The Framework Programme for Research & Innovation
Research & Innovation Action (RIA)

Project Title:

SMart mobILity at the European land borders

SMILE

Grant Agreement No: 740931

[H2020-DS-2016-2017] SEC-14-BES-2016 Towards reducing the cost of technologies in land border security applications

Deliverable

D8.6. Ethics Manual and Guidelines for land BCPs

Deliverable No.		**D8.6**	
Workpackage No.	**WP8**	Workpackage Title and task type	**Legal and Ethical assessment on data privacy, Adaptive Ethics, Standardization and Regulatory Activities**
Task No.	**T8.4**	Task Title	**Societal/Ethical framework**
Lead beneficiary		**NTNU**	
Dissemination level		**Public**	
Nature of Deliverable		**Report**	
Delivery date		**Original Submission: 31 March 2018** **Revision: 05 November 2018**	
Status		**Final**	
File Name:		**[SMILE] D8.6_v2.0.pdf**	
Project start date, duration		**01 June 2017, 36 Months**	

This project has received funding from the European Union's Horizon 2020 Research and innovation programme under Grant Agreement n°740931

Authors List

Leading Author (Editor)				
Name		*Initials*	*Beneficiary Name*	*Contact email*
Mohamed Abomhara		MA	NTNU	
Co-authors (in alphabetic order)				
#	*Name*	*Initials*	*Beneficiary Name*	*Contact email*
1	Sule Yildirim Yayilgan	SYY	NTNU	
2	Lénárd Zsákai	LZ	HNP	
3	Andrei Baltatu	AB	RBP	

Reviewers List[1]

List of Reviewers (in alphabetic order)				
#	*Name*	*Initials*	*Beneficiary Name*	*Contact email*
1	*Alexandru-Aurelian Todor*	*ATO*	*Fraunhofer*	
2	*Santosh Kumar Rajaguru*	*SKR*	*Fraunhofer*	
3	*Yacine Rebahi*	*YRE*	*Fraunhofer*	
4	*Gemma Galdon Clavell*	*GGC*	*External ethical expert*	

[1] The minutes and the Action Items produced at each consortium meeting have been composed by the Coordinator of the Project and have been reviewed and accepted by all Consortium members before they were considered finalized.

Document history			
Version	Date	Status	Modifications made by
V1	20.03.2018	D	SYY
V1.1	22.03.2018	1st Draft	MA
V1.2	27/03/2018	2nd Draft	MA
V2	29/03/2018	Inputs from partners/ Telco	MA
V3	01/04/2018	3rd Draft	SYY
V4	06/10/2018	Revised version based on EC reviewers comments	MA
V4.1	23/10/2018	Update according to ethical helpdesk meeting/ comments	MA
V4.2	03/11/2018	Addressed comments from external ethical expert	MA

List of definitions & abbreviations

Term	Description
Personal data	Personal data is any information that relates to an identified or identifiable living individual. Different pieces of information, which collected together can lead to the identification of a person, also constitute personal data (Art. 4(1) GDPR).
Data subjects	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 (Art. 4(1) GDPR).
Consent	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 (Art. 4(11) GDPR).
Data controller	A legal person, public authority, agency or other body which, alone or jointly with partners determines the purposes and means of data processing (Art. 4(7) GDPR).
Data processor	A legal person, public authority, agency or other body which process personal data on behalf of the controller (Art. 4(8) GDPR).
Processing of personal data	Any operation or set of operations that is performed on personal data or on sets of personal data (Art. 4(2) GDPR). This is including operations such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.
Identification	The action or process of identifying someone. Biometric identification refers to identifying an individual based on his/her distinguishing physiological and/or behavioral characteristics.
Verification	A verification is referred to as 1:1 matching of a person makes a claim to his or her identity, presents biometric data, and the biometric system compares the presented biometric data to the data on file only for the claimed identity.
Authentication	Authentication is the process of determining whether someone or something is, in fact, who or what it declares itself to be.

Abbreviation	Definition
CFREU	Charter of Fundamental Rights and the European Convention on Human Rights
DPO	Data Protection Officer
EES	Entry/Exit System
EU	European Union
GDPR	General Data Protection Regulation
HNP	Hungarian National Police

RBP	Romanian Border Police
SIS II	Second-generation Schengen Information System
SLTD	Stolen and Lost Travel Documents
TCN	Third Country National
ETIAS	Travel Information and Authorization System
VIS	Visa Information System
UDHR	Universal Declaration of Human Rights

Executive Summary

Biometric technologies are the automated recognition of individuals based on their behavioral and biological characteristics. They are successfully and efficiently used as a valuable element of border control systems. The SMILE project, as a border control tool, increases the tendency to collect, use and process sensitive biometric data like fingerprints, face recognition and iris recognition etc. to improve travelers flow and enhance border security. On the one hand, SMILE technologies aiming to enhance the security level and make identification and authentication procedures of travelers easy, fast and convenient. On the other hand, SMILE technologies as other biometrics technologies have raised new threats to fundamental rights and personal privacy. It has been noted in the literature that biometric recognition have had a positive impact on border crossing at airports, identifying fugitives and criminals, and with the right development, can also be implemented at land borders. Biometric technologies provide a computerized decision-making support to border control authorities, and are intended to increase the reliability and efficiency of border control measures. However, lack of transparency and lawfulness of the data processing could lead to risks to the rights of person such as discrimination against individuals, social exclusion and intrusion into an individual's private life etc.

The main objective of this deliverable is to discuss the ethical implications of the existing and forthcoming biometric technologies that are (or are considered to be) employed in the border control application area. This deliverable provides a brief overview of SMILE project and biometric technologies as a tools for border control systems to control cross-border traffic, discusses possible proportionality ethical issues and privacy risks raised by the increasingly widespread use of biometric data, as well as good/best practises developed in SMILE project members concerning SMILE system design and implementation with a specific attention to ethical issues as well as participant recruitment and involvement.. The findings of this deliverable bring to the fore the main challenges which SMILE should deal with, during the SMILE system development and on a long-term basis, as a consequence of the SMILE technologies being used as border control tools. Ethical and legal considerations with regards to biometric data usage are directly related to the right to protection of personal data, which is part of the rights protected under the European Convention of human rights. Specific protection is required to the process and use of sensitive data which reveals certain personal characteristic and is related to the health status of individuals. Moreover, privacy concerns have become widely shared due to the fact that every time the biometric of a person is checked, a trace is left that could reveal personal and confidential information. This

deliverable increase SMILE consoritum and public awareness of potential violations of privacy and human rights and could be useful for future investigations in the area of border control and biometrics technologies.

Table of Contents

List of figures

List of Tables

1. Introduction

In this deliverable, ethical issues surrounding the actual and proposed use of biometrics technologies within the EU are identified. The deliverable starts by giving a brief background on the use of biometrics and ethics in **Section 1.1**. This is followed by an expilanation of the use of biometric technologies in the SMILE project in **Section 1.2**. and a short descriptiontion of the prupose of this deliverable in **Section 1.3**. Furthermore, **Section 2** summarizes ethics definitions and ethical theories underpinning the SMILE project, followed by a summary of ethical standards and norms governing border guard officials and a description on ethical reasoning and decision making and how ethical actions and decision can be taken with respect to presented ethical theories and ethical standards and norms. **Section 3** discusses ethical implications in the context of biometrics technologies with regards to human rights and privacy, human dignity, seniors and minors rights, etc., followed by a preliminary conclusion about the ethical implications and list of a recommendations for SMILE. **Section 4** presents the SMILE ethical framework. It presents the role of the SMILE ethical helpdesk and discusses a the ethical considerations for SMILE with respect to human rights, travelers with physical or mental impairment and considerations privacy and data protection, followed by the procedures for monitoring of SMILE ethics and the plan for ethical and privacy impact assessments integration in SMILE with check-list for SMILE ethics assessment. **Section 5** provides the guidelines for SMILE research ethics. It discusses the role of DPO and data control in SMILE project. **Section 6** presents the process of recruiting participants for the SMILE project and how their privacy is ensured by reviewing general principles of privacy such as informed consent. **Section 7** concludes the document.

1.1 Biometric technology and ethics

Biometric technologies are automated methods of recognizing and verifying the identity of individuals based on physiological or behavioural attributes [1, 2]. The main applications are government-related, e.g. ID cards, e-passports, e-borders and national security as well as policing systems etc. [3-5]. For instance, the European States are starting more and more projects that make use of biometrics technologies [6]. More significantly, in many settings across Europe potential or actual uses include traveler identification and verification by storing data in EU biometric information systems, such as EURODAC, VIS and SIS II [7]. In addition, four new IT systems are planned: The Entry-Exit System (EES), the European Travel Information and Authorization System (ETIAS) [8, 9], the European Criminal Records Information System for Third-Country Nationals (ECRIS-TCN) and most crucially, the IT system meant to ensure interoperability across existing and planned systems [7, 10]. Information technology is

at the heart of current border reconstruction. SMILE[2] is a research project, based on biometric technonlogies, aimed to achieve an automated, rapid and highly secure self-service clearance process, such that increasing passenger throughput does not compromise border control reliability. Information systems (e.g., SIS II, VIS and EES) employed for migration and border control and management in the EU involve several highly complex processes, leading to a number of ethics and privacy challenges [11]. The combination of biometric information systems and mobile technologies particularly leads to increased surveillance including collecting and storing face images, licence plates, fingerprints, etc. as individuals cross borders, apply for visas or request asylum [4].

The key issue is related to individual rights, such as respect for personal privacy [12, 13], human dignity [14], bodily integrity [15, 16], equity and personal liberty [11, 16, 17]. Personal data protection and confidentiality is also an issue, especially when biometric information is stored in centralized databases [18, 19]. People have the rigth to choose to what extent and how to engage with the systems and devices (e.g., biometric sensors and readers). For example, some people may avoid having their photographs taken for a face recognition system due to concerns about how the images will be used. Moreover, other people may refuse or feel uncomfortable to undergo iris scans or have photos taken for health reasons. Such concerns may impact particular groups on accounting of differences in how they interpret cultural beliefs, values and specific behaviors.

Another major concern with biometrics technologies usage is the seemingly immutable link between biometric traits and persistent information storage about a person [2]. Biometrics techniques are dependent on individuals' physical bodies. The tight link between personal records and biometrics can have both positive and negative consequences for individuals and the society overall. Recent research [20] on biometrics data shows that biometric data can reveal more personal information, such as gender, age, ethnicity and even critical health problems like diabetes, vision problems, Alzheimer's disease, etc. Such confidential information might be used for example to discriminate between individuals when it comes to border entry/exit enforcement and so on.

All in all, a range of complex and interconnected issues must be addressed in decision-making on the use of biometric technology as a tool for border control [6]. Regarding the fundamental rights and freedoms (e.g., *Charter of Fundamental Rights* and the *European Convention on Human Rights (CFREU)*) [21], a certain ethics guidelines must be formulated for SMILE to avoid

[2] http://smile-h2020.eu/smile/

harmful effects on society as well as to allow the continuous development of the technology. Biometrics data need special protection in terms of processing and usage. Data related to individuals including personal information revealing ethnic or racial origin, etc., is considered sensitive data. Legislation such as EU Charter focus particularly on protecting specific fundamental rights and freedoms of individuals. Table 1 summarize the fundamental ethical concerns from the the *Universal Declaration of Human Rights (UDHR)* [22, 23] and the CFREU.

Table 1: Summary of the fundamental ethical concerns and cross-references the relevant articles of CFREU and UDHR

Ethical concerns	*CFREU*	*UDHR*
Rights of individuals	• **Article 1:** Human dignity • **Article 3:** Right to the integrity of the person • **Article 6:** Right to liberty and security • **Article 7:** Respect for private and family life • **Article 8:** Protection of personal data • **Article 18 :** Right to asylum	• **Article 1** • **Article 3** • **Article 12**
Non-discrimination rights	• **Article 21:** Non-discrimination • **Article 22:** Respect cultural, religious and linguistic diversity	• **Article 7** • **Article 18**
Rights to Equality	• **Article 22:** Equality before the law • **Article 23:** Equality between men and women • **Article 24:** Rights of the child • **Article 25:** Rights of the elderly • **Article 26:** Integration of persons with disabilities	• **Article 2** • **Article 20**

1.2 The use of biometric technologies in SMILE for boder control

The SMILE project as a border control tool increases the ability to collect, use and process sensitive biometric data like fingerprints, face recognition and iris recognition etc. The intention is to implement an accurate, automated verification, control and monitoring system that is linked to land border management systems to optimize people flows. SMILE can be a very effective tool to improve border control as (1) to minimise the exposure of BCPs to security risks and threats and (2) to help BCPs successfully respond to security incidents while relieving them of all unnecessary and costly efforts to identify, acquire and use appropriate technology.

The potential and the actual use of biometrics in SMILE for border control include:

- Identification of travelers (one individual out of many) through data storage in national databases, such as the National Schengen Information System (N.SIS II) and EU biometric database (e.g., VIS and SIS II).

- Authentication or control (one-to-one and groups) using data stored in a travel document with the national option of identification via data stored in national and EU databases.

More about the SMILE use cases that consists of four operation modes (enrolment and preregistration as well as border crossing and verification) is discussed in depth in deliverable D2.2.

The tendency to use biometrics data in SMILE should improve and speed up border control management. SMILE system will store the personal data, including soft biometrics and hard biometrics including but not limited to, face characteristics, iris, fingerprint, face biometric, etc.). Travelers' biometric profiles definition is discussed in deliverable D3.1. However, because individuals (travelers) are surrounded by so many biometric sensors, serious ethical and privacy challenges arise. The efficacy of a biometric system can be affected by the ethical, cultural, social, and legal considerations that shape how people engage and interact with these systems [3, 6, 16, 17, 24, 25] (ethical implications are discussed in depth in section 3). According to the general principle of the *Universal Declaration of Human Rights* (UDHR) [22, 23], *"everyone has the right to freedom of movement and residence within the borders of each state and the right to leave any country, including his own, and to return to his country"* (Article 13 UDHR) [23]. Hence, it must be known that biometric technologies have major impacts on fundamental rights, notably on the right to dignity (Article 1 of the *Charter of Fundamental Rights of the European Union*) [26]; the right to liberty and security (Article 6), respect for private and family life (Article 7), the protection of personal data (Article 8), the right to asylum (Article 18), protection in the event of removal, expulsion or extradition (Article 19), the right to non-discrimination (Article 21) and the rights of the child (Article 24).

Furthermore, the EU has circumscribed regulations and rules pertaining to the protection of individuals' rights against the powers of authorities (e.g., border control authority) and their law enforcement branches. These rules specify under what conditions (strength of suspicion, severity of the suspected crime) a person may be required to provide biometric data such as fingerprints. Moreover, the right to privacy is specified in GDPR [27, 28] and in the police and criminal justice Directive 2016 (**Directive 2016/680**[3]), whereby data subjects must be informed of the purpose of data processing, the obligation to have biometric data collected, the right to rectify data, and finally, the right to request to have factually inaccurate or unlawfully recorded data be corrected or erased. If consent is required, rules are in place

[3] Directive (EU) 2016/680 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 by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA.

pertaining to what exactly a given consent covers; if a forced biometric search is allowed, specifications are usually given about when, how and who may perform the search [15].

This deliverable mainly focuses and discusses the ethical implications surrounding the use of biometrics as a means of recognizing individuals. To facilitate cross-border movement and maintain security (e.g., counter-terrorism) as well as increase smooth people mobility, it can surely be argued that balancing fundamental rights with biometric technologies are not absolute, but respect thereof remains a principle and any interference with rights must be carefully assessed.

1.3 Purpose of the document

This document is Deliverable D8.6 of Task T8.4 in WP8. The aim of D8.6 is to analyze the social and ethical implications of the SMILE services using biometric technologies and supportive material (i.e. ethical manual) and it will drive the developments of SMILE as well as similar projects in the future. Concerning the ethical recommendations and privacy issues for the SMILE technology, special attention will be given to address ethical, privacy issues raised by the project as well as the mobile biometry in general.

2. Moral, ethics and code of ethics

Morals are the general views, thoughts and convictions of people in making judgments about what is right or wrong. According to *Kizza* [24], morality is definded as *"a set of rules (code) of conduct that governs human behavior in matters of right and wrong, good and bad."* The moral judgment of what is good or bad and right or wrong is often based on a set of shared rules, principles, and duties applicable to all in a group or society. Ethics, on the other hand, is a branch of philosophy that deals with people's attitude and is also known as moral philosophy [24, 29]. Ethics concerns the way we can come to moral judgments of what is right and wrong for individuals and society. A code of ethics is a written set of ethical principles and guidelines that govern decisions and behaviors in an organization according to its primary values and ethical standards [30-32]. Before concluding what is right and what is not, we shall analyse and understand the set of rules (standards and norms) and eithcal theories comes from the code of ethics. The following subsection discusses a number of ethical theories and principles and presents an example of a code of ethics used by border police. The review of ethical theories and principles as well as standards and norms would help the decision makers to decide what is right and what is wrong?

2.1 Ethics theories underpinning the SMILE project

Ethical theories and principles are the foundation of ethical analysis in the SMILE project. They are the viewpoints that provide guidance along the path towards a final SMILE project. There are many ethical theories, each of which emphasizes different points, such as predicting an outcome and carrying out one's duties to others to reach an ethically correct decision. In the book "*Ethical and social issues in the information age*" [24] (page 32), *Kizza* discusses the most widely used ethical theories, namely consequentialism and deontology as well as absolutism and relativism.

Consequentialism emphasizes the consequences of human actions, whether good or bad, right or wrong. Deontological ethics does not concern the consequences of an action but rather it consider the will behind the action [33]. It is sometimes described as duty-based or rule-based ethics. The deontological prespective regards the action itself; the decision whether the action is right or wrong is not dependent on the consequences. Whereas in consequentialism (so-called result-based ethics), the outcome determines if the action is moral or not. Three consequentialism theory types that are frequently discussed are altruism, egoism and utilitarianism. According to the altruism theory, an action is right if its consequences are favorable to everyone except the actor [33]. In contrast, the egoism theory places an individual's interests and happiness above everything else. Unlike the altruism and egoism theories, utilitarianism is one of the most powerful and persuasive approaches to normative ethics concerning action consequences for the greatest number of people. The utilitarianism theory states that everyone's happiness counts the same and everybody should obey the rules that bring the maximum happiness to the greatest number of people. The classical utilitarian *Jeremy Bentham* identified the good with pleasure and happiness to maximize pleasure and minimize pain [34]. Therefore, one's good counts for no more than anyone else's good.

Absolutism assumes there is a fixed set of rules or ethical principles that apply at all times and should always be obeyed regardless of situational factors (e.g., authority, work roles) or individual factors (age, race, religion, gender, etc.) [35]. Absolute ethics is expressed as *"it is always right to…," "it is never right to…"* or *"it is always wrong to…"* For instance, it is always wrong to steal. Stealing is always considered immoral, even if it is done for the well-being of others (e.g., stealing food to feed a starving family). Relativist ethics, however, assumes that real ethical situations are more complicated than in absolutism. There are various acceptable ethical beliefs and practices and it is believed that the correct and most appropriate belief

depends on the situation. The best outcome is obtained by examining the situation and making ethical assessments based on the optimum outcomes to that situation [35].

When morally judging an action in reference to the outcomes or consequences, that action's benefits or harms remain debateable. To justifiy a person's action (e.g., the stealing to feed a starving family dilemma) in understanding how and why the decision was taken, *Kohlberg* presented a moral development theory of the processes the same person undergoes when making ethical decisions [36-38]. *Kohlberg's* moral theory consists of three moral development levels. Individuals at different levels of moral development might make the same moral decisions, but they will do so as a result of different reasoning processes: preconventional, conventional and postconventional. At the preconventional level, morality is viewed in terms of rewards, punishments and instrumental motivation. At the conventional level, morality is understood in terms of compliance with either or both peer pressure/social expectations or regulations, laws and guidelines. A high degree of compliance is deemed highly moral. At the postconventional level, morality conforms with perceived 'higher' or 'universal' ethical principles. Postconventional assumptions often challenge existing regulatory regimes and social norms; thus, postconventional behavior may be costly in personal terms. Ethics are not absolute and can be influenced by many factors: age, gender, culture, beliefs, education, moral imagination etc.

2.2 Ethical standards and norms governing border guard officials

Even though the distinction between law and ethics is often unclear, they are fundamentally different. They are both normative, but ethical norms are formulated as guidelines rather than prescriptions and prohibitions. The aim of the Code of Ethics for border guards is to provide moral guidance during service shifts and out of service shifts. Moreover, the Code of Ethics is to provide a moral basis for emerging professional choices and provide adequate protection for all those who act in a statutory manner, and to recognize the unworthy practices associated with the police profession. This section provide an overview of Code of Ethics for Romanian Border Police, Hungarian National Police (HNP) and the police in the Republic of Bulgaria (natioanl data protection regualtions and guidelines of Romanian, Hungarian and Republic of Bulgaria are discussed in Deliverable D8.1). Despite minor terminology differences, the intent of all both Code of Ethics is the same. Their intents are to (to name a few):

- Respect for and protection of fundamental rights and freedoms of a person.
- Non-discrimination, or equal treatment of persons.
- Confidentiality and respect for privacy.
- A prohibition on torture and cruel, unusual or degrading treatment.

2.2.1 Code of Ethics for Romanian Border Police (RBP)

The profession of border police officer can only be performed by those persons who possess physical, psychological and moral qualities that are appropriate to the society's needs. The border police officer, having the status of civil servant, must act in accordance with professional ethics, which includes specific rules derived from the particularities and requirements of his profession. The police ethics is the morality of the profession of the border police officer, reflected in the professional debts, and encompasses all the norms, rules and principles regarding the policeman's attitude towards citizens, society and colleagues, manifested in the exercise of the duties stipulated by the law. The border police officer's code of ethics and deontology groups (discussed in section 2.1) the whole issue of the morale of the police profession and consequently its provisions must be known and appropriated by all border police officers. The public opinion asks the civil servant and especially the border police officer a much more correct and dignified behavior than the other citizens of society. Through all they do, border police officers are called upon to combat and prevent those intentional evil actions, that represent dangers for Romania, to accommodate the evolution of conflicting states, because the stability, the state of tranquility and the order of any community are constantly claiming this thing. The code of ethics and deontology of the police officers was developed by the Romanian government decision 2005/991 with the intention of officially regulating the conduct of police officers in relations with members of the community being structured in 26 articles, which contain the moral norms that the police officers must observe in his activity and in life particular. According to Article 6, the principles governing the policeman's professional conduct are as follows:

1. **Legality** - in the exercise of its duties the police officer (border) is obliged to respect the law as well as the constitutional rights and liberties of the persons.
2. **Equality, impartiality and non-discrimination** - in the performance of professional duties, the police apply equal treatment to all persons, taking the same measures for similar situations of violation of the rules protected by the law, without being influenced by ethnic considerations, nationality, race, religion, political opinion or any other opinion, age, gender, sexual orientation, wealth, national or social origin, or any other situation.
3. **Transparency** - consists of the opening that the police officer must manifest to the society within the limits established by police regulations.
4. **Capacity and duty of expression** - is the ability of the police officer to analyse the professional situations he encounters and to express his / her point of view, according to his / her

training and experience, in order to improve the quality and effectiveness of the police service in relation to them.

5. **Availability** - requires the police to intervene in any situation in which they are aware of the attainment of any of the lawful values, regardless of the moment of its finding, the ability to listen and solve the problems of those in difficulty, or to point to other authorities' cases that are outside their competence or attributions.
6. **The priority of the public interest** - is manifested by the fact that, in order to fulfill the functional attributions, the policeman gives priority to the realization of the service for the benefit of the community
7. **Professionalism** - presupposes the correct and responsible application of the theoretical knowledge and of the practical skills for the exercise of the job attributions
8. **Confidentiality** - determines the duty of the policeman to guarantee the security of the data and information obtained in the exercise of the authority conferred by the law
9. **Respect** - is manifested by the consideration given by the police officer to persons, colleagues, superiors, subordinates, their rights and freedoms, institutions, laws, social values, ethical and deontological norms.
10. **Moral integrity** - presupposes the adoption of behavior according to ethical norms accepted and practiced in society.
11. **Operational independence** – consist in fulfilling attributions and missions according to the competencies established for the hierarchical level he / she occupies within the police, without the illegal interference of other policemen, persons or authorities.
12. **Loyalty** - it is expressed through the attachment to the institution and the values promoted by it, the conscious adherence manifested by the cop, on its own initiative, towards the objectives of the institution, respect for the hierarchy of the institution, honesty in interpersonal relations, respect for truth and justice , conscientiousness in the fulfillment of the attributions, observance of the assumed commitments, ensuring the confidentiality of the information obtained during the work process.

2.2.2 Code of Ethics for Hungarian National Police (HNP)

After the integration of the national Border Guard authority in Hungary (1st January, 2008), all the tasks related to border policing were allocated to the Hungarian National Police (HNP). Therefore, all of border policing officers has one Code of Ethics, which is the Code of Ethics of the Hungarian Police [39]. The Hungarian Police Code of Ethics consists of, among many others:

1. **Public service and participating in public service:** The members of the HNP do their tasks according to social will, in the public interest, among the opportunities provided by society. The members vocation is exercised in accordance with the instructions of the leaders and the executives, according to their oath, and offer the best of their knowledge.
2. **Honesty:** The members of the HNP shall be honest, disciplined, dutiful, refusing any open or covert request containing any content that is intended to deviate from the rules, eject corruption, act against all its forms and do not use police information except within the law-based service shifts.
3. **The prohibition of discrimination:** The members of the HNP should respect and protects human dignity, respects human and personal rights.
4. **Humanity and assistance:** The members of the HNP should be careful and do their tasks without prejudice and bad will. They shall not use torture, relentless, inhuman or degrading treatment and shall not tolerate it. They empathize, provide protection and help the needy.
5. **Collaboration:** The members of the HNP shall cooperate with the colleagues, cultured with them, in the spirit of mutual respect and appreciation. They shall share their knowledge and practical experience with the colleagues. They shall defend the lives of their companions and protect reputation.
6. **Responsibility:** The members of the HNP are responsible for the execution of their duties and their decisions in legal, moral and material terms. They shall be aware that all their judgements and acts are being taken on behalf of the whole Police.
7. **Quality of work:** The members of the HNP shall be well aware of the regulations governing their activity, they work with conscientiousness, high standards, lawfully, professionally and efficiently.
8. **Information:** The police member shall adhere to the privacy and data protection regulations, both in service and in private life.shall adhere to the privacy and data protection regulations, both in service and in private life.

2.2.3 Code of Ethics for police in the Republic of Bulgaria

2.2.3.1 Code of Ethics for officials of the Ministry of the Interior with police functions, 2004 [40]

The police in the Republic of Bulgaria is a state institution whose activities are aimed at serving the community [40]. It protects the life and property of citizens, maintains public order and counters crime under strict observance of the law, consideration of the basic rights and freedoms of citizens and affirmation of the principles of the state ruled by law. In its day-to-day activities the police strives after introducing professional standards and practices,

reaffirmed at European and world levels, in order to respond to the expectations of people and to build up a positive public image for itself. The rules of ethics for behaviour comprise the moral duty of every official. Every single police officer, carrying out his or her professional duties in service of the community, contributes to building up the image of the whole police institution. The officials of the Ministry of the Interior with police authorities are expected to accept the ethical norms of behaviour and to do their best in order to perform their duties in accordance with the principles of professional ethics. Non-compliance with the ethical norms of behaviour leads to undermining the prestige of the police institution, loss of public confidence and decrease in the support towards the police work in general.

PART II in the Code of Ethics [40] is about the consideration of human rights and freedoms and avoiding discriminatory behaviour;

- **Point 18.** The police considers and respects the rights of all people, stipulated by the European Convention on Human Rights and Basic Freedoms, the relevant international acts and the Bulgarian legislation.
- **Point 19.** The police adheres to the principle that every person accused of crime must be considered innocent until otherwise proven by the court.
- **Point 20.** In all its activities, the police respects the right of every individual to live, by using physical power, auxiliary devices or weapons only in cases, determined by the law, in case of absolute necessity and proportionate to the level of threat in the concrete situation.
- **Point 21.** In performing its professional duties, the police respects the dignity of every human being, and by no means performs, provokes or tolerates any acts of torture, inhumane or degrading behaviour or punishment.
- **Point 22.** The police respects the right of personal freedom and security and limits such right only in cases determined by the law and in a lawful manner.
- **Point 23.** The police respects the right of personal and family life, the forbidden access to homes and the confidentiality of correspondence, and limits such rights only in order to achieve lawful purposes.
- **Point 24.** The police performs its duties guided by the principles of equal treatment, avoiding discrimination, and forms its inner conviction only on the basis of the facts collected through legal means, and the data on the specific case.
- **Point 25.** The police, in its activities, always respects basic human rights, amongst which the right of freedom of thought, conscience, religion, expressing opinion, the right of peaceful gatherings, freedom of movement and peaceful use of property of every human being.

- **Point 26.** The police respects the individual citizens and communities, by considering their traditions, belief and way of life, in compliance with the state ruled by law.
- **Point 27**. In performing its professional duties, the police does not allow discrimination, based on any of the following grounds: sex, race, language, religion, education and belief, political attitudes, opinion, national or social origin, ethnic origin, disabilities, age, sexual orientation, personal and public position or possession of property or other/etc.

2.2.3.2 Code of Ethics for state officials

The civil servants of the Ministry of Interior, hereinafter referred to as “civil" servants/staff, are required to know the ethical rules of conduct by studying them included in their professional training. The rules of conduct contained in this Code, are an integral part of the day-to-day activity of civil servants/staff according to theirs functional competence. The activity of civil servants/staff is carried out in compliance with the following ethical principles principles of behavior (translated from Bulgarian language – an overview [41]):

- **Protection of human life** - in the performance of his/her duties he/she should behave to protect the right to life and personal security of the citizens by protecting and observing the constitutionally established principle of the right to life of everyone has the belief that the assault on human life is being pursued and punished as the worst offense;
- **respecting the dignity and rights of citizens** - respects the dignity of every person both in the performance of their official duties and outside the service and prefers no preference, bias or prejudices based on race, background, ethnicity and political affiliation, gender, religion, education, convictions, personal and social status or property status;
- **impartiality** - accurate, objective and unbiased performance of official duties, creating the conditions for equality between citizens in exercising their powers and avoiding behavior that can be perceived as privilege, predisposition or bias;
- **confidentiality** - behavior in line with international data protection principles and national legislation guaranteeing the privacy and privacy of citizens by preserving the facts and / or information that has become known to the employee in the course of or in connection with the performance of his / her duties;

The processing of personal data by civil servants/staff takes place in accordance with international data protection principles and domestic law and should be limited to the extent necessary for the fulfillment of legitimate specific objectives The official information available to the civil servant can not be or to be disclosed to persons other than those provided for by the order of the law.

2.3 Ethical reasoning and decision making

In view of the ethical theories and Code of Ethics discussed above as well as the open dilemma of what is right and what is wrong, it is clear that the situation is similar, particularly surrounding the SMILE project and the use of biometric technology. On the one hand, one group of people (e.g., travelers or/and border police officers) may see biometrics technology used by SMILE as a liberator, believing in the power of technology to bring convenience (e.g., avoid queues) and efficiency (e.g., cut costs) and increase mobility (e.g., enhance convenient border-crossing for citizens). This group may also welcome more powerful surveillance to improve border security (e.g., monitor migration, combat identity theft and fraud etc). We may agree with this group. First and foremost the SMILE system will be used to improve security at the land borders, however besides this main goal, it will maximize the benefits for the society (e.g., travelers) and minimize the human workload (e.g., border police officers) while improving security and detecting fraud. With respect to the utilitarianism theory (as discussed in section 2.1) and RBP Code of Eithcs (point(f), the priority of the public interest), HNP Code of Eithcs (point(1), public service and participating in public service) as well as the Code of Ethics for Bulgaria state officials, every society member (e.g., travelers, border police officers) benefit the same and it is not specific to any individual. Furthermore, the reason one individual must promote the overall good is the same reason why anyone else has to promote the good. Hence, it can be said that the ethics of the SMILE project is related to utilitarianism. The utilitarianism theory places a group's interest and happiness above those of an individual for the good of many.

On the other hand, other groups of people may object and perceive biometrics technology as a threat to their personal life and privacy. Such groups might believe that surveillance technology is untrustworthy and destructive to liberty, dignity and privacy. For example, collecting biometric data such as iris scanning from veiled Muslim women [42] in stressful situations (e.g., inappropriate police behaviour due to exhaustion or stress) may undermine the dignity of the women being scanned. An FRA report *"Under watchful eyes: Biometrics, EU IT systems and fundamental rights"* [10] showed that disproportionate force has been used when fingerprinting asylum seekers and migrants in irregular situations. Considering deontological ethics (duty-based or rule-based ethics) and given the vulnerability of the people concerned as well as the obligation to use the least invasive means, it is difficult to imagine justifying the use of physical or psychological force solely to obtain biometrics for the purpose of identification and verification. When it comes to border control and border rules, ethical theories might change according to circumstance. Border officers have a duty to do

the right thing (e.g., verify the identity of a traveler before entering/exiting the border, etc.) even if it produces an undesirable outcome. In the case of veiled Muslim women, it would be difficult to judge the action of an officer based on the outcome.

From the our review, it could be concluded that ethics are not absolute, and clearly, views on biometrics technology vary according to the differing needs of people and institutions. However, different perceptions of biometrics technology such as SMILE also reflect the diverse value judgements as influenced by many factors: age, gender, cultural beliefs, education, moral imagination, etc. An important conclusion to this subsection is that we are not attempting to provide an answer to what is ethical and what is not, or what is right and what is not. We see SMILE and biometrics technology usage in border control as a "two-edged sword." One edge is the main intention and aim of SMILE to improve border control management and enhance people flow etc. using biometric data. The other edge represents the risk of violating personal rights. As said, conflicts with decisions based on what to choose (e.g., privacy versus security, autonomy versus solidarity) make it difficult to have a broad and consistent position in favour of, or against expanding or restricting biometric technologies [11].

3. Ethics implications arising from biometric technologies

With the SMILE deployment, biometrics technology is acknowledged to potentially raise critical ethical, social and legal concerns. These can influence the social acceptability of biometric identification and verification methods. The following subsections highlight the fundamental ethical considerations regarding several aspects of the SMILE biometrics technology and services including right to privacy, right to liberty, right to non-discrimination and right to children and elderly etc.

3.1 Biometrics technology and right to privacy

Privacy can be described as individuals' state of deciding when, to whom and to what degree other individuals or organizations communicate or use discretely recognized data concerning them [12]. Every individual has the right to privacy protection of personal information when it is collected and shared. Generally, data protection and privacy provisions describe personal information protection throughout all steps from collection to storage and dissemination. According to GDPR [28], an individual's information can include personal information, such as identity number, sexual orientation, medical information, financial information and/or personal activities. Such information is a valuable asset because it very important to everyone.

The use of biometrics technology in SMILE as a border control tools introduces problems with maintaining individuals' privacy. The SMILE system will also probably increase the risk of available information misuse as a result of unethical and/or illegal practices if sensitive traveler data and privacy are not protected adequately (mitigation plans, proposed countermeasures and recommendations for the SMILE system development to mitigate/reduce navigate impacts are discussed in deliverable D8.4). From the utilitarianism theory perspective whereby a group's interests and benefits are above those of an individual, SMILE may encounter various ethical issues related to personal information privacy. For the interest and benefit of all (EU citizens and TNC travelers), SMILE collects, stores and transmits vast amounts of personal information (including biometrics data) to improve the flow of legal travelers across land borders. The purpose is also to enhance countries' security against illegal immigration and prevent falsified and forged documents, identities, etc. From travelers' point of view, the concern with personal data has raised a number of questions including how the data should be collected, stored and shared. Travelers need their information to be kept private and only processed by authorized users (e.g., authorized border officers/authorities).

According to our literature review, the priavcy concerns related to SMILE biometrics technology are as follows:

1. ***Unnecessary and unauthorized*** collection of biometrics data for traveler indentification and verification [43]. *Universal Declaration of Human Rights* [22], the EU Charter of Fundamental Rights [26], GDPR [28] and Directive 2016/680, among other legislations, state that to best preserve an individual's privacy, the amount of personal data collected should always be kept to a minimim. Moreover, personal data like biometrics data should only be used when individuals or authorities will benefit from the collection. Unnecessary collection may involve biometrics data such as fingerprints and facial images that are required in e-passport (**Regulation (EC) 2004/2252**[4] with amended **Regulation (EC) 444/2009**[5]) to validate the passport holder's identity and document authenticity. For instance, to minimize and limit the collected fingerprints, four fingerprints in combination with a facial image should be registered in the EES instead of ten fingerprints (**Regulation (EU) 2017/2226**[6]).

4 Council Regulation 2252/2004/EC of 13th December 2004 on standards for security features and biometrics in passports and travel documents issued by Member States.

5 Regulation (EC) 444/2009 of the European Parliament and of the Council of 28th May 2009 amending Council Regulation (EC) No 2252/2004 on standards for security features and biometrics in passports and travel documents issued by Member States.

6 Regulation (EU) 2017/2226 of the European Parliament and of the Council of 30 November 2017 establishing an Entry/Exit System (EES) to register entry and exit data and refusal of entry data of third-country nationals crossing the external borders of the Member States and determining the conditions for access to the EES for law

2. ***Unauthorized and concealed*** collection of biometrics data via cameras, computer equipment, audio devices and many other hidden gadgets [24, 43]. Cameras, for instance, are now widely used to monitor our everyday life. People often benefit from such monitoring, especially at borders to control people flows and detect suspicious activities (e.g., illegal border crossing). However, extensive data collection and analysis can also lead to privacy violations. Moreover, *unauthorized access* are well-founded [13, 24, 43]. Biometrics data are classified as personal data. In the EU, an organization storing and collecting data must comply with data protection regulations such as GDPR. Biometric data should essentially be well-protected against unauthorized access.
3. ***Information linkage and compromise of anonymity*** is another concern [12, 43]. Various kinds of information about individuals stored in a range of databases have the potential to become yet another means through which information can be linked to purposes ranging from commercial marketing to law enforcement. Recent research [10, 20] explores the possibility of extracting supplementary information from primary biometric traits, face, fingerprints, hand geometry and the iris. Such ancillary information includes personal attributes like gender, age, ethnicity, hair color, height, weight and so on. These attributes are known as soft biometrics [44] and are applied in surveillance and biometric database indexing.
4. **Collection of individuals' biometric data for different purposes** is also privacy concern arises. Unrelated applications can be cross-referenced by comparing stored biometric templates [45].

Despite all the benefits of using biometrics technology in SMILE, privacy concerns have become widespread because each time a person's biometric data is checked, a trace is left that could reveal personal and confidential information.

3.2 Biometric technology and human dignity

SMILE combine the hard biometric and soft biometric to facilitate easy border crossing for travelers (travelers biometric profile is discussed in deliverable D3.1). By linking hard and soft biometrics to border control systems, SMILE can strengthen the integrity of existing processes and significantly improve operation efficiency. The capability to verify travelers' identities is extremely important and regards human dignity [11, 14, 24]. People may feel uncomfortable (or humiliated to some extent) when authorities like the border police are recording body features algorithmically. Many factors, for example physical work or physical incapacity (e.g.,

enforcement purposes, and amending the Convention implementing the Schengen Agreement and Regulations (EC) No 767/2008 and (EU) No 1077/2011.

physical disabilities, sight impairment and mental health problems), can make it hard for some people or they may be unwilling to provide biometrics data. For instance, damaged fingers due to manual work can impact the way people are treated when providing fingerprint data [46, 47]. In these cases, challenges with collecting biometrics data and remaining respectful of human dignity may emerge.

People who cannot provide fingerprints or other biometrics data sometimes face a greater risk of negative consequences than people who can [10]. Biometrics data is strictly linked to the human body, whose integrity (physical and psychological) constitutes a key element of human dignity. The main EU legal instruments protect human dignity as a fundamental human right (Article 1 – *Human dignity of Charter of Fundamental Rights of the European Union*). Moreover, privacy is an integral part of human dignity. The right to data protection was originally conceived in both the 1948 *Universal Declaration of Human Rights* (Preamble and Article 1) and the EU *Charter of Fundamental Rights*. For one, the *European Data Protection Supervisor (EDPS)* stressed that "*better respect for, and the safeguarding of, human dignity could be the counterweight to the pervasive surveillance and asymmetry of power which now confronts the individual. It should be at the heart of a new digital ethics."* Moreover, According to GDPR, the expression of human dignity appears in Article 88, which indicates that rules "*shall include suitable and specific measures to safeguard the data subject's human dignity, legitimate interests and fundamental rights, with particular regard to the transparency of processing, the transfer of personal data within a group of undertakings, or a group of enterprises engaged in a joint economic activity and monitoring systems at the work place.*"

Biometrics data collection from vulnerable persons including those with disabilities requires particular attention. Human dignity is evidently a complex notion of the individual and is the basis for the right to privacy and individual control over their own constitutive information. Thus, SMILE should promote research on policies for enhanced privacy and respect for human dignity. SMILE must ensure that data is collected with full respect to one's dignity. In positive terms, respecting a person's intrinsic worth requires recognizing that the person is always entitled to participate in social and community life regardless of age, disability, health, etc. Dignity must always be respected even when a right is restricted [48]. For example, according to Code of Ethics discussed above, respect for and protection of fundamental rights and freedoms is highly requested and has the priority. Section 4 provides further discussion on the SMILE risk assessment of vulnerable people (e.g., the disabled).

3.3 Social inclusion/exclusion and risk of discrimination

The introduction of soft and hard biometrics and their fusion for improved identity verification at land borders raises serious objections to the potential to facilitate discriminatory social profiling [17]. For example, SMILE presumes that a traveler is able to enroll and pre-register in a SMILE system. However, the enrolment of injured and disabled travelers/groups could lead to higher false rejection rates than average. Senior citizens and children who have particular problems with using technologies like mobile devices may also face enrolment difficulties. Although discrimination of vulnerable individuals might be involuntary and unintentional, it may deeply affect them and impact the principle of equity. Furthermore, religious aspects (e.g., beard, headscarf) or interpersonal contact (e.g., photographs, touching, exposing parts of the body) may render a biometrics system an unacceptable intrusion. For example, those of faith who wear head or face coverings have difficulties with enrolling facial biometrics [17]. Verification of such biometrics in public (e.g., at the border crossing points) may lead to embarrassment or offence, causing avoidance of situations where this is necessary. Therefore, mandatory or strongly encouraged use of such system may undermine religious authority and create de facto discrimination against certain groups whose members are not allowed to travel freely or obtain certain services without violating their religious beliefs and privacy.

EU regulations and laws specify equal rights for border crossing (**Regulation (EU) 2016/399**[7]). Article 7(2) of **Regulation (EU) 2016/399,** stipulates that while carrying out border checks, "*border guards shall not discriminate against persons on grounds of sex, […], disability, age or sexual orientation."* Therefore, biometrics platforms should consider travelers with special needs/categories including individuals with special beliefs, senior citizens, children and the physically or mentally impaired etc. An extra attention should be given to, among many others, (1) people with temporary injuries who might have difficulties to provide biometric sample due to temporary wound (e.g., injured face and/or broken arm/fingers), (2) people with total permanent disability whom have difficulties to freely move their limbs due to sensory damage and/or muscle damage, (3) people with poor eyesight can have difficulties to read texts in mobile devices and colour-blind people would also have difficulties to distinguishing some colours and read some texts used in the mobile device interface, (4) people with technological illiteracy, for example, elderly people who lack knowledge of using technology/tools (e.g., smart phones) would have a difficulty to use and interact with SMILE

[7] Regulation (EU) 2016/399 of the European Parliament and of the Council 9 March 2016 on a Union Code on the rules governing the movement of persons across borders (Schengen Borders Code)

system, and (5) people of certain religions and races who may refuse or feel uncomfortable to participate in the system.

3.4 Biometrics technology and children

Biometric technology and data collection also present several ethical questions regarding children's rights. These include the right to information, the right to privacy, security and the right no discrimination, etc. FRA research [10] shows there is limited effort to inform children in a child-friendly and child-sensitive manner in accordance with their age and maturity. Although, police and border guards often do take extra time during biomectics data collection like fingerprinting to adapt to children's needs, FRA research also points out there are allegations of the use of force to fingerprint children. The risk of traumatising children is clear in such instances. Furthermore, there are no special arrangements to inform children about the biometric technology benefits and risks. According to the right to information provisions (Article 12 of the GDPR, Article 12 of the *Convention on the Rights of the Child* and Article 24 (1) of Charter), information is usually not changed in concise, transparent, intelligible and easily accessible form in clear and plain language to make it understandable specifically for children. Since parents or adults accompany children, kids are not individually informed. With respect to children and biometric technology, the main concerns are:

1. Children will not fully know or understand the implications of the accessibility to, and subsequent use of the data collected. While children (and indeed their parents) may be aware of basic privacy settings and risks, even sophisticated users face great difficulties.
2. Concern regards ensuring consent and safeguarding child rights in EU legislative and regulatory frameworks indicate that guardians or parents are responsible for providing consent for data collection from children under eighteen or the relevant age of majority. Article 24 of the Charter emphasises that the best interests of the child must be a primary consideration in all actions that public authorities and private actors take concerning children. This also applies to biomectrics such as fingerprinting.
3. Child identification introduces the requirement for greater levels of care. The problem is that there are several reasons why not all biometrics can be used for child identification and biometric recognition of toddlers and preschool children. For example, a study by *Basak et al*. [49] found that "*capturing fingerprints for children less than three years is hard due to very small fingerprint area, smooth skin, and thin fingers.*" Therefore, very young kids with small fingerprints might not be identified efficiently. According to studies [49-51], *"children can have significantly different behaviour during the enrolment and vervifiction processes compared to adults due to lack of sufficient understanding of the process or*

simply due to their children-specific attitude." This behaviour can be considered as less cooperative with respect to the objective to obtain fingerprint images of adequate quality." Accordingly, sophisticated technologies are required such as multispectral imaging to extract fingerprint characteristics from both the skin surface and sub-surface.

Children are particularly entitled to effective privacy protection. This is because children cannot develop privacy expectations for reasonable legal protection. The biometric data of children should be treated with enormous care and the procedures need to comply with data protection principles such as GDPR (Artical 8 *"conditions applicable to child's consent in relation to information society services"* [27, 28]). Parents must always be notified when their children's biometric data is to be collected or used, and written consent must be obtained in advance. Moreover, biometric match accuracy diminishes as children grow. Fingerprinting young children affects the quality and reliability of future matches to the initial fingerprints [50]. According to the European Data Protection Supervisor (EDPS), *"facial recognition of children (whether automated in the future or 'human') based on reference pictures that are a few years old is likely to be problematic. Even if the technology of facial recognition makes significant progress, it is very unlikely that software will be able to compensate for the effect of growth on children's faces in the near future [52]."* The risk of a wrong match increases when the fingerprints or facial images are compared more than five years after the initial collection. Therefore, biometrics of childern ought to be collected in a child-friendly as well as child- and gender-sensitive manner. Childern are entitled to receive child-friendly and child-sensitive information about their data collection and use, even when parents or guardians assist and accompany them. Besides, child data processing could be done more effectively for child protection purposes. This may be particularly relevant in cases such as missing children, for exmple in SIS II [7, 10, 43].

3.5 Biometric technology and function creep/misuse

Function or purpose creep occurs when the biometrics data is collected for one specific purpose and subsequently used for another unintended or unauthorized purpose without the user's consent [43]. A famous example of a large-scale biometric function creep is the European Dactyloscopy (EURODAC) fingerprint database (**Regulation (EC) 2725/2000**[8]). The original purpose of this EURODAC database was to compare fingerprints for the effective

[8] Council Regulation (EC) No 2725/2000 of 11th December 2000 concerning the establishment of 'Eurodac' for the comparison of fingerprints for the effective application of the Dublin Convention.

application of the Dublin **Regulation (EU) 603/2013**[9] [53-55]. It enables EU countries to identify asylum applicants as well as illegal immigrants within the EU. However, soon after the database was established, other police and law enforcement agencies were also granted access. There are many other large-scale, centralised EU national and international databases, such as SIS II and VIS with the same risks. More details about EURODAC and other EU large-scale biometric information systems are found in D4.1.

Similar concerns also arise in the SMILE case. Hard and soft biometrics are likely to strengthen the potential for function creep due to the very sensitive nature of the data collected and the possibility to use centrally stored biometric data for purposes other than the original purpose. *European Data Protection Supervisor* (EDPS) Peter Hustinx officially stated, *"just because the data has already been collected, it should not be used for another purpose which may have a far-reaching negative impact on the lives of individuals. To intrude upon the privacy of individuals and risk stigmatizing them requires strong justification and the Commission has simply not provided sufficient reason why asylum seekers should be singled out for such treatment."* Therefore, the purpose specification principle (**Article 5(1)(b)** of **GDPR**), which is among the main principles of EU data protection legislation, has a key role. It prescribes that biometric data should be collected only for specified, explicit and legitimate purposes. The problem of function creep is not to be underestimated. Nonetheless, it can be limited with stricter laws, particularly by limiting the use of specified biometric data to certain purposes [4]. Thus, clarity of purpose regarding the intention of biomectric data collection is paramount. It is important to be clear about the system's needs (e.g. SMILE) and how biometrics will help to fulfill those needs.

3.6 Summary of ethical implications and preliminary conclusion

It is clear that there are critical issues with biometrics technology that conflict with fundamental human rights such as the right of liberty and the rights to privacy, etc. The centralized storage of biometric data is a further problem linked the violation of data subjects privacy. Also, as discussed earlier, biometrics data are linked to human body and having massive number individual's biometric data stored in one place increases the potential to

[9] Regulation (EU) No 603/2013 of the European Parliament and of the Council of 26th June 2013 on the establishment of EURODAC for the comparison of fingerprints for the effective application of Regulation (EU) No 604/2013 establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third-country national or a stateless person and on requests for the comparison with EURODAC data by Member States' law enforcement authorities and Europol for law enforcement purposes, and amending Regulation (EU) No 1077/2011 establishing a European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice (recast).

explores the possibility of extracting supplementary information from primary biometric traits and lead to compromise privacy in a deep and thorough fashion as biometrics data can reveal more about a person than only his identity, including medical history, (e.g. retinal data may divulge information about diabetes or hypertension) [11, 20].

Futhuremore, a serious remarks over the use of biometrics technology for large populations, especially if the consequences lead to social exclusion, either as a result of the individual being unable to reliably enrol or verify their data, or simply not having confidence in the system and avoiding having to interact with it (example of veiled Muslim women discussed above). Certainly, when it comes to border control and the use of biometrics technology to incease border security, monitor migration and combat identity theft and fraud etc., the argument is essentially utilitarian (utilitarianism theory) where the collective right of a group (group interest) is balanced against the rights of the individual. It makes the individual simply a means to the ends of the majority. However, this is the wrong argument. *Wickins* in [17] and *Townend* in [56] argue that public interest must be judged by considering the balance between individuals, i.e. the rights of single individuals must be balanced against other single individuals if individuals are not to be used instrumentally.

Individual acceptance of biometrics technology should be actively promoted through ensuring transparency of decision-making, clear policy reagarding the purpose of bicometric technology and how it is used, as well as increased measures dedicated to preserve personal rights and personal data protection. Since greater use of personal data impacts upon human rights, there needs to be an honest and assertive study of what the risks are to perosnal rights and privacy as well as how these risks are mitigated. For this reason, Deliverable D8.4 intended to identify and address the ethical and privacy implications of the SMILE system to ensure that SMILE technology is in compliance with fundamental human rights legistaltion as well as privacy and data protection legistaltion. In Deliverable D8.4, the ethical and privacy impact assessement process will be conducted by SMILE consortium together with the end-users to consider the ethical issues and impacts posed by the SMILE solution to identify ethical and privacy risks and propose/plan the appropriate mitigation solutions. Following are a recommendations for SMILE derived from the *Charter of Fundamental Rights,* the presented Code of Ethics, GDPR and Directive (EU) 2016/680 as well as the discussion above:

1. **Compliance with human rights legislation:** The SMILE ethical and privacy impact assessement should encompasses human rights legislation, and the implementation of the SMILE platform should be in line with such legislation. SMILE policy-makers should encourage respect for fundamental rights in the implementation of SMILE system and

other biometrics technologies. Also, comprehensive measures should be in place to monitor compliance with all legislation.

2. **Repect human dignity:** SMILE must protect personal integrity, preserve individual freedom and self-determination (i.e., choice and consent with respect to which biometrics data he/she prefer to use), respect privacy and family life, and safeguard against harm and unreasonable force for data processing.
3. **Protection of children:** SMILE should treat minors as independent individuals. When a child is unble to give a consent (e.g., a child < 16 year old), parents or guardians should provide formal consent. However, it is important to clarify the child's capacity to grant consent on his/her own and ensure that the children themselves accept participation to the extent that they are able to do so.
4. **Individual participation:** SMILE should ensure respect and compliance to Articles 21-23 of the EU Charter outlining nondiscrimination policy as well as Article 7(2) of **Regulation (EU) 2016/399**. SMILE should not discrimnate against individuals on ethically irrelevant grounds of sex, race, colour, ethnic or social origin, genetic features, language, religion or belief, political or any other opinion, membership of a national minority, property, birth, disability, age or sexual orientation etc (refer to RBP Code of Ethics (point (b) and HNP Code of Ethics (point(4)).
5. **Transparency:** The SMILE system should share knowledge with users and the public, ensuring transparency of the system. All people have a right to be informed, in a language they can understand and in a manner that is polite and respectful, of both the nature of any control they are subject to and their rights in relation to that control.
6. **Purpose specification**: SMILE should clearly define the purpose of the system and ensure a sufficient protection against unauthorised use of the syetm beyond the original purpose to avoid the function creep problems. Also, The SMILE system end users (e.g., border policy) should respect the purpose limitation principle, i.e., using the system only for its designated purpose, demonstrating legitimate use and minimising the potential for misuse of the system outside border control context.
7. **Proportionality:** Biometric data collected by SMILE should be adequate, relevant and proportional in relation to the defined purpose. SMILE Should not collect and/or store any unnecessary data outside of its specified purpose. Once data is no longer needed for the immediate purpose, the SMILE system should delete the collected information.
8. **Compliance with security requirements**: Security requirements deal with security issues, such as confidentiality, integrity and availability when collecting personal related data.

Designers and developers of SMILE systems should follow the recommundations of ethical and privacy impact assessment results as a reference point, and review the recommendations of other similar projects that have considered ethical, legal, privacy and societal aspects. This would help to improve the the security and integrity of the system, and protect it against internal compromises and external attacks. They should use strong encryption and optimise access controls.

9. **Compliance with the data protection regulation:** SMILE must take into consideration all the requirements and main principle presented in the GDPR and Directive (EU) 2016/680. These include (to name a few):
   a. Collection limitation principle
   b. Lawfulness of the data processing principle
   c. Accountability principle
   d. Right to data subject principle

More discssion about these GDPR and Directive (EU) 2016/680 principles are given in deliverable D8.1 with a comparative analysis of GDPR and Directive (EU) 2016/680.

4. SMILE Ethical framework

According to Article 7, Regulation (EU) 2016/399 (amended in Regulation (EU) 2017/458) and Article 7, Regulation (EC) 767/2008, competent authorities should ensure that the human dignity and integrity of persons whose data are requested are respected and should not discriminate against persons on grounds of sex, racial or ethnic origin, religion or belief, disability, age or sexual orientation. Thus, SMILE platform at land border should be designed to support privacy-compliant biometric systems, related to technological, ethical and sociological aspects. For SMILE systems to be successful with its use case scenarios (discussed in Deliverable D2.2) and actual implementation, it should not only consider the security and privacy of personal data, but it also need to guarantee that the users can interact with the system and make the user experience acceptable. To do so, SMILE team must consider all challenges related to the system design. These challenges include usability and ergonomics aspects. Usability is defined as "*the extent to which a product can be used by specified users to achieve specified goals with effectiveness, efficiency and satisfaction in a specified context of use*" [57, 58]. Whilst, ergonomics refers to "*the design principles used to arrange the components of the system that require interaction with the user such that the people can use the system easily and safely*". In SMILE platform, usability is related to the design of user interface, whereas ergonomics is related to the position of the biometric devices (SMILE

mobile devices, laptops or/and SMILE booth) inside the SMILE fast lane and how biometric devices will be used for travel identification and verification.

4.1 Ethical considerations for human rights

Ethical concerns	SMILE
Respect for and protection of fundamental rights and freedoms	• SMILE **MUST** protect personal integrity, preserve individual freedom and self-determination, respect privacy and family life, and safeguard against harm and unreasonable strain. • SMILE **MUST** ensure free and informed consent for individuals according to procedures laid down by law.
Discrimination and social sorting	• SMILE **SHOULD** prohibit personal profiling which may lead to discrimination based on any ground such as sex, race, colour, ethnic or social origin, genetic features, language, religion or belief, political or any other opinion, membership of a national minority, property, birth, disability, age or sexual orientation.
Rights to children	• SMILE **MUST** pay particular attention to minors, whether travelling accompanied or unaccompanied and **MUST** respect the specific needs of children and their interests must be protected in ways supplementary to the general treatment of adult subjects. Moreover, SMILE **SHOULD** understand that children are developing individuals, and they have different needs and abilities at various phases.
Rights to data privacy	• Each individual has specific rights in relation to their privacy. Legislation ensures that the right to privacy is protected by those who collect, use and disclose personal information. Under legislation, everyone is entitled to: i. have their information used only for its original stated purpose(s) ii. know who can access their personal information and why iii. access and receive a copy of any information held about them iv. check that the information held about them is correct, complete and up to date v. change any details that are factually incorrect or remove any information that is not held for a valid reason. vi. feel confident that their personal information is kept safely and securely

4.2 Ethical considerations for travelers with physical or mental impairment

EU regulations and laws specify equal rights for border crossing. Article 7(2), **Regulation (EU) 2016/399,** stipulates that while carrying out border checks, "*border guards shall not discriminate against persons on grounds of sex, […], disability, age or sexual orientation"*. For these reasons, with regards to SMILE user use cases (presented in Deliverable D2.2), SMILE platform should consider travelers with special needs/categories including (to name a few):

1. **Travelers with temporary injuries**: These types of travelers might have difficulties to provide biometric sample due to temporary wound. For example, injured face and/or

broken arm/fingers. In this case, SMILE **SHOULD NOT** discriminate against such travelers and shall use mobile devices which perform acquisition in a greater number of situations during SMILE pre-registration, authentication and verification processes.

2. **Travelers with total permanent disability:** Always have difficulties to freely move their limbs due to sensory damage and/or muscle damage. For example, in case of fingerprints verification, travelers with a hand disability may lack the ability to place the required finger and keep it steady for a sufficient time on the fingerprints scanner. Moreover, in case of SMILE face recognition/iris scanning verification, travelers with neck disabilities may have difficulties in correctly placing their face near the iris scanning device/face recognition camera. Thus, SMILE mobile devices **SHOULD** be able to work in off-axis acquisitions and be adjustable to support such travelers with biometrics recognition and make it more comfort.
3. **Pedestrian with walking weaknesses:** Travelers with walking aids (e.g., crutches or/and wheelchaired) might also have difficulties to walk throughout the SMILE fast lane. Therefore, SMILE fast lane **SHOULD** be easily accessible for travelers walking with aids and provide the necessary help of trained operator/border guard to help pedestrian with walking aids in performing the biometric recognition and passing SMILE fast lane with more comfort.
4. **Travelers with visual impairments:** Travelers with poor eyesight can have difficulties to read texts in mobile devices. Colour-blind travelers would also have difficulties to distinguishing some colours and read some texts used in the mobile device interface. In these case, the interface of the SMILE mobile devices **SHOULD** consider larger symbols and a pleasant combination of colours to support those travelers. Furthermore, travelers with total visual impairment (blindness) cannot see the graphical/texted instructions and cannot place their finger/face in the placement of the biometric reading. Therefore, sounds could also be used in conjunction with graphical/texted instructions to help guide such travelers [59].
5. **Travelers with technological Illiteracy:** For example, elderly people who lack knowledge of using technology/tools (e.g., smart phones) would have dificulties to use and interact with the SMILE system. In this case, SMILE **SHOULD** design an interface that taking into consideration elder's needs.

In all cases presented above, SMILE systems shall be operated under the supervision of a border guard who should be trained to support such travelers. Also, who is in charge of detecting any inappropriate, fraudulent or abnormal use of the SMILE system with accordance

to Article 8(c) and (d), **Regulation (EU) 2017/2225**[10]). Moreover, where Member States decide to use SMILE systems, they shall ensure the presence of a sufficient number of staff to assist vulnerable travelers with the use of such systems (Article 8(a), **Regulation (EU) 2017/2225**). Furthermore, SMILE shall provider an appropriate training for border guards and travelers to improve performance and increase acceptance and satisfaction.

4.3 Ethical considerations for privacy and data protection

The processing of biometric data in SMILE raises many concerns privacy and data protection concerns. On the one hand, biometric data can be used to recognize individuals automatically with greater accuracy. On the other hand, a misuse of such biometric data can have dangerous consequences which pose serval security and privacy challenges such data destruction and/or unauthorised disclosure of, or access to personal data, to name a few. Thus, SMILE platform shall be designed to support privacy-compliant biometric systems. Perceived risks are related to how travelers view the biometric technology, whether they trust it, and whether they like to use it. With respect to this, EU regulation (e.g., GDPR [60, 61]) prohibit the use of special categories personal data such as biometric data without the user's awareness and permission. Also, prohibit the use of the biometric data different from the purpose of the system (function creep issue discussed in section 3.5). For example, biometric data stored in e-passports can only be used for issuing electronic documents and verification of document holder (**Regulation (EC) 444/2009**[11]). Moreover, collection and storing of personal data using technology challenges the Union right to freedom of movement, as it provides the opportunity to track citizens movements in and out of the Schengen area. More information about GDPR and SMILE *Priavcy by Desgin* strategies and *Security by Desgin* policy with a respect to personal data protection is presented in Deliverable D8.1.

Based on the presented SMILE use cases (discussed in Deliverable D2.2), SMILE implementation should consider several privacy aspects for protecting the privacy of personal data. These aspects include:

1. **The purpose of biometric data:** The legitimate purpose of biometric data collection and processing during SMILE pre-registration and verification phases used only for verifying the identity of the individual during the border crossing procedure (Article. 6 (1) (f), **GDPR**).

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

[11] Regulation (EC) 444/2009 of the European Parliament and of the Council of 28th May 2009 amending Council Regulation (EC) 2252/2004 on standards for security features and biometrics in passports and travel documents issued by Member States.

Article. 13 (1) of the **GDPR** stipulates that "*information to be provided to data subject where personal data are collected from the data subject*". This information shall include, purpose of the system, the enrolment and verification processes, and the methods used for data protection, among other.

2. **Travelers control of personal data:** According to Article. 32 (2) of the **GDPR**, the data subject (traveler) has the right to ask for removal or erasure of biometric data in electronic documents. Also, the traveler should have the possibility to decide when he/she no longer be authenticated and verified using the SMILE system and choice to proceed with manual checks.
3. **Data protection measures:** Article. 32 (2) of the **GDPR** stipulates that "*the controller and processer must implement appropriate technical and organizational measures to protect personal data against "destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed and against all other unlawful forms of processing*". Therefore, SMILE shall deploy a privacy enhancing technologies and secure access control techniques to avoid any misuse of personal data. A set of privacy enhancing techniques for multimodal biometrics are discussed in Deliverable D8.3.
4. **Reuse of data for law-enforcement purposes:** According to **Regulation (EU) 2016/399** and its amendment **Regulation (EU) 2017/458**, citizens should be checked in criminal databases such as **SIS II** and **SLTD** on a systematic and non-systematic basis. As the majority of these travelers are presumably innocent individuals. Therefore, saving and cross checking their data on a systematic basis with law-enforcement databases would be disproportionate. Any reuse of personal data done for the purpose of law enforcement should be done in accordance with **Directive (EU) 2016/680**[12] [62, 63]. Deliverable D8.1 has discussed **Directive (EU) 2016/680** in more depth and provides a comparative analysis of **GDPR** and **Directive (EU) 2016/680**.

4.4 Ethics helpdesk board

To ensure maximum compliance with ethical principles, the SMILE project will rely on an ethics helpdesk board. The ethics helpdesk will report on the conduct of the project, and provide guidance for improvements in ethical conduct throughout the project. This analysis will be based on whether partners are appropriately meeting the recommendations set out under this ethics manual and guidelines for land BCPs.

[12] Directive (EU) 2016/680 of the European Parliament and of the Council of 27th April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA.

As shown in Table 2, the ethics helpdesk board displays a range of expertise with experience necessary to provide a competent and rigorous overview of ethics of all SMILE research. It is multidisciplinary and is made up of both men and women. The ethics helpdesk board may also seek advice and assistance from experts outside the helpdesk or even outside the SMILE consortium in considering certain matters.

Table 2: Representatives in the ethics helpdesk board

Role	Name	Partner
Helpdesk head	Sule Yildirim Yayilgan	NTNU
Ethics Expert	Dimosthenis Ioannidis	CERTH
End-users representative	Velina Dobreva	CDBP
End-users representative	Andrei Baltau	RBP
End-users representative	Lenard Zsakai	HNP

The ethics helpdesk board responsibilities include::

1. Conducting discussions with appropriate work package leaders and end users to identify and discuss ethical considerations and measures to meet ethical considerations.
2. Work with those involved in WP8 and WP10 (ethics requirements) to ensure that the SMILE research and SMILE system are conforming to European legislation and respect of human rights and human privacy etc.
3. Ensuring the consortium abide by the ethics manual and guidelines throughout the duration of the project.
4. Reporting on the ethical monitoring exercise throughout the project. Reports are due to M18 (D8.7) and M36 (D8.12).

4.5 Monitoring of SMILE ethics

It is not enough to conduct an ethical review and ethical impact assessment. For this deliverable to be meaningful, it has to be integrated into the project during all phases of SMILE development. Table 3 provides an outlines how the SMILE ethical helpdesk board and other partenrs of SMILE consurtim will integrate ethical and privacy impact assessment (refer to Deliverable D8.4) into the SMILE system devolpment.

Table 3: Integrating and monitoring of SMILE ethics

Action to be taken	Period for completion of actions	Responsibility for action
Reviewing of ethical aspects	Duration of the project with a monthly Telco meeting	• NTNU • End user

		• Ethical helpdesk board
Monitoring of ethical aspects	Duration of the project	• Ethical helpdesk board
Ethical advice and support	Duration of the project	• Ethical helpdesk board
Conducting of the SMILE ethical and privacy impact assessment	M12-M36	• NTNU • End users
Implementation of ethical recommendations	During design, development and testing of SMILE system.	• SMILE consortium partners
Review of the SMILE ethical impact assessemnt	M12-M36	• Ethical helpdesk board • SMILE consortium partners

4.6 Integrating ethical and privacy impact assessments: Plan and team

Ethical impact assessment (EIA) [64-67] is a means of ensuring that ethical implications are examined by SMILE consortium prior to the deployment of a SMILE solution in order to identfy all potential ethical risks and propose mitigation measures which can be adopted as necessary. The main objectives of an EIA for the SMILE project are as follows (EIP is conducted in D8.4):

1. Investigate the critical infrastructure that will form the basic frameworks for the development of the SMILE platform, specifically with regard to legal and regulatory concerning border control, border ethics and priavcy as well as data protection issues.
2. Conduct an EIA of the SMILE technologies and procedures to be developed in the SMILE project to ensure that the outcomes of SMILE project comply with ethical standards as well as relevant national and European regulations regarding border control checkes, privacy and data protection.
3. Consider the ethical issues arising from the pilot scenarios.
4. Develop an informed consent policy, procedure and form (see section 6).

Expertise for the EIA are found within SMILE consortium to preform the EIA. The EIA team, lead by NTNU have the following responsibilities:

1. Identification of legal, ethical, privacy and policy issues and requirments with respect to SMILE project and proposed system.
2. Identification of ethical and privacy factors to be considered in SMILE system.
3. Carry out an impacts assessment of the identified ethical and priavcy factors on the implementation of SMILE.
4. Provide consultation and recommendation to SMILE consortium and system developers through a EIA reports to ensure that ethical issues are identified, dicussed and dealt with, preferably as early in the project development as possible.

The EIA team will provide the drafts of EIA report to the SMILE ethics helpdesk at month 18, month 24 and month 35, and invite comments from the SMILE ethics helpdesk and other memebres of SMILE consortium. Members of the SMILE consortium with the EIA team would have meetings to discuss the key ethical and privacy issues and seek to ensure possible mitigation measures to address the identified issues. Proposed meetings in the consortium as follows:

- **Plenary meetings:** Once every four months. The consurtium have met in M15 and approximately the next meeting is planned for M19-M20. After that probably have one in M22-M23, then sometime in M26-M27 and M32-M34.
- **Telco meetings:** Twice a month.
- **Work packages meetings:** upon request depends on the necessity.

Note that, the date/days of the plenary meetings and work packages meetings are not fixed. They depend on the availability of the consortium members. Whereas, the date for Telco meetings are fixed. However, in Telco meeting, not all consortium members are required to attend. It depends on the agenda of the meetings. Moreover, somewhere in between or in conjunction with the above mentioned meetings, the SMILE consortium will probably have pilot preparation/execution meetings. This is depending on how the project proceeds and more face-to-face meetings will be performed if needed.

4.7 SMILE ethics assessment

Table 4 provide the assesement checklist template for SMILE ethical helpdesk board to monitor and assess the ethical outcome from SMILE project.

Table 4: Assesement checklist template for SMILE

Ref	Action	Refer-ence deliver-able	Related WP or Task	Yes/No	Comments	Data
EA1	Purpose and definition					
EA1.1	Has SMILE clearly describe the new technology in ques-tion?					
EA1.2	Has SMILE readily identify whether re-lated new technol-ogy ideas are within the scope or outside the scope of SMILE definition?					

Ref	Action	Reference deliverable	Related WP or Task	Yes/No	Comments	Data
EA1.3	Has you identified which new technology/(ies) are within the scope of your project/system?					
EA.1.4	Has SMILE identified who will benefit from the SMILE system and in what way?					
EA1.5	Has SMILE identified what are the consequences of not proceeding with SMILE system					
EA2	**Data collection**					
EA2.1	Can SMILE clearly define what types of personal data that will be collected by the system when implemented?					
EA2.2	Has SMILE clearly defined who will collect the data and why?					
EA2.3	Can SMILE clearly describe who will use the information and why?					
EA2.4	Has SMILE decided how the data will be retained and for how long?					
EA2.5	Has SMILE decided on how the data will be secured?					
EA2.6	Can SMILE decide to whom and how the data might be disclosed?					
EA2.6	Can SMILE decided how and when the data will be disposed?					
EA3	**Issues analysis**					

Ref	Action	Reference deliverable	Related WP or Task	Yes/No	Comments	Data
EA3.1	Can SMILE proceed without impact assessments?					
EA3.2	Has SMILE clearly identify all the assets and agents involved in the SMILE system?					
EA3.3	Can SMILE clearly state the initial ethical question(s) that SMILE wish to answer in respect SMILE system?					
EA3.4	Has SMILE policy-maker and/or SMILE developer developed a process for identifying and considering ethical issues?					
EA3.5	Has SMILE clearly identified individuals who may be positively or negatively affected by SMILE system					
EA3.6	Has SMILE undertaken ethical and privacy impact assessment to identify possible risk to SMILE system					
EA3.7	Has SMILE considered all the recommendation from impact assessment and implemented all proposed mitigation plan					
EA3.8	Has SMILE ensured that risks and rewards are sufficiently examined from each of the following perspectives of human right (right to life, liberty and security of per-					

Ref	Action	Reference deliverable	Related WP or Task	Yes/No	Comments	Data
	son and Respect cultural, religious and linguistic diversity) discussed in Table1					
EA3.9	Have SMILE cross-referenced rewards to risks?					
EA4	**Consulting, engagement and accountability**					
EA4.1	Has SMILE identify the ethical assessment team?					
EA4.2	Has ethical assessment team been invited to participate in a consultation and/or to provide their views on the SMILE project?					
EA4.3	Has SMILE clearly identify who is responsible for identifying and addressing positive and negative consequences of SMILE system and service?					
EA4.5	Does SMILE make clear where responsibility lies for liability, equality, property, privacy, autonomy, accountability, etc.?					
EA5	**Assessment of ethical issues in consideration**					
EA6.1	Has SMILE taken all steps to provide the formation about the SMILE project to the public, not simply in response to requests, but proactively?					
EA6.2	Has SMILE identify, if anyone objects to the project, to whom they can contact to					

Ref	Action	Reference deliverable	Related WP or Task	Yes/No	Comments	Data
	make known their objection?					
EA6.3	Has SMILE identify what measures could be taken to avoid curtailment of person's rights to liberty and security in any way					
EA6.4	Does SMILE recognise and respect the right of persons with disabilities to benefit from SMILE system and services.					
EA6.5	Does SMILE provide a meaningful of choice, i.e., a person to choose what data he/she want to enrol and use? If not, what could be done to provide such choice?					
EA6.6	Has SMILE considered that the technology should be developed and implemented in a way that recognises and respects the right of citizens to lead a life of dignity and independence? If not, what changes can be made?					
EA6.7	Does SMILE system compromise or violate human dignity? What measures have been put in place to minimise or avoid compromising human dignity?					
EA6.8	Will SMILE system/services obtain the free and informed consent of those persons to be involved in or affected by the SMILE? If not, why not?					

Ref	Action	Reference deliverable	Related WP or Task	Yes/No	Comments	Data
EA6.9	If the individual is not able to give informed consent, what measures SMILE has taken for avoid violation of personal right with respect to consent can his consent?					
EA6.10	Is there a risk that use of SMILE technology will be seen as stigmatising, e.g., in distinguishing the user from other people?					
EA6.11	Could SMILE be perceived as discriminating against any groups? If so, what measures SMILE has taken to ensure this does not happen?					
EA6.12	Does SMILE system or service use profiling technologies? If so, what measures SMILE has taken to ensure this does not happen?					
EA6.13	Does SMILE system or service facilitate social sorting? If so, why/ and what measures SMILE has taken to ensure this does not happen?					
EA6.14	Will SMILE system improve personal safety, increase dignity, independence or a sense of freedom?					

5. Guidelines for SMILE research ethics

This section provides standards and guidelines to ensure that the collection and processing of personal information is undertaken in an ethical and privacy preserving manner as well as in compliance with standards and regulations. The SMILE consortium will follow the guidelines set out in this ethical manual when collecting, storing, using and analysing data and results.

Note requirement and recommendation with respect to data collection, procesing, etc and data protection are presented in Deliverable 1.4.

5.1 Respect for gender, culture, ethnicity, religion and race differences

During the course of SMILE project, SMILE members will have respect for gender, cultural, ethnicity, religion and race differenc. Also, SMILE members will pay more attention to people with physical and/or learning disability, elderly and children to increase their participation in the SMILE project. As we have discussed earlier, it is important to understand that each individual is unique, and allows for the creation and maintenance of a positive research outcomes, wherein the similarities and differences of individuals are valued. The principle of dignity also affirms that any human should be respected, independent of their age, gender, condition, ethnicity, religion, etc. With respect to gender, SMILE will ensure that a proportional number of participants are female and that gender analysis is built into the project.

5.2 Role of SMILE Data Protection Officer (DPO)

The DPO within SMILE consortium is assigned to **Mr. Eugen Badea** from SPP (cf. Deliverable D10.4). The responsibilities of DPO includes (in accordance to Article 39 GDPR):

1. Provide advice and guidance to the consortium on the requirements of the data protection.
2. Maintaining comprehensive records of all data processing activities conducted by the consortium, including the purpose of all processing activities and ensure compliance with a relevant regulation such as GDPR.
3. Be consulted and provide advice during Data Protection Impact Assessments (DPIA).
4. Be the point of contact for data subjects and for consulting with national supervisory authorities.

5.3 The role of SMILE data controller

CERTH, **NTNU**, **RBP**, **HNP**, **SPP**, **CDBP**, **TEC** and **eGovCD** are acting as joint data controllers (Article 26 GDPR). **CERTH** is responsible for producing the **Data Management Plan** (DMP)(WP1: Deliverable 1.4). The DMP includes information relating to the types of data the SMILE project has generated/collected, standards it should be used, how data can be processed, verified and stored, and lastly, how the data should be deleted.

The SMILE consortium will collect data during the lifespan of the SMILE project. All personal data collected should be appropriately managed and stored in according to the DMP. **CERTH** with other joint data controllers (**NTNU**, **RBP**, **HNP**, **SPP**, **CDBP**, **TEC** and **eGovCD**), in a transparent manner, lead by **CERTH**, will have the responsibility to implement appropriate

technical and organisational security and privacy measures to ensure and be able to demonstrate that processing of personal data is performed in accordance with data protection Regulation. These responsibilities concern the necessity to keep personal data secure from unauthorised access, disclosure, destruction or accidental loss (Artical 27-29 GDPR). The role of joint data controllers as follows:

- Defining data collection purposes, scope, and procedures
- Defining policies for data classification (security levels) and data access control
- Defining the data breach reporting procedures and plans for incident response and disaster recovery
- Operating the data management including:
  - Design, create, and implement IT processes and systems that would enable the data controllers to gather personal data.
  - Define the used tools and strategies to gather personal data.
  - Implement security measures that would safeguard personal data.
  - Store personal data gathered by the data controllers.
  - Transfer data from the data controller to another partner (data processor) and vice versa.

5.4 The role of SMILE data processor

Authorized processor (**data processor**) will only process personal data on the instructions of the data controller. Data controller shall ensure that processor authorized to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality (Artical 27-29 GDPR). A data processor (**Fraunhofer**, **TEIC**, **FINT**, **SIVECO**, **IDEMIA** and **EULAMBIA**) should carry out the actual processing of the data under the specific instructions of the data controller.

6. Recruitment and privacy of participants

6.1 Recruitment

The SMILE project deals with humans participants whom will be involoved in interviews, surveys and a course of the trials of SMILE project. Only adults (persons over 18 years of age) with the explicit capacity to consent will be recruited for the purpose of the SMILE study. Where possible, the consortium will try to ensure a gender and socio-cultural balance among research participants with respect to culture, ethnicity, religion, race differences, etc. The participation will be from voluntary adults and these will include:

- The members of the SMILE consortium

- Voluntary travelers
- Border control officers

These individuals will be engaged in:

- Interviews and online questionnaires
- Observation and recording of border checks activities during requirements gathering and analysis.
- Observation and recording of border checks activities during pilot simulations and exercises.

In recruiting participants for questionnaires and interviews, the SMILE consortium will rely on the following strategy:

- Use of own contacts: The partners of the SMILE have a rich list of contacts that can be approached to facilitate access to a high number of participants.
- Use of contacts established through the SMILE dissemination team

The trials of the SMILE will involve existing personnel of RBP, HBP and CDBP that are already working at the specific border crossing points (BCP). For each trial, a specific part of the border control and the travelers monitoring section will be selected for the Tasks T7.4 and T7.5 in WP7 of the project. The selected areas at the BCPs will be defined according to the requirements and specifications derived from task T7.4. A detailed observation plan will be prepared in strict collaboration with the ethical component of the SMILE consortium.

The recruitment method and the informed consent procedures will be particularly stringent to ensure no coercion (not even soft or indirect) is exerted. The specific criteria for the selection of the volunteer participants are determined by the pilot requirements. There will be participants with various roles including travelers and border control officers as described in the use cases of the SMILE project (discussed in deliverable D2.2). More specifically, for the CDBP, RBP and HBP end-user pilot, the research participants are those that hold a position as "*Border Guard*" (in CDBP so-called border police).

6.2 Information and instructions

It is essential that before participants give their consent to participate in the course of the pilot, they should be briefed in a clear manner and with a language they understand about the background, objectives, and possible risks of the SMILE project in general and about the specific experiment, he/she will participate in. In this regard, all participants involved in the SMILE pilot will be given an information sheet (paper or/and electronic formats) which contains the following information:

1. **The background and the purpose of the SMILE project:** Information sheet will include a summary about the objectives/aims/goals of the SMILE project, the relevance of the SMILE project, how participants will benefit from the SMILE project as well as what data will be collected during the project life-cycle and the mode of data collection.
2. **The rights and arrangements made for participations:** Information sheet will also include a summary about the participants's rights. Participants must also be informed that participation is fully voluntary and participant is allowed to withdraw at any time of the SMILE project without giving a reason and with no consequences attached.
3. **Participant tasks:** The information sheet will include a clear exaplantion and instructions about; what participants will be asked to do, how long will it take, potential risks and responsibilities of participation in the pilot task.
4. **Confidentiality of personal information:** Information sheet will include detalis about; who will have access to participant data, where and how long the data will be stored.
5. **Compensation and financial incentives:** Infromation sheet will clearly state that no costs of participating and no payment (of any type) for participation in the SMILE pilot.
6. **Contact detalis:** Finally, the information sheet will provide a contact information (full name, email addree and phone number) of the person in charge as a means to reach the project team.

In addition, the information sheet will be translated into relevant languages if necessary. If there is circumstances which requires that the information sheet has to be read and summarised verbally, a member of the SMILE team should do so. Moreover, all participants will be given the right to ask questions if any details in the information sheet are not clear. The SMILE team members (those who are participanting in the course of the pilot) are responsible and obligated to answer all questions and clarify all details.

6.3 Informed consent

The processing of all personal data will be based on freely given and specific, informed consent. Every volunteer participating in the SMILE project will be fully aware of what they will be asked to do (accomplished through the information sheet (Section 3.2)). The SMILE consortium will guarantee that no participants will participate in the course of the SMILE project without assuring and obtaining an individual informed consent (informed consent template is persneted in Annex II). The consent form will contain the following confirmations:

- a confirmation that the participant has read and understood the information given in the information sheet; and

- a confirmation that the participant has the opportunity to ask questions to clarify unclear information and have received satisfying answers and sufficient time to consider participation; and
- a confirmation that the participant has understood that participation is voluntary and always have the possibility/right to withdraw at any time, without giving a reason and
- a confirmation that the participant is aware of that no payment of incentives or rewards to participant will be made.

In addtion, the consent form will contain the following permissions asked from the participant:

- a permission for participation in the SMILE project; and
- a permission for authorized processing of collected data (mentioned in the information sheet) ; and
- a permission to store anonymous data (if necessary) for a furture investigation and reporting; and
- date, first and last names, and signature of the participant; and
- date, first and last names, and signature of the SMILE team representative.

A summary of the process of taking informed consent is shown in Figure 1.

6.4 Dealing with complaints

Occasionally, a participant may want to make a complaint during the course of the SMILE project. Participants are allowed and would be given a chance to fully explain their concerns. Participants can file a formal complaint to the project coordinator and also an independent contact will also be provided should the participant request this.

- Project Quality Assurance Manager: Georgios Stavropoulos (Email: stavrop@iti.gr)

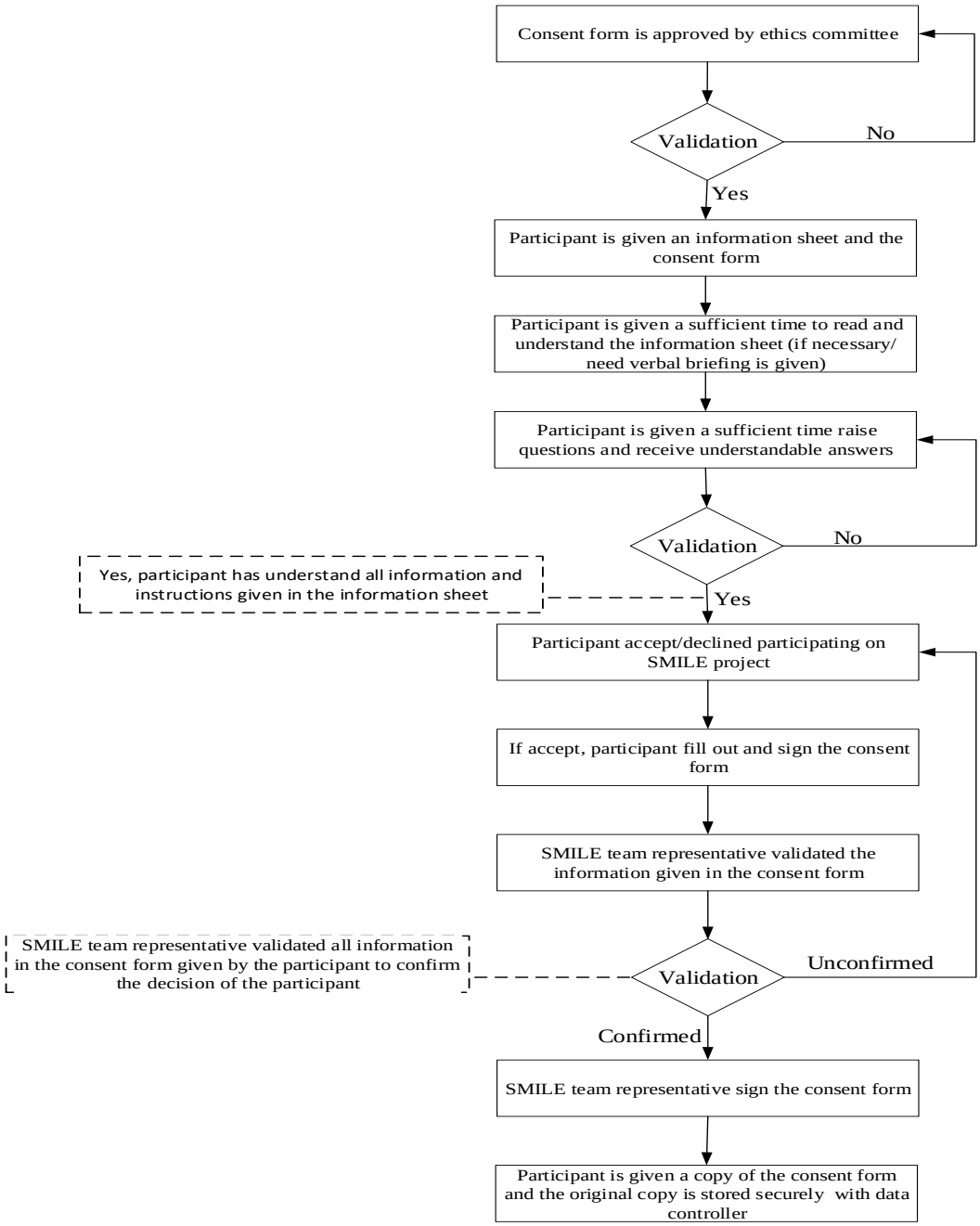

Figure 1: Procedure for taking informed consent

7. Conclusion

As dicussed in this deliverable and other deliverables of SMILE project, the tendency to use biometrics data in SMILE should improve and speed up border control management. However, because individuals are surrounded by so many biometric sensors, serious ethical and privacy challenges are arised. The efficacy of a SMILE system can be affected by the ethical, cultural, social, and legal considerations that shape how people engage and interact with SMILE systems. It is clear from the discussion above that there are critical issues with biometrics technology that conflict with fundamental human rights such as the right of liberty and the

rights to privacy etc. The lack of awareness of the rights of data subjects and absence of clear procedures to protect rights is the main concerns.

The main objective of this deliverable is is to analyze the social and ethical implications of the SMILE services using biometric technologies and create mutual understanding about the ethical issues related to personal data processing and how the SMIEL consortium will handle them. To compliance with regulations, the SMILE consortium partner will ensure that data processing within SMILE project is conducted in an ethical manner under the specific instructions of ethcial helpdesk board and in accordance to recommendations and guideline in this document as well as the recommendations and mitigation plans provided by the ethical and privacy impact assessments reports (Deliverables D8.4 and D8.10).

While this document is only one version in a form of deliverable, more updated about different legal, technical and ethical problems as well as rules for safeguarding of fundamental rights with respect to processing of sensitive biometric data will be provided in other deliverables.

References

1. Mordini, E. and S. Massari, *Body, biometrics and identity.* Bioethics, 2008. **22**(9): p. 488-498.
2. National Research Council and Whither Biometrics Committee, *Biometric recognition: challenges and opportunities*. 2010: National Academies Press.
3. Mordini, E. and C. Petrini, *Ethical and social implications of biometric identification technology.* Annali dell'Istituto superiore di sanita, 2007. **43**(1): p. 5-11.
4. Kenk, V.S., et al., *Smart surveillance technologies in border control.* European Journal of Law and Technology, 2013. **4**(2).
5. European Commission. *Electronic Identities – a brief introduction*. Available from: http://ec.europa.eu/information_society/activities/ict_psp/documents/eid_introduction.pdf.
6. Sprokkereef, A. and P. De Hert, *Ethical practice in the use of biometric identifiers within the EU.* Law Science and Policy, 2007. **3**(2): p. 177.
7. European Union Agency for Fundamental Rights. *Biometric data in large EU IT systems in the areas of borders, visa and asylum – fundamental rights implications*. 2014; Available from: http://fra.europa.eu/en/project/2014/biometric-data-large-eu-it-systems-areas-borders-visa-and-asylum-fundamental-rights.
8. Radjenovic, A. *European Travel Information and Authorisation System (ETIAS)-Briefing EU Legislation in Progress European Parliamentary Research Service*. ; Available from: http://www.europarl.europa.eu/RegData/etudes/BRIE/2017/599298/EPRS_BRI(2017)599298_EN.pdf.
9. Vavoula, N., *European Travel Information and Authorisation System (ETIAS): A Flanking Measure of the EU's Visa Policy with Far Reaching Privacy Implications.* 2017.
10. European Union Agency for Fundamental Rights. *Under watchful eyes – biometrics, EU IT-systems and fundamental rights*. 2018; Available from: http://fra.europa.eu/en/publication/2018/biometrics-rights-protection.
11. Sutrop, M., *Ethical issues in governing biometric technologies*, in *Ethics and Policy of Biometrics*. 2010, Springer. p. 102-114.
12. Zeadally, S. and M. Badra, *Privacy in a Digital, Networked World: Technologies, Implications and Solutions*. 2015: Springer.

13. Gellman, R., *Privacy and Biometric ID Systems: An Approach Using Fair Information Practices for Developing Countries.* Center for Global Development, 2013.
14. Floridi, L., *On human dignity as a foundation for the right to privacy.* Philosophy & Technology, 2016. **29**(4): p. 307-312.
15. van der Ploeg, I., *Biometrics and the body as information: normative issues of the socio-technical coding of the body: Normative issues of the socio-technical coding of the body*, in *Surveillance as Social Sorting*. 2005, Routledge. p. 71-88.
16. van der Ploeg, I., *Genetics, biometrics and the informatization of the body.* Annali-Istituto Superiore di Sanita, 2007. **43**(1): p. 44.
17. Wickins, J., *The ethics of biometrics: the risk of social exclusion from the widespread use of electronic identification.* Science and Engineering Ethics, 2007. **13**(1): p. 45-54.
18. Sprokkereef, A., *Data Protection and the Use of Biometric Data in the EU*, in *The Future of Identity in the Information Society*. 2008, Springer. p. 277-284.
19. Campisi, P., *Security and privacy in biometrics*. Vol. 24. 2013: Springer.
20. Dantcheva, A., P. Elia, and A. Ross, *What else does your biometric data reveal? A survey on soft biometrics.* IEEE Transactions on Information Forensics and Security, 2016. **11**(3): p. 441-467.
21. Robertson, A.H. and J.G. Merrills, *Human rights in Europe: A study of the European Convention on Human Rights*. 1993: Manchester Univ Pr.
22. Rights, U.D.o.H., U.N.A.M.i. Afghanistan, and U.N.O.o.t.H.C.f.H. Rights, *Universal declaration of human rights*. 2006: United Nations Assistance Mission in Afghanistan (UNAMA), Office of the High Commissioner for Human Rights (OHCHR).
23. Assembly, U.G., *Universal declaration of human rights.* UN General Assembly, 1948.
24. Kizza, J.M., *Ethical and social issues in the information age*, ed. S. Edition. 2017: Springer International Publishing AG.
25. Renaud, K., A. Hoskins, and R. von Solms. *Biometric identification: Are we ethically ready?* in *Information Security for South Africa (ISSA), 2015*. 2015. IEEE.
26. SCHNEIDER, C.B., *The Charter of Fundamental Rights of the European Union.* 2014.
27. intersoft consulting. *General Data Protection Regulation (GDPR)*. [cited 2018 20/08/2018]; Available from: https://gdpr-info.eu/.
28. Voigt, P. and A. Von dem Bussche, *The EU General Data Protection Regulation (GDPR)*. Vol. 18. 2017: Springer.
29. Rainbow, C. *Descriptions of ethical theories and principles*. Davidson College 2002; Available from: http://www.bio.davidson.edu/people/kabernd/indep/carainbow/Theories.htm.
30. Butler, I., *A code of ethics for social work and social care research.* British Journal of Social Work, 2002. **32**(2): p. 239-248.
31. Hatcher, T. and S.R. Aragon, *A code of ethics and integrity for HRD research and practice.* Human Resource Development Quarterly, 2000. **11**(2): p. 179-185.
32. Riek, L. and D. Howard, *A code of ethics for the human-robot interaction profession.* 2014.
33. Kagan, S., *Normative ethics*. 2018: Routledge.
34. Driver, J. *The history of utilitarianism*. 2009; Available from: https://plato.stanford.edu/entries/utilitarianism-history/.
35. McDonald, G., *Ethical relativism vs absolutism: research implications.* European Business Review, 2010. **22**(4): p. 446-464.
36. Gibbs, J.C., *Moral development and reality: Beyond the theories of Kohlberg, Hoffman, and Haidt*. 2013: Oxford University Press.
37. Kohlberg, L. and R.H. Hersh, *Moral development: A review of the theory.* Theory into practice, 1977. **16**(2): p. 53-59.
38. Lapsley, D.K., *Moral psychology*. 2018: Routledge.

39. The official website of the Hungarian National Police. *The Code of Ethics of the Hungarian Police*. Available from: http://www.police.hu/a-rendorsegrol/testulet/altalanosan/a-rendori-hivatas-etikai-kodexe.
40. Legal Affairs-Bulgaria *Code of Ethics for officials of the ministry of the interior with police functions*. 2004; Available from: http://www.refworld.org/pdfid/4c2dd6d22.pdf.
41. affairs, T.M.o.I. *Code of Ethics for state officials, Republic of Bulgaria*. 2016; Available from: https://www.mvr.bg/docs/default-source/structura/96de0a6d-etichen_kodeks-pdf.pdf.
42. Rahman, Z., P. Verhaert, and C. Nyst, *Biometrics in the Humanitarian Sector.* 2018.
43. Al-Assam, H., et al., *Privacy in Biometric Systems*, in *Privacy in a Digital, Networked World*. 2015, Springer. p. 235-262.
44. Dantcheva, A., et al., *Bag of soft biometrics for person identification.* Multimedia Tools and Applications, 2011. **51**(2): p. 739-777.
45. Marasco, E. and B. Cukic. *Privacy protection schemes for fingerprint recognition systems*. in *Biometric and Surveillance Technology for Human and Activity Identification XII*. 2015. International Society for Optics and Photonics.
46. Drahansky, M., et al., *Influence of skin diseases on fingerprint recognition.* BioMed Research International, 2012. **2012**.
47. Beslay, L. and J. Galbally. *Fingerprint identification technology for its implementation in the Schengen Information System II (SIS-II)*. 2015; Available from: http://publications.jrc.ec.europa.eu/repository/bitstream/JRC97779/lbna27473enn.pdf.
48. Mordini, E., et al., *Ethics, e-inclusion and ageing.* Studies in Ethics, Law, and Technology, 2009. **3**(1).
49. Basak, P., et al. *Multimodal biometric recognition for toddlers and pre-school children*. in *Biometrics (IJCB), 2017 IEEE International Joint Conference on*. 2017. IEEE.
50. European Commission Joint Research Centre Institute for the Protection and Security of the Citizen. *Fingerprint Recognition for Children: Final Report* 2013; Available from: http://publications.jrc.ec.europa.eu/repository/bitstream/JRC85145/fingerprint%20recognition%20for%20children%20final%20report%20%28pdf%29.pdf.
51. van Greunen, D., *Ethics, Children, and Biometric Technology.* IEEE Technology and Society Magazine, 2016. **35**(3): p. 67-72.
52. The European Data Protection Supervisor (EDPS). *Opinion of the European Data Protection Supervisor on the Proposal for a Regulation of the European Parliament and the Council amending the Common Consular Instructions on visas for diplomatic missions and consular posts in relation to the introduction of biometrics including provisions on the organisation of the reception and processing of visa applications (COM (2006) 269 final) — 2006/0088 (COD)*. Available from: https://edps.europa.eu/sites/edp/files/publication/06-10-27_cci_en.pdf.
53. Guild, E. and J. Niessen, *The developing immigration and asylum policies of the European Union: adopted conventions, resolutions, recommendations, decisions and conclusions*. 1996: Kluwer Law International The Hague.
54. Lambert, H., *An Introduction to the Common European Asylum System for Courts and Tribunals: A Judicial Analysis*. 2017, Oxford University Press UK.
55. Robinson, N. and J. Gaspers, *Information security and data protection legal and policy frameworks applicable to European Union institutions and agencies.* 2014.
56. Townend, D., *Overriding data subjects' rights in the public interest*, in *The Data Protection Directive and Medical Research Across Europe*. 2017, Routledge. p. 89-102.
57. Iso, W., *9241-11. Ergonomic requirements for office work with visual display terminals (VDTs).* The international organization for standardization, 1998. **45**: p. 9.
58. Jokela, T., et al. *The standard of user-centered design and the standard definition of usability: analyzing ISO 13407 against ISO 9241-11*. in *Proceedings of the Latin American conference on Human-computer interaction*. 2003. ACM.
59. Labati, R.D., et al., *Biometric recognition in automated border control: a survey.* ACM Computing Surveys (CSUR), 2016. **49**(2): p. 24.

60. Voigt, P. and A. von dem Bussche, *The Eu General Data Protection Regulation (gdpr): A Practical Guide*. 2017: Springer.
61. Tikkinen-Piri, C., A. Rohunen, and J. Markkula, *EU General Data Protection Regulation: Changes and implications for personal data collecting companies.* Computer Law & Security Review, 2017.
62. Directive, T.P.a.C.J., *Directive (EU) 2016/680 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JH.* Official Journal of the European Union, 2016. **119**(04.05): p. 43.
63. Salami, E., *The Impact of Directive (EU) 2016/680 on the Processing of Personal Data by Competent Authorities for the Purposes of the Prevention, Investigation, Detection or Prosecution of Criminal Offences or the Execution of Criminal Penalties and on the Free Movement of Such Data on the Existing Privacy Regime.* 2017.
64. Wright, D., *A framework for the ethical impact assessment of information technology.* Ethics and information technology, 2011. **13**(3): p. 199-226.
65. Gurzawska, A. and P. Brey, *Principles and Approaches in Ethics Assessment.* Institutional Integritym University of Twente, 2015. **3**.
66. Wright, D. and E. Mordini, *Privacy and ethical impact assessment*, in *Privacy impact assessment*. 2012, Springer. p. 397-418.
67. Wright, D. and M. Friedewald, *Integrating privacy and ethical impact assessments.* Science and Public Policy, 2013. **40**(6): p. 755-766.

Annex I: informed consent form – template

The Framework Programme for Research & Innovation

Research & Innovation Action (RIA)

Project Title:

SMart mobILity at the European land borders

SMILE

Grant Agreement No: 740931

[H2020-DS-2016-2017] SEC-14-BES-2016 Towards reducing the cost of technologies in land border security applications

Informed consent

I,……., the undersigned, volunteer to participate in this interview/pilot conducted by the SMILE consortium, in project entitled "SMart mobILity at the European land borde". I confirm that (please tick box as appropriate):

1.	I have read and understood the information about the project, as provided in the Information Sheet.	☐
2.	I have been given the opportunity to ask questions about the project and my participation.	☐
3.	I voluntarily agree to participate in the project.	☐
4.	I understand I can withdraw at any time without giving reasons and that I will not be penalised for withdrawing nor will I be questioned on why I have withdrawn.	☐
1.	I am aware of that no payment of incentives or rewards to me will be made.	☐
5.	The procedures regarding confidentiality have been clearly explained (e.g. use of names, pseudonyms, anonymisation of data, etc.) to me.	☐
6.	The use of the data in pilot, publications, sharing and archiving has been explained to me.	☐

7.	I understand that SMILE team members will have access to this data only if they agree to preserve the confidentiality of the data and if they agree to the terms I have specified in this form.	☐
8.	I, along with the SMILE team representative, agree to sign and date this informed consent form.	☐

I hereby, agree to give personalized permission to SMILE to collect, analyze and publish/ report my data (when nesseacry) as provided in the Information Sheet and in compliance with standards and regulations.

Participant:

_____ _____ _____
Name of Participant Signature Date

SMILE team representative:

_____ _____ _____
Name of Researcher Signature Date