requirements, including the adequacy, relevance, proportionality and accuracy of the data collected and the requirements regarding the period of data retention. The most crucial issue is that Article 5, 1(b) imposes the purpose to be *legitimate*. This notion goes beyond the requirement to have a legal ground for the processing under Article 6 of the GDPR and also extends to other areas of law, such as norms regulating travel documents (which were analysed in D2.2)[2].

For this reason, this Deliverable analyses whether, as an alternative to D3.1 scenarios, emerging biometric modalities could be processed in a "passport companion" such as a smartphone for "comfort and convenience purposes" of travellers on basis of a contract and explicit consent. The idea is to analyse – from a privacy and data protection point of view – the possibility and the conditions to enrol contactless biometrics in a smartphone app for travellers willing to join a "PROTECT programme". This would allow them priority in waiting areas for "traditional" security and border checks and/or allow them to benefit from additional convenience services such as access to VIP parking zones or waiting lounges. Such a purpose seems legitimate since, in a consultation of 2005, the CNIL (the French Data Protection Authority) authorized the use of fingerprints on a chip card for frequent travellers of the airport of Nice.[3] The system, as no password was required, was designed for convenience purposes of the travellers ("faciliter la vie"). The CNIL accepted such a system based on these two criteria: the voluntary use (the free choice of the data subject) and the storage on a local object on which the data subject has control.

1.1 Scenario being analysed in this deliverable

The purpose of the scenario being analysed in this Deliverable differs from those described in D3.1 in that it does not aim to allow public border control authorities to speed up their public interest missions, but instead processes emerging biometrics of frequent travellers in order to allow them to benefit from "convenience

[2] This finding of illegality in "real-world conditions" does not oppose to the fact that in the demonstration phase of the PROTECT project, and exclusively for research purposes, trials could demonstrate the feasibility of combining passport information (including traditional biometrics) and additional contactless biometrics of volunteers on the basis of their explicit consent with the aim to match their identities against fictional (emulated) "watchlists" specifically developed for these scientific trials. The data protection safeguards of such trials (such as consent forms and security requirements) will be described in a future version of D2.1 – "Data management Plan".

[3] Délibération 2005-115 du 07 juin 2005 portant autorisation de la mise en oeuvre par la Chambre de Commerce et d'Industrie de Nice-Côte d'Azur d'un traitement automatisé de données à caractère personnel ayant pour finalité la gestion d'une carte de fidélité impliquant l'utilisation d'un dispositif biométrique de reconnaissance des empreintes digitales - http://data.socnum.com/2005/06/07/deliberation-2005-115-du-07-juin-2005/

services" having no link with public interest missions. Also, for pragmatic reasons, it was decided to only legally analyse our "passport companion" scenario (for convenience purposes) at an air or sea border (whereby travellers are walking on-the-move). The main reason is that the aim of this deliverable is to provide an example of how to fill in the CNIL's Data Protection Impact Assessment (DPIA) methodology, and that this document would be too lengthy if different scenarios had to be analysed.

This being said, the system would be mainly composed of an Enrolment Kiosk, a Biometric, Capture Area (BCA), a smartphone app ("the Passport Companion") and a PROTECT Control System as illustrated in the figure below.

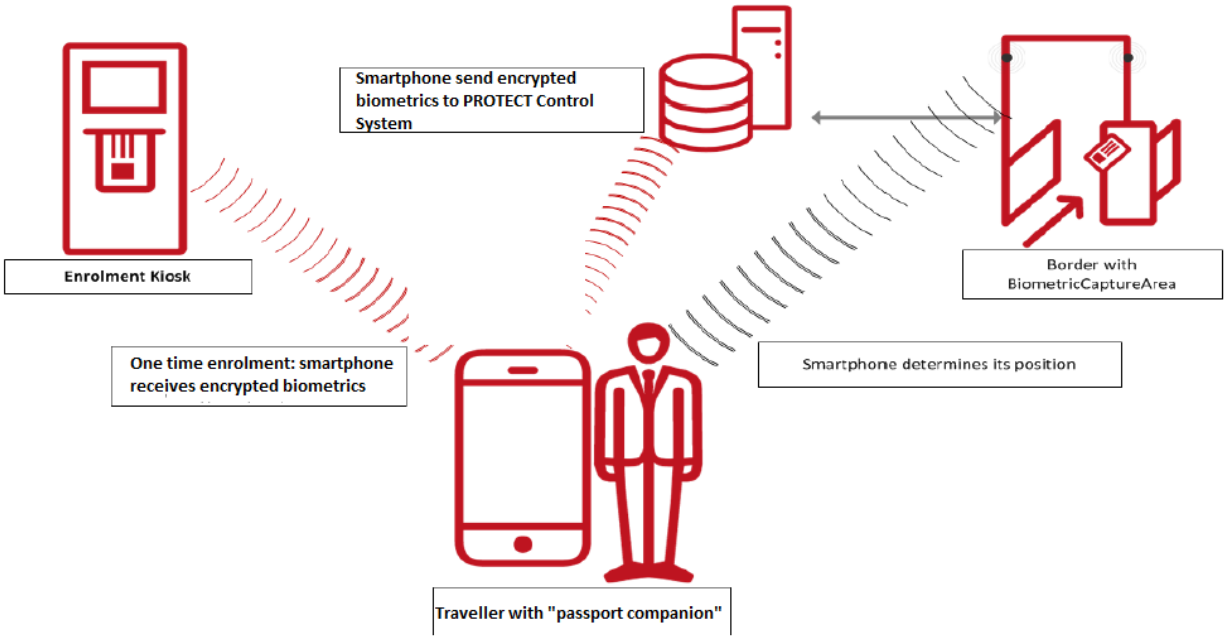


Figure 1 - General overview of the PROTECT system

1.1.1 Enrolment Kiosk

The enrolment begins by the traveller presenting a passport to authorized staff of the PROTECT programme. After the traveller's identity is verified and he has signed the PROTECT programme contract, the traveller is directed to an enrolment kiosk under supervision of authorized staff where he proceeds to supply a set of biometrics including face, hand veins, voice (speaker utterance) and anthropometrics. Finally, these biometrics are encrypted and sent to the traveller's PROTECT application on the mobile phone.

1.1.2 The Passport Companion

The smartphone application ("passport companion") has to communicate with two external systems: the Enrolment Kiosk (in order to receive the necessary set of encrypted biometrics) and the PROTECT Control System (in order to achieve both decryption of the biometrics and to perform user position tracking). The transmission with the Enrolment Kiosk and the PROTECT Control System is achieved using the IEEE 802.11 protocol (WIFI). This technology was chosen due to its high speed transmission rates and nearly 100% smartphone market coverage. At the Enrolment Kiosk, encrypted biometrics are downloaded onto the device, while at the PROTECT Control Station the same data is uploaded into a temporary storage. To ensure connection security, the WIFI will use the WPA2 encryption standard. The HTTPS-Protocol will be used to exchange data packages between the application and the servers of the PROTECT Control Station. Long range proximity measurement is also done using IEEE 802.11 protocol. All PROTECT Control-WIFIs will use the same

SSID, which are also indicating that it is an "AirSeaBorder-Station". The application is able to detect nearby PREOTECT Control Stations by constantly checking for networks in range that are broadcasting the PROTECT Control System SSID. The connection would incorporate SSL, and hence, the "passport companion" application will only connect to WIFIs that are valid (i.e., valid PROTECT Control-WIFI). Position tracking is done via Bluetooth Low Energy (BLE). The Biometric Capture Area sends iBeacon signals that are interpreted by the phone app. BLE is available on every modern mobile phone.

1.1.3 Biometric Capture Area (BCA)

The Biometric Capture Area has as its main objective the identification of a traveller at the border entry while they are on the move. The traveller passes through a physical 3D space equipped with sensors able to extract a set of biometrics. In order to enhance security levels, the PROTECT Biometric Capture Area incorporates a multimodal set of contactless biometrics, including 2D and 3D face, iris, periocular, finger vein, speaker recognition and anthropometrics. The Biometric Capture Area solution addresses the process of "on the move" traveller identification. In other words, different biometrics are successively acquired as a traveller passes through the Biometric Capture Area and traveller verification is performed via multimodal biometric fusion by the time the traveller reaches the end of the Biometric Capture Area.

The BCA works in conjunction with a mobile application (the "Passport Companion") that can be installed on a mobile phone and with the PROTECT Control System.

1.1.4 The PROTECT Control System

The main goal of the PROTECT Control System is to perform the verification process. The process starts with the person approaching the Biometric Capture Area. The encrypted biometric templates of the traveller are transmitted to the PROTECT Control System (the "passport companion" installed on the traveller's mobile device is used to transmit in an encrypted way via WIFI the biometric templates to the PROTECT Control System). As the traveller enters the walking corridor in the Biometric Capture Area, two main operations are triggered: Person tracking through re-identification (re-identification system), and biometrics verification (including Anthropometrics, Face and Periocular). Person tracking through re-identification is not a biometric *per se*, but supports the biometric verification by providing an identifier to the person entering the Biometric Capture Area. It then tracks the location of the person moving through the Biometric Capture Area so that the biometric verification can be reduced from a 1:m match to a 1:few or even 1:1 match. The PROTECT Control system communicates with the biometric verification system to feed forward the biometric template of the individual moving through the Biometric Capture Area. The Border Control system also communicates with the re-identification system to associate a person identifier number and its corresponding biometric template. Once each biometric is verified, the final decision on identity acceptance/rejection is performed fusing all individual biometric evaluations.

1.2 Purpose of the document

This document is Deliverable D2.3 of Task T2.2, WP2 – Privacy of the PROTECT project. The aim of D2.3 is to analyse if, as an alternative to D3.1 scenarios, emerging biometric modalities could be processed in a "passport companion" such as a smartphone for "comfort and convenience purposes" of travellers on basis of a contract with the PROTECT's data controller and their explicit consent. The idea is to analyse − from a privacy and data protection point of view − the possibility and the conditions in real-world conditions to enrol emerging biometrics in a smartphone app for travellers willing to join a "PROTECT programme", which would give them priority in waiting areas for "traditional" security and border checks and/or allow them to benefit of additional convenience services such as access to VIP parking zones or waiting lounges. In order to carry out this analysis, this Deliverable performs a Data Protection Impact Assessment (DPIA), which is required by Article 35 of the GDPR. A DPIA is a process designed to describe the processing, assess its necessity and proportionality and help manage the risks to the rights and freedoms of natural persons resulting from the processing of personal data by assessing them and determining the measures to address them. In this

Deliverable, the methodology which was chosen to conduct this DPIA is based on the one which was developed by the French Data Protection Authority (CNIL) in February 2018.

1.3 Document scope

The document consists of an introduction and four main sections:

- **Section 2** recalls that biometrics are considered as sensitive data by the General Data Protection Regulation (GDPR), presents the Data Protection Impact Assessment (DPIA) requirement, justifies the reason why a DPIA must be carried out for the PROTECT solution and describes the French Data Protection Authority's (CNIL) DPIA methodology;
- **Section 3** applies the CNIL's DPIA methodology to a PROTECT solution which processes contactless biometrics for "convenience purposes". The aim of this section is to create a new category of access-control mechanism particularly suited for border-crossings based on multimodal biometric fusion "on the move" while respecting the legal framework and personal data security.
- **Section 4** provides an overall conclusion.

2 Biometrics and privacy

2.1 Introduction

The rapid progress of biometric technologies and their expanded application in recent years necessitates careful scrutiny from a data protection perspective. Their use in various places of our everyday life is just around the corner. Indeed, biometric data processing is now often used in automated authentication/verification and identification procedures, in particular for the control of entry to both physical and virtual areas (i.e. access to particular electronic systems or services). In 2003, the Article 29 Working Party ("hereafter WP29") stressed that "a wide and uncontrolled utilisation of biometrics raises concerns with regard to the protection of fundamental rights and freedoms of individuals. This kind of data is of a special nature, as it relates to the behavioural and physiological characteristics of an individual and may allow his or her unique identification".[4] As biometric technologies are closely linked to certain characteristics of an individual, some of them can be used to reveal sensitive data. In addition, many of them allow for automated tracking, tracing or profiling of persons and as such their potential impact on the privacy and the right to data protection of individuals is high. This impact is increasing through the growing deployment of these technologies. Every individual is likely to be enrolled in one or several biometric systems.

Hence, since the very beginning of their implementation, biometric systems have been acknowledged to have the potential to raise strong concerns in several fields, including privacy and data protection, which have certainly influenced their social acceptance and fuelled the debate over the legality and limits of their use and the safeguards and guarantees needed to mitigate the identified risks.

2.2 Biometric data are sensitive

In S & Marper v the UK, the ECtHR held that biometric features constitute personal data containing *"certain external identification features"* which contain *"unique information about the individual concerned [sic] allowing his or her identification [to be made] with precision in a wide range of circumstances".*[5] Biometric features hence belong to a special category of more sensitive data.[6] In the same way, the General Data

[4] Article 29 Working Party, Working document on biometrics, WP80, Adopted on 1 August 2003, p.2.
[5] ECtHR, S. & Marper v the United Kingdom, para. 84.
[6] ECtHR, S. & Marper v the United Kingdom, para. 103.

Protection Regulation (GDPR)[7] considers biometric data as personal data being sensitive.[8] In the GDPR, "biometric data" are defined 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 accordance with the GDPR definition, measures of biometric identification or their digital translation in a template form can always be considered as "information relating to a natural person" as it concerns data, which provides, by its very nature, information about a given person.[9] For this reason, the processing of biometric data needs to carefully comply with the data protection principles enshrined in EU and national law.

2.3 Impact on privacy and data protection

In 2012, the Article 29 Working Party recalled that classical reluctance to biometric systems has been linked to the protection of individual rights, and still is. Nevertheless, new systems and developments to existing systems raise a range of concerns.[10] This includes the possibility of covert collection, storage and processing as well as the collection of material with highly sensitive information that can invade the most intimate space of the individual.

The WP29 recalls that "function creep has been a serious concern since the biometric technologies and systems were first used; even though that is a well-known and addressed risk in traditional biometrics, it is undoubtedly clear that the higher technical potential of new computer systems raises the risk of data being used against their original purpose. Covert techniques allow for the identification of individuals without their knowledge, resulting in a serious threat for privacy and a leak of control over personal data. That has serious consequences on their capacity to exercise free consent or simply get information about the processing"[11]. The WP29 also stresses that "taking into account the fact that biometric technologies cannot ensure full accuracy, there is always an implicit risk coming from incorrect identifications. Such false positives result in decisions affecting individual rights. Identity theft based on the use of spoofed or stolen biometric sources can lead to serious damages. Unlike in other identification systems, the individual cannot be simply provided with a new identification just because it is compromised"[12]. Finally, the Working Party states that "reference should be made to profiling in the context of taking automated decisions or to predict behaviour or preferences in a specific situation. Some biometric data can reveal physical information about an individual. This can be used for targeting and profiling purposes but also end up in discrimination, stigmatization or unwanted confrontation with non-expected / desired information".[13]

2.4 The Data Protection Impact Assessment (DPIA) requirement

2.4.1 Introduction

The Article 29 Working Party has always supported the inclusion of a "risk-based approach" in the EU data protection legal framework.[14] It is important to note that – even with the adoption of a risk-based approach

[7] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)

[8] On 4 May 2016, the official texts of the Regulation and the Directive have been published in the EU Official Journal. The GDPR entered into force on 24 May 2016 and applies since 25 May 2018.

[9] Article 29 Working Party, Opinion 4/2007 on the concept of personal data, WP 136, Adopted on 20th June 2007, p. 8.

[10] Article 29 Working Party, Opinion 3/2012 on developments in biometric technologies, WP193, adopted on 27th April 2012, p.17.

[11] Ibidem.

[12] Ibid, p18.

[13] Ibidem.

[14] Article 29 Working party, Statement on the role of a risk-based approach in data protection legal frameworks, WP 218, adopted on 30 May 2014.

– there is no question of the rights of individuals being weakened in respect of their personal data. Those rights must be just as strong even if the processing in question is relatively 'low risk'. Rather, the scalability of legal obligations based on risk addresses compliance mechanisms.

In line with this risk-based approach, the GDPR requires controllers to implement appropriate measures to ensure and be able to demonstrate compliance with the GDPR, taking into account among others the "the risks of varying likelihood and severity for the rights and freedoms of natural persons". The reference to "the rights and freedoms" of data subjects primarily concerns the rights to data protection and privacy but may also involve other fundamental rights such as freedom of speech, freedom of thought, freedom of movement, prohibition of discrimination, right to liberty, conscience and religion.

In consistence with the risk-based approach, Article 35 of the GDPR introduces the concept of a Data Protection Impact Assessment (DPIA). A DPIA is a process designed to describe the processing, assess its necessity and proportionality and help manage the risks to the rights and freedoms of natural persons resulting from the processing of personal data by assessing them and determining the measures to address them. DPIAs are important tools for accountability, as they help controllers not only to comply with requirements of the GDPR, but also to demonstrate that appropriate measures have been taken to ensure compliance with the GDPR. In other words, a DPIA is a process for building and demonstrating compliance. This being said, carrying out a DPIA is not mandatory for every processing operation. A DPIA is only required when the processing is "likely to result in a high risk to the rights and freedoms of natural persons".

In order to ensure a consistent interpretation of the circumstances in which a DPIA is mandatory, the Article 29 Working Party issued guidelines to clarify this notion and provide criteria to help identify the circumstances in which a DPIA is needed[15].

2.4.2 DPIA required for the PROTECT solution

According to the Article 29 Working Party in its WP 248, a DPIA "is particularly relevant when a new data processing technology is being introduced".[16] The Working Party details that a DPIA is required for "innovative use or applying new technological or organisational solutions, like combining use of finger print and face recognition for improved physical access control, etc.". Indeed, Recital 89 of the GDPR states that processing operations needing a DPIA to be carried out "may be those which in, particular, involve using new technologies, or are of a new kind and where no data protection impact assessment has been carried out before by the controller". The GDPR makes it thus clear that the use of a new technology, defined in "accordance with the achieved state of technological knowledge" (recital 91), can trigger the need to carry out a DPIA. This is because the use of such technology can involve novel forms of data collection and usage, possibly with a high risk to individuals' rights and freedoms. Indeed, the personal and social consequences of the deployment of a new technology may be unknown. A DPIA will help the data controller to understand and to treat such risks. To our knowledge, no DPIA has been previously carried out for a technology like that being developed within PROTECT, and which consists of a multimodal biometric solution for identity confirmation "on-the-move" of travellers with the aim to facilitate and speed up their border crossings. Please also note that the UK's data protection authority considers that DPIA must always been carried out when biometric data is planned to be processed.[17]Hence it seems doubtful that a DPIA is required to assess the data protection impact of the technology product being developed in the PROTECT project.

This reasoning will also help the consortium to demonstrate data protection compliance and transparency towards the European Commission.

[15] See Article 29 Working Party, Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679, WP 248 rev.01, adopted on 4 April 2017, last revised and adopted on 4 October 2017

[16] Ibid., p. 8.

[17] See https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-impact-assessments/

2.4.3 General content of the DPIA

The GDPR sets out the minimum features of a DPIA (Article 35(7), and recitals 84 and 90):

- "a description of the envisaged processing operations and the purposes of the processing";
- "an assessment of the necessity and proportionality of the processing";
- "an assessment of the risks to the rights and freedoms of data subjects";
- "the measures envisaged to:
  - "address the risks";
  - "demonstrate compliance with this Regulation".

The figure hereunder of the Article 29 Working Party illustrates the generic iterative process for carrying out a DPIA.

Figure 2 - Process for carrying out a DPIA

2.4.4 Criteria for an acceptable DPIA methodology

The GDPR provides flexibility to determine the precise structure and form of the DPIA to allow it to fit with existing working practices. Different methodologies could be used to assist in the implementation of the basic requirements set out in the GDPR. To standardise these different approaches, common criteria have been identified by the Article 29 Working Party.[18] The criteria listed in the figure below can be used to show that a particular DPIA methodology meets the standards required by the GDPR.

[18] Ibid., p.22.

- ☐ a systematic description of the processing is provided (Article 35(7)(a)):
  - ☐ nature, scope, context and purposes of the processing are taken into account (recital 90);
  - ☐ personal data, recipients and period for which the personal data will be stored are recorded;
  - ☐ a functional description of the processing operation is provided;
  - ☐ the assets on which personal data rely (hardware, software, networks, people, paper or paper transmission channels) are identified;
  - ☐ compliance with approved codes of conduct is taken into account (Article 35(8));
- ☐ necessity and proportionality are assessed (Article 35(7)(b)):
  - ☐ measures envisaged to comply with the Regulation are determined (Article 35(7)(d) and recital 90), taking into account:
    - ☐ measures contributing to the proportionality and the necessity of the processing on the basis of:
      - ☐ specified, explicit and legitimate purpose(s) (Article 5(1)(b));
      - ☐ lawfulness of processing (Article 6);
      - ☐ adequate, relevant and limited to what is necessary data (Article 5(1)(c));
      - ☐ limited storage duration (Article 5(1)(e));
    - ☐ measures contributing to the rights of the data subjects:
      - ☐ information provided to the data subject (Articles 12, 13 and 14);
      - ☐ right of access and to data portability (Articles 15 and 20);
      - ☐ right to rectification and to erasure (Articles 16, 17 and 19);
      - ☐ right to object and to restriction of processing (Article 18, 19 and 21);
      - ☐ relationships with processors (Article 28);
      - ☐ safeguards surrounding international transfer(s) (Chapter V);
      - ☐ prior consultation (Article 36).
- ☐ risks to the rights and freedoms of data subjects are managed (Article 35(7)(c)):
  - ☐ origin, nature, particularity and severity of the risks are appreciated (cf. recital 84) or, more specifically, for each risk (illegitimate access, undesired modification, and disappearance of data) from the perspective of the data subjects:
    - ☐ risks sources are taken into account (recital 90);
    - ☐ potential impacts to the rights and freedoms of data subjects are identified in case of events including illegitimate access, undesired modification and disappearance of data;
    - ☐ threats that could lead to illegitimate access, undesired modification and disappearance of data are identified;
    - ☐ likelihood and severity are estimated (recital 90);
  - ☐ measures envisaged to treat those risks are determined (Article 35(7)(d) and recital 90);
- ☐ interested parties are involved:
  - ☐ the advice of the DPO is sought (Article 35(2));
  - ☐ the views of data subjects or their representatives are sought, where appropriate (Article 35(9)).

Figure 3 - Criteria for an acceptable DPIA methodology

2.4.5 Choice of a methodology

On November 2017, the French Data Protection Authority (CNIL) released on its website an open source ready to use software tool for DPIAs, which can be downloaded for free.[19] In February 2018, to assist in this process and take into account all GDPR requirements, CNIL has updated its "PIA Guides" as well as its DPIA

[19] See https://www.cnil.fr/en/open-source-pia-software-helps-carry-out-data-protection-impact-assesment

tool.[20] The method describes how to use the EBIOS[21] method in the specific context of "Personal Data Protection". It is consistent with the WP29 Guidelines and with risk management international standards.

CNIL's DPIA method is composed of three guides:

- The method explains how to carry out a PIA;
- The models help to formalize a PIA by detailing how to handle the different sections introduced in the method;
- The knowledge base is a code of practice that lists measures to be used to treat the risks.

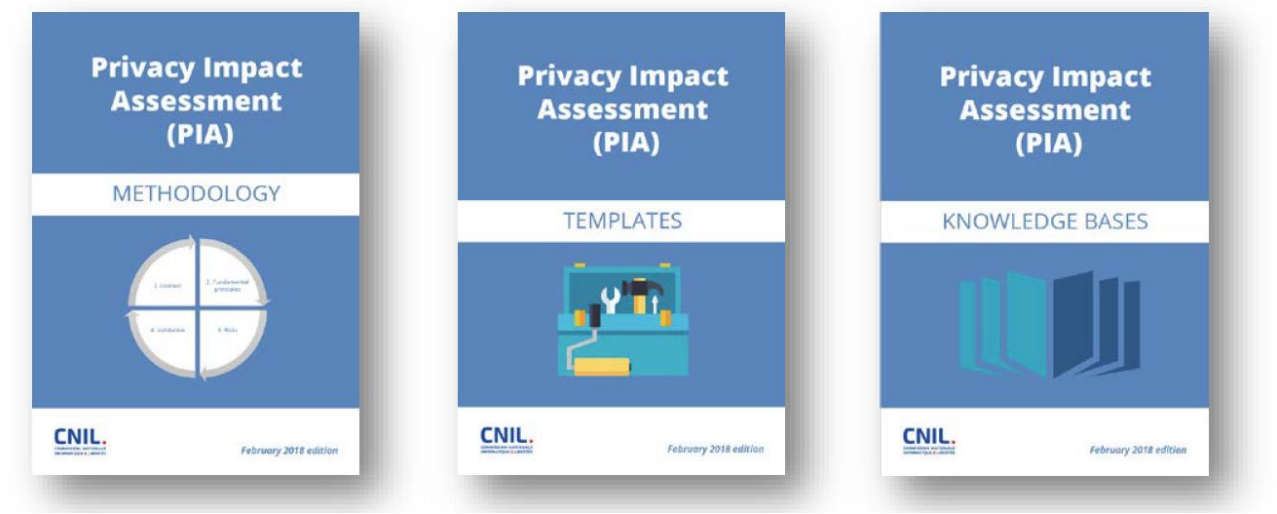


Figure 4 - CNIL's DPIA methodology

Given the broad recognition of CNIL's fulfilment in the protection of personal data, the fact that the CNIL's DPIA tool is open source and is well documented, it was decided to base PROTECT's DPIA on this methodology.

3 PROTECT's system DPIA

3.1 Study of the context

The objective of this section is to gain a clear overview of the personal data processing operations under consideration.

3.1.1 Overview of the processing

This section should:

- Present a brief outline of the product under consideration, its nature, scope, context, purposes and stakes
- Identify the data controller and any processors.
- List the references applicable to the processing, which are necessary or must be complied with, not least the approved codes of conduct.

[20] See https://www.cnil.fr/en/cnil-publishes-update-its-pia-guides

[21] EBIOS – Expression des Besoins et Identification des Objectifs de Sécurité (Expression of Needs and Identification of Security Objectives) – is the name of the risk management methodology published by the Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI/French National Cybersecurity Agency).

Description of the processing under consideration	
Description of the processing	The PROTECT system processes contactless biometrics (2D (VIS and NIR) Face, 3D Face, Periocular (VIS and NIR) and Anthropometrics) of travellers in a smartphone app ("passport companion") which communicates with a Biometric Capture Area (BCA) in which biometric sensors are placed for their identity confirmation "on the move".
Processing purposes	The aim of the "PROTECT programme" is to allow travellers joining the programme to be given priority in waiting areas for "traditional" security and border checks and/or allowing them to benefit of additional convenience services such as access to VIP parking zones or waiting lounges. The aim of processing contactless biometrics in the passport companion and in the BCA is to keep the flow of travellers moving at an acceptable rate.
Processing stakes	Create a new category of access-control mechanism particularly suited for border-crossings based on multimodal biometric fusion "on the move" while in keeping with the legal framework and personal data security.
Controller	Not identifiable at this stage. The controller will be the firm or the public authority which will factually decide to use the PROTECT System.
Processor(s)	None

Table 1- Description of the processing under consideration

Sector-specific standards applicable to the processing[22]	
Standards applicable to the processing	**Consideration**
No codes of conduct or certifications regarding data protection are applicable in the field at this moment.	

Table 2 - Sector-specific standards applicable to the processing

3.1.2 Data, processes and supporting assets

This section should define and describe the scope in detail:

- the personal data concerned, the categories thereof, the recipients and persons with access thereto;
- description of the processes and personal data supporting assets for the entire personal data life cycle (from collection to erasure).

3.1.2.1 Data processed

Below you will find a table setting out a detailed list of the data processed and persons with access thereto.

Personal data	Categories	Recipients	Persons with access thereto
Information processed only		Data controller	

[22] This table should contain a list of the references applicable to the processing, which are necessary or must be complied with, not least the approved codes of conduct (see Art. 40 of the GDPR) and certifications regarding data protection (see Art. 42 of the GDPR)

manually by authorized staff: passport data (containing biometric data)	Sensitive data (in the meaning of the GDPR): biometric data		Authorized staff from data controller
Information processed only at the enrolment kiosk:			
Biometric modalities (2D (VIS and NIR) Face, 3D Face, Periocular (VIS and NIR) and Anthropometrics)	Sensitive data (in the meaning of the GDPR): biometric data	Data controller	Authorized staff from data controller
WIFI information	Common personal data (in the meaning of the GDPR): traffic data	Data controller	Authorized staff from data controller
Information enrolled at kiosk which are recorded on the smartphone app ("passport companion"):			
Encrypted additional biometric modalities (2D (VIS and NIR) Face, 3D Face, Periocular (VIS and NIR) and Anthropometrics)	Sensitive data (in the meaning of the GDPR): biometric data	Data controller	Authorized staff from data controller
Information stored in the key database:			
Unique decryption key for the additional biometrics which are encrypted on the smartphone	Information perceived as sensitive (in the meaning of the GDPR): provides a mean to decrypt biometric data	Data controller	Authorized staff from data controller

Information processed by the PROTECT Control System when passing through the BCA:			
WIFI information (to connect the smartphone to the PROTECT Control System)	Common personal data (in the meaning of the GDPR): traffic data	Data controller	Authorized staff from data controller
IBeacons (Bluetooth Low Energy for position tracking at the BCA)	Common personal data (in the meaning of the GDPR): localization data	Data controller	Authorized staff from data controller
Multimodal set of decrypted biometrics, extracted and fused for verification. There are four (six) biometrics extracted in the Biometric Capture Area for passengers on foot. These are: 2D (VIS and NIR) Face, 3D Face, Periocular (VIS and NIR) and Anthropometrics.	Sensitive data (in the meaning of the GDPR): biometric data	Data controller	Authorized staff from data controller

Table 3 - List of the data processed

3.1.2.2 Life cycle of data and processes

In this section, we present and describe how the PROTECT system generally works during both the enrolment and the verification phases in the scenario at an air or sea border, with diagrams of data flows and a detailed description of the processes being carried out.

3.1.2.2.1 Enrolment phase

In our scenario, a biometric passport is presented to authorized staff at the enrolment kiosk in order to verify the identity of the traveller willing to join the "PROTECT convenience programme". In a second step, the traveller will then proceed to supply a set of biometrics including face, hand veins, voice (speaker utterance) and anthropometrics. Finally, these emerging biometrics are encrypted and sent to the traveller's PROTECT application ("Passport companion") on the mobile phone.

The figure below illustrates the enrolment process:

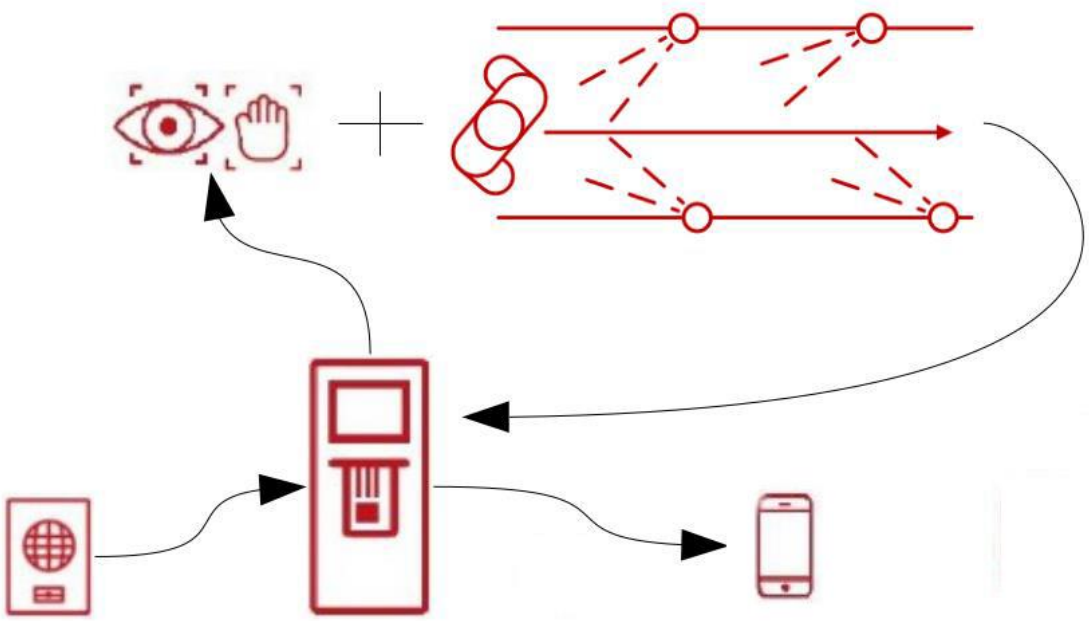


Figure 5 - Enrolment process

3.1.2.2.2 Verification phase

In our scenario, the verification process is automatically initiated when the user approaches the Biometric Capture Area on foot. The traveller's own mobile device computes from iBeacon signals that they are approaching the Biometric Capture Area. The PROTECT "passport companion" then transfers the encrypted biometric data; there is no need for the traveller to stop at the entry kiosk. The PROTECT Control System then decrypts the biometric templates. In a second step the user then enters the Biometric Capture Area so that their biometrics can be extracted and matched with those decrypted from their mobile device.

In other words, as the traveller enters the walking corridor in the Biometric Capture Area, two main operations are triggered: Person tracking through re-identification (re-identification system), and biometrics verification (Including anthropometrics, Face and Periocular). Person tracking through re-identification is not a biometric *per se* but supports the biometric verification by providing an identifier to the person entering the Biometric Capture Area, then tracks the person moving through the Biometric Capture Area so that the biometric verification can be reduced from a 1:m match to a 1:few or even 1:1 match. The PROTECT Control system communicates with the biometric verification system to feed forward the biometric template of the individual moving through the Biometric Capture Area. The PROTECT Control system communicates as well with the re-identification system to associate a person identifier number and its corresponding biometric template. Once each biometric is verified, the final decision on identity acceptance/rejection is performed fusing all individual biometric evaluations.

The following graphic provides a short, simplified overview of the verification process:

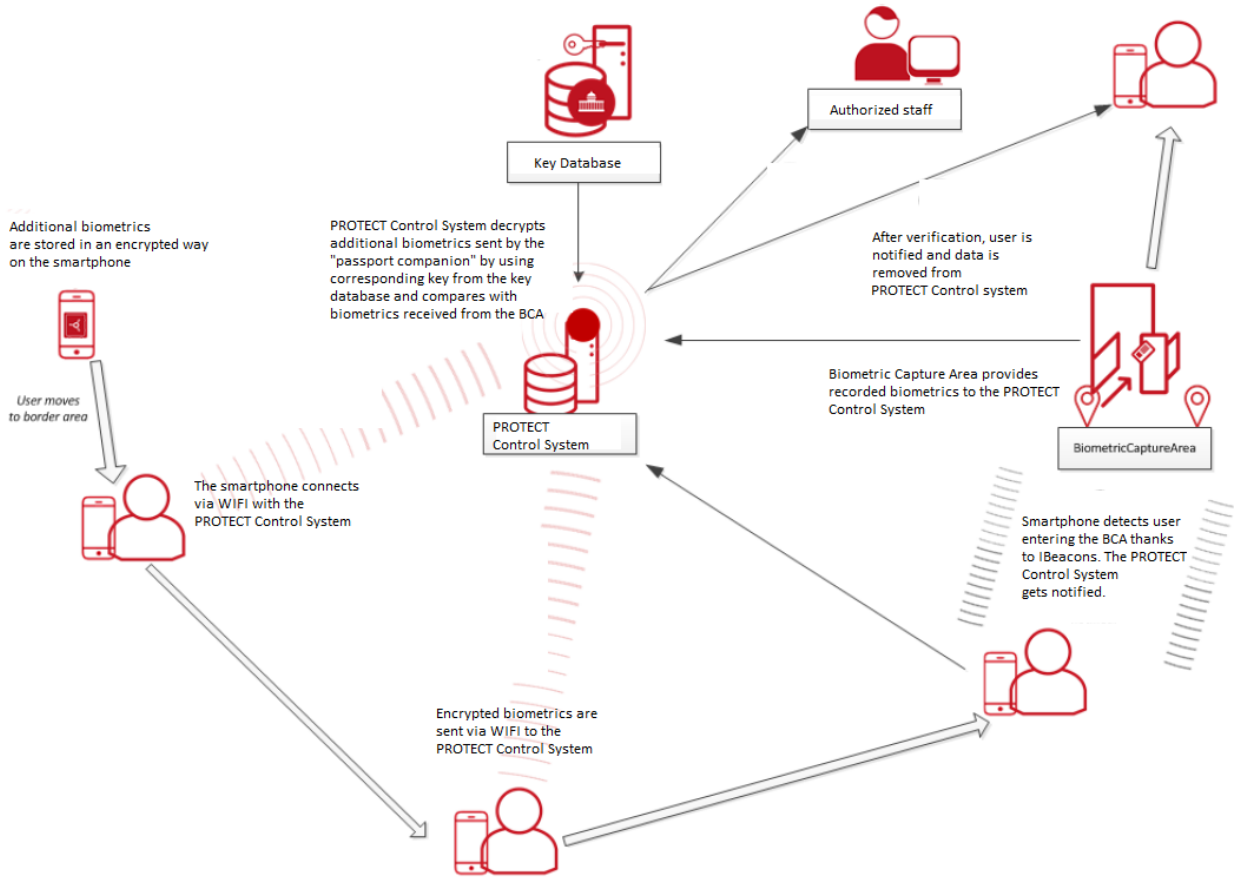


Figure 6 - Verification process

3.1.2.2.3 Overall description of processes being carried out

Below you will find a table for listing in detail all the data processing operations carried out.

Processes	Detailed description of the process
1. The traveller wishes to enrol to the PROTECT programme	At the enrolment kiosk, authorized staff manually authenticate a traveller presenting a passport. After identification, the traveller signs a contract specifying the convenience services for which he wants to use the PROTECT system.
2. The traveller proceeds to enrolment	At the enrolment kiosk, the traveller provides emerging biometrics: 2D (VIS and NIR) Face, 3D Face, Periocular (VIS and NIR) and Anthropometrics. The enrolment kiosk encrypts the set of biometrics and issues a unique encryption key, which is sent to the key database.
3. Biometrics are stored on the passport companion	The traveller downloads the “passport companion” from the app store. The encrypted biometrics are sent (via WIFI) by to the traveller’s mobile phone.
4. The traveller wishes to identify himself at the border entry	The passport companion uploads (via WIFI) the enrolled encrypted biometrics (which are stored on the smartphone) to the PROTECT Control System.
5. The traveller walks to the Biometric Capture Area	The smartphone detects the traveller entering the BCA with IBeacons (Bluetooth Low Energy for position tracking) and the PROTECT Control System gets notified.
6. The traveller passes through the Biometric Capture Area	The BCA provides (via WIFI) recorded biometrics from the tunnel to the PROTECT Control System.

7. The PROTECT Control System proceeds to the verification of the identity of the traveller	The PROTECT Control System decrypts the biometrics with the corresponding key from the key database and verifies the traveller by comparing with biometrics received from the BCA
8. The Border Control System notifies authorized staff and the traveller about the result of the verification	The PROTECT Control System notifies authorized staff and the traveller about the result of the verification and removes the biometrics from the PROTECT Control System.

Table 4 - Overall description of processes

3.1.2.3 Data supporting assets and storage duration

Below you will find a table for listing in detail the data supporting assets with corresponding data types and storage duration.

Data Types	IT systems on which the data rely	Storage duration
Passport data	No IT system. Manual verification by authorized staff at controller's premises.	No storage
Templates of biometric data: 2D (VIS and NIR) Face, 3D Face, Periocular (VIS and NIR) and Anthropometrics.	Enrolment kiosk at controller's premises	Duration of the encryption process during the enrolment phase in order to issue the encryption key
	PROTECT Control System at controller's premises	Duration of the verification of the templates against biometrics recorded in the BCA
Encrypted templates of biometric data: 2D (VIS and NIR) Face, 3D Face, Periocular (VIS and NIR) and Anthropometrics.	Smartphone of the traveller	Duration of the traveller's registration to the PROTECT programme
	PROTECT Control System at controller's premises	Duration of the decryption process only during the verification process
Encryption key of the traveller's passport data	Enrolment kiosk at controller's premises.	Duration of the encryption process during the enrolment phase in order to issue the encryption key
	Key database at controller's premises	Duration of the traveller's registration to the PROTECT programme
	PROTECT Control System at controller's premises	Duration of decryption process only in order to obtain readable templates of additional biometrics for the verification process
Live biometric data: 2D (VIS and NIR) Face, 3D Face, Periocular (VIS and NIR) and Anthropometrics.	Biometric Capture Area at controller's premises	Duration of the walk through the BCA
	PROTECT Control System at controller's premises	Duration of the verification process against the biometric templates

WIFI information	WIFI infrastructure at Controller's premises Smartphone of the traveller	Duration of the enrolment phase for the connection between smartphone and enrolment kiosk
	WIFI infrastructure at Controller's premises Smartphone of the traveller	Duration of the verification phase for the connection between smartphone and the PROTECT Control System
IBeacons (Bluetooth Low Energy for position tracking)	Infrastructure at Controller's premises Smartphone of the traveller	Duration of the verification phase for positioning purposes

Table 5 - Data supporting assets and storage duration

3.2 Study of the fundamental principles

The overall objective of this section is to ensure that the system is built in compliance with privacy principles.

3.2.1 Controls guaranteeing the proportionality and necessity of the processing

The aim of this sub-section is to:

- Explain and justify the choices made to comply with the following requirements:
  1. purpose(s): specified, explicit and legitimate (see Art. 5.1 (b) of the GDPR);
  2. basis: lawfulness of processing, prohibition of misuse (see Art. 6 of the GDPR);
  3. data minimisation: adequate, relevant and limited (see Art. 5 (c) of the GDPR);
  4. quality of data: accurate and kept up-to-date (see Art. 5 (d) of the GDPR);
  5. storage periods: limited (see Art. 5 (e) of the GDPR).
- Check that improving the way in which each point is planned, clarified and justified, pursuant to the [GDPR], is either not necessary or not possible.
- Where applicable, review their description or propose additional controls.

3.2.1.1 Explanation and justification of purposes

According to Article 5.1 (b) of the GDPR, personal data must be "collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes […] ('purpose limitation')". This principle implies firstly a clear determination of the purpose for which the biometric data are collected and processed. Furthermore, an evaluation of the respect for proportionality and the respect for legitimacy is necessary, taking into account the risks for the protection of fundamental rights and freedoms of individuals and notably whether or not the intended purpose could be achieved in a less intrusive way. Proportionality has been the main criterion in almost all decisions taken to date by the Data Protection Authorities on the processing of biometric data.

The table below sets out in detail the data processing purposes and for justifying their legitimacy[23].

Purposes	Legitimacy
Scenario 1: The aim of the PROTECT system is to provide the possibility for travellers to enrol emerging biometric	**Applicable:** In a 2005 deliberation, the CNIL (French DPA) authorized the use of fingerprints on a fidelity chipcard (not a travel document) for frequent travellers

[23] On the legitimacy of the purpose, see opinion WP 203 of the Article 29 Data Protection Working Party - http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf

modalities (other than fingerprints and facial image) in a smartphone application ("the passport companion") for comfort and convenience purposes. The idea to process emerging contactless biometrics in the "passport companion" and to verify them[24] against biometrics recorded in the biometric capture area (BCA)[25] is to allow travellers joining the "PROTECT programme" to be given priority in waiting areas for "traditional" security and border checks and/or to allow them to benefit of additional convenience services such as access to VIP parking zones or waiting lounges. In short, the general purpose of the PROTECT system is to provide travellers to access controlled zones. No further processing is envisaged.

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).[26]

Questions à ...

Guy ROSIER

Conseiller maître honoraire à la Cour des comptes
Commissaire en charge du secteur « Affaires économiques »

En quoi l'autorisation de la CNIL portant sur la carte de fidélité biométrique de la chambre de commerce de Nice-Côte d'Azur est-elle novatrice ?

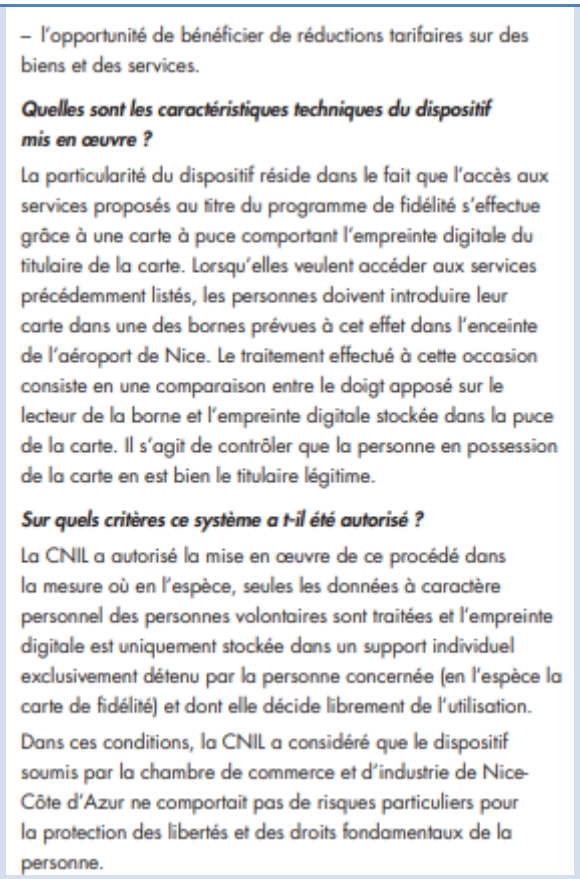
C'est la première fois que la CNIL autorise le recours à un dispositif biométrique reposant sur la reconnaissance des empreintes digitales à destination du grand public et en l'absence d'impératif de sécurité, ces données biométriques étant stockées sur une carte à puce individuelle, sans base centrale. Le dispositif en question a essentiellement pour objet de « faciliter la vie » des personnes. C'est ce que l'on pourrait appeler de la « biométrie de confort », on supprime la contrainte liée à la mémorisation d'un énième mot de passe.

En l'espèce, il s'agit d'identifier les voyageurs réguliers de l'aéroport de Nice détenteurs d'une carte de fidélité lorsqu'ils accèdent aux services spécifiques suivants :
– l'accès à des zones de stationnement réservées ;
– la possibilité de profiter d'un système de « coupe-file » afin de ne pas attendre pour accéder à la salle d'embarquement ;
– l'envoi par SMS d'informations sur les vols ;

[24] In other words, different biometrics are successively acquired as a traveller passes through the Biometric Capture Area and traveller verification is performed via multimodal biometric fusion by the time the traveller reaches the end of the Biometric Capture Area.

[25] The Biometric Capture Area is instrumented with sensors to capture images and data from travellers as they pass through the area.

[26] Délibération 2005-115 du 07 juin 2005 portant autorisation de la mise en oeuvre par la Chambre de Commerce et d'Industrie de Nice-Côte d'Azur d'un traitement automatisé de données à caractère personnel ayant pour finalité la gestion d'une carte de fidélité impliquant l'utilisation d'un dispositif biométrique de reconnaissance des empreintes digitales - http://data.socnum.com/2005/06/07/deliberation-2005-115-du-07-juin-2005/



– l'opportunité de bénéficier de réductions tarifaires sur des biens et des services.

Quelles sont les caractéristiques techniques du dispositif mis en œuvre ?

La particularité du dispositif réside dans le fait que l'accès aux services proposés au titre du programme de fidélité s'effectue grâce à une carte à puce comportant l'empreinte digitale du titulaire de la carte. Lorsqu'elles veulent accéder aux services précédemment listés, les personnes doivent introduire leur carte dans une des bornes prévues à cet effet dans l'enceinte de l'aéroport de Nice. Le traitement effectué à cette occasion consiste en une comparaison entre le doigt apposé sur le lecteur de la borne et l'empreinte digitale stockée dans la puce de la carte. Il s'agit de contrôler que la personne en possession de la carte en est bien le titulaire légitime.

Sur quels critères ce système a t-il été autorisé ?

La CNIL a autorisé la mise en œuvre de ce procédé dans la mesure où en l'espèce, seules les données à caractère personnel des personnes volontaires sont traitées et l'empreinte digitale est uniquement stockée dans un support individuel exclusivement détenu par la personne concernée (en l'espèce la carte de fidélité) et dont elle décide librement de l'utilisation.

Dans ces conditions, la CNIL a considéré que le dispositif soumis par la chambre de commerce et d'industrie de Nice-Côte d'Azur ne comportait pas de risques particuliers pour la protection des libertés et des droits fondamentaux de la personne.

Figure 7 - CNIL accepts biometrics for convenience

Scenario 2: The aim of the PROTECT system is to provide the possibility for travellers to enrol passport data (including traditional biometrics – fingerprints and facial image) as well as additional biometric modalities in a smartphone application for the purpose of "facilitating" border control by border authorities (including checks against border control IT databases such as VIS, SIS, EES, and SLTD). In this scenario, the PROTECT system not only processes new biometric modalities but also travel document data in mobile devices so that data capture for border control purposes can be more convenient to travellers and more timely for border authorities.

Not applicable: Under current EU Regulation, additional multimodal biometrics features (being not facial image or fingerprints) developed within the PROTECT project cannot legally be integrated in ePassports (or residence permits) without a national legislation of a Member State allowing it. Furthermore, even if a national law would allow such integration of additional biometrics, it would certainly be challenged in Court for privacy reasons related to proportionality and data minimization.

It is also important to note that under current EU law, mobile devices such as smartphones cannot legally be used to replace travel documents as a result of strict rules regulating the materials of travel documents. In other words, smartphones cannot be considered as "travel documents" under current EU law and therefore cannot support traditional biometrics (fingerprints and facial image) as well as an enhanced set of contactless biometrics for the purpose of border control management.

A third important point is that Recital 43 of the GDPR 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 it seems that consent of travellers cannot be considered as a legitimate basis of lawfulness in PROTECT scenarios to allow public border control authorities to speed up their public interest missions by enrolling additional biometrics in travel documents. For additional details concerning these findings, see D2.2 - Legal framework of biometric border control.

Table 6 - Explanation and justification of purposes

According to the Article 29 Working Party, the requirement according to which "personal data must be collected for legitimate purposes" means that the purposes must be "in accordance with the law" in the broadest sense: "this includes all forms of written and common law, primary and secondary legislation, municipal decrees, judicial precedents, constitutional principles, fundamental rights, other legal principles, as well as jurisprudence, as such 'law' would be interpreted and taken into account by competent courts".[27] Therefore, in table 6, scenario 2 must be considered as "illegitimate" since that it would be in contradiction with the current legal framework on biometric border control as analysed in D2.2. For this reason, as an alternative, scenario 1 (see table 6) will be analysed in this Deliverable.

3.2.1.2 Explanation and justification of lawfulness

Below you will find the list of lawfulness criteria. Processing shall be lawful only if and to the extent that at least one of the following applies[28]:

Lawfulness criteria	Applicable	Justification
The data subject has given consent to the processing of his or her personal data for one or more specific purposes	Yes	Applicable but, in the absence of other alternative legitimate grounds, the PROTECT biometric authentication system could be used only if the travellers are free to decide whether to avail themselves of the said system. This means that alternative, less privacy-intrusive mechanisms must be made available by the controller of PROTECT. Such a system will permit a traveller who is unwilling or unable to undergo biometric processing because of his/her personal circumstances to dissent. The sole choice between not using a service and giving one's biometric data is a strong indicator that the consent

[27] Article 29 Working Party, Opinion 03/2013 on purpose limitation, WP203, adopted on 2 April 2013, p.20.
[28] See article 6 of the GDPR.

		was not freely given and cannot be considered as legitimate ground.
Processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract	Yes	Applicable. Processing of biometric data can be necessary for the performance of a contract to which the data subject is party or can be necessary in order to take steps at the request of the data subject prior to entering into a contract. In our scenario, the purpose of the contract is to offer convenience services to travellers “on the move”.
Processing is necessary for compliance with a legal obligation to which the controller is subject	No	The processing of contactless biometrics is not necessary for compliance with a legal obligation to which the controller is subject.
Processing is necessary in order to protect the vital interests of the data subject or of another natural person	No	The processing of contactless biometrics is not necessary to protect the vital interests of the data subject or of another natural person.
Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller	No	The processing of contactless biometrics is not necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.
Processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child	No	Not applicable. As a general rule, the use of biometrics for general security requirements of property and individuals cannot be regarded as legitimate interest overriding the interests or fundamental rights and freedoms of the data subject. On the contrary, the processing of biometric data can only be justified as a required tool securing the property and/or individuals, where there is evidence, on the basis of objective and documented circumstances, of the concrete existence

	of a considerable risk. To that end the controller needs to prove that specific circumstances pose a concrete, considerable risk, which the controller is required to assess with special care.

Table 7 - Explanation and justification of lawfulness

The processing of biometric data must be based on one of the grounds of legitimacy provided for in Article 6 of the GDPR. In our scenario, the two possibilities are consent of the traveller or a contract with him.

1. If consent is used as a legitimacy ground by the controller:
    - It must comply with the definition provided in Article 4(11) of the GDPR, which states that "'consent of the data subject 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". According to the Article 29 Working Party, "Consent is only valid when sufficient information on the use of biometric data is given. Since biometric data may be used as a unique and universal identifier providing clear and easily accessible information on how the specific data are used is to be regarded as absolutely necessary to guarantee fair processing. Therefore, this is a crucial requirement for a valid consent in the use of biometric data".[29]
    - Furthermore, if consent is used as a ground to process "special categories of personal data" under which "biometric data for the purpose of uniquely identifying a natural person"[30], this consent must be an "explicit consent to the processing of those personal data for one or more specified purposes […]".
    - Finally, if consent is used as a basis of legitimacy, it must respect the conditions set up in Article 7 of the GDPR according to which: "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". According to the Article 29 Working Party, "as consent can be revoked at any time, data controllers need to implement technical means that can reverse the use of biometric data in their systems. A biometric system operating on the basis of consent needs therefore to be able to efficiently remove all identity links it created".[31]

[29] Article 29 Working Party, Opinion 3/2012 on developments in biometric technologies, WP193, adopted on 27th April 2012, p. 11.
[30] See article 9 of the GDPR.
[31] Article 29 Working Party, Opinion 3/2012 on developments in biometric technologies, WP193, adopted on 27th April 2012, p. 11.

- It is important to note that according to the Article 29 Working Party: "in many cases in which biometric data are processed, without a valid alternative like a password or a swipe card, the consent could not be considered as freely given. For instance, a system that would discourage data subjects from using it (e.g. too much time wasted for the user or too complicated) could not be considered as a valid alternative and then would not lead to a valid consent".[32] Hence, in the absence of other alternative legitimate grounds, the PROTECT biometric authentication system could be used only if the travellers are free to decide whether to avail themselves of the said system. This means that alternative, less privacy-intrusive mechanisms must be made available by the controller of PROTECT. Such a system will permit a traveller who is unwilling or unable to undergo biometric processing because of his/her personal circumstances to dissent. The sole choice between not using a service and giving one's biometric data is a strong indicator that the consent was not freely given and cannot be considered as legitimate ground.

2. If contract is used as a legitimacy ground by the controller: according to the Article 29 Working Party, "processing of biometric data can be necessary for the performance of a contract to which the data subject is party or can be necessary in order to take steps at the request of the data subject prior to entering into a contract. It has however to be noted that this applies in general only when pure biometric services are provided (which is the case in our scenario). This legal basis cannot be used to legitimate a secondary service that consists in enrolling a person into a biometric system. If such a service can be separated from the main service, the contract for the main service cannot legitimate the processing of biometric data. Personal data are not goods that can be asked for in exchange of a service, therefore contracts that foresee that or contracts that offer a service only under the condition that someone consents to the processing of his biometric data for another service cannot serve as legal basis for that processing".[33]

As a result of the analysis carried out in this section, the most appropriate ground of legitimacy for the use of the PROTECT system in our scenario would be a contract signed with a traveller for the purpose of offering him convenience services "on the move" such as giving him priority in waiting areas for "traditional" security and border checks and/or allowing him to benefit of additional convenience services such as access to VIP parking zones or waiting lounges. Furthermore, given that biometric data is processed for the purpose of this contract, the traveller should provide an explicit consent to the controller of the PROTECT system.[34]

3.2.1.3 Explanation and justification of data minimization[35]

It is important to reduce the severity of the risks by minimizing the number of personal data that will be processed, by limiting such data to what is strictly necessary for the purposes for which they are processed (otherwise they should not be collected). With this regard, the Article 29 Working Party has the opinion that "a specific difficulty may arise as biometric data often contain more information than necessary for matching functions. The principle of data minimisation has to be enforced by the data controller. Firstly, this means that only the required information and not all available information should be processed, transmitted or stored. Second, the data controller should ensure that the default configuration promotes data protection, without having to enforce it". This second step minimizes the data themselves, via controls aimed at reducing their sensitivity.

The table below lists the data processed, reduced to what is strictly necessary, alongside the justification of the need and any additional minimization controls.

[32] Article 29 Working Party, Opinion 3/2012 on developments in biometric technologies, WP193, adopted on 27th April 2012, p. 10.
[33] Ibid, p.12.
[34] See article 9.2 (b) of the GDPR.
[35] See Article 5.1 (c) of the GDPR.

Data types	Data categories	Details about the data processed	Justification of the need and relevance of the data	Minimization controls
Common data	Identity, biographic data	First name, last name, birthday, nationality, physical address.	Information needed to register a traveller to the PROTECT programme.	According to CNIL, good practices are: • Pseudonymization • Separate storage of identifying data in an encrypted base.
	Bank and payment data	Bank account (or credit card account number) and amount of payments	Information needed to register/manage a traveller to the PROTECT programme.	According to CNIL, good practices are: • Pseudonymization • Separate storage of bank and payment data in an encrypted base.
	Economic and financial information (income, financial situation, tax situation, etc.)	Not collected		
	WIFI connection data	Wi-Fi information (for connecting to Wi-Fi). Session id (Random number for authentication).	Required as part of the communication features between the Passport Companion and the Enrolment Kiosk/PROTECT Control System	According to CNIL, good practices are: • Use the WPA or WPA2 protocol with AES-CCMP encryption or the "Enterprise" mode of the WPA and WPA2 protocols (using a RADIUS server as well as the EAP-TLS or PEAP subprotocols). • Prohibit ad-hoc networks. • Use and configure a firewall at network entry and exit points in order to partition off connected hardware as needed. • Use the SSL protocol (HTTPS) to ensure server authentication

				and confidentiality of communications. In our scenario, to ensure connection security, the WIFI will use the WPA2 encryption standard. The HTTPS-Protocol will be used to exchange data packages between the application and the servers of the PROTECT Control system.
	Position tracking data	Position tracking is done via Bluetooth Low Energy (BLE). The Biometric Capture Area sends iBeacon signals that are interpreted by the phone app.	Required as part of the communication features between the Passport Companion and the Biometric Capture Area/PROTECT Control System	According to CNIL, good practices are: • Impose mutual authentication with remote devices. • Encrypt sharing traffic. These best practices should be embedded in our scenario.
	Events logs	Application traces, timestamps of new biometric enrolment for the same traveller, technical logs.	Required for security reasons and to measure performance and transaction times	Pseudonymization for statistical use and security reasons
Data perceived as sensitive	Passport data, including traditional biometrics contained therein (face and fingerprints).	Not collected		
	Opinions bearing on philosophy, politics, religion, trade union involvement, sexuality, health data, racial or ethnic origin, data	Not collected		

	concerning health or sexuality			
	Offences, convictions, security measures	Not collected		
Sensitive data	Biometric data	2D Face VIS, 2D Face NIR, 3D Face, Periocular VIS, Periocular NIR, Anthropometrics	Multi-modal biometric modalities required to perform the purpose of the "on the move" service which is offered to the traveller	According to the WP29, good practices are: • Pseudonymization • Use of biometric templates • Storage on a personal device vs. centralised storage • Renewability and revocability • Encrypted form • Anti-spoofing • Biometric encryption and decryption • "Weak link" databases These best practices should be embedded in our scenario.

Table 8 - Data minimization controls

3.2.1.4 Explanation and justification of data quality

Article 5(d) of the GDPR provides that personal data must be "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')". However, according to the Article 29 Working Party, "when biometric systems are used it is difficult to produce 100% error-free results. This may be due to differences in the environment at data acquisition (lighting, temperature, etc.) and differences in the equipment used (cameras, scanning devices, etc.)".[36] In order for biometric data to be accurate and relevant in proportion to the purpose for which there they were collected, the data must be accurate at enrolment and when establishing the link between the person and the biometric data. Accuracy at enrolment is also relevant to the prevention of identity fraud.

Below you will find a table for setting out in detail the data quality compliance controls as well as a justification on the arrangements for or impossibility of implementing them.

Data quality controls	Justification
Regular checks of the accuracy of the user's personal data	Regular checks of the accuracy of the user's multimodal data will be performed "naturally"

[36] Article 29 Working Party, Opinion 3/2012 on developments in biometric technologies, WP193, adopted on 27th April 2012, p.9.

	each time he walks through a BCA. In case of non-accuracy, the traveller will be given the possibility to proceed to a new enrolment process by the authorized staff. Updating biographic or bank data is also possible at enrolment kiosk.
Invitation for the user to check and, where necessary, update his or her data	In case of a failure of the verification process, the user will be invited to proceed to a new enrolment process by the authorized staff.
Traceability of data amendments	Timestamps of new enrolment events of multimodal data by the same traveller are pseudonymously stored in a separate database for security reasons and performance assessment of the system.

Table 9 - Data quality controls

According to the Article 29 Working Party, "taking into account the fact that biometric technologies cannot ensure full accuracy, there is always an implicit risk coming from incorrect identifications. Such false positives result in decisions affecting individual rights".[37] The specific impact on data protection of inaccuracy of a particular biometric system will depend on its purpose and particular circumstance. In the case of our scenario, a user subject to a false reject[38] would face limited consequences such as a refusal to access to the commercial convenience services for which he paid. Given such limited consequences, a procedure which permits a data subject to proceed to a new enrolment at the Enrolment Kiosk seems to be an appropriate safeguard. The situation would of course be totally different if the PROTECT system was used for immigration control purposes or other public border control missions. In that case, implications on fundamental rights of data subjects would be much more severe, such as a violation of the right to free movement or to the right of liberty. In such a scenario, safeguards against false reject rates should be much more stringent.

3.2.1.5 Explanation and justification of storage durations

A storage duration must be defined for each type of data and justified by the legal requirements and/or processing needs. Functional traces will also have to be purged, as will technical logs which may not be stored indefinitely.

Data types	Storage duration	Justification of the storage duration	Erasure mechanism at the end of the storage duration
Passport data	No storage, only manual check at enrolment by authorized staff.		
Identity, biographic data	3 years maximum	The information is needed to register a traveller to the PROTECT programme and to manage him until the end of his registration. Registration to the programme must be renewed	Automatic deletion after 3 years or alternatively as soon as the traveller

[37] Article 29 Working Party, Opinion 3/2012 on developments in biometric technologies, WP193, adopted on 27th April 2012, p. 18.

[38] The False Reject Rate (FRR): It is the probability that the system produces a false reject. A false reject occurs when an individual is not matched to his/her own existing biometric template. It is also known as the false negative rate.

		after 3 years. Information can also be updated at the travel kiosk in case of inaccuracy.	cancels his registration (when all due payments are done).
Bank and payment data	3 years maximum	The information is needed to register a traveller to the PROTECT programme and to manage him until the end of his registration. Registration to the programme must be renewed after 3 years. Information can also be updated at the travel kiosk in case of inaccuracy.	Automatic deletion after 3 years or alternatively as soon as the traveller cancels his registration (when all due payments are done).
WIFI information	Duration of the enrolment phase for the connection between smartphone and enrolment kiosk. Duration of the verification phase for the connection between smartphone and the PROTECT Control System	Storage of WIFI information is limited to what is needed for the communication features of the PROTECT system.	Automatic deletion after enrolment or verification phase (depending on the process carried out).
Position tracking data	Duration of the verification phase for positioning purposes	Position tracking is done via Bluetooth Low Energy (BLE). The Biometric Capture Area sends iBeacon signals that are interpreted by the phone app. Storage of BLE data is limited to what is required as part of the communication features between the Passport Companion and the Biometric Capture Area/PROTECT Control System	Automatic deletion after verification phase.
Events logs	3 years	Application traces, timestamps of new biometric enrolment for the same traveller, technical logs are kept pseudonymously during 3 years for security reasons and performance assessment of the system.	Automatic deletion after 3 years.
Encrypted templates of biometric data in the smartphone app	3 years maximum	The information is needed to register a traveller to the PROTECT programme and to	Automatic deletion after 3 years or

		manage him until the end of his registration. Registration to the programme must be renewed after 3 years. Information can also be updated at the travel kiosk in case of inaccuracy.	alternatively as soon as the traveller cancels his subscription (by removing the application from his smartphone)
Encrypted templates of biometric data in the PROTECT Control System	Duration of the verification of the templates against biometrics recorded in the BCA	Information is needed for the functioning of the system	Automatic deletion after decryption process during the verification phase
Templates of biometric data in the enrolment kiosk	Duration of the encryption process during the enrolment phase in order to issue the encryption key	Information needed for the functioning of the system	Automatic deletion after the encryption process during the enrolment phase
Templates of biometric data in the PROTECT Control System	Duration of the verification of the templates against biometrics recorded in the BCA	Information needed for the functioning of the system	Automatic deletion after the verification phase
Encryption key in key database	Maximum 3 years	The information is needed to process a traveller during his registration to the PROTECT programme. Registration to the programme must be renewed after 3 years.	Automatic deletion after 3 years or alternatively as soon as the traveller cancels his registration.
Live biometric data recorded in the BCA and processed in the PROTECT Control System	Duration of the verification of the templates against biometrics recorded in the BCA	Information needed for the functioning of the system	Automatic deletion after the verification phase

Table 10 - Storage durations

3.2.1.6 Assessment of the controls

Controls guaranteeing the proportionality and necessity of the processing	Acceptable/can be improved on?	Corrective controls

Purposes: specified, explicit and legitimate	Acceptable if "scenario 1" is used. Not acceptable if "scenario 2" is used. For a description of these scenarios, see table 6.	None
Basis: lawfulness of processing, prohibition of misuse	Acceptable	None
Data minimization: adequate, relevant and limited	Acceptable if best practices of WP29 and CNIL are embedded in our scenario 1.	None
Data quality: accurate and kept up-to-date	Acceptable	None
Storage durations: limited	Acceptable	None

Table 11 - Assessment of fundamental principles

3.2.2 Controls protecting data subjects' rights

The aim of this sub-section is to:

- Identify or determine, and describe, the controls (existing or planned) selected to comply with the following legal requirements (it is necessary to explain how it is intended to implement them):

  1. information for the data subjects (fair and transparent processing, see Art. 12, 13 and 14 of the GDPR);

  2. obtaining consent, where applicable13: express, can be demonstrated and withdrawn (see Art. 7 and 8 of the GDPR);

  3. exercising the right of access and right to data portability (see Art. 15 and 20 of the GDPR);

  4. exercising the rights to rectification and erasure (see Art. 16 and 17 of the GDPR);

  5. exercising the right to restriction of processing and right to object (see Art. 18 and 21 of the GDPR);

  6. processors: identified and governed by a contract (see Art. 28 of the GDPR);

  7. transfers: compliance with the obligations bearing on transfer of data outside the European Union (see Art. 44 to 49 of the GDPR).

- Check that improving each control and its description, in accordance with the GDPR, is either not necessary or not possible.
- Where applicable, review their description or propose additional controls.

3.2.2.1 Information for the data subjects

Transparency is not defined in the GDPR. Recital 39 of the GDPR is informative as to the meaning and effect of the principle of transparency in the context of data processing: *"It should be transparent to natural persons that personal data concerning them are collected, used, consulted or otherwise processed and to what extent the personal data are or will be processed. The principle of transparency requires that any information and communication relating to the processing of those personal data be easily accessible and easy to understand, and that clear and plain language be used. That principle concerns, in particular, information to the data subjects on the identity of the controller and the purposes of the processing and further information to ensure fair and transparent processing in respect of the natural persons concerned and their right to obtain confirmation and communication of personal data concerning them which are being processed…".*

The key articles in relation to transparency in the GDPR, as they apply to the rights of the data subject, are found in Chapter III (Rights of the Data Subject). Article 12 sets out the general rules which apply to the provision of information to data subjects (under Articles 13 - 14); communications with data subjects

concerning the exercise of their rights (under Articles 15 - 22); and communications in relation to data breaches (Article 34). In particular Article 12 requires that the information or communication in question must comply with the following rules:

- it must be concise, transparent, intelligible and easily accessible (Article 12.1);
- clear and plain language must be used (Article 12.1);
- the requirement for clear and plain language is of particular importance when providing information to children (Article 12.1);
- it must be in writing "or by other means, including where appropriate, by electronic means" (Article 12.1);
- where requested by the data subject it may be provided orally (Article 12.1) ; and
- it generally must be provided free of charge (Article 12.5).

According to the Article 29 Working Party, "the requirement that the provision of information to, and communication with, data subjects is done in a "concise and transparent" manner means that data controllers should present the information/ communication efficiently and succinctly in order to avoid information fatigue. This information should be clearly differentiated from other non-privacy related information such as contractual provisions or general terms of use. In an online context, the use of a layered privacy statement/ notice will enable a data subject to navigate to the particular section of the privacy statement/ notice which they want to immediately access rather than having to scroll through large amounts of text searching for particular issues".[39] WP29 recommends in particular that layered privacy statements/ notices should be used to link to the various categories of information which must be provided to the data subject, rather than displaying all such information in a single notice on the screen, in order to avoid information fatigue. Layered privacy statements/ notices can help resolve the tension between completeness and understanding, notably by allowing users to navigate directly to the section of the statement/ notice that they wish to read. It should be noted that layered privacy statements/ notices are not merely nested pages that require several clicks to get to the relevant information. The design and layout of the first layer of the privacy statement/ notice should be such that the data subject has a clear overview of the information available to them on the processing of their personal data and where/ how they can find that detailed information within the layers of the privacy statement/ notice. It is also important that the information contained within the different layers of a layered notice is consistent and that the layers do not provide conflicting information.

Furthermore, according to the WP29, "a central consideration of the principle of transparency outlined in these provisions is that the data subject should be able to determine in advance what the scope and consequences of the processing entails and that they should not be taken by surprise at a later point about the ways in which their personal data has been used".[40] In accordance with the principle of accountability and in line with Recital 39, data controllers should assess whether there are particular risks for natural persons involved in this type of processing which should be brought to the attention of data subjects. This can help to provide an overview of the types of processing that could have the highest impact on the fundamental rights and freedoms of data subjects in relation to the protection of their personal data. As for the "easily accessible" element, this means that the data subject should not have to seek out the information; it should be immediately apparent to them where and how this information can be accessed, for example by providing it directly to them, by linking them to it, by clearly signposting it, or as an answer to a natural language question.

[39] Article 29 Working Party, Guidelines on transparency under Regulation 2016/679, WP260, last Revised and Adopted on 11 April 2018, p.7.
[40] Ibidem.

As a result, the controller of the PROTECT system she should publish a privacy statement/ notice on his website concerning the proposed service. A direct link to this privacy statement/ notice should be clearly visible on the website, on the Enrolment Kiosk and on the mobile application ("passport companion") under a commonly used term (such as "Privacy", "Privacy Policy" or "Data Protection Notice"). Indeed, for apps, the WP29 considers that "the necessary information should also be made available from an online store prior to download. Once the app is installed, the information still needs to be easily accessible from within the app. One way to meet this requirement is to ensure that the information is never more than "two taps away" (e.g. by including a "Privacy"/ "Data Protection" option in the menu functionality of the app). Additionally, the privacy information in question should be specific to the particular app and should not merely be the generic privacy policy of the company that owns the app or makes it available to the public"[41].

Controls for the right to information	Implementation
Presentation and possibility of accessing the terms & conditions for use/confidentiality	• A "Privacy policy" must be available on the website of the controller of the PROTECT system. • A link to this Privacy Policy will be available in the contract which is signed between the controller of the PROTECT system and the user • A link to this privacy policy will be available on the online store prior to downloading the app. Moreover, this concise text will be shown on the store in order to present the "passport companion" application: "The passport companion is a smartphone application allowing travellers willing to join the PROTECT programme to be given priority in waiting areas for security and border checks and allowing them benefit of additional convenience services such as access to VIP parking zones and waiting lounges. Exclusively for this purpose, the application processes sensitive data consisting of encrypted biometric templates of 2D (VIS and NIR) Face, 3D Face, Periocular (VIS and NIR) and Anthropometrics allowing contactless identification in Biometric Capture Areas". • The same information will be provided on the "passport companion" as follows:

[41] Ibid, p.8.

Figure 8 - Information screen 1

Legible and easy-to-understand terms	When the user clicks on the “here” button, the following additional information is provided:

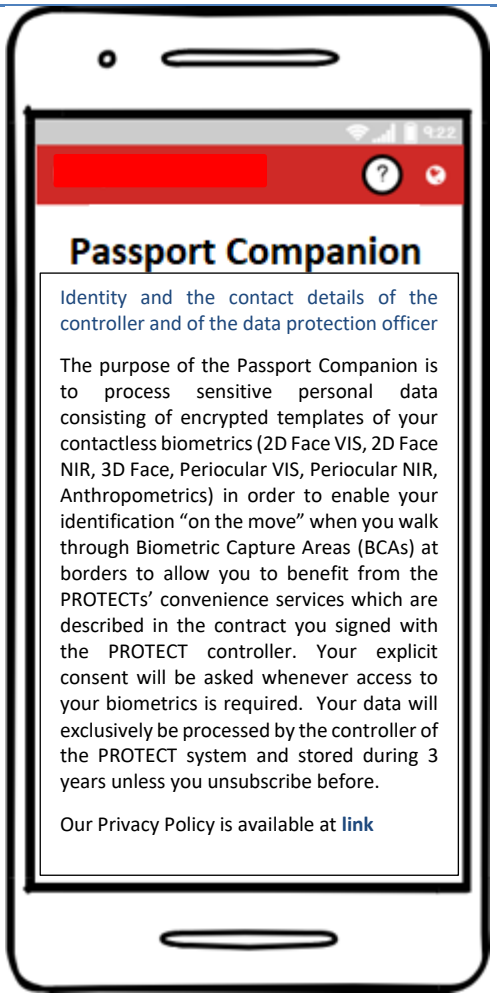


Figure 9 - Information screen 2

Detailed presentation of the data processing purposes (specified objectives, data matching where applicable, etc.)	The Privacy Policy will detail the purpose of the PROTECT system as follows: "The PROTECT system processes contactless biometrics 2D (VIS and NIR) Face, 3D Face, Periocular (VIS and NIR) and Anthropometrics of travellers in a smartphone app ("passport companion") which communicates with a Biometric Capture Area (BCA) in which biometric sensors are placed for their identity confirmation "on the move". The aim of the "PROTECT programme" is to allow travellers joining the programme to be given priority in waiting areas for "traditional" security and border checks and/or allowing them to benefit of additional convenience services such as access to VIP parking zones or waiting lounges. The aim of processing contactless biometrics in the passport companion and in the BCA is to keep the flow of travellers moving at an acceptable rate".
Detailed presentation of the personal data collected	The Privacy Policy will detail the personal data being processed as follows: "In order to be able to provide the convenience services specified by contract, the PROTECT system processes your following personal data:

	• In the administrative server (during 3 years maximum unless subscription is cancelled before and all due payments are done): - Biographic data: First name, last name, birthday, nationality, physical address; - Accounting data: Bank account/Credit card number and data related to payments; • In the Enrolment Kiosk (stored only during enrolment phase for the purpose of encrypting your biometric data): - Biometric templates of 2D face (visual and near-infrared); - Biometric template of 3D face; - Biometric templates of Periocular (visual and near-infrared); - Biometric template of Anthropometrics. • A unique encryption key is stored in the key database within the PROTECT Control System during 3 years maximum unless subscription is cancelled before. • In the "passport companion" (during 3 years maximum unless subscription is cancelled before by removing the application from your smartphone): - Encrypted biometric templates of 2D face (visual and near-infrared); - Encrypted biometric template of 3D face; - Encrypted biometric templates of Periocular (visual and near-infrared); - Encrypted biometric template of Anthropometrics. • In the Biometric Capture Area, sensors are placed to capture live biometrics of 2D (VIS and NIR) Face, 3D Face, Periocular (VIS and NIR). These data are not stored but only processed during verification phase in order to be perform your identification "on the move". • For communication purposes between your smartphone and the PROTECT system, WIFI and Bluetooth information is being processed during the enrolment and verification phases only. • Pseudonymized technical logs of events are stored during 3 years for security reasons and performance assessment of the system.
Presentation of any access to the identifiers of the device, the smartphone/tablet or computer, by specifying whether these identifiers are communicated to third parties	WIFI information (Session id and Random number for authentication) and Bluetooth information are processed only by the PROTECT controller for communication reasons between the smartphone application and the PROTECT system. No third parties have access to these identifiers.
Presentation of the user's rights (consent withdrawal, data erasure, etc.)	Concerning the encrypted biometric templates in the passport companion, the user's rights to consent withdrawal and data erasure can simply be performed by removing the application from the smartphone.

	Concerning the biographic data, accounting data and unique encryption key, the user's rights to consent withdrawal and data erasure can be performed by contacting the PROTECT controller (or data protection officer).
Information on the secure data storage method	• Biographic data and accounting data are stored encrypted and linked to a pseudonym stored in a different database; • The encryption key is linked to the same pseudonym; • Biometric templates are encrypted in the smartphone application; • To ensure connection security, the WIFI will use the WPA2 encryption standard. The HTTPS-Protocol will be used to exchange data packages between the application and the servers of the PROTECT Control system.
Arrangements for contacting the company (identity and contact details) about confidentiality issues	Identity and the contact details of the controller and of the data protection officer should be mentioned here.
Where applicable, information for the user on any change concerning the data collected, the purposes and confidentiality clauses	If PROTECT contractual services are changing or added, the user will be notified through the smartphone application.

Table 12 - Controls for the right to information

3.2.2.2 Determination and description of the controls for obtaining explicit consent

Where processing is based on consent, the controller shall be able to demonstrate that the data subject has consented. The data subject must be able to withdraw his/her consent easily at any time.

As the lawfulness of the PROTECT system is based on a contract with the traveller providing explicit consent for processing sensitive data (biometric templates)[42], extra efforts should be undertaken in order to obtain this explicit consent of a data subject in line with the GDPR. The term explicit refers to the way consent is expressed by the data subject. It means that the data subject must give an express statement of consent. An obvious way to make sure consent is explicit would be to expressly confirm consent in a written statement. Where appropriate, the controller could make sure the written statement is signed by the data subject, in order to remove all possible doubt and potential lack of evidence in the future.[43] In the case of the PROTECT system, an initial written consent for the processing of biometric modalities will be obtained by the signature of the PROTECT contract.

However, according to the Article 29 Working Party, "such a signed statement is not the only way to obtain explicit consent and, it cannot be said that the GDPR prescribes written and signed statements in all circumstances that require valid explicit consent. For example, in the digital or online context, a data subject may be able to issue the required statement by filling in an electronic form, by sending an email, by uploading

[42] Explicit consent is also one of the exemptions to the prohibition on the processing of special categories of data: See Article 9 GDPR.

[43] Article 29 Working Party, Guidelines on consent under Regulation 2016/679, WP259, last Revised and Adopted on 10 April 2018, p. 18.

a scanned document carrying the signature of the data subject, or by using an electronic signature. In theory, the use of oral statements can also be sufficiently express to obtain valid explicit consent, however, it may be difficult to prove for the controller that all conditions for valid explicit consent were met when the statement was recorded. […] Two stage verification of consent can also be a way to make sure explicit consent is valid. For example, a data subject receives an email notifying them of the controller's intent to process a record containing medical data. The controller explains in the email that he asks for consent for the use of a specific set of information for a specific purpose. If the data subject agrees to the use of this data, the controller asks him or her for an email reply containing the statement 'I agree'. After the reply is sent, the data subject receives a verification link that must be clicked, or an SMS message with a verification code, to confirm agreement".[44]

Below you will find a list of controls intended to ensure that users' explicit consent has been obtained, that there has been a reminder and confirmation of their consent, and the settings associated with the latter have been maintained.

Controls for obtaining consent	Implementation
Express consent during registration in the mobile application ("passport companion").	After having downloaded the passport companion, the following information is provided to the traveller. If the traveller agrees, he can click on the "proceed" button.

[44] Ibidem.

Figure 10 - Consent screen 1

When the user clicks on the "proceed" button, the following invitation is shown to the traveller:

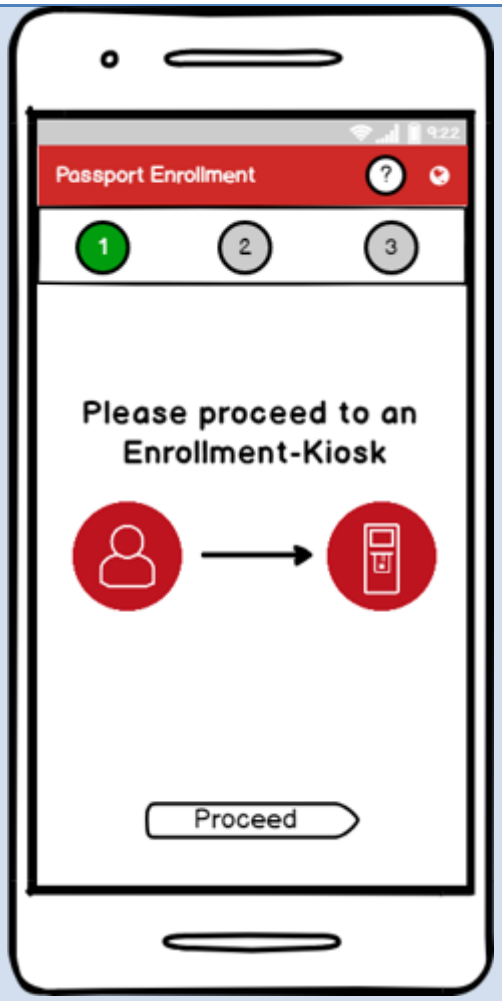


Figure 11 - Consent screen 2

When arriving at the Enrolment Kiosk (under supervision of authorized staff which has proceeded to the manual passport control to confirm the identity of the traveller and once the PROTECT contract has been signed by the user), the user clicks on "proceed" and enrolment screen 2 opens which contains a barcode scanner to scan the barcode displayed on the Enrolment Kiosk. The following screen is showed to the traveller in order to obtain a first step of explicit consent before proceeding to biometric enrolment.

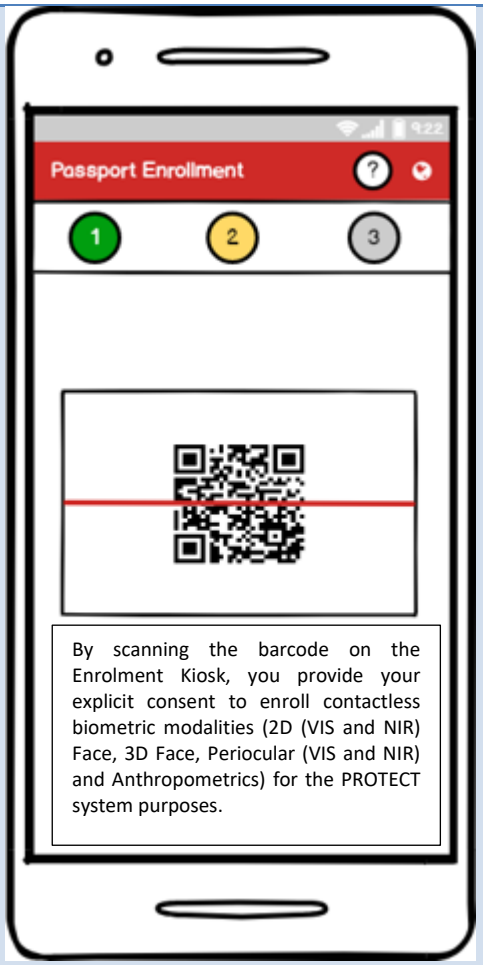


Figure 12 - Consent screen 3

The following screen appears after the user successfully scanned the Kiosk-Connection-Barcode.

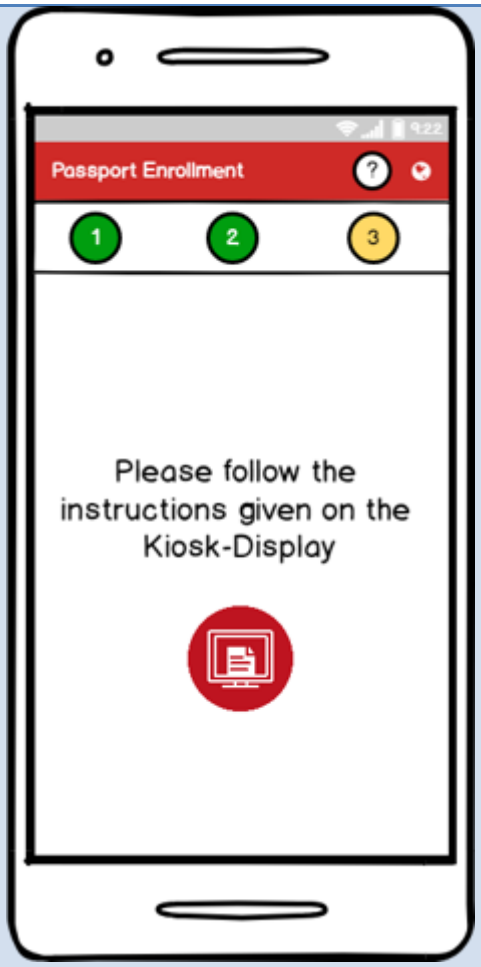


Figure 13 - Consent screen 4

Consent segmented per data category or processing type	On the Enrolment Kiosk, explicit consent is asked before proceeding to the enrolment of each biometric modality. Once the enrolment process is completed, the following screen is showed:

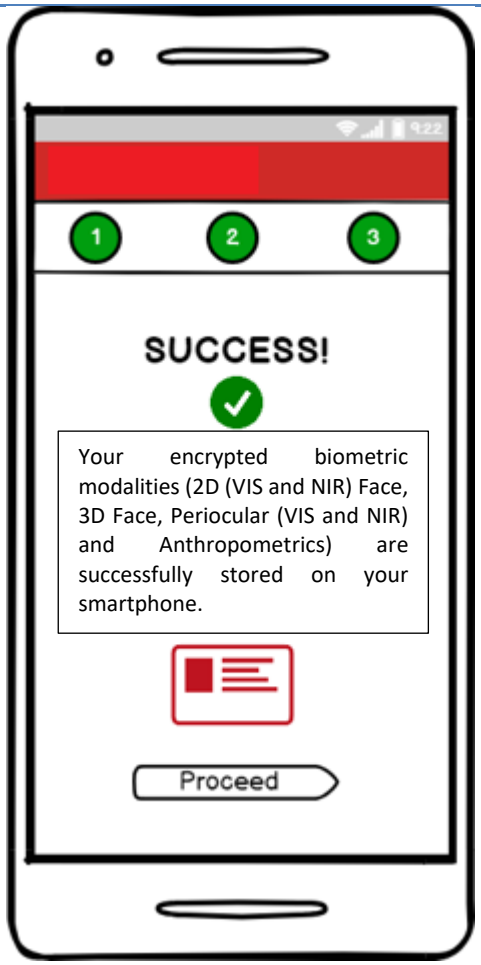


Figure 14 - Consent screen 5

Express consent prior to sharing data with the system	When approaching a PROTECT Control System and before connecting, the following screen is showed:

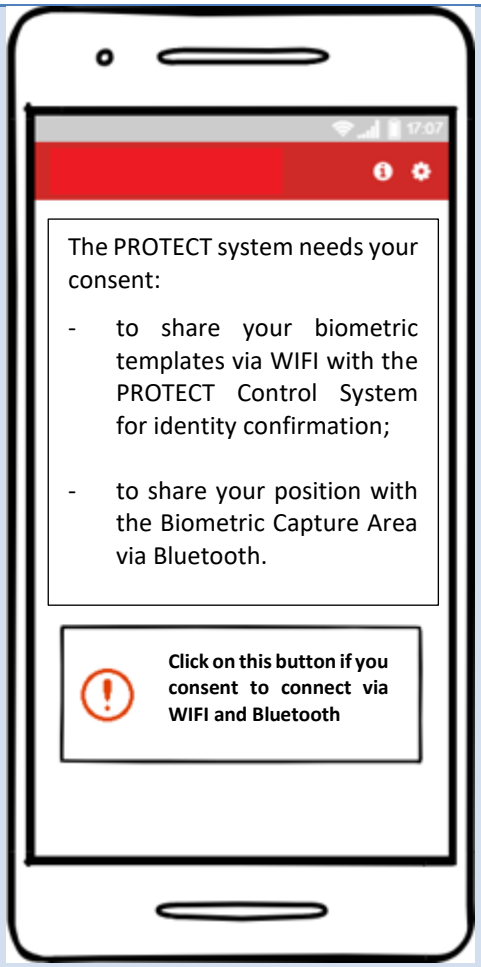


Figure 15 - Consent screen 6

Obtaining parents' consent for minors.	Not applicable. The PROTECT programme is not available for minors.
After a long period without use, the user must be asked to confirm his/her consent	Applicable. If the user does not use the system during one year, the application will ask the traveller whether he still wants to use it or wants to remove it.
Where the user has consented to the processing of special data (e.g. his/her location), the interface clearly indicates that said processing takes place (icon, light)	When approaching to the Biometric Control Area, the following screen is showed to the traveller:

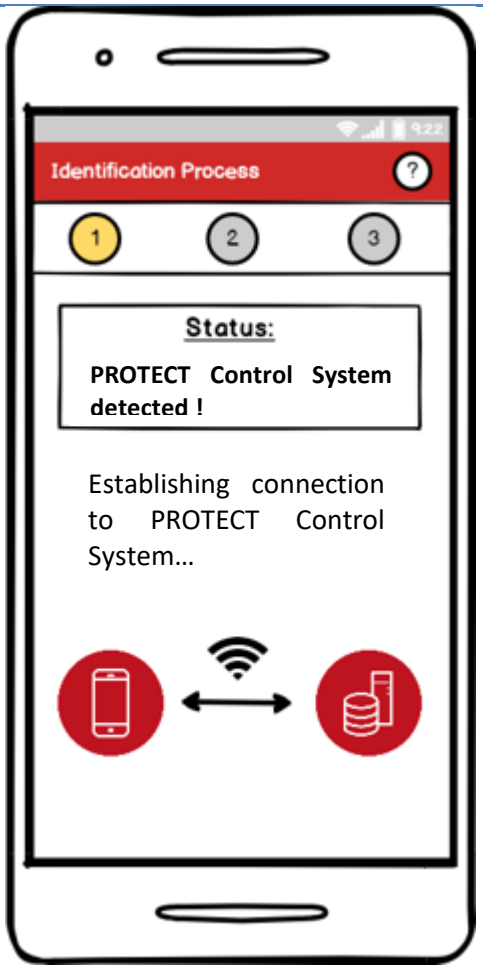


Figure 16 - Consent screen 7

The following is screen appears once the application is connected to the PROTECT Control System:

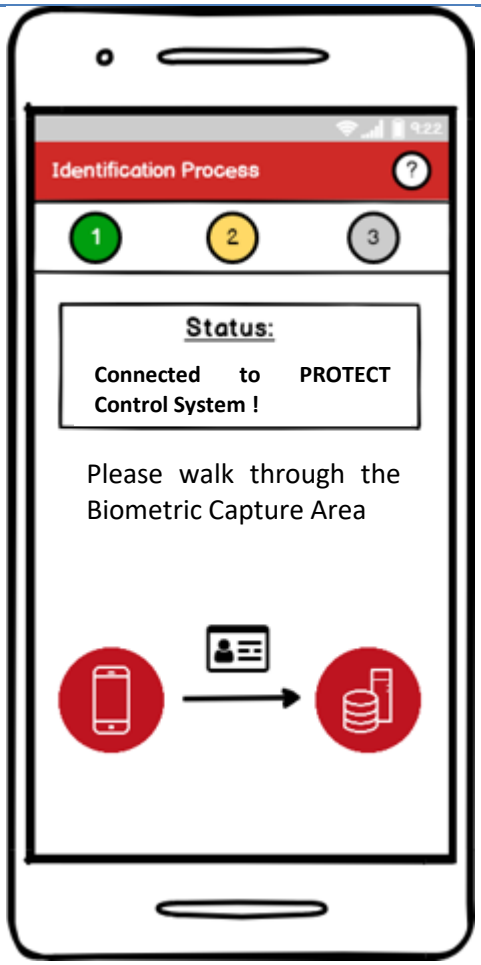


Figure 17 - Consent screen 8

This screen appears after the user's biometric templates where successfully compared against the once gathered in the Biometric Capture Area:

Figure 18 - Consent screen 9

Where the user changes device, smartphone or computer, reinstalls the mobile app, the settings associated with his/her consent are maintained	Not feasible. If the user changes device or removes application, he must proceed to a new enrolment of biometric modalities at the Enrolment Kiosk.

Table 13 - Controls for obtaining consent

3.2.2.3 Controls for the rights of access and to data portability

Article 15 of the GDPR provides data subjects with the right to obtain from the data controller access to their data, in general including their biometric data. If the data controller has to ascertain the identity of the data subjects to grant this access, it is essential that such access is provided without processing additional personal data.

In the figure below, you will find a list of the controls intended to ensure users' right of access to all personal data concerning them.

Controls for the right of access	Mobile app	PROTECT's servers	Justification
Possibility of accessing the user's personal data, via the	Possibility to access the encrypted templates of biometric modalities which are stored on the smartphone	However, possibility to access the biographic data, accounting data and unencrypted templates of biometric modalities by	Access to raw biometric modalities is not feasible since that they are not stored by the system.

common interfaces		sending a request of access to the PROTECT's controller	Direct access to unencrypted templates is not feasible since that the cryptographic key is internally stored in PROTECT's servers for security reasons.
Possibility of securely consulting the traces of use associated with the user	Possibility to access the traces of use generated by the mobile application	Possibility to access event logs (Application traces, timestamps of new biometric enrolment for the same traveller) by sending a request of access to the PROTECT's controller	N/A
Possibility of downloading an archive of all the personal data associated with the user	Possibility to download the encrypted templates of the biometric modalities which are stored on the smartphone	Not directly feasible. However, possibility to download an archive of the biographic data, accounting data, event logs and unencrypted templates of biometric modalities by sending a request of access to the PROTECT's controller	N/A

Table 14 - Controls for the right of access

The right to data portability applies to the PROTECT processing pursuant to Article 20 of the GDPR. It allows for data subjects to receive the personal data that they have provided to a controller, in a structured, commonly used and machine-readable format, and to transmit those data to another data controller. The new right to data portability aims to empower data subjects regarding their own personal data, as it facilitates their ability to move, copy or transmit personal data easily from one IT environment to another (whether to their own systems, the systems of trusted third parties or those of new data controllers)[45]. The right to data portability contains two parts:

- Firstly, data portability is a right of the data subject to receive a subset of the personal data processed by a data controller concerning him or her, and to store those data for further personal use. Such storage can be on a private device or on a private cloud, without necessarily transmitting the data to another data controller.
- Secondly, Article 20(1) provides data subjects with the right to transmit personal data from one data controller to another data controller "without hindrance". Data can also be transmitted directly from one data controller to another on request of the data subject and where it is technically feasible. In essence, this element of data portability provides the ability for data subjects not just to obtain and reuse, but also to transmit the data they have provided to another service provider (either within the same business sector or in a different one).

This being said, this right to data portability only applies "when technically feasible"[46] and when it does "not adversely affect the rights and freedoms of others"[47]. With this regard, it is important to recall the Article 29 Working Party's opinion according to which "biometric templates should be extracted in a way that is specific

[45] See Article 29 Working Party, Guidelines on the right to data portability, WP 242, as last revised and adopted on 5 April 2017.
[46] Article 20(2) of the GDPR.
[47] Article 20(4) of the GDPR.

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"[48]. In order to avoid function creep and violation of the purpose limitation principles, it is hence not technically feasible to provide data subjects with "re-useable" biometric templates.

The figure below describes its implementation in the PROTECT system.

Controls for the right to data portability	Mobile app	PROTECT's servers	Justification
Possibility of retrieving, in an easily reusable format, personal data provided by the user so as to transfer them to another service	Encrypted biometric templates are stored on the smartphone. These are accessible to the data subject. However, re-use of these templates by a different data controller is not technically feasible while ensuring respect of the purpose limitation principle (avoiding function creep).	Only data stored in servers is biographic data and accounting data. These can be retrieved in XML format.	Function creep has been a serious concern since the biometric technologies and systems were first used. Therefore, the WP29 recommends that "biometric templates 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".

Table 15 - Controls for the right to data portability

3.2.2.4 Controls for the rights to rectification and erasure

Controls for the rights to rectification and erasure	Mobile app	PROTECT's servers	Justification
Possibility of rectifying personal data	Possibility to proceed to a new enrolment of biometric templates at the Enrolment Kiosk	Possibility to rectify biographic and accounting data by request to the PROTECT's data controller	N/A
Possibility of erasing personal data	Possibility to erase the application including the biometric templates	Possibility to erase biographic and accounting data by request to the PROTECT's data controller	N/A

[48] See Article 29 Working Party, Opinion 3/2012 on developments in biometric technologies, WP193, Adopted on 27th April 2012, p. 31.

Indication of the personal data that will nevertheless be stored (technical requirements, legal obligations, etc.)	N/A	Application traces, timestamps of new biometric enrolment for the same traveller, technical logs are kept pseudonymously during 3 years for security reasons and performance assessment of the system. Biographic and accounting data are stored until all payments are done.	N/A
Implementing the right to be forgotten for minors	The PROTECT system is not available for minors	The PROTECT system is not available for minors	N/A
Clear indications and simple steps for erasing data before scrapping the device	The "passport companion" will provide a screen containing clear indications and simple steps for erasing data before scrapping the device.	N/A	N/A
Advice given about resetting the device before selling it	The "passport companion" will provide a screen containing advice about resetting the device before selling it.	N/A	N/A
Possibility of erasing the data in the event the device is stolen	Not technically feasible unless the users' smartphone settings allow erasing data at distance in case of theft. The passport companion will strongly advice users to implement such settings.	N/A	N/A

Table 16 - Controls for the rights to rectification and erasure

3.2.2.5 Controls applicable to processors

A processing contract must be signed with each processor, setting out all of the aspects stipulated in Art. 28 of the GDPR: duration, scope, purpose, documented processing instructions, prior authorization where a processor is engaged, provision of any documentation providing evidence of compliance with the GDPR, prompt notification of any data breach, etc.

This section of CNIL's methodology does not apply to our scenario since that no data processors are involved.

3.2.2.6 Controls on transfer of data outside the European Union

EU data protection rules apply to the European Economic Area (EEA), which includes all EU countries and non-EU countries Iceland, Liechtenstein and Norway. When personal data is transferred outside the European Economic Area, special safeguards are foreseen to ensure that the protection travels with the data.

The reform of EU data protection legislation offers a diversified toolkit of mechanisms to transfer data to third countries: adequacy decisions, standard contractual rules, binding corporate rules, certification

mechanism, codes of conduct, so-called "derogations" etc. Depending on the country in question to which the controller of PROTECT wishes to transfer the data, he will have to justify the choice of remote hosting and indicate the legal supervision arrangements implemented in order to ensure adequate protection of the data subject to a cross-border transfer.

3.3 Study of data security risks

The CNIL defines a "privacy risk" as a *"hypothetical scenario that describes a feared event and all the threats that would allow this to occur"*[49]. More specifically, it describes:

- how risk sources (e.g.: identity fraud)
- could exploit the vulnerabilities of supporting assets (e.g.: biometric data require specific attention because they unambiguously identify an individual)
- in a context of threats (e.g.: spoofing)
- and allow feared events to occur (e.g.: unwanted use of personal data)
- on personal data (e.g.: a user's biometric templates)
- thus generating impacts on the privacy of data subjects (e.g.: misappropriation of commercial services not compensated).

The following diagram summarises all the concepts above:

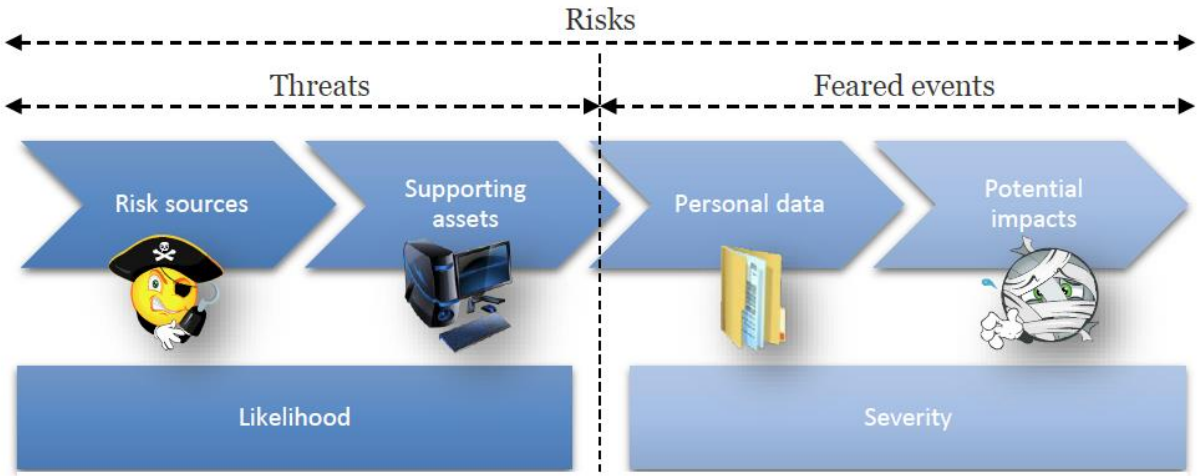


Figure 19 - Risk components

The risk level is estimated in terms of severity and likelihood:

- severity represents the magnitude of a risk. It primarily depends on the prejudicial nature of the potential impacts[50];
- likelihood expresses the possibility of a risk occurring. It primarily depends on the level of vulnerabilities of the supporting assets when under threat and the level of capabilities of the risk sources to exploit them.

[49] CNIL, PIA Methodology, February 2018, p. 8.
[50] In view of the context of the processing of personal data (nature of data, data subjects, purpose of the processing, etc.).

3.3.1 Best practices related to the assessment of security controls

The aim of this section is to provide to a potential data controller of the PROTECT system, best practices to identify or determine the existing or planned controls (already undertaken), which can take three different forms:

- controls bearing specifically on the data being processed: encryption, anonymization, partitioning, access control, traceability, etc.;
- general security controls regarding the system in which the processing is carried out: operating security, backups, hardware security, etc.;
- organizational controls (governance): policy, project management, personnel management, management of incidents and breaches, relations with third parties, etc.

3.3.1.1 Best practices for controls treating the risks related to data security

According to the Article 29 Working Party, *"given their nature, the processing of biometric data requires special technical and organisational measures and precautions to prevent adverse effects to the data subject in the event of a data breach - in particular because of the risks of unlawful conduct resulting into the unauthorised "reconstruction" of a biometric feature from the reference template, their interlinking with different databases, their further "use" without the data subjects knowledge for non-compatible purposes with the original ones and/or the possibility that some biometrics data could be used to reveal racial or health information about subjects".*[51]

The table hereunder presents the best practices recommended by the Article 29 Working Party for controls bearing specifically on biometric data.

Controls bearing specifically on biometric data	Best practices
Use of biometric templates	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.
Storage on a personal device vs. centralised storage	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.

[51] Article 29 Working Party, Opinion 3/2012 on developments in biometric technologies, WP193, Adopted on 27th April 2012, p.31.

	However, for specific purposes and in presence of objective needs centralised database containing biometric information and/or templates can be considered admissible. 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. Furthermore, such decentralised systems provide for a better protection of the biometric data by design as the data subject stays in physical control of his biometric data and there is no single point that can be targeted or exploited. The Working Party also stresses that the idea of a centralised database covers a wide range of technical implementations from the storage within the reader to a network hosted database.
Renewability and revocability	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 multiple and independent biometric templates to 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.
Encrypted form	As for the security issue, adequate measures should be adopted to safeguard the data stored and processed by the biometric system: biometric information must always be stored in encrypted form. A key management framework must be defined to ensure that the decryption keys are only accessible on a need to know basis. Given the widespread use of public and private databases containing biometric information and the increasing interoperability of different systems using biometrics, the use of specific technologies or data formats that make interconnections of biometric databases and unchecked disclosures of data impossible should be preferred.
Anti-spoofing	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.
Biometric encryption and decryption	Biometric encryption is a technique using biometric characteristics as part of the encryption and decryption algorithm. In this case, an extract from biometric data is generally used as a key to encrypt an identifier needed for the service. This system has many advantages. With this system, there is no storage of the identifier or of the biometric data: only the result of the identifier encrypted with the biometrics is stored. Moreover, the personal data is revocable as it is possible to create another identifier that can be protected with biometric encryption as well. Finally, this system is more secure and

	easier to use to the person: it solves the problem of remembering long and complex passwords. However, the cryptographic problem to overcome is not easy because encryption and decryption are intolerant to any changes in the key, whereas biometric provides different pattern which may give rise to changes in the extracted key. The system must therefore be able to compute the same key from slightly different biometric data, without increasing the False Acceptance Rate.
Automated data erasure mechanisms	In order to prevent biometric information being 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.
"Weak link" databases	When a central database is used to counter identity fraud, the Working Party considers that technical measures must be implemented to avoid any purpose diversion. First, the data minimisation principle demands that only the data necessary to authenticate the person must be collected. For instance, it is considered that the comparison of the fingerprints of two fingers is precise enough to authenticate a person. Moreover, data controllers can use "weak link" databases where the identity of a person is not linked to a single biometric data set but rather to a group of biometric data set. The design of the database should guarantee the authentication of the person with a very good probability and make sure the database cannot be used for identification. The Working Party supports the use of such systems when large biometric databases are used for the purpose of struggle against identity fraud.

Table 17 - Security controls bearing specifically on biometric data

The aim of encryption is to make personal data unintelligible to anyone without access authorization. In the table below are detailed the CNIL's best practices to be followed if the measure is used to address risks.

Controls bearing on encryption	Best practices
General measures	• Determine what should be encrypted (including an entire hard disk, a partition, a container, certain files, data from a database or a communications channel, etc.) based on the form in which data is stored, the risks identified and the performance required. • Choose the type of encryption (symmetric or asymmetric) based on the context and the risks identified. • Adopt encryption solutions based on public algorithms known to be strong.

	• Establish measures to ensure the availability, integrity and confidentiality of the information necessary to recover lost secrets.
Specific measures for symmetric encryption	• Only use a key for a single purpose. • Choose a mechanism that is recognized by the appropriate organizations. CNIL recommends the use mechanisms such as the AES algorithm which use a processed block size equal to at least 128 bits, a non-deterministic encryption scheme (such as a CBC mechanism with a random initialization vector), cryptographic keys of a length appropriate to the expected useful life (for example, at least 128 bits for confidentiality guaranteed until 2020) and which are not weak keys, etc. • Formally document the key management system.
Specific measures for asymmetric (public key) encryption	• Only use a key for a single purpose. • Choose a mechanism recognized by the appropriate organizations and that provides security proof. The CNIL recommends to use mechanisms such as the RSAES-OAEP which use cryptographic keys of a length appropriate to the expected useful life (for example, at least 128 bits for confidentiality ensured until 2020). • CNIL recommends generating the keys using a registered electronic certificate service provider. • Establish mechanisms for verifying the electronic certificates. CNIL recommends that when an electronic certificate is received, confirm, at a minimum, that it includes an indication of purpose consistent with expectations, is valid and has not been revoked and that a proper certification chain exists at all levels. • Protect the security of key generation and use consistent with their level in the key hierarchy. CNIL recommends protecting users' keys when stored (including restrictive rules governing access rights, password, chip and PIN card, etc.) and applying heightened security measures (for example: require that several of the holders of part of the secrets use the keys or store them in a safe deposit box) to the generation and use of a key management infrastructure's root keys (those that will be used to sign the other keys), etc. • Formally document the key management system. CNIL recommends developing a "certification policy" that specifies responsibilities, identification and authentication, certificate life-cycle operational requirements, non-technical and technical security measures, certificate and revocation list profiles and compliance audits and other evaluations.
Specific measures for encrypting equipment	• Encrypt data at the hardware level (surface of the hard disk) or at the operating system level (encryption of a partition or a container).

	• Choose systems that do not store keys on the equipment that will be encrypted unless this implements a secure storage device (such as a TPM chip for laptops).
Specific measures for encrypting databases	Based on the risks identified, encrypt the storage area (at the level of the hardware, operating system or database) so as to provide protection from physical theft, of the piece of data itself (encryption by application), with a view to guaranteeing the confidentiality of certain data as regards the administrators themselves. In the event of partitioned IT teams, database encryption can make data accessible only to database administrators, to the exclusion of system administrators.
Specific measures for encrypting a communications channel	• Encrypt the communications channel between an authenticated server and a remote client. CNIL recommends to use a service authentication certificate that complies with the most recent version of the TLS protocol (formerly SSL; consider requiring a password to use the private key and protecting access to it via very restrictive access rights), or SSH to set up a secure tunnel (VPN) or IP (VPN-IPSec) encryption solutions.
Specific measures for Wi-Fi	• Use the WPA or WPA2 protocol with AES-CCMP encryption or the "Enterprise" mode of the WPA and WPA2 protocols (using a RADIUS server as well as the EAP-TLS or PEAP subprotocols).

Table 18 - Controls bearing on encryption

The table below enumerates CNIL's best practices related to additional measures for treating the risks related to data security.

Additional measures for treating the risks related to data security	Best practices
Data partitioning (in relation to the rest of the information system)	The aim of data portioning is to reduce the possibility of personal data being correlated and of a blanket data breach occurring (identify the datasets specific to each business and separate them in logical fashion, etc.). With this regard, CNIL's recommendations are: • Identify the sole data necessary for each business process. The goal is to provide individuals with access only to the data they need. For example, do not provide the statistics department with access to first and last names. • Separate the data useful to each process in logical fashion. Manage the different access rights according to the business processes and establish a dedicated IT environment for systems that process the most sensitive data. • Regularly confirm that personal data are partitioned effectively and that recipients and interconnections have not been added.
Logical access control	• Manage users' profiles by separating tasks and areas of responsibility (preferably in centralized fashion) to limit access to personal data exclusively to authorized users by applying need-to-know and least-privilege principles. • Identify every person with legitimate access to personal data by a unique identifier.

	• Limit access to the tools and administration interfaces to authorized persons. • Where applicable, specify the rules applicable to passwords (minimum length, required characters, validity duration, number of failed attempts before access to account is locked, etc.). • Log information connected to the use of privileges.
Traceability (logging)	The aim of traceability is to ensure that consultation and action carried out by users of the processing are recorded and attributed, such that it is possible to provide evidence during investigations (logging system, protection, analysis, storage, etc.). With this regard, CNIL's recommendations are: • Set up an applicative logging system that retains a record of data modifications and access carried out by the users and the time they took place. Date- and timestamp the logged incidents based on UTC time (Coordinated Universal Time), use a reliable time source (such as an NTP (Network Time Protocol) server or radio synchronization) to synchronize the equipment, centralize locally (assemble all the logs on a relatively isolated collection machine supported by a dedicated consultation workstation), export the logs (scheduled dispatches, automatic transfer or an administration network), provide for sufficient storage capacity, set up an archiving and backup system for the incident logs, protect the logging equipment and the information logged against sabotage and unauthorized access, ensure the strict confidentiality of logs, etc. • Set up user authentication, making it possible to attribute the logged incidents. Prohibit generic or shared identifiers, give precedence to strong, two-factor authentication, etc. • Comply with the requirements of the GDPR as regards logged events attached to an identified user. It is necessary to inform users of the traceability set up and not to use the records collected for other purposes, etc. • Conduct periodic analyses of the logged information and, if needs be, establish a system that detects abnormal activity automatically.
Integrity monitoring	The aim of integrity monitoring is to be warned in the event of an unwanted modification or disappearance of personal data (hash function, message authentication code, electronic signature, preventing SQL injections, etc.). With this regard, CNIL's recommendations are: • Identify the data that must be monitored for integrity based on the risks identified. • Choose a method for monitoring their integrity based on the context, the risks assessed and the robustness required.

	• Determine when the function is to be applied and when the monitoring should be performed based on implementation of the business process. • When the data are sent to a database, analytical measures must be set up to prevent scripting or SQL injection attacks.
Paper document security	As a reminder, in our scenario the PROTECT data processing is based on a contract with data subjects. Where paper documents containing data are used during the processing, indicate here how they are printed, stored, destroyed and exchanged.

Table 19 - Additional measures for treating the risks related to data security

3.3.1.2 Best practices for controls treating the risks related to the processing system

The following CNIL's best practices for controls generally concern the security of the whole system in which the processing is carried out. They can particularly be formally documented in a cybersecurity policy (PSSI) or equivalent.

General security controls regarding the system in which the processing is carried out	Best practices
Operating security	The PROTECT data controller should describe here how the software updates (operating systems, applications, etc.) and application of security corrective controls are carried out.
Clamping down on malicious software	The PROTECT data controller should state here whether an antivirus software is installed and updated at regular intervals on the workstations.
Managing workstations	The PROTECT data controller should describe here the controls implemented on workstations (automatic locking, firewall, etc.).
Backups	The PROTECT data controller should indicate here how backups are managed and clarify whether they are stored in a safe place.
Maintenance	The PROTECT data controller should describe here how physical maintenance of hardware is managed, and state whether this is contracted out. Indicate whether the remote maintenance of apps is authorized, and according to what arrangements. Specify whether defective equipment is managed in a specific manner.
Security of computer channels (networks)	The PROTECT data controller should indicate here the type of network on which the processing is carried out (isolated, private or Internet. In our scenario, the Enrolment Kiosk, the PROTECT control system and the BCA should all be disconnected from Internet. Specify which firewall system, intrusion detection systems or other active or passive devices are in charge of ensuring network security.
Monitoring	The PROTECT data controller should indicate here whether real-time monitoring of local network is implemented and with what means. Indicate whether monitoring of hardware and software configurations is carried out and by what means.
Physical access control	The PROTECT data controller should indicate here how physical access control is carried out regarding the premises accommodating the processing (zoning, escorting of visitors, wearing of passes, locked doors and so on). Indicate whether there are warning procedures in place in the event of a break-in.

Hardware security	The PROTECT data controller should indicate here the controls bearing on the physical security of servers and workstations belonging to customers (secure storage, security cables, confidentiality filters, secure erasure prior to scrapping, etc.).
Avoiding sources of risk	The PROTECT data controller should indicate here whether the implantation area is subject to environmental disasters (flood zone, proximity to chemical industries, earthquake or volcanic zone, etc.). Specify if dangerous products are stored in the same area.
Protecting against non-human sources of risks	The PROTECT data controller should describe here the means of fire prevention, detection and fighting. Where applicable, indicate the means of preventing water damage. Also specify the means of power supply monitoring and relief.

Table 20 - Controls treating the risks related to the processing system

3.3.1.3 Best practices for organizational controls (governance)

Organizational controls (governance)	Best practices
Organization	The PROTECT data controller should indicate if the roles and responsibilities for data protection are defined. Specify whether a person is responsible for the enforcement of privacy laws and regulations. Specify whether there is a monitoring committee (or equivalent) responsible for the guidance and follow-up of actions concerning the protection of privacy.
Policy (management of rules)	The PROTECT data controller should indicate whether there is an IT charter (or equivalent) on data protection and the correct use of IT resources.
Risk management	The PROTECT data controller should indicate here whether the privacy risks posed by new treatments on data subjects are assessed, whether or not it is systematic and, if applicable, according to which method. Specify whether an organization-level mapping of privacy risks is established.
Project management	The PROTECT data controller should indicate here whether device tests are performed on non-real/anonymous data.
Management of incidents and data breaches	The PROTECT data controller should indicate here whether IT incidents are subject to a documented and tested management procedure.
Personnel management	The PROTECT data controller should indicate here what awareness-raising controls are carried out with regard to a new recruit. Indicate what controls are carried out when persons who have been accessing data leave their job.
Relations with third parties	As a reminder, in our scenario, no data processors are involved. However, if it was the case, the PROTECT data controller should indicate here, for processors requiring access to data, the security controls and arrangements carried out as regards such access.
Supervision	The PROTECT data controller should indicate here whether the effectiveness and adequacy of privacy controls are monitored.

Table 21 - Organizational controls (governance)

3.3.2 Risk assessment: potential privacy breaches

According to the Article 29 Working Party, in data processing activities involving biometrics, a DPIA should aim to assess how the three following risks can be avoided or substantially limited by the system it analyses[52]:

1) The first risk is identity fraud/inaccuracy, especially in the case of identification and authentication. The biometric device should not be fooled by a spoofing attack and ensure that the person who is attempting to perform the matching really is the person that is registered in the system.
2) The second risk is the purpose diversion either by the data controller itself or by a third-party including law enforcement authorities. This common threat regarding personal data becomes a crucial one when biometric data are used. Manufacturers should take all security measures to avoid any improper use of the data and make sure that any data that are not needed anymore for the purpose of the processing are deleted immediately. As with any other data, legitimately processed or stored biometric data or the sources of biometric may not be processed or enrolled by the controller for any new or other purpose unless there is a new legitimate ground for this new processing of these data.
3) The third risk is data breach that requires in the biometric data context special actions depending on which kind of data have been compromised. If a system is used that creates biometric data based on an algorithm that converts a biometric template into a certain code, and either the biometric data or the algorithm is stolen or compromised they need to be replaced. When a data breach involves the loss of directly identified biometric data that are very close to the source of biometric data such as pictures of faces or fingerprints, the concerned person needs to be notified in detail in order to be able to defend himself in a possible future incident where these compromised biometric data may be used against him as evidence.

The general objective of the next sections is to gain a good understanding of the causes and consequences of risks of the PROTECT system for the data subjects. Hence, for each feared event (identity fraud/inaccuracy, purpose diversion, and data breach[53]), the aim of these sections is to:

1. determine the potential impacts on the data subjects' privacy if it occurred[54];

2. estimate its severity, particularly depending on the prejudicial nature of the potential impacts and, where applicable, controls likely to modify them;

3. identify the threats to personal data supporting assets that could lead to this feared event[55] and the risk sources that could cause it;

4. estimate its likelihood, particularly depending on the level of vulnerabilities of personal data supporting assets, the level of capabilities of the risk sources to exploit them and the controls likely to modify them.

.

[52] Ibidem, p.30.
[53] They are not or no longer available (breach of personal data availability).
[54] Answer the question "What do we fear might happen to data subjects?".
[55] Answer the question "How might this happen?".

3.3.2.1 Identity fraud

Risk	Main risk sources[56]	Main potential impacts[57]	Main controls reducing the severity and likelihood	Severity[58]	Likelihood[59]
Identity fraud (spoofing)	Rogue acquaintances Rogue neighbour Rogue employee Negligent data subject Hacker targeting a user's smartphone Hacker targeting the PROTECT control system Hacker targeting the Biometric Capture Area	Unanticipated payments (e.g. erroneously), additional costs (e.g. bank charges) Lost opportunities of comfort Blocked services account Feeling of invasion of privacy without irreversible damage Minor but objective psychological ailments (defamation, reputation)	Pseudonymization Use of biometric templates Storage on a personal device vs. centralised storage Renewability and revocability of the templates Encrypted communications channels Anti-spoofing measures Biometric encryption and decryption Multimodal biometric fusion	Limited: Data subjects may encounter significant inconveniences, which they will be able to overcome despite a few difficulties.	Limited: It seems difficult for the selected risk sources to materialize the threat by exploiting the properties of supporting assets.
Inaccuracy	Data subject (improperly processes to enrolment or verification) Improper system tuning and setup adjustment at enrolment or verification (e.g. lightning conditions)	Denial of access to commercial services Deterioration in the service quality Need to proceed to a new enrolment at the	Employee clearance Physical access control Logical access control Traceability (logging) Notification of data subject	Data subjects may be subject to loss of time in repeating formalities or waiting for them to be fulfilled.	

[56] See typology of risk sources in CNIL, PIA Knowledge Bases, February 2018 edition, p.3.
[57] See typology of the outcomes of feared events in CNIL, PIA Knowledge Bases, February 2018 edition, p.3.
[58] See scales and rules for estimating severity in CNIL, PIA Knowledge Bases, February 2018 edition, p.4.
[59] See scale and rules for estimating likelihood in CNIL, PIA Knowledge Bases, February 2018 edition, p.6.

	External factors: biometric modality of data subject has changed over time	Enrolment Kiosk	violations and recommendation of suitable preventive controls		

Table 22 - Risk assessment of identity fraud

3.3.2.2 Purpose diversion

Risk	Main risk sources	Main potential impacts	Main controls reducing the severity and likelihood	Severity	Likelihood
Purpose diversion	Rogue acquaintances Rogue neighbour Rogue employee Hacker targeting a user's smartphone Hacker targeting the PROTECT control system Illegitimate request by law enforcement authorities	Improper use of biometric data by the data controller itself or by a third-party including law enforcement authorities. Inaccurate or inappropriate profiling Feeling of violation of fundamental rights (e.g. discrimination, freedom of movement) Criminal penalty	Pseudonymization Use of biometric templates Storage on a personal device vs. centralised storage Renewability and revocability of the templates Encrypted communications channels Anti-spoofing measures Biometric encryption and decryption Multimodal biometric fusion Employee clearance Physical access control Logical access control	Significant: Data subjects may encounter significant consequences, which they should be able to overcome albeit with real and serious difficulties	Limited: It seems difficult for the selected risk sources to materialize the threat by exploiting the properties of supporting assets

			Traceability (logging) Notification of data subject violations and recommendation of suitable preventive controls		

Table 23 - Risk assessment of purpose diversion

3.3.2.3 Data breach

Risk	Main risk sources	Main potential impacts	Main controls reducing the severity and likelihood	Severity	Likelihood
Data breach	Rogue acquaintances Rogue neighbour Rogue/negligent employee Negligent data subject Hacker targeting a user's smartphone Hacker targeting the PROTECT control system	Disappearance of data Loss of evidence in the context of litigation	Pseudonymization Use of biometric templates Storage on a personal device vs. centralised storage Renewability and revocability of the templates Encrypted communications channels Anti-spoofing measures Biometric encryption and decryption Multimodal biometric fusion Employee clearance Physical access control Logical access control	Limited: Data subjects may encounter significant inconveniences, which they will be able to overcome despite a few difficulties	Limited: It seems difficult for the selected risk sources to materialize the threat by exploiting the properties of supporting assets

	Traceability (logging) Notification of data subject violations and recommendation of suitable preventive controls

Table 24 - Risk assessment of data breach

4 Conclusion

This Deliverable "D2.3 - Privacy impact of next-generation biometric border" applies the French data protection authority's (CNIL) data protection impact assessment methodology (DPIA) to an alternative (and legitimate in real-world conditions) scenario for the use of the PROTECT system in which emerging biometric modalities are processed in a "passport companion" such as a smartphone for "comfort and convenience purposes" of travellers on basis of a contract with the PROTECT's data controller and their explicit consent. In this scenario, emerging contactless biometrics are enrolled in a smartphone app for travellers willing to join a "PROTECT programme" allowing them to be given priority in waiting areas for "traditional" security and border checks and/or allowing them to benefit of additional convenience services such as access to VIP parking zones or waiting lounges. The aim of this DPIA is to assess the impact on data protection of a new category of access-control mechanism particularly suited for border-crossings based on multimodal biometric fusion "on the move" while respecting the legal framework and personal data security. The main findings of this DPIA are the following:

- According to the Article 29 Working Party, the requirement that "personal data must be collected for legitimate purposes" means that the purposes must be "in accordance with the law" in the broadest sense: "this includes all forms of written and common law, primary and secondary legislation, municipal decrees, judicial precedents, constitutional principles, fundamental rights, other legal principles, as well as jurisprudence, as such 'law' would be interpreted and taken into account by competent courts". Therefore, D3.1 scenarios[60] must be considered as "illegitimate" since that these would be in contradiction with the current legal framework on biometric border control as analysed in D2.2. For this reason, in this DPIA, the purpose of the PROTECT system is deemed to be the allowance of "comfort and convenience" services to frequent travellers.
- The most appropriate ground of legitimacy for the use of the PROTECT system in our scenario would be a contract signed with a traveller for the purpose of offering him convenience services. Furthermore, given that biometric data is processed for the purpose of this contract, the traveller should provide an explicit consent to the controller of the PROTECT system.
- In order to achieve data minimization, no passport data neither raw biometric data is processed by the PROTECT system. In principle the raw biometric data may not be reconstructed from the templates. Furthermore, the use of pseudonymization and of multimodality using different biometrics in a simultaneous way makes it possible to use a "weak link" process where the pseudonym of a person (not directly his real identity) is not linked to a single biometric data set but rather to a group of biometric data sets. As a consequence, data minimization is improved by the fact

[60] In D3.1 scenarios, the purpose of the PROTECT system is to "facilitate" public border control authorities to speed up their public interest missions of border control management by enrolling emerging biometrics in travel documents (or smartphone apps acting as travel documents) in addition of passport information (including traditional biometric modalities – facial image and fingerprints).

that each single set of biometric data does not have to provide a very high probability of authentication as long as the fused biometric data set guarantees a high probability of authentication of a given pseudonym.

- According to the Article 29 Working Party, "taking into account the fact that biometric technologies cannot ensure full accuracy, there is always an implicit risk coming from incorrect identifications. Such false positives result in decisions affecting individual rights". The specific impact on data protection of inaccuracy of a particular biometric system depends on its purpose and particular circumstance. In the case of our scenario, a user subject to a false reject would face limited consequences such as a refusal to access to the commercial convenience services for which he paid. Given such limited consequences, a procedure which permits a data subject to proceed to a new enrolment at the Enrolment Kiosk seems to be an appropriate safeguard. The situation would of course be totally different if the PROTECT system was used for immigration control purposes or other public border control missions. In that case, implications on fundamental rights of data subjects would be much more severe, such as a violation of the right to free movement or to the right of liberty. In such a scenario, safeguards against false reject rates should be much more stringent.
- In order to prevent biometric information being 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 by the PROTECT system. With regards to this in our scenario, a very important safeguard is that almost no sensitive data are centrally stored. The biometric system is based on the reading of biometric data stored as encrypted templates on media that are held exclusively by the relevant data subjects (smartphones). The data subjects can easily remove any biometric templates on their phones by removing the application.
- The controller of the PROTECT system should publish a privacy statement/ notice on his website concerning the proposed service. A direct link to this privacy statement/ notice should be clearly visible on the website, on the Enrolment Kiosk and on the mobile application ("passport companion") under a commonly used term (such as "Privacy", "Privacy Policy" or "Data Protection Notice"). Indeed, for apps, the WP29 considers that "the necessary information should also be made available from an online store prior to download. Once the app is installed, the information still needs to be easily accessible from within the app. One way to meet this requirement is to ensure that the information is never more than "two taps away" (e.g. by including a "Privacy"/ "Data Protection" option in the menu functionality of the app). Additionally, the privacy information in question should be specific to the particular app and should not merely be the generic privacy policy of the company that owns the app or makes it available to the public".
- Explicit consent for the processing of biometric templates of data subjects should be sought at different stages of the PROTECT process. Furthermore, data subjects should be provided with controls for the rights of access and to data portability.
- The most critical security risks which are identified are identity fraud/inaccuracy, purpose diversion, and data breach. Each of these feared events have been assessed to be limited both in likelihood and in severity if the following main controls are implemented: pseudonymization, use of biometric templates, storage on a personal device vs. centralised storage, renewability and revocability of the templates, encrypted communications channels, anti-spoofing measures, biometric encryption and decryption, multimodal biometric fusion, employee clearance, physical access control, logical access control, traceability (logging), notification of data subject violations and recommendation of suitable preventive controls.

The findings of this Deliverable concern a suitable scenario for use of the system in "real-world conditions". These findings do not oppose demonstration of PROTECT technologies during the demonstration phase of

the project. Trials conducted exclusively for research purposes could demonstrate the feasibility of combining passport information (including traditional biometrics) and additional contactless biometrics of volunteers on the basis of their explicit consent with the aim to match their identities against fictional (emulated) “watchlists” specifically developed for these scientific trials. The data protection safeguards of such trials (such as consent forms and security requirements) will be described in a future version of D2.1 – “Data management Plan”.

Pervasive and UseR Focused BiomeTrics BordEr ProjeCT

(PROTECT)

H2020 – 700259

Security Sensitivity Assessment

Publication number:	D2.3
Publication title:	Privacy impact of next-generation biometric border control
Publication type:	Deliverable
Related WP number:	WP2
Which conference/journal, etc.	
Dissemination level: (Confidentiality)	PU
Version reviewed:	1.0
Date:	17/08/2018

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*:** The purpose of this Deliverable "D2.3 - Privacy impact of next-generation biometric border control" is to analyse if, as an alternative to D3.1 scenarios, emerging biometric modalities could be processed in a "passport companion" such as a smartphone for "comfort and convenience purposes" of travellers on basis of a contract with the PROTECT's data controller and their explicit consent. The idea is to analyse − from a privacy and data protection point of view − the possibility and the conditions in real-world conditions to enrol emerging biometrics in a smartphone app for travellers willing to join a "PROTECT programme" allowing them to be given priority in waiting areas for "traditional" security and border checks and/or allowing them to benefit of additional convenience services such as access to VIP parking zones or waiting lounges.

***List the results developed and presented in the publication/deliverable*:** This Deliverable performs a Data Protection Impact Assessment (DPIA) which is required by Article 35 of the GDPR. A DPIA is a process designed to describe the processing, assess its necessity and proportionality and help manage the risks to the rights and freedoms of natural persons resulting from the processing of personal data by assessing them and determining the measures to address them. In this Deliverable, the methodology which was chosen to conduct this DPIA is based on the one which was developed by the French Data Protection Authority (CNIL) in February 2018.

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: 17/08/2018

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	30/08/2018
Name: **On behalf of the Security Advisory Board (SAB)**	Krzysztof Romanowski
Signature of the member of the SAB	Krzysztof Romanowski